IBM Master Data Management on Cloud
Version 1 Release 6

User Guide
(Last updated: 2019-01-09)

Note

Before using this information and the product that it supports, read the information in Notices and trademarks.

Edition Notice

This edition applies to version 1, release 6, modification 0 of IBM Master Data Management on Cloud and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. About IBM Master Data Management on Cloud

IBM® Master Data Management on Cloud (IBM MDM on Cloud) provides IBM InfoSphere® Master Data Management (InfoSphere MDM) Advanced Edition on the IBM SoftLayer global cloud infrastructure.

IBM MDM on Cloud offers the rich features of an on-premises InfoSphere MDM deployment without the cost, complexity, and risk of managing your own infrastructure. IBM MDM on Cloud provides preinstalled MDM configurations for production and development environments in an IBM SoftLayer cloud hosted environment. These configurations are multi-domain and can be deployed in physical MDM or virtual MDM style.

Chapter 2. Overview of IBM MDM on Cloud

IBM® Master Data Management on Cloud provides a proven master data management (MDM) solution on the IBM SoftLayer global cloud platform. It offers the rich features of an on-premises MDM deployment without the cost, complexity, and risk of managing your own infrastructure.

Based on IBM InfoSphere® Master Data Management Advanced Edition, IBM MDM on Cloud is a multi-domain solution that comes pre-installed and ready to run in small, medium, and large server configurations. IBM MDM on Cloud also includes capabilities from IBM Business Process Manager and IBM InfoSphere Information Server.

IBM MDM on Cloud provides a cost-effective entry point to InfoSphere MDM and a path to easily add new environments. It supports the following use cases:

- Quickly deploy development or test environments for new InfoSphere MDM projects.
- Move all or part of your InfoSphere MDM workload to the cloud.
- Comply with corporate mandates to move to the cloud.
- Reduce risk and initial cost for new projects and deliver faster return on investment.

Each data center facility where IBM MDM on Cloud is hosted has the same specifications regarding quality deployment and management methodologies. Leveraging the standardization across all geographic locations, IBM optimizes key data center performance variables such as space, power, network, personnel, and internal infrastructure.

As a hosted offering, IBM MDM on Cloud gives you the same control over your data as the on-premises system. As with an on-premises deployment, the ongoing management of the applications and cloud environment is your responsibility.

To maintain and control the IBM MDM on Cloud services, you must:

- Actively monitor and report any issues that you encounter with IBM MDM on Cloud.
- Maintain the software platform, InfoSphere MDM and the operating system, to meet your security standards.
- Maintain software firewalls on servers that face the internet to provide the required protection.
- Develop integration, transformation, and other jobs, as well as establish connectivity between data sources and applications. You can also develop your own workload, business rules, monitoring, and scheduling for all jobs.

  Note: You are responsible for the quality and performance of programs, applications, and jobs that you develop for IBM MDM on Cloud
- Provide user access to IBM MDM on Cloud once the cluster is provisioned, by sharing the web address, username, and password.
- Ensure the continuity, compatibility, and performance of the IBM SaaS platform by installing only permissible software, including any open source packages, and regularly upgrading your IBM MDM on Cloud environment and operating system.
- Create and maintain regular backups of data.
- Setup and manage the encryption of IBM MDM on Cloud according to your security policy and the service terms.

Note the following limitations and restrictions of IBM MDM on Cloud:

- If your offering is designated as "Non-Production", IBM MDM on Cloud can be deployed only as part of your development and test environments for internal non-production activities. These activities include, but are not limited to:
  - testing
  - performance tuning

  - fault diagnosis
  - internal benchmarking
  - staging
  - quality assurance activity
  - developing internally used additions or extensions to the offering by using published application programming interfaces
- Restricted to SOAP over HTTP as Service Binding.

Default values for MDM on Cloud instances

By default, IBM® MDM on Cloud instances are configured with certain values upon deployment. You can customize these values if necessary.

Application language

The default MDM Application language is English.

Time zone

IBM MDM on Cloud is installed with a default time zone value of `America/Atikokan`. To modify the time zone, follow the steps provided in the Knowledge Center.

Industry type

By default, the industry type is set to `insurance`. If this is not appropriate for this deployment, modify the industry type by running the `changeIndustryType` madconfig target

Important: Back up your MDM database before running the `changeIndustryType` madconfig target. The command will clear and recreate rows in the following MDM database tables: CDCLIENTIMPTP, CDCLIENTPOTENTP, CDCLIENTSTTP, CDCONTRACTRELTP, CDCONTRACTROLETP, CDCONTRACTSTTP, CDCONTRCOMPTP, CDERRMESSAGETP, CDPRODTP, CDCAMPAIGNTP, H_CDCLIENTIMPTP, H_CDCLIENTPOTENTP, H_CDCLIENTSTTP, H_CDCONTRACTRELTP, H_CDCONTRACTROLETP, H_CDCONTRACTSTTP, H_CDCONTRCOMPTP, H_CDERRMESSAGETP, H_CDPRODTP, and H_CDCAMPAIGNTP.

To change the industry type:

1. Back up the MDM database.
2. Browse to the folder `<MDM_INSTALL_HOME>/mds/scripts`.
3. Run the `changeIndustryType` madconfig target.

   Microsoft Windows:

   ```
   madconfig changeIndustryType
   ```

   Linux or UNIX:

   ```
   ./madconfig.sh changeIndustryType
   ```

4. Restart the IBM MDM on Cloud instance.

Chapter 3. Non-Production Plans

IBM MDM on Cloud Non-Production plan The IBM MDM on Cloud Non-Production plan offers InfoSphere MDM Advanced Edition installed into a virtualized environment. It is suitable as an environment for development, customization, and functional testing of the MDM Hub and related processes. The Non-Production plan includes two shared non-production InfoSphere MDM runtime instances: one for development integration testing and a second for QA testing. The plan also includes two InfoSphere MDM developer instances and two IBM Business Process Manager developer instances.

The non-production offering contains 6 virtual machines with the following software:

- Two InfoSphere MDM developer virtual machines. Each developer machine contains InfoSphere MDM Advanced Edition, WebSphere Application Server, DB2, Rational® Application Developer, and the MDM Workbench. Two instances of InfoSphere MDM Advanced Edition runtime.
- One IBM BPM Process Center & Process Server on one virtual machine
- One IBM InfoSphere Information Server virtual machine
- Two Windows client machines with MDM Workbench, BPM Designer and IIS Client installed.

IBM Master Data Management on Cloud Additional Developer and Test Environment The Additional MDM Developer plan provides an additional InfoSphere MDM developer instance for the IBM MDM on Cloud non-production environment. This is in addition to the two MDM developer instances already available by default with the Non-Production plan. The Additional MDM Developer plan enables you to add an MDM developer to the two provisioned with the Non-Production plan.

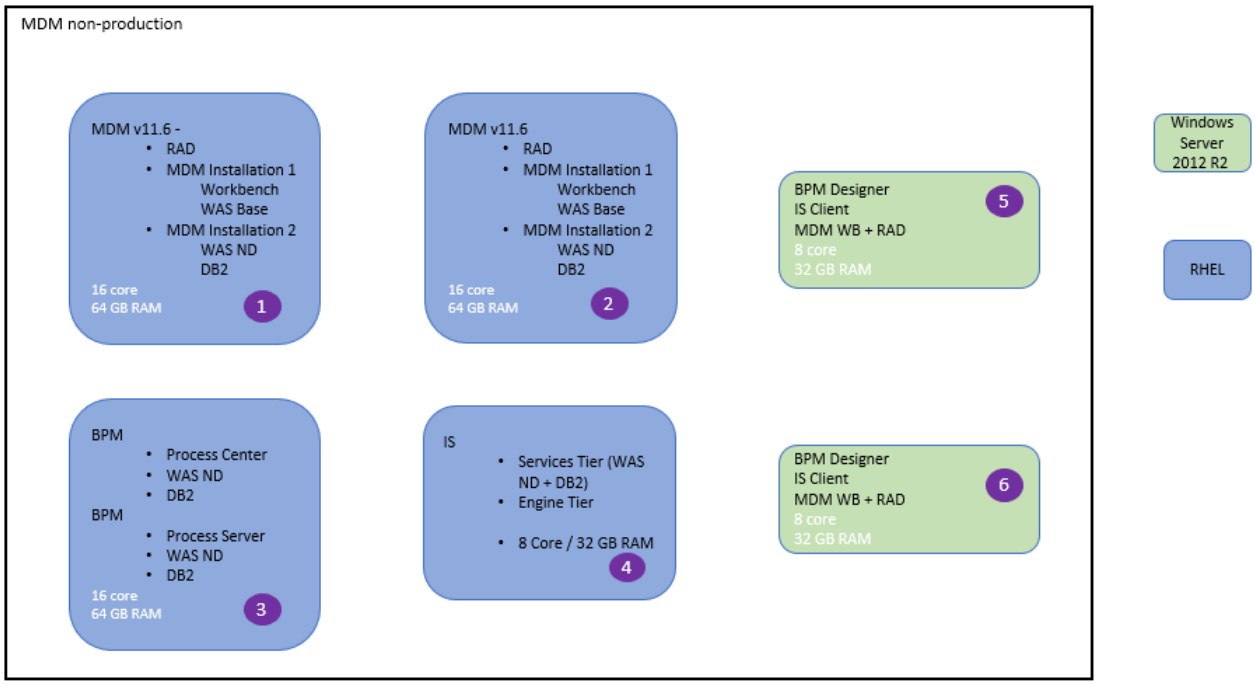
The additional developer offering includes a single MDM developer virtual machine containing InfoSphere MDM Advanced Edition, WebSphere Application Server, DB2, Rational Application Developer, and the MDM Workbench. One MDM QA instance.

IBM Master Data Management on Cloud Additional Client Master Data Management on Cloud Additional Client plan provides an additional IBM Business Process Manager designer instance, MDM Workbench instance and IIS Clients for the IBM MDM on Cloud non-production environment. This is in addition to the two Client instances already available by default with Non-Production plan.

The additional client offering includes a single virtual machine containing IBM BPM Process Designer, MDM Workbench and IIS Clients.

IBM Master Data Management on Cloud Non Production

Topology



Host Name

Machine	Hostname
IBM MDM Developer Environment 1	`<orderID>-d-mdc1.<domain>`
IBM MDM Developer Environment 2	`<orderID>-d-mdc12.<domain>`
Information Server	`<orderID>-d-iisd.<domain>`
MDM BPM & IIS Dev Client 1	`<orderID>-d-bpd1.<domain>`
MDM BPM & IIS Dev Client 2	`<orderID>-d-bpd2.<domain>`
BPM Process Center & Process Server	`<orderID>-d-bdpc.<domain>`

Specifications

Refer to below link

https://public.dhe.ibm.com/cloud/bluemix/hosted/mdmoncloud_specifications.pdf

Security

Users

Machine	SSH / RDP Users	Non SSH Users	Application Users
IBM MDM Developer Environment 1	<orderID>	root, mdmdvplr, mdmqausr, mdmdbusr	wasadmin, mdmadmin

Machine	SSH / RDP Users	Non SSH Users	Application Users
IBM MDM Developer Environment 2	root	mdmqausr, mdmdbusr	wasadmin, mdmadmin
Information Server	root	dsadm, iauser, dsodb, srduser, xmetasr, xmeta, isadmin, wasadmin, db2inst1	wasadmin
Information Server Designer Client	Administrator		
BPM Designer Client 1/2	Administrator		
BPM Process Center	root	bpmdbusr	bpmdeadmin, bpmcelladmin, DSUser1

Encryption

Machine	Encryption type	Encrypted Location	Keys Location
IBM MDM Developer Environment 1	Disk Encryption	/home/mdmdvplr, /home/mdmqausr	/keystore/keyfile
IBM MDM Developer Environment 1	DB2 native Encryption	NA	/home/db2inst1/iiskeystore.p12
IBM MDM Developer Environment 2	Disk Encryption	/home/mdmdvplr, /home/mdmqausr	/keystore/keyfile
IBM MDM Developer Environment 2	DB2 native Encryption	NA	/home/db2inst1/iiskeystore.p12
Information Server	Disk Encryption	/home2	/keystore/keyfile
Information Server	DB2 native Encryption	NA	/home_/db2inst1/iiskeystore.p12
BPM Process center	Disk Encryption	/bpm, /bpm_ps, /software,/dbdata, /tmp	/keystore/keyfile
BPM Process center	DB2 native Encryption	NA	/home/db2inst1/iiskeystore.p12

Ports

IBM MDM Developer Environment 1

Ports	Source	Comments
4362	All machines	Used to ssh to mdc1 machine
9353, 9043, 9443, 5061, 7286, 9633, 5901, 8880, 9355, 9044, 8879, 9444, 9445, 5063, 7287, 9634, 50602	Open to all machines in this environment	General MDM Ports

IBM MDM Developer Environment 2

Ports	Source	Comments
4362	Open from Gateway Machine	SSH from Gateway machine

Ports	Source	Comments
9353, 9043, 9443, 5061, 7286, 9633, 5901, 8880, 9355, 9044, 8879, 9444, 9445, 5063, 7287, 9634, 50602	Open to all machines in this environment	General MDM Ports

Information Server

Ports	Source	Comments
4362	Open from Gateway Machine	Used to ssh to Information Server machine
9446	Open from IIS Designer Client, MDM Runtime machines and MDM Runtime DB	Used to connect to Information Server machine
9043	Open from IIS Designer Client, MDM Runtime machines and MDM Runtime DB	Used to connect to Information Server machine
31538	Open from IIS Designer Client, MDM Runtime machines and MDM Runtime DB	Used to connect to Information Server machine
2825	Open from IIS Designer Client	Used to connect to Information Server machine
5076	Open from IIS Designer Client	Used to connect to Information Server machine
5077	Open from IIS Designer Client	Used to connect to Information Server machine
5558	Open from IIS Designer Client	Used to connect to Information Server machine
5578	Open from IIS Designer Client	Used to connect to Information Server machine
7284	Open from IIS Designer Client	Used to connect to Information Server machine
7286	Open from IIS Designer Client	Used to connect to Information Server machine
8882	Open from IIS Designer Client	Used to connect to Information Server machine
9043	Open from IIS Designer Client	Used to connect to Information Server machine
9060	Open from IIS Designer Client	Used to connect to Information Server machine
9080	Open from IIS Designer Client	Used to connect to Information Server machine
9081	Open from IIS Designer Client	Used to connect to Information Server machine
9108	Open from IIS Designer Client	Used to connect to Information Server machine

Ports	Source	Comments
9353	Open from IIS Designer Client	Used to connect to Information Server machine
9403	Open from IIS Designer Client	Used to connect to Information Server machine
9404	Open from IIS Designer Client	Used to connect to Information Server machine
9405	Open from IIS Designer Client	Used to connect to Information Server machine
9446	Open from IIS Designer Client	Used to connect to Information Server machine
9633	Open from IIS Designer Client	Used to connect to Information Server machine
10000	Open from IIS Designer Client	Used to connect to Information Server machine
10001	Open from IIS Designer Client	Used to connect to Information Server machine
10002	Open from IIS Designer Client	Used to connect to Information Server machine
10003	Open from IIS Designer Client	Used to connect to Information Server machine
10004	Open from IIS Designer Client	Used to connect to Information Server machine
10005	Open from IIS Designer Client	Used to connect to Information Server machine
13401	Open from IIS Designer Client	Used to connect to Information Server machine
13402	Open from IIS Designer Client	Used to connect to Information Server machine
31531	Open from IIS Designer Client	Used to connect to Information Server machine
31538	Open from IIS Designer Client	Used to connect to Information Server machine
5986	Open from IIS Designer Client	Used to connect to Information Server machine
19443	Open from IIS Designer Client	Used to connect to Information Server machine

BPM Process Center

Ports	Source	Comments
9354, 9043, 8879, 9443, 5061, 7286, 9633, 9045, 8881, 9444, 5063, 7287, 9635, 50000	MDM Developer 1 &2, BPM Process Designer 1 &2	General BPM Ports
4362	MDM Developer 1	Gateway Port

Administration

Restarting services for the IBM MDM on Cloud Non-Production offering.

IBM MDM on Cloud developer environment 1

1. Log in to the database server as the db2inst user.
2. Start Db2 by running the command `db2start`
3. To start MDM developer instance, Log in to the MDM developer environment 1 server as the MDM OS user1 for this instance.
4. Start WebSphere Application Server by running the following command: `<WAS_INSTALL_HOME>/profiles/AppSrv01/bin$ ./startServer.sh server1`
5. To start MDM QA instance, Log in to the MDM runtime instance server as the MDM OS user2 for this instance.
6. Start WebSphere Application Server by running the following command:

- `<WAS_INSTALL_HOME>/profiles/Dmgr01/bin$ ./startManager.sh`
- `<WAS_INSTALL_HOME>/profiles/AppSrv01/bin$ ./startNode.sh`

1. Log in to the WebSphere Application Server Integrated Solutions Console (admin console) as the wasadmin user.
2. Start the MDM operational server and the MDM user interface server.

Admin / UI URLs

1. `https://<IBM MDM Developer Environment 1 IP>:9043/ibm/console`
2. `https://<IBM MDM Developer Environment 1 IP>:9443/CustomerBusinessAdminWeb/faces/login.jsp`
3. `https://<IBM MDM Developer Environment 1 IP>:9443/inspector`
4. `https://<IBM MDM Developer Environment 1 IP>:9443/webreports`
5. `https://<IBM MDM Developer Environment 1 IP>:9443/accessweb`
6. `https://<IBM MDM Developer Environment 1 IP>:9443/mdmconsent`

IBM MDM on Cloud developer environment 2

1. Log in to the database server as the db2inst user.
2. Start Db2 by running the command `db2start`
3. To start MDM developer instance, Log in to the MDM developer environment 1 server as the MDM OS user1 for this instance.
4. Start WebSphere Application Server by running the following command: `<WAS_INSTALL_HOME>/profiles/AppSrv01/bin$ ./startServer.sh server1`
5. To start MDM QA instance, Log in to the MDM runtime instance server as the MDM OS user2 for this instance.
6. Start WebSphere Application Server by running the following command:

- `<WAS_INSTALL_HOME>/profiles/Dmgr01/bin$ ./startManager.sh`
- `<WAS_INSTALL_HOME>/profiles/AppSrv01/bin$ ./startNode.sh`

1. Log in to the WebSphere Application Server Integrated Solutions Console (admin console) as the wasadmin user.
2. Start the MDM operational server and the MDM user interface server.

Admin UI URLs

https://<IBM MDM Developer Environment 2 IP>:9044/ibm/console

https://<IBM MDM Developer Environment 2 IP>:9445/CustomerBusinessAdminWeb/faces/login.jsp

https://<IBM MDM Developer Environment 2 IP>:9445/inspector

https://<IBM MDM Developer Environment 2 IP>:9445/webreports

https://<IBM MDM Developer Environment 2 IP>:9445/accessweb

https://<IBM MDM Developer Environment 2 IP>:9444/mdmconsent

IBM InfoSphere Information Server

No action required. All services restart automatically when the server restarts.

Admin / Launchpad URLs

1. https://< IIS Machine IP >:9446/ibm/console
2. https://< IIS Machine IP >:9446/ibm/iis/launchpad

BPM Process Center and Process Server installed with non root user

1. Log in to the database server as the db2inst user.
2. Start Db2 by running the command `db2start`
3. Log in as bpmpcusr user.
4. To start BPM Process Center, Start WebSphere Application Server for Process Center by running the following command:

- `/bpm/profiles/DmgrProfile/bin$ ./startManager.sh`
- `/bpm/profiles/Node1Profile/bin$ ./startNode.sh`

1. Log in to the WebSphere Application Server Integrated Solutions Console (admin console) as the bpm admin user.
2. Start the BPM PC Cluster.
3. Switch to bpmpsusr to start BPM Process Server.
4. To start BPM Process Server, Start WebSphere Application Server for Process Server by running the following command:

- `/bpm_ps/profiles/DmgrProfile/bin$ ./startManager.sh`
- `/bpm_ps/profiles/Node1Profile/bin$ ./startNode.sh`

1. Log in to the WebSphere Application Server Integrated Solutions Console (admin console) as the bpm admin user.
2. Start the BPM PS Cluster.

Process Center Admin / Portal URLs
https://< BPM Server Machine Public IP >:9043/ibm/console

https://< BPM Server Machine Public IP >:9443/ProcessAdmin

https://< BPM Server Machine Public IP >:9443/ProcessPortal

Process Server Admin / Portal URLs

1. https://< BPM Server Machine Public IP >:30001/ibm/console
2. https://< BPM Server Machine Public IP >:30025/ProcessAdmin
3. https://< BPM Server Machine Public IP >:30025/ProcessPortal

BPM Process Center and Process Server

1. Log in to the database server as the db2inst user.
2. Start Db2 by running the command `db2start`

3. Log in as root user.
4. To start BPM Process Center, Start WebSphere Application Server for Process Center by running the following command:

- `/bpm/profiles/DmgrProfile/bin$ ./startManager.sh`
- `/bpm/profiles/Node1Profile/bin$ ./startNode.sh`

1. Log in to the WebSphere Application Server Integrated Solutions Console (admin console) as the bpm admin user.
2. Start the BPM PC Cluster.
3. To start BPM Process Server, Start WebSphere Application Server for Process Server by running the following command:

- `/bpm_ps/profiles/DmgrProfile/bin$ ./startManager.sh`
- `/bpm_ps/profiles/Node1Profile/bin$ ./startNode.sh`

1. Log in to the WebSphere Application Server Integrated Solutions Console (admin console) as the bpm admin user.
2. Start the BPM PS Cluster.

First Steps

Gateway Machine : IBM MDM on Cloud developer environment 1

Logging in to the machines for first time

1. SSH into the Gateway machine using unique user provided in the welcome letter using port 4362.
2. Change the password and su to root user.
3. Change the root password.
4. SSH into other machines in the plan from the gateway machine using root user using port 4362. The access is allowed only from gateway machine.
5. Change the root passwords.

Open up required ports

Complete this step for any access, such as for the business administration user interface or ssh.

Important Access to all other machines in the environment is allowed only through gateway machine by default configuration. It is highly recommeded to provide direct ssh accesss to your trusted IP's as part of initial configuration. This will help to access the available machine, in case, the gateway machine fails.

1. Edit the /opt/iig/scripts/ports.prop file and add the ports that you want to open.
2. Run the script that automates the IPTables changes for you.

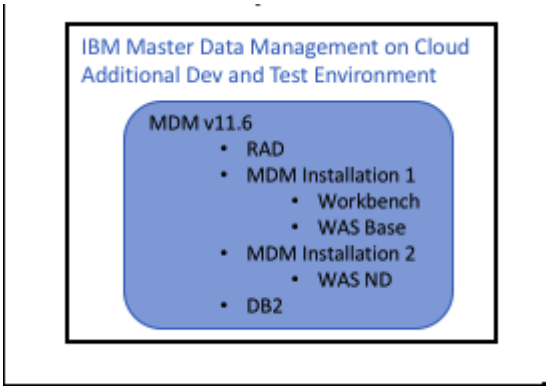
```
sudo /opt/iig/scripts/enable_ports.sh <Trusted IP Address>
```

Trusted IP Address: This is the IP address of your computer from which you want to access hosted machines. If you are inside an enterprise LAN, the enterprise gateway IP will be the trusted IP.

3. If you want to open separate set of ports to different trusted IPs, you need to execute the command multiple times with right set of ports and trusted IP.

IBM Master Data Management on Cloud Additional MDM Developer and Test

Topology



Host Name

Machine	Hostname
Additional MDM Developer and Test	<orderID>-a-mdc.<domain>

Specifications

Refer to below link

https://public.dhe.ibm.com/cloud/bluemix/hosted/mdmoncloud_specifications.pdf

Security

Users

Machine	SSH Users	Non SSH Users	Application Users
Additional MDM Developer	<orderID>	root, mdmdvplr, mdmqausr, mdmdbusr	wasadmin, mdmadmin

Encryption

Machine	Encryption type	Encrypted Location	Keys Location
Additional MDM Developer and Test	Disk Encryption	/home/mdmcloud	/keystore/keyfile
Additional MDM Developer and Test	DB2 native Encryption	NA	/home/db2inst1/ iiskeystore.p12

Ports

Additional MDM Developer

Ports	Source	Comments
4362	All machines	Used to ssh to Additional MDM Developer and Test

Administration

Restarting services for IBM MDM on Cloud Additional MDM Developer offering.

IBM MDM on Cloud developer environment.

1. Log in to the database server as the db2inst user.
2. Start Db2 by running the command db2start
3. To start MDM developer instance, Log in to the MDM developer environment 1 server as the MDM OS user1 for this instance.
4. Start WebSphere Application Server by running the following command:

```
<WAS_INSTALL_HOME>/profiles/AppSrv01/bin$ ./startServer.sh server1
```

5. Start VNC Server as the MDM OS user for this instance using the following command:

```
./vncserver
```

6. To start MDM QA instance, Log in to the MDM runtime instance server as the MDM OS user2 for this instance.
7. Start WebSphere Application Server by running the following command:

```
<WAS_INSTALL_HOME>/profiles/Dmgr01/bin$ ./startManager.sh
```

```
<WAS_INSTALL_HOME>/profiles/AppSrv01/bin$ ./startNode.sh
```

8. Log in to the WebSphere Application Server Integrated Solutions Console (admin console) as the wasadmin user. Start the MDM operational server and the MDM user interface server.

First Steps

Gateway Machine : Additional MDM Developer

Logging in to the machines for first time

1. SSH into the Gateway machine using unique user provided in the welcome letter using port 4362.
2. Change the password and su to root user.
3. Change the root password.
4. SSH into other machines in the plan from the gateway machine using root user using port 4362. The access is allowed only from gateway machine.
5. Change the root passwords.

Open up required ports

Important Access to all other machines in the environment is allowed only through gateway machine by default configuration. It is highly recommeded to provide direct ssh accesss to your trusted IP's as part of initial configuration. This will help to access the available machine, in case, the gateway machine fails.

1. Edit the /opt/iig/scripts/ports.prop file and add the ports that you want to open.
2. Run the script that automates the IPTables changes for you.

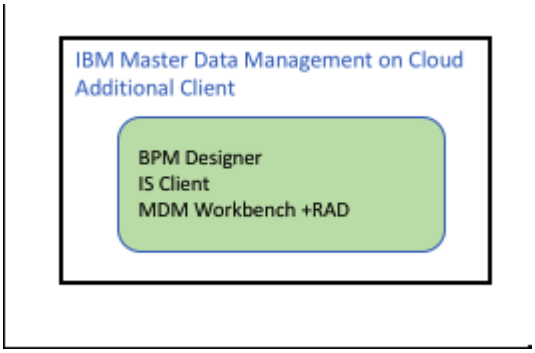
```
sudo /opt/iig/scripts/enable_ports.sh <Trusted IP Address>
```

Trusted IP Address: This is the IP address of your computer from which you want to access hosted machines. If you are inside an enterprise LAN, the enterprise gateway IP will be the trusted IP. Any access such as business administration user interface, ssh need this steps to be completed.

3. If you want to open separate set of ports to different trusted IPs, you need to execute the command multiple times with right set of ports and trusted IP.

IBM Master Data Management on Cloud Additional Client

Topology



Host Name

Machine	Hostname
Windows Additional Client	`<orderID>-a-bpd.<domain>`

Specifications

Refer to below link

https://public.dhe.ibm.com/cloud/bluemix/hosted/mdmoncloud_specifications.pdf

Security

Users

Machine	Remote Desktop Users	Non SSH Users	Application Users
Windows Additional Client	Administrator(Maximum 2 concurrent users)	NA	NA

Setting up a non-production environment

If you have the IBM® MDM on Cloud Non-Production offering plan, then there are some extra steps to complete to set up your non-production environment.

1. Connect to the following virtual machines using the addresses and credentials listed in your Welcome letter:
   - Windows CLients
   - IBM InfoSphere® Information Server
   - InfoSphere MDM developer and test machines.
   - BPM Process Center and Process Server machine.

   You can connect to the MDM developer virtual machines using a tool such as VNC Viewer. IBM Rational® Application Developer, including the MDM Workbench, is installed on each developer virtual machine.
2. For Microsoft Windows clients such as IBM BPM Designer and IBM InfoSphere Information Server client, connect the clients to the server by adding the IBM BPM Process Center and IBM InfoSphere Information Server IP addresses and host names to the hosts file.
   a. Log in to the Windows 2012 client machine as the administrator user.

b. Open the hosts file located at `C:\Windows\System32\drivers\etc`.

c. Add the IP address, fully qualified host name, and host name to the end of the file.

d. Save the file.

Example:

```
132.27.134.78 mdmwa30-d-bdpc.dal09.us-south.services.bluemix.net mdmwa30-d-bdpc
```

3. Link two InfoSphere MDM instances to a single IBM BPM Process Center instance. For details, see Connecting two InfoSphere MDM instances to a single BPM Process Center.

Launching the MDM Workbench

The MDM Workbench development tools enable developers to extend and configure their IBM® MDM on Cloud solutions. Launch the Workbench by connecting to an MDM developer environment server.

This task is valid only for the following IBM MDM on Cloud offerings:

- Non-Production
- Additional Developer

Other offerings do not include access to the MDM Workbench development tools.

1. Log in as the `mdmcloud` user to one of the IBM MDM on Cloud developer environment virtual machines using the public IP address.
2. Start VNC Server:

```
mdmcloud@<servername>:~/IBM$ vncserver
```

3. When prompted for a password, enter any value. This password value will be used again when you connect from the local client using VNC Viewer.
4. On a local machine, open the VNC Viewer. When prompted, provide the password that you used for the VNC Server.
5. From the VNC Viewer command prompt, browse to the folder where IBM Rational® SDP is installed, such as `/home/mdmcloud/IBM/SDP`.
6. Run `./eclipse`. The MDM Workbench application will launch within IBM Rational Application Developer.
7. Browse to select the workspace that you wish to work with and click **OK**.
8. When prompted, provide your WebSphere® Application Server user ID, such as `wasadmin`, and the corresponding password. Click **Finish**.

You can now use the MDM Workbench development tools to extend and configure your IBM MDM on Cloud solution.

Connecting InfoSphere MDM to BPM Process Center

In an non-production environment, MDM on Cloud must set up the connection between the InfoSphere MDM instances and the BPM Process Center instance.

The steps described in this procedure are required only in the BPM Process Center environment. In Process Server environments, running the install scripts is sufficient.

1. Open the Process Admin Console (PAC). The typical URL to access PAC is `https://<hostname>:<port>/ProcessAdmin/login.jsp`.
2. Configure the EPV settings. For each of the listed InfoSphere MDM applications complete the following steps:
   - MDM Party Maintenance

- Physical MDM Suspected Duplicates
- Virtual MDM Suspected Duplicates
- MDM Data Stewardship Dashboard
- MDM Hybrid Data Quality

a. In the Installed Apps tab, activate the latest snapshot for the application.
b. Navigate back to the Server Admin tab.
c. Select **Admin Tools > Manage EPVs** from the navigation menu.
d. Choose the tip entry for the applications.
e. Set the EPV values for MDM_Connection_Details, if the values are not already set.
f. Choose the named snapshot of the applications.
g. Set the EPV values for MDM_Connection_Details. Ensure that the values set in the tip entry and snapshot entry are same.

3. Cache the code tables from the InfoSphere MDM operational server into BPM:
   a. In the Server Admin window, select the MDM Party Maintenance menu.
   b. Select **Refresh MDM Code Table Data Cache**.
   c. To retrieve the code table data from the MDM operational server and refresh the cache, click **OK**.
   d. A confirmation message appears when the cache is refreshed. Click **OK**.

Connecting two InfoSphere MDM instances to a single BPM Process Center

In an non-production environment, you might need to connect two different InfoSphere MDM instances to a single BPM Process Center instance.

The steps are ordered in groups:

A. First InfoSphere MDM instance (MDM1)

In the WebSphere Application Server Integrated Solutions Console (admin console) of the first InfoSphere MDM instance (MDM1), complete these steps:

1. Create an Alias Destination on the InfoSphere MDM server's SIBus:
   a. Navigate to **Service Integration > Buses > *BusName***.
   b. Click the *BusName* link to open the configurations of the bus.
   c. Click on the **Destination** link to open the list of destinations.
   d. Click **New**, then select **Alias**. Click **Next**.
   e. Provide the destination attribute values:
      - **Identifier** MDMBPMAlias
      - **Bus** Select the SIbus of the InfoSphere MDM environment. The bus name in a typical InfoSphere MDM installation will be `MDM.SIB.server1`.
      - **Target identifier** Select Other, please specify from the drop down list. Specify the identifier of the BPM environment target. The target identifier name in a typical Process Center installation will be `eventqueueDestination.SingleCluster`.
      - **Target bus** Select Other, please specify from the drop down list. Specify the identifier of the BPM environment target. The target bus name in a typical Process Center installation will be `BPM.ProcessCenter.Bus`.
   f. Click **Next**, then click **Finish**.
   g. Save the configuration.
2. Create a JMS queue in the MDM environment:

a. Navigate to **Resources > JMS > Queues**.

b. Select the scope.

1) If it is a standalone InfoSphere MDM server, set it to Node, Server.

2) If InfoSphere MDM is installed in a cluster, set it to Cluster.

c. Click **New**.

d. Select Default messaging provider, then click **OK**.

e. Set the values of the attributes:

- **Name** MDMBPMQueue
- **JNDI name** notification/MDMBPMQueue
- **Bus name** Select the SIbus of the MDM environment. The bus name in a typical MDM installation is `MDM.SIB.server1`.
- **Queue name** MDMBPMAlias

f. Click OK and Save the configuration.

3. Create a JMS Queue Connection Factory in the MDM environment:

a. Navigate to **Resources > JMS > Queue connection factories**.

b. Select the scope.

- If it is a standalone MDM server, set it to **Node, Server**. For example, `Node=mdmNode`, `Server=server1`.
- If MDM is installed in a cluster, set the scope to Cluster.

c. Click **New**.

d. Select Default messaging provider and click **OK**.

e. Set the values of the attribute:

- **Name** MDMBPMQueueConnectionFactory
- **JNDI name** notification/MDMBPMQueueConnectionFactory
- **Bus name** Select the SIbus of MDM environment. The Bus name in typical InfoSphere MDM installation will be `MDM.SIB.server1`.
- **Provider endpoints** Provide an endpoint, normally with the format `<host>:<port>:<Inbound Transport Chain>`. You can look at the existing queue connection factories of InfoSphere MDM to get this value.

4. Create the Foreign Bus Connection in the InfoSphere MDM environment:

a. Navigate to **Service integration > Buses > *BusName***. The bus name in a typical InfoSphere MDM installation will be `MDM.SIB.server1`.

b. Click the *BusName* link to open the configurations of the bus.

c. Click the Foreign Bus Connection link to open the list of destinations.

d. Click **New**.

e. Select Direct Connection, then click **Next**.

f. Select Service Integration bus, then click **Next**.

g. Select the messaging engine in the InfoSphere MDM environment from the list, then click **Next**.

h. Set the values of the attribute:

- **Name of service Integration bus to connect to (the foreign bus)** Set the value to the name of the SIBus in the BPM environment. The bus name in a typical Process Center installation will be BPM.ProcessCenter.Bus.
- **Gateway messaging engine in the foreign bus** Set the value to the name of the messaging engine of the BPM environment. The messaging name in a typical BPM Process Center installation will be `SingleCluster.000-BPM.ProcessCenter.Bus`.

- **Service integration bus link name** MDM_BPM_LINK_ONE
- **Bootstrap service integration bus provider endpoints** Set the value using the format `<bpmNodeHostName>:<port>:<protocol>`. For example, `mdmdemowin:7278:BootstrapBasicMessaging`. If the BPM cluster has multiple nodes, provide the endpoints for all the nodes as comma-separated list.

i. Click **Next**.

j. Review the summary, then click **Finish** and **Save** the configurations.

B. Second InfoSphere MDM instance (MDM2)

In the WebSphere Application Server Integrated Solutions Console (admin console) of the second InfoSphere MDM instance (MDM2), complete these steps:

1. Create a new Service Integration Bus on MDM2. The reason for this is because both if InfoSphere MDM environments are identical and have same SIBus names, connecting back from BPM will be an issue because BPM will have to connect to two SIBuses with same name.
   a. Navigate to **Service integration > Buses > *BusName***.
   b. Click **New**.
   c. Give a name to the new SIBus to be created such as `MDM.SIB.NewBPMSer`.
2. For the new SIBus, add a bus member. This is required to create a messaging engine for the new bus.
   a. Navigate to **Service integration > Buses > *BusName***.
   b. Click the *BusName* link to open the configurations of the bus, then click the SIBus created during the previous step.
   c. Click Bus members, then click **Add**.
   d. Choose the server or cluster to add to the new bus.
      - If InfoSphere MDM is installed on a server, then select the server option and the corresponding server.
      - If InfoSphere MDM is installed in a cluster, then select the cluster option.
   e. If InfoSphere MDM is installed on a server, complete these steps:
      1) Select Data store for the type of message store.
      2) Select Create default data source with generated JNDO name from the properties of data store.
      3) Click **Next**.
   f. Leave the default values for the performance parameters, then click **Next**.
   g. Review the details and finish the configuration.
3. Follow the steps in A to repeat the changes made to MDM1 for the MDM2 instance.

C. BPM instance

In the WebSphere Application Server Integrated Solutions Console (admin console) of the BPM instance, complete these steps:

1. Create the Foreign Bus Connection in the BPM environment:
   a. Navigate to **Service integration > Buses > *BusName***.
   b. Click the *BusName* link to open the configurations of the bus.
   c. Click the **Foreign Bus Connection** link to open the list of foreign bus connections.
   d. Click **New**.
   e. Select Direct Connection, then click **Next**.
   f. Select **Service Integration bus**, then click **Next**.

g. Select the messaging engine in the BPM environment from the list. Provide the inbound user ID as the admin user ID of BPM, then click **Next**.

h. Set the values of the attributes:

- **Name of service Integration bus to connect to (the foreign bus)** Set the value to the name of the SIBus in the MDM1 instance.
- **Gateway messaging engine in the foreign bus** Set the value to the name of the messaging engine of the MDM1 instance.
- **Service integration bus link name** MDM_BPM_LINK_ONE
- **Bootstrap service integration bus provider endpoints** Set the value using the format `<mdmInstance1HostName>:<port>:<protocol>`. If the InfoSphere MDM cluster has multiple nodes, you can provide the endpoints for all the nodes as comma-separated list.

i. Click **Next**.

j. Review the summary, then click **Finish** and **Save** the configurations.

2. Repeat step C.1, but this time using the details of the MDM2 instance. Give the following values for the MDM2 attributes:

- **Name of service Integration bus to connect to (the foreign bus)** Set the value to the name of the SIBus in the MDM2 instance.
- **Gateway messaging engine in the foreign bus** Set the value to the name of the messaging engine of the MDM2 instance.
- **Service integration bus link name** MDM_BPM_LINK_TWO
- **Bootstrap service integration bus provider endpoints** Set the value using the format `<mdmInstance2HostName>:<port>:<protocol>`. If the InfoSphere MDM cluster has multiple nodes, you can provide the endpoints for all the nodes as comma-separated list.

At this point in the procedure, you now have two foreign bus connections created on BPM:

- MDM_BPM_LINK_ONE pointing to the MDM1 instance
- MDM_BPM_LINK_TWO pointing to the new SIBus created on the MDM2 instance

D. BPM Process center

Complete these steps in the BPM Process Center console:

1. Log in to the BPM Process Center Console with admin access.
2. Import the process applications for the IBM Stewardship Center (ISC) if they are not already imported. All of the process applications for the IBM Stewardship Center are available at the installed location `<ISC_INSTALLED_FOLDER>/mdmg/processes`.
3. Create two snapshops for testing (TESTSNAPSHOTONE and TESTSNAPSHOTTWO) for both the MDM Party Maintenance and Physical MDM Suspected Duplicates process applications. We will focus on testing only these two.
4. Make all four of these new snaphots active.

E. BPM Process admin console

Complete these steps in the BPM Process Admin Console:

1. Log in to the BPM Process Admin Console with admin access.
2. Navigate to **Admin Tools > Manage EPVs**.
3. Select MDM Party Maintenance(TESTSNAPSHOTONE) and then select **EPV MDM_Connection_Details**. Set the details of the MDM1 instance here. Provide a non-secure port such as 9080 for simplicity purposes. Do not select the `usessl` option.

4. Select MDM Party Maintenance(TESTSNAPSHOTTWO) and select **EPV MDM_Connection_Details**. Set the details of the MDM2 instance here. Provide a non-secure port such as 9080 for simplicity purposes. Do not select the `usessl` option.
5. Select Physical MDM Suspected Duplicates(TESTSNAPSHOTONE) and select **EPV MDM_Connection_Details**. Set the details of the MDM1 instance here. Provide a non-secure port such as 9080 for simplicity purposes. Do not select the `usessl` option.
6. Select Physical MDM Suspected Duplicates(TESTSNAPSHOTTWO) and select **EPV MDM_Connection_Details**. Set the details of the MDM2 instance here. Provide a non-secure port such as 9080 for simplicity purposes. Do not select the `usessl` option.

F. MDM databases

Complete these steps on the MDM databases:

1. Run the following SQL commands on the database connected to the MDM1 instance:

```
UPDATE CONFIGELEMENT SET
      VALUE = 'true', LAST_UPDATE_DT = CURRENT_TIMESTAMP WHERE NAME =
      '/IBM/DWLCommonServices/Notifications/enabled';
UPDATE CDEVENTDEFTP SET
      ENABLE_NOTIFY='Y', LAST_UPDATE_DT=CURRENT_TIMESTAMP WHERE (LANG_TP_CD=100 AND
      EVENTDEF_TP_CD=8);
update configelement set value='true',
      last_update_dt=current_timestamp where
      name='/IBM/Party/SuspectProcessing/enabled';
INSERT INTO BPMNOTIFICATIONTYPE VALUES
      ('ntem','MDMSDP', 'TESTSNAPSHOTONE', null, 'MDM_EVT_SDP', null, null, null, null,
      CURRENT_TIMESTAMP, null);
INSERT INTO BPMNOTIFICATIONTYPE VALUES ('nt1','MDMSDP',
      'TESTSNAPSHOTONE', null, 'MDM_EVT_SDP', null, null, null, null, CURRENT_TIMESTAMP,
      null);
INSERT INTO BPMNOTIFICATIONTYPE VALUES ('nt2','MDMSDP', 'TESTSNAPSHOTONE', null,
      'MDM_EVT_SDP', null, null, null, null, CURRENT_TIMESTAMP, null);
INSERT INTO
      BPMNOTIFICATIONTYPE VALUES ('nt3','MDMSDP', 'TESTSNAPSHOTONE', null, 'MDM_EVT_SDP',
null,
      null, null, null, CURRENT_TIMESTAMP, null);
INSERT INTO BPMNOTIFICATIONTYPE VALUES
      ('ntpe','MDMHDQ', 'TESTSNAPSHOTONE', null, 'PERSIST_ENTITY', null, null, null, null,
      CURRENT_TIMESTAMP, null);
```

2. Run the following SQL commands on the database connected to the MDM2 instance:

```
UPDATE CONFIGELEMENT SET
      VALUE = 'true', LAST_UPDATE_DT = CURRENT_TIMESTAMP WHERE NAME =
      '/IBM/DWLCommonServices/Notifications/enabled';
UPDATE CDEVENTDEFTP SET
      ENABLE_NOTIFY='Y', LAST_UPDATE_DT=CURRENT_TIMESTAMP WHERE (LANG_TP_CD=100 AND
      EVENTDEF_TP_CD=8);
update configelement set
      value='true', last_update_dt=current_timestamp where
      name='/IBM/Party/SuspectProcessing/enabled';
INSERT INTO BPMNOTIFICATIONTYPE VALUES
      ('ntem','MDMSDP', 'TESTSNAPSHOTTWO', null, 'MDM_EVT_SDP', null, null, null, null,
      CURRENT_TIMESTAMP, null);
INSERT INTO BPMNOTIFICATIONTYPE VALUES ('nt1','MDMSDP',
      'TESTSNAPSHOTTWO', null, 'MDM_EVT_SDP', null, null, null, null, CURRENT_TIMESTAMP,
      null);
INSERT INTO BPMNOTIFICATIONTYPE VALUES ('nt2','MDMSDP', 'TESTSNAPSHOTTWO', null,
      'MDM_EVT_SDP', null, null, null, null, CURRENT_TIMESTAMP, null);
INSERT INTO
      BPMNOTIFICATIONTYPE VALUES ('nt3','MDMSDP', 'TESTSNAPSHOTTWO', null, 'MDM_EVT_SDP',
null,
      null, null, null, CURRENT_TIMESTAMP, null);
INSERT INTO BPMNOTIFICATIONTYPE VALUES
      ('ntpe','MDMHDQ', 'TESTSNAPSHOTTWO', null, 'PERSIST_ENTITY', null, null, null, null,
      CURRENT_TIMESTAMP, null);
```

Tips:

- If you give snapshot names in the Process Center Console different than these, make sure to change the SQLs as well. Make sure all the SQLs complete successfully.

- If any duplicate errors come up while inserting data to BPMNOTIFICATIONTYPE table, delete the existing entries causing the issue and run the SQLs again.

All

Restart all instances: MDM1, MDM2, and BPM. Ensure that all of the application servers, node agents, and deployment managers are restarted.

Chapter 4. Premium Production Plans

IBM MDM on Cloud Small, Medium, and Large production premium plans

Premium plans support Backup Infrastructure for production offerings

The premium production offerings include six machines with the following software:

- A primary InfoSphere MDM virtual machine with:
  - InfoSphere MDM Advanced Edition
  - WebSphere Application Server deployment manager (Dmgr)
  - One node
- A secondary InfoSphere MDM virtual machine with:
  - WebSphere Application Server deployment manager (Dmgr)
  - Secondary node
- An MDM Database virtual machine with IBM DB2. HA offering will have two database machines
- An IBM Business Process Manager virtual machine. HA offering will have two Business Process Manager machines.
- An IBM InfoSphere Information Server virtual machine
- A backup Infrastructure machine

IBM Master Data Management on Cloud Premium Small

Host Names

Machine	Hostname
InfoSphere® MDM primary operational server	`<orderID>-s-mdmp.ibm.com`
InfoSphere MDM secondary operational server	`<orderID>-s-mdms.ibm.com`
MDM database	`<orderID>-s-mdmd.ibm.com`
IBM Business Process Manager	`<orderID>-s-bpmp.ibm.com`
InfoSphere Information Server	`<orderID>-s-iisp.ibm.com`
Backup Server	`<orderID>-s-bckp.ibm.com`

Specifications & Topology

Refer to below links

https://public.dhe.ibm.com/cloud/bluemix/hosted/mdmoncloud_specifications.pdf

https://public.dhe.ibm.com/cloud/bluemix/hosted/MDM_Topology_V_1_6.pdf

Related Topics

- Common Specifications
- First Steps
- Administration

IBM Master Data Management on Cloud Premium Medium

Host Names

Machine	Hostname
InfoSphere® MDM primary operational server	`<orderID>-m-mdmp.ibm.com`
InfoSphere MDM secondary operational server	`<orderID>-m-mdms.ibm.com`
MDM database	`<orderID>-m-mdmd.ibm.com`
IBM Business Process Manager	`<orderID>-m-bpmp.ibm.com`
InfoSphere Information Server	`<orderID>-m-iisp.ibm.com`
Backup Server	`<orderID>-m-bckp.ibm.com`

Specifications & Topology

Refer to below links

https://public.dhe.ibm.com/cloud/bluemix/hosted/mdmoncloud_specifications.pdf

https://public.dhe.ibm.com/cloud/bluemix/hosted/MDM_Topology_V_1_6.pdf

Related Topics

- Common Specifications
- First Steps
- Administration

IBM Master Data Management on Cloud Premium Large

Host Names

Machine	Hostname
InfoSphere® MDM primary operational server	`<orderID>-l-mdmp.ibm.com`
InfoSphere MDM secondary operational server	`<orderID>-l-mdms.ibm.com`
MDM database	`<orderID>-l-mdmd.ibm.com`
IBM Business Process Manager	`<orderID>-l-bpmp.ibm.com`
InfoSphere Information Server	`<orderID>-l-iisp.ibm.com`
Backup Server	`<orderID>-l-bckp.ibm.com`

Specifications & Topology

Refer to below links

https://public.dhe.ibm.com/cloud/bluemix/hosted/mdmoncloud_specifications.pdf

https://public.dhe.ibm.com/cloud/bluemix/hosted/MDM_Topology_V_1_6.pdf

Related Topics

- Common Specifications

- First Steps
- Administration

Common Specifications

Security

Users

Machine	SSH Users	Non SSH Users	Application Users
MDM primary	mdmcloud, unique_user	root	mdmadmin, wasadmin
MDM Secondary	mdmcloud, root	NA	mdmadmin
DB2	root	db2inst1, db2fenc1, dasusr1, mdmdbusr	NA
BPM	root	bpmdbusr	bpmdeadmin, bpmcelladmin,DSUser1
Information Server	root	dsadm, iauser, dsodb, srduser, xmetasr, xmeta, isadmin, wasadmin, db2inst1	wasadmin
Spectrum Protect Server	root	tsminst, tsminst1, tsminst2	NA

Encryption

Machine	Encryption Type	Encrypted Location	Keys Location
MDM Primary	Disk	/home/mdmcloud	/keystore/keyfile
MDM Secondary	Disk	/home/mdmcloud	/keystore/keyfile
DB2	Disk	/opt/DBNode, /keys	/keystore/keyfile
DB2	DB2 Native	NA	/keys/iiskeystore.p12
BPM	Disk	/bpm, /dbdata	/keystore/keyfile
BPM	DB2 Native	NA	/keys/iiskeystore.p12
Information Server	Disk	/keys, /home2, /opt	/keystore/keyfile
Spectrum Protect Server	Disk	/storage1, /storage2, /storage3, /storage4	/keystore/keyfile

Ports

MDM primary

Ports	Source	Comments
1550, 1552, 1553, 1650, 1652, 1653	Spectrum Protect Server	Ports opened to Spectrum Protect Server
9354,9043,9443,5061,7286,9633,9444,7277,8879,1025	MDM Secondary, DB2, Information Server, BPM, and WAS remote node	

DB2

Ports	Source	Comments
50602	MDM primary, MDM secondary, and Information Server machines	
1550, 1552, 1553, 1650, 1652, 1653	Spectrum Protect Server	Ports opened to Spectrum Protect Server
4362	MDM Primary Machine	Gateway Port

MDM secondary

Ports	Source	Comments
1550, 1552, 1553, 1650, 1652, 1653	Spectrum Protect Server	Ports opened to Spectrum Protect Server
9354, 9043, 9443, 9444, 5061, 7286, 9633, 7272, 8878	MDM primary, DB2, BPM and Information Server machines	All ports belong to WebSphere Application Server
4362	MDM Primary Machine	Gateway Port

BPM

Ports	Source	Comments
1550, 1552, 1553, 1650, 1652, 1653	Spectrum Protect Server	Ports opened to Spectrum Protect Server
9354, 9043, 9443, 5061, 7286, 9633	MDM primary and MDM secondary machines	WebSphere Application Server owns all of these ports
4362	MDM Primary Machine	Gateway Port

Information Server

Ports	Source	Comments
2825, 5076, 5077, 5558, 5578, 7284, 7286, 8882, 9043, 9060, 9080, 9081, 9108, 9353, 9403, 9404, 9405, 9446, 9633, 10000, 10001, 10002, 10003, 10004, 10005, 13401, 13402, 31531, 31538, 50000, 5986, 19443	MDM primary, MDM secondary, and DB2 machines	WebSphere Application Server owns all of these ports
1550, 1552, 1553, 1650, 1652, 1653	Spectrum Protect Server	Ports opened to Spectrum Protect Server
4362	MDM Primary Machine	Gateway Port

Spectrum Protect Server

Ports	Source	Comments
1550, 1552, 1553, 1650, 1652, 1653	MDM primary, MDM secondary, DB2, BPM and Information Server machines	Used to access Spectrum Protect clients
4362	MDM Primary Machine	Gateway Port

All six machines

Ports	Source	Comments
SSH - 4362	All machines	Port 4362 is exposed by all machines to Gateway Machine
Bootp - 68 UDP port	All machines	Port 68 is exposed by all machines
HTTP+SSL 443	All machines	Port 443 is exposed by all machines
PING - ICMP	All machines	Used to allow ping

Administration

MDM Primary/MDM Secondary

Start MDM Server

1. Log in as mdmcloud to MDM Primary machine and MDM Secondary Machine. **Warning: Attempting to start the applications server with root or any other user will corrupt the profile.**
2. Start the dmgr
   a. su to mdmcloud
   b. Change directory to Dmgr Profile home/bin
   c. Run `./startManager.sh`
3. Start the node agents on MDM Primary and MDM Secondary
   a. su to mdmcloud
   b. Change directory to Application Profile home/bin
   c. Run ./startNode.sh
   d. Change the directory to Proxy Profile Home/bin
   e. Start the nodes ./startNode.sh
4. Start the server on MDM Primary and MDM Secondary
   a. su to mdmcloud
   b. Change directory to Dmgr Profile home/bin
   c. Run ./startServer.sh servername
   d. Change the directory to Proxy Profile Home/bin
   e. Start the servers ./startServer.sh proxy

MDM Database

1. Log in to the MDM Database as root
2. Switch to db2 instance owner user

```
su - db2inst1
```

3. Run the command db2start on MDM database

```
db2 start db manager
```

4. For more information DB2 Knowledge center

BPM Server

Start BPM Server

1. Start Deployment Manager. Refer to Welcome Letter for BPM install user.
2. Start Node Agents
3. Start Servers
4. For more information DB2 Knowledge center

Information Server

Start Information Server

Spectrum Protect (backup) Server

Start Spectrum Protect Server

1. Open Spectrum Protect server using putty or terminal. Executed below commands.
2. cd `/bckp/opt/tivoli/tsm/server/bin/`
3. Below commands start spectrum Protect Server 1.

```
. /bckp/tsminst1/sqllib/db2profile
./dsmserv -u tsminst1 -i /bckp/tsminst1  -q &
```

4. Below commands start spectrum Protect Server 2.

```
. /bckp/tsminst2/sqllib/db2profile
./dsmserv -u tsminst2 -i /bckp/tsminst2  -q &
```

Start Operation Center

1. Open Spectrum Protect server using putty or terminal. Executed below commands.
2. cd /bckp/opt/tivoli/tsm/ui/Liberty/bin

```
service opscenter.rc status
service opscenter.rc start
```

3. Initially Spectrum Protect server second instance will be down, it'll take 5 to 10 minutes to come up. You can check if both instances are up , under overview tab in operation center console.

```
https://<PUBLIC_IP>:11090/oc
```

First Steps

Gateway Machine : MDM Primary

Logging in to the machines for first time

1. SSH into the Gateway machine using unique user provided in the welcome letter using port 4362.
2. Change the password and su to root user.
3. Change the root password.
4. SSH into other machines in the plan from the gateway machine using root user using port 4362. The access is allowed only from gateway machine.
5. Change the root passwords.

Open up required ports

Complete this step for any access, such as for the business administration user interface or ssh.

Important Access to all other machines in the environment is allowed only through gateway machine by default configuration. It is highly recommeded to provide direct ssh accesss to your trusted IP's as part of initial configuration. This will help to access the available machine, in case, the gateway machine fails.

1. Edit the /opt/iig/scripts/ports.prop file and add the ports that you want to open.

2. Run the script that automates the IPTables changes for you.

```
sudo /opt/iig/scripts/enable_ports.sh <Trusted IP Address>
```

   Trusted IP Address: This is the IP address of your computer from which you want to access hosted machines. If you are inside an enterprise LAN, the enterprise gateway IP will be the trusted IP.

3. If you want to open separate set of ports to different trusted IPs, you need to execute the command multiple times with right set of ports and trusted IP.

Chapter 5. High Availability Production Plans

This section describes the high availability features supported by the high availabiltiy part numbers

Technologies and Concepts

The technologies used in MDM high availability

Pacemaker

Pacemaker is a cluster resource manager. It achieves maximum availability for your cluster services (aka. resources) by detecting and recovering from node and resource-level failures by making use of the messaging and membership capabilities provided by your preferred cluster infrastructure (either OpenAIS or Heartbeat).

Portable IP

A special IP provided by Softlayer which is portable across machines. It will be assigned by Pacemaker to available machines. The end user should use the portable IP for accessing UI applications and exposed REST/Webservices from other machines.

Websphere Proxy

The WebSphere proxy server was introduced in WebSphere Application Server Network Deployment V6.0.2. The purpose of this server instance is to act as a surrogate that can route requests to back end server clusters using routing rules and load balancing schemes.

HADR

The DB2® Data Server High Availability Disaster Recovery (HADR) feature is a database replication feature that provides a high availability solution for both partial and complete site failures. HADR protects against data loss by replicating data changes from a source database, called the primary, to a target database, called the standby.

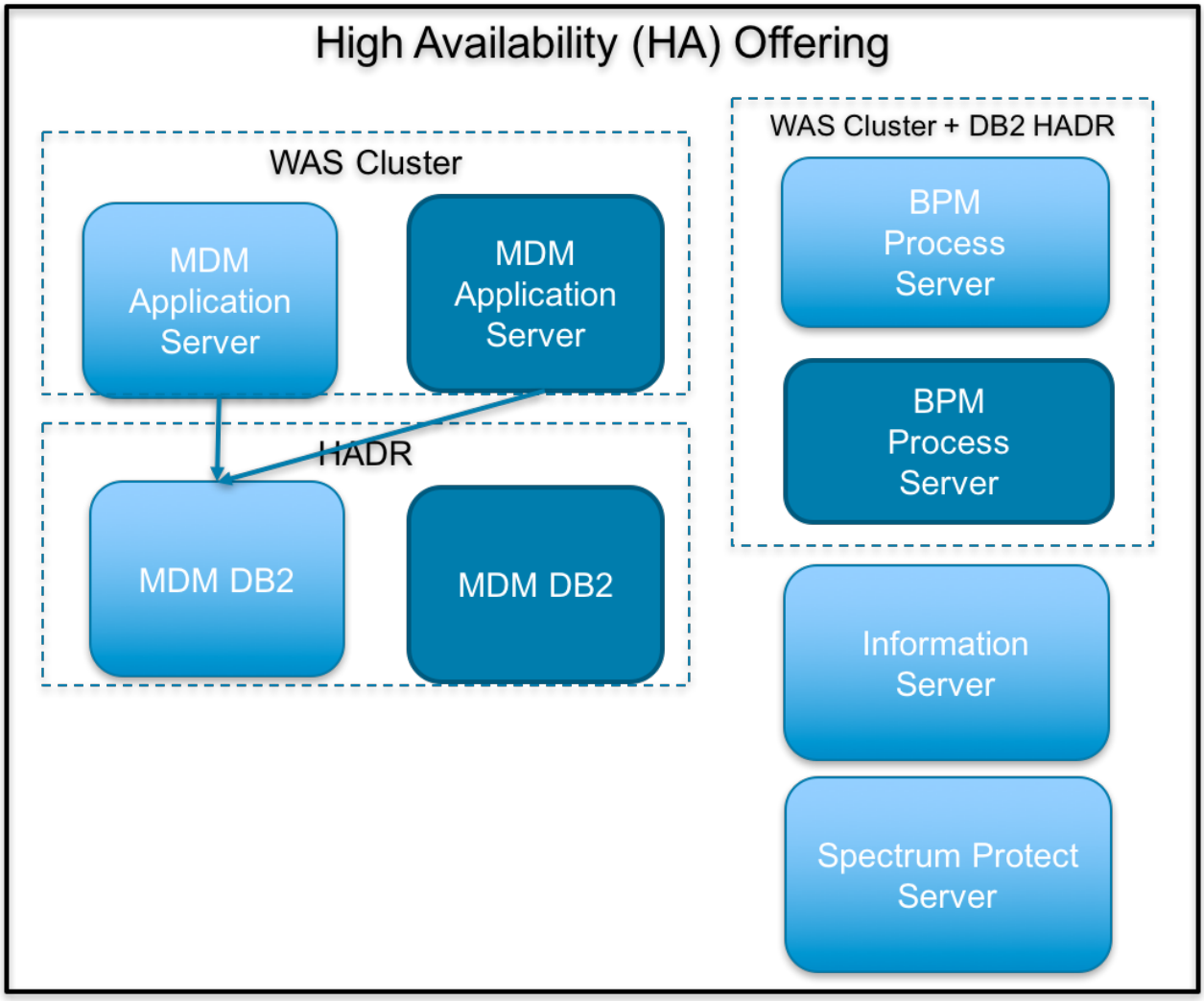
Automatic Client Reroute

The main goal of the automatic client reroute feature is to enable an IBM® Data Server Client application to recover from a loss of communications so that the application can continue its work with minimal interruption. As the name suggests, rerouting is central to the support of continuous operations. But rerouting is only possible when there is an alternate location that is identified to the client connection.

This capability allows WebSphere data sources to connect to available database server.

HA Topology

Consists of highly available Master Data Management and BPM Process Servers. Spectrum protect server will provide the infrastructure for backup. The environment also provide a Information Server installation.



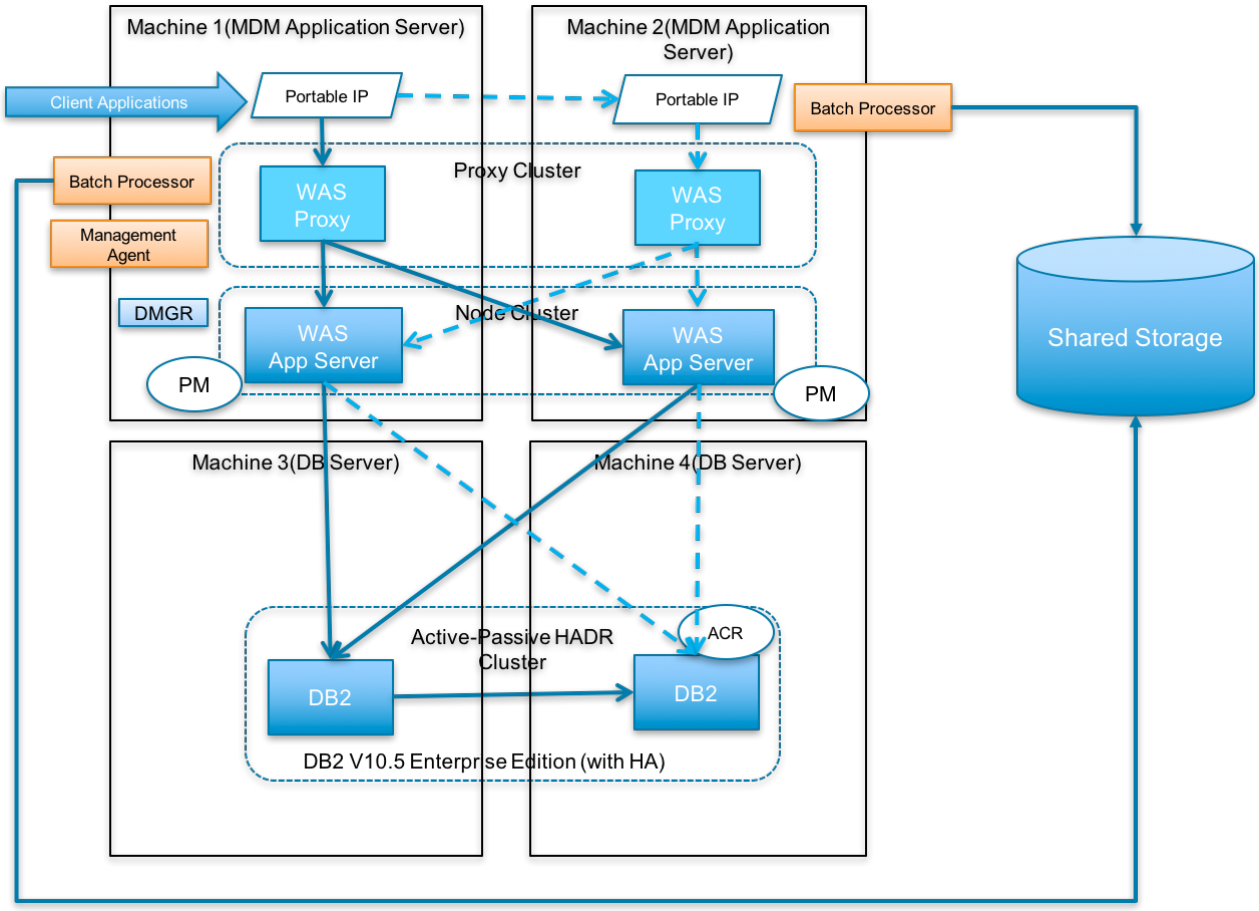
MDM HA Topology

MDM Installation

IBM Websphere Application Server ND is installed on Machine 1 and Machine 2. IBM DB2 is installed on machine 3 and machine 4.

MDM application is installed on top of these middle-ware installations. Websphere Proxy Server cluster is configured on Websphere nodes for HTTP(s) load balancing and sharing. Pacemaker and Corosync are installed on machine 1 and machine 2 to do the failover management. A public portable IP and private portable IP is configured as pacemaker resources.

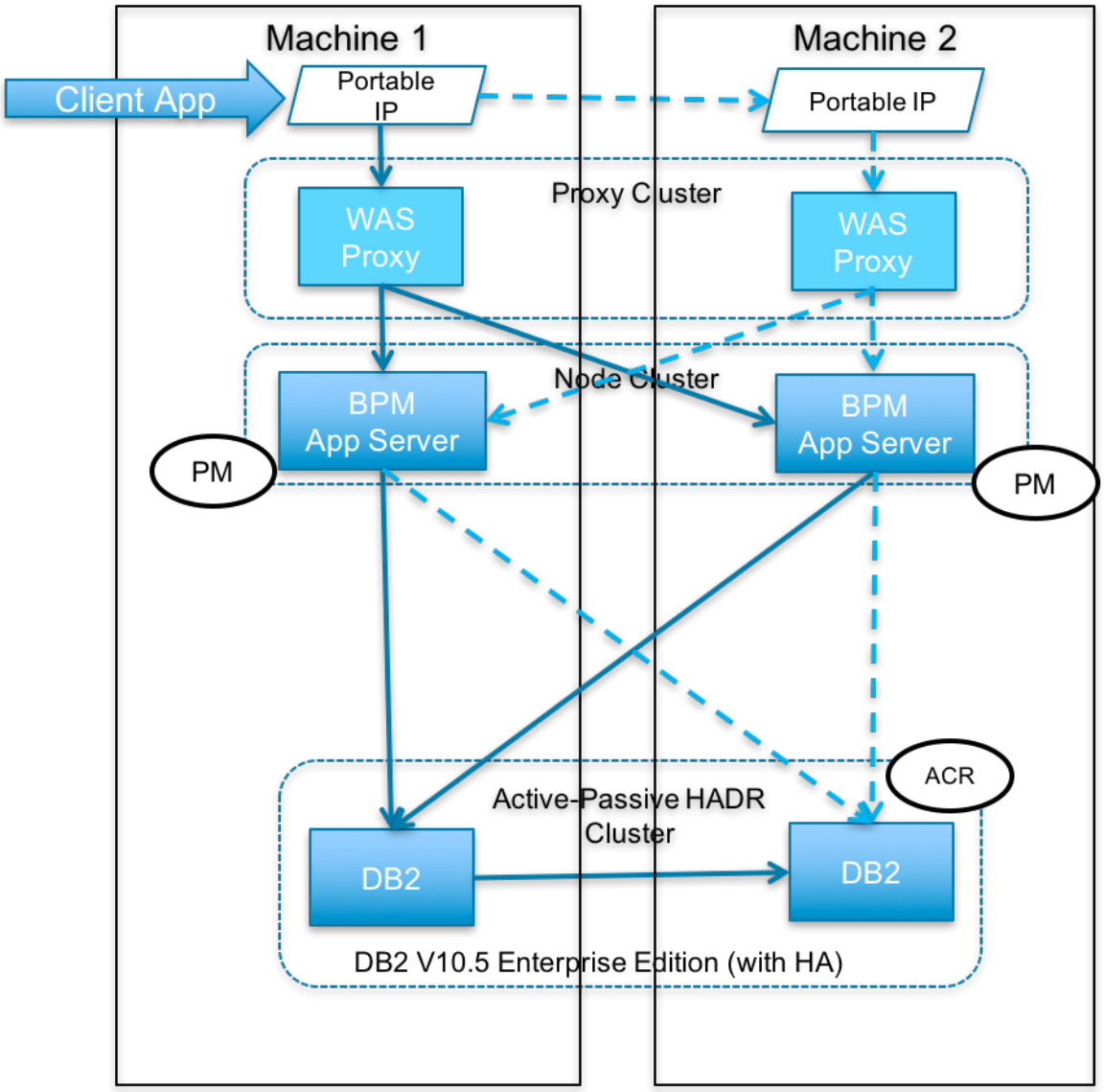
Deployment manager is configured in machine 1 and Batch Processor is present in the machine 1 and machine 2. A shared storage is provided at mount point /batch to use with the batch processor for data loading. Websphere Embedded Messaging engine is configured in a highly available manner. HADR is configured with machine 3 acting as primary and machine 4 as standby. Automatic client reroute is configured in the data sources for seamless connectivity with backend database.



BPM HA Topology

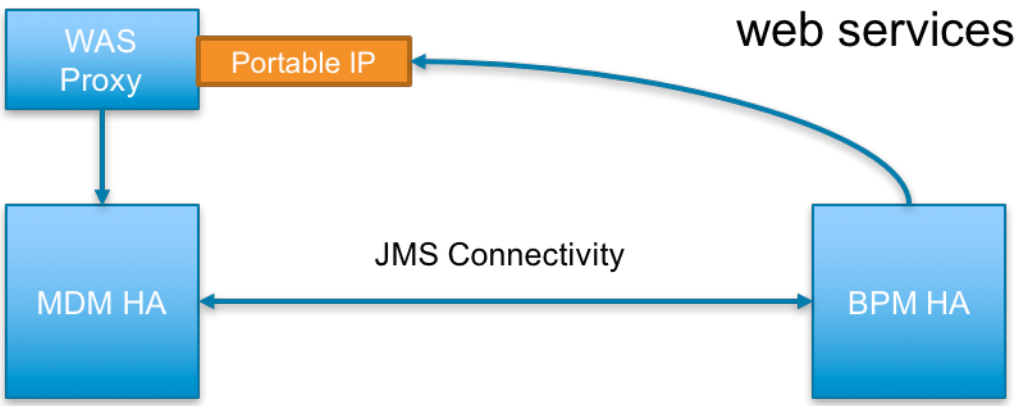
There are two machines in this topology. The BPM Process Server is installed on both machines in a Websphere Application Server ND Cluster. The cluster nodes are located on both machines which provide the high availability. The IBM DB2 server for BPM is installed on both machines which are configured using HADR. The databases in Machine 1 act as primary and Machine 2 as standby. Websphere Proxy Server cluster is configured on this machine to provide HTTP(s) load balancing. Pacemaker installation on both machines provides failover. It uses portable IP provided by the Softlayer.

Websphere Transaction Logs are configured to use the database. Automatic Client Reroute is configured in data sources for seamless connectivity. Websphere Embedded Messaging configured as Highly Available.



MDM BPM Integration

MDM HA Environment is pre-integrated with BPM HA Environment. Suspect notifications from MDM will use the highly available messaging infrastructure to trigger BPM HA workflows. MDM web services exposed over a private portable IP will be used by the BPM Processes.



IBM Master Data Management on Cloud with High Availability Small

Host Names

Machine	Hostname
InfoSphere® MDM primary operational server	<orderID>-s-mdmp.ibm.com
InfoSphere MDM secondary operational server	<orderID>-s-mdms.ibm.com
MDM database	<orderID>-s-mdmd.ibm.com
MDM standby database	<orderID>-s-mdb2.ibm.com
IBM Business Process Manager	<orderID>-s-bpmp.ibm.com
IBM Business Process Manager - Standby	<orderID>-s-bpms.ibm.com
InfoSphere Information Server	<orderID>-s-iisp.ibm.com
Backup Server	<orderID>-s-bckp.ibm.com

Specifications

Refer to below link

https://public.dhe.ibm.com/cloud/bluemix/hosted/mdmoncloud_specifications.pdf

Related Topics

- Common Specifications
- First Steps
- Administration

IBM Master Data Management on Cloud with High Availability Medium

Host Names

Machine	Hostname
InfoSphere® MDM primary operational server	<orderID>-m-mdmp.ibm.com
InfoSphere MDM secondary operational server	<orderID>-m-mdms.ibm.com
MDM database	<orderID>-m-mdmd.ibm.com
MDM standby database	<orderID>-m-mdb2.ibm.com
IBM Business Process Manager	<orderID>-m-bpmp.ibm.com
IBM Business Process Manager - Standby	<orderID>-m-bpms.ibm.com
InfoSphere Information Server	<orderID>-m-iisp.ibm.com
Backup Server	<orderID>-m-bckp.ibm.com

Specifications

Refer to below link

https://public.dhe.ibm.com/cloud/bluemix/hosted/mdmoncloud_specifications.pdf

Related Topics

- Common Specifications
- First Steps
- Administration

IBM Master Data Management on Cloud with High Availability Large

Host Names

Machine	Hostname
InfoSphere® MDM primary operational server	`<orderID>-l-mdmp.ibm.com`
InfoSphere MDM secondary operational server	`<orderID>-l-mdms.ibm.com`
MDM database	`<orderID>-l-mdmd.ibm.com`
MDM standby database	`<orderID>-l-mdb2.ibm.com`
IBM Business Process Manager	`<orderID>-l-bpmp.ibm.com`
IBM Business Process Manager - Standby	`<orderID>-l-bpms.ibm.com`
InfoSphere Information Server	`<orderID>-l-iisp.ibm.com`
Backup Server	`<orderID>-l-bckp.ibm.com`

Specifications

Refer to below link

https://public.dhe.ibm.com/cloud/bluemix/hosted/mdmoncloud_specifications.pdf

Related Topics

- Common Specifications
- First Steps
- Administration

Common Specifications

Security

Users

Machine	SSH Users	Non SSH Users	Application Users
MDM primary	mdmcloud, unique_user	root	mdmadmin, wasadmin
MDM Secondary	mdmcloud, root	NA	mdmadmin
DB2	root	db2inst1, db2fenc1, dasusr1, mdmdbusr	NA
DB2 Standby	root	db2inst1, db2fenc1, dasusr1, mdmdbusr	NA
BPM	root	bpmdbusr	bpmdeadmin, bpmcelladmin,DSUser1

Machine	SSH Users	Non SSH Users	Application Users
BPM Standby	root	bpmdbusr	bpmdeadmin, bpmcelladmin,DSUser1
Information Server	root	dsadm, iauser, dsodb, srduser, xmetasr, xmeta, isadmin, wasadmin, db2inst1	wasadmin
Backup Server	root	tsminst, tsminst1, tsminst2	NA

Encryption

Machine	Encryption Type	Encrypted Location	Keys Location
MDM Primary	Disk	/home/mdmcloud	/keystore/keyfile
MDM Secondary	Disk	/home/mdmcloud	/keystore/keyfile
DB2	Disk	/opt/DBNode, /keys	/keystore/keyfile
DB2	DB2 Native	NA	/keys/iiskeystore.p12
DB2 Standby	Disk	/opt/DBNode, /keys	/keystore/keyfile
DB2 Standby	DB2Native	NA	/keys/iiskeystore.p12
BPM	Disk	/bpm, /dbdata	/keystore/keyfile
BPM	DB2 Native	NA	/keys/iiskeystore.p12
BPM Standby	Disk	/bpm, /dbdata	/keystore/keyfile
BPM Standby	DB2 Native	NA	/keys/iiskeystore.p12
Information Server	Disk	/keys, /home2, /opt	/keystore/keyfile
Backup Server	Disk	/storage1, /storage2, /storage3, /storage4	/keystore/keyfile

Ports

MDM primary

Ports	Source	Comments
9354,9043,9443,5061,7286,9633,9444,7277,8879,1025	MDM Secondary, BPM Server, BPM Standby,	MDM Primary Ports
5404,5405,5406	MDM Secondary Node	Pacemaker Ports

MDM secondary

Ports	Source	Comments
9354, 9043, 9443, 5061, 7286, 9633, 7272, 8878	All Machines in Environment	General Purpose
9354,9043,9443,5061,7286,9633,9444,7277,8879,1025	BPM Server and Standby	Ports opened from MDM secondary machine to BPM machine

Ports	Source	Comments
2810, 9902, 9203, 9204, 9355, 7273, 5002, 5003, 9903, 8879, 9630, 7063, 11005, 11006, 9354, 9356,, 2809, 9900, 9202, 9201, 9353, 7272, 5001, 5000, 9901, 8878, 9629, 7062, 11004	MDM Primary Machine	WAS HA Connection
4362	MDM Primary Machine	Gateway Port
5404,5405,5406	MDM Primary Node	Pacemaker Ports

DB2

Ports	Source	Comments
50602	MDM primary, MDM secondary, and Information Server machines	SSL Port
60666	DB2 Server Standby	hadr ports
4362	MDM Primary Machine	Gateway Port

DB2 Standby

Ports	Source	Comments
50602	MDM primary, MDM secondary, and Information Server machines	SSL Port
60666	DB2 Server	hadr ports
4362	MDM Primary Machine	Gateway Port

BPM

Ports	Source	Comments
9354, 9043, 9443, 5061, 7286, 9633	MDM primary and MDM secondary machines	WebSphere Application Server owns all of these ports
50602, 5404, 5405, 5406, 60666, 60667, 60668, 9443, 9444, 7286, 7287,7277, 9809, 8879, 9100, 9060, 9352, 9632, 9043, 9401, 9402, 9403	BPM Secondary	Ports opened for BPM Secondary machine
4362	MDM Primary Machine	Gateway Port

BPM Standby

Ports	Source	Comments
9354, 9043, 9443, 5061, 7286, 9633	MDM primary and MDM secondary machines	WebSphere Application Server owns all of these ports

Ports	Source	Comments
50602, 5404, 5405, 5406, 60666, 60667, 60668, 9443, 9444, 7286, 7287, 2810, 9902, 9354, 7273, 5002, 5003, 8879, 9630, 9903, 9203, 9204, 9900, 9353, 7272, 5001, 5000, 8878, 9629, 9901, 9202, 9201, 9356, 9355	BPM Primary Machine	Ports opened for BPM primary machine
4362	MDM Primary Machine	Gateway Port

Information Server

Ports	Source	Comments
2825, 5076, 5077, 5558, 5578, 7284, 7286, 8882, 9043, 9060, 9080, 9081, 9108, 9353, 9403, 9404, 9405, 9446, 9633, 10000, 10001, 10002, 10003, 10004, 10005, 13401, 13402, 31531, 31538, 50000, 5986, 19443	MDM primary, MDM secondary, and DB2 machines	WebSphere Application Server owns all of these ports
9446, 9043, 31538	All machines	Ports are exposed to all IPs

All five machines

Ports	Source	Comments
SSH - 4362	All machines	Port 22 is exposed by all machines
Bootp - 68 UDP port	All machines	Port 68 is exposed by all machines
HTTP+SSL 443	All machines	Port 443 is exposed by all machines
PING - ICMP	All machines	Used to allow ping

Administration

MDM Primary/MDM Secondary

Start MDM Server

1. Log in as mdmcloud to MDM Primary machine and MDM Secondary Machine. **Warning: Attempting to start the applications server with root or any other user will corrupt the profile.**
2. Start the dmgr
   a. Switch user to mdmcloud `su mdmcloud`
   b. Change directory to Dmgr Profile home/bin
   c. Run `./startManager.sh`
3. Start the node agents on MDM Primary and MDM Secondary
   a. su to mdmcloud
   b. Change directory to Application Profile home/bin
   c. Run ./startNode.sh

d. Change the directory to Proxy Profile Home/bin
e. Start the nodes ./startNode.sh

4. Start the server on MDM Primary and MDM Secondary
   a. su to mdmcloud
   b. Change directory to Dmgr Profile home/bin
   c. Run ./startServer.sh servername
   d. Change the directory to Proxy Profile Home/bin
   e. Start the servers ./startServer.sh proxy

Verify Pacemaker Configuration

1. Login as root
2. Run the status command

```
crm status
```

MDM Database Primary and Standby

Verify HADR setup

1. Log in to the Primary Database as root
2. Switch to db2 instance owner user `su - db2inst1`
3. Run the command db2pd on MDM database

```
db2pd -hadr -db mdmdb
```

4. The status of the db2 hadr configuration will be shown in the result. It should be in connected mode.

Takeover of database

Note: Takeover is required when primary database goes down.

1. Login to the standby database.
2. Run the db2 takeover command

```
TAKEOVER HADR ON DB MDMDB
```

3. If the command fails, run the command using force

```
TAKEOVER HADR ON DB MDMDB BY FORCE
```

4. For more information DB2 Knowledge center

BPM Server Primary and Standby

Start BPM Server

1. Start Deployment Manager. Note Refer to Welcome Letter for BPM install user.
2. Start Node Agents
3. Start Servers

Takeover of database

Note: Takeover is required when primary database goes down.

1. Login to the standby database.
2. Run the db2 takeover command

```
TAKEOVER HADR ON DB CNMDB
TAKEOVER HADR ON DB PDWDB
TAKEOVER HADR ON DB BPMDB
```

3. If the command fails, run the command using force

```
TAKEOVER HADR ON DB CNMDB BY FORCE
TAKEOVER HADR ON DB PDWDB BY FORCE
TAKEOVER HADR ON DB BPMDB BY FORCE
```

4. For more information DB2 Knowledge center

Verify Pacemaker Configuration

1. Login as root
2. Run the status command

```
pcs resources show
```

Information Server

Start Information Server

First Steps

Gateway Machine : MDM Primary

Logging in to the machines for first time

1. SSH into the Gateway machine using unique user provided in the welcome letter using port 4362.
2. Change the password and su to root user.
3. Change the root password.
4. SSH into other machines in the plan from the gateway machine using root user using port 4362. The access is allowed only from gateway machine.
5. Change the root passwords.

Open up required ports

Complete this step for any access, such as for the business administration user interface or ssh.

Important Access to all other machines in the environment is allowed only through gateway machine by default configuration. It is highly recommeded to provide direct ssh accesss to your trusted IP's as part of initial configuration. This will help to access the available machine, in case, the gateway machine fails.

1. Edit the /opt/iig/scripts/ports.prop file and add the ports that you want to open.
2. Run the script that automates the IPTables changes for you.

```
sudo /opt/iig/scripts/enable_ports.sh <Trusted IP Address>
```

Trusted IP Address: This is the IP address of your computer from which you want to access hosted machines. If you are inside an enterprise LAN, the enterprise gateway IP will be the trusted IP.

3. If you want to open separate set of ports to different trusted IPs, you need to execute the command multiple times with right set of ports and trusted IP.

MDM High Availability Scenarios

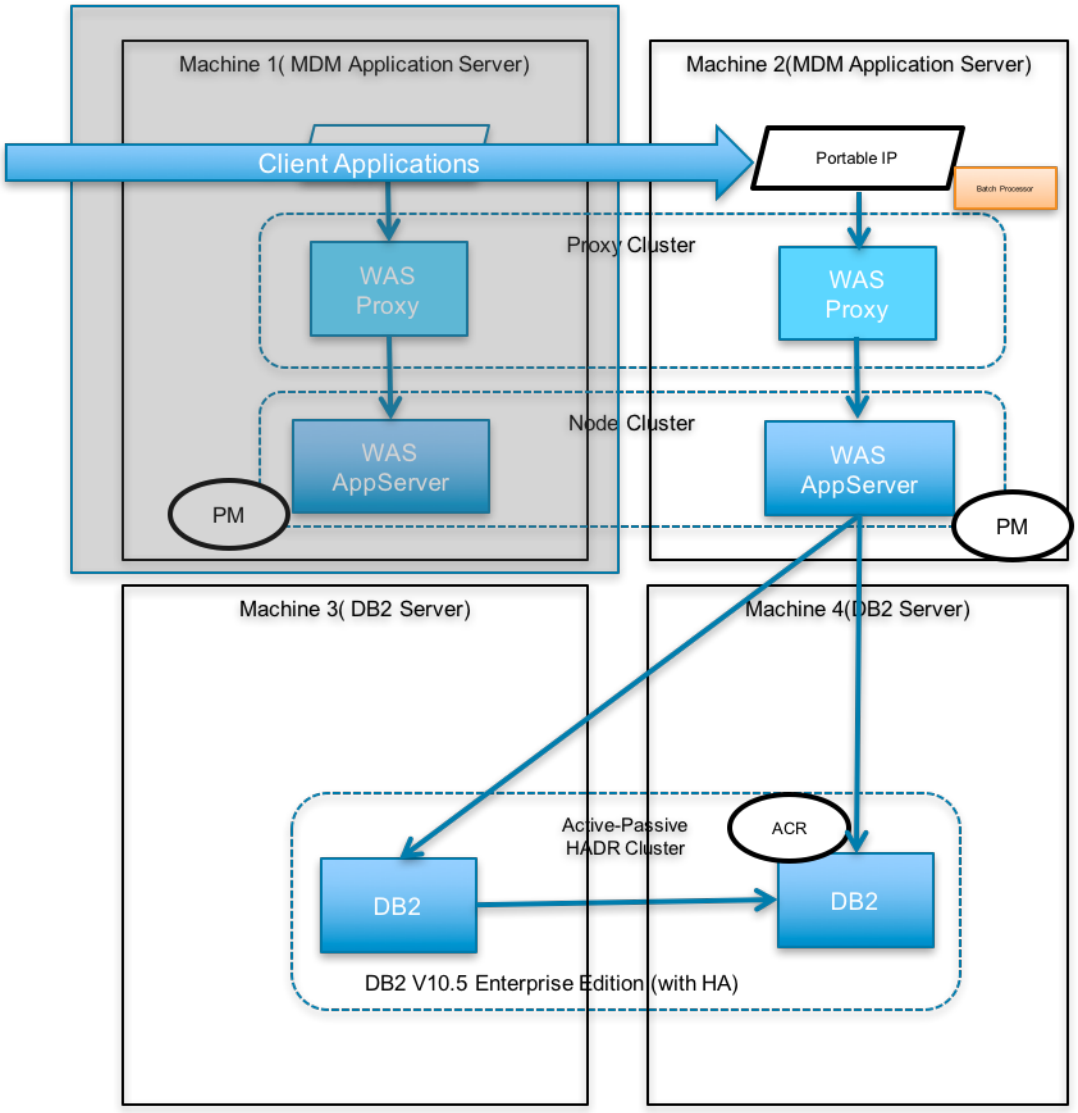
This section depicts different HA Scenarios

MDM Application Server Machine Failover

In a typical production environment there are chances that the machine could go down. This is one of those scenarios.

Scenario

- Machine 1 failed and all communications to that machine is stopped
- Pacemaker component detects that failure and assigns the portable IP to Machine 2
- WebSphere Proxy will receive all Web Service requests and sends to MDM for processing.

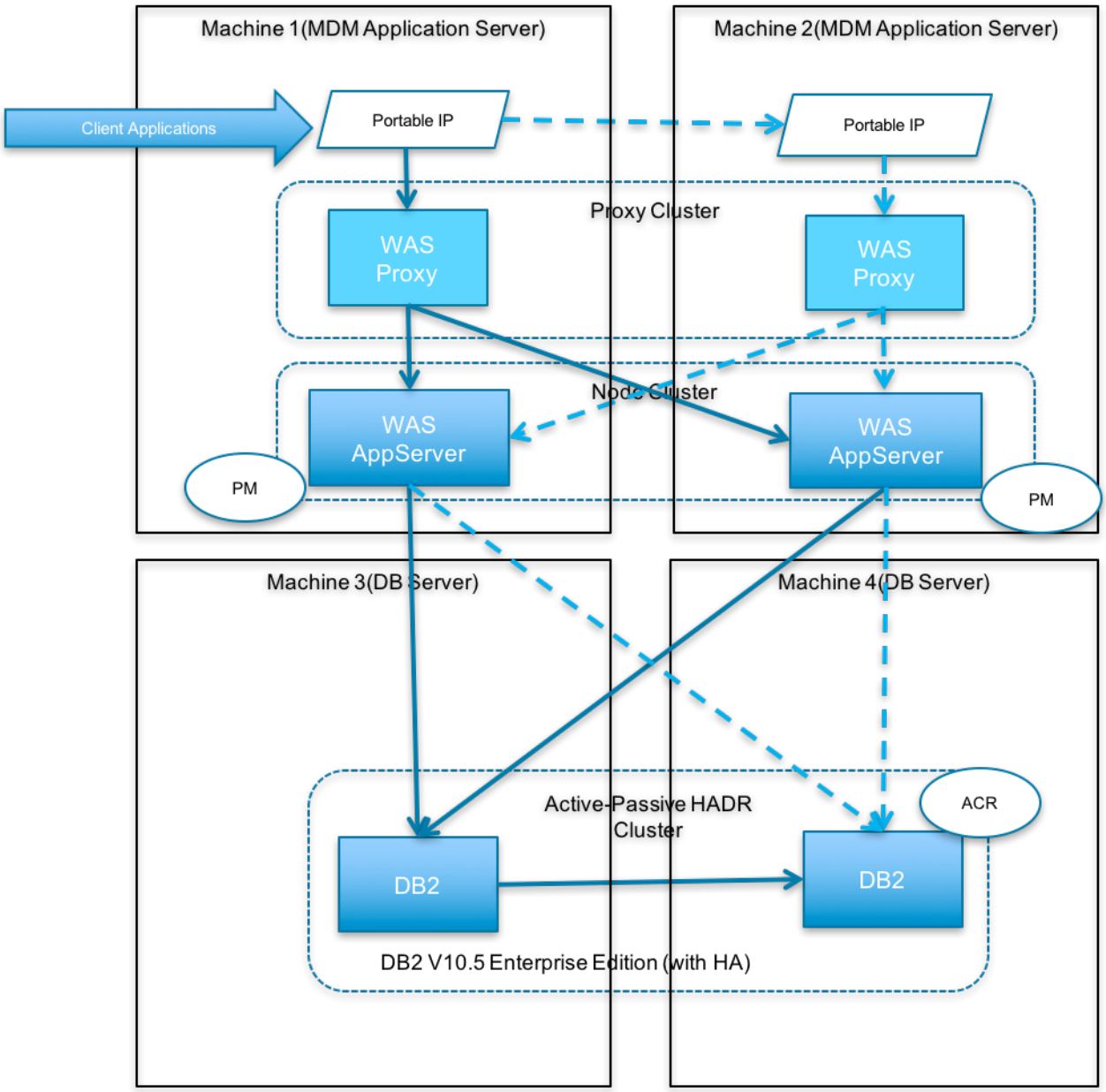


Web Services Load sharing

The webservices requests generated by the client application will be shared across two application servers.

Scenario

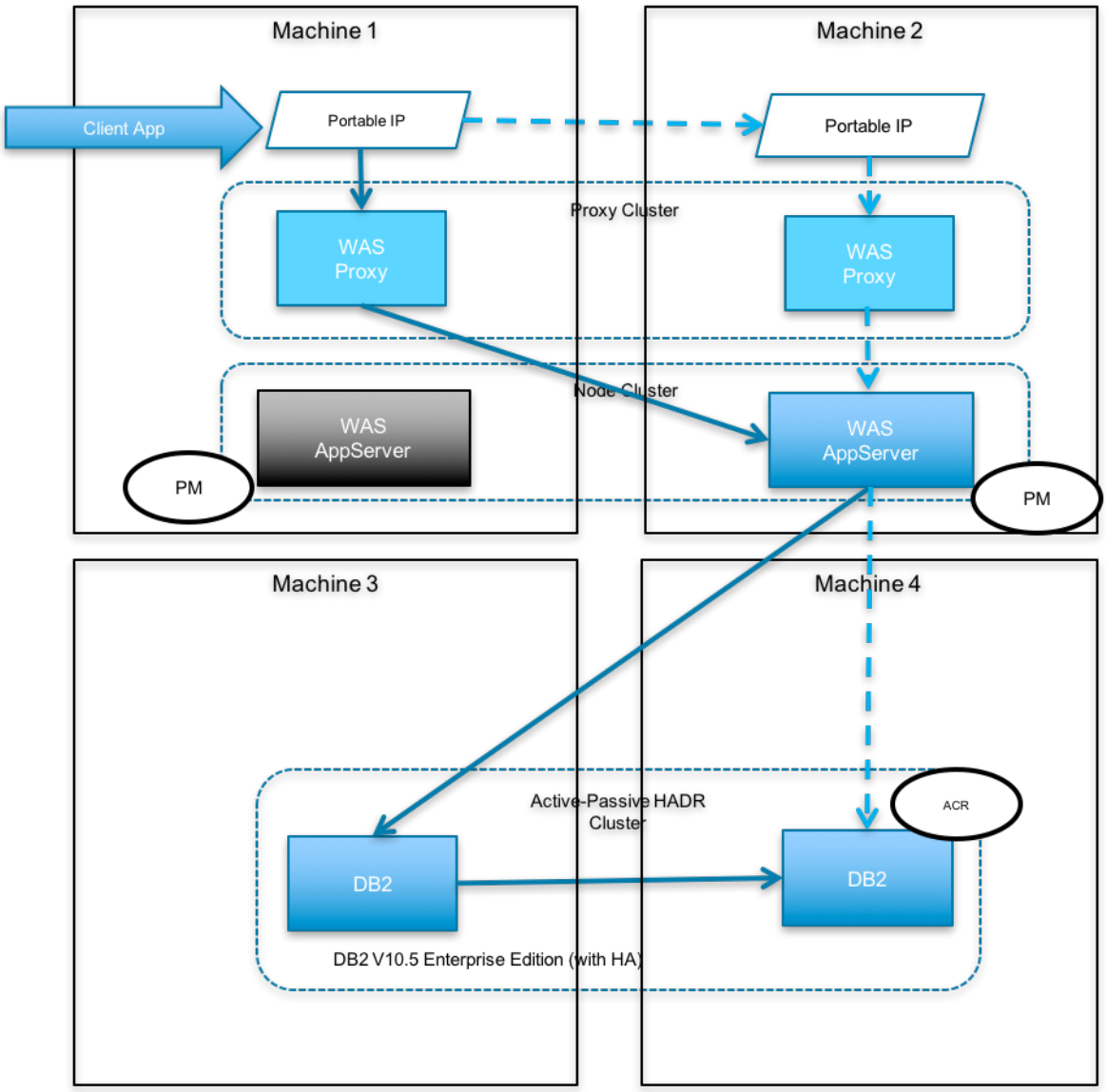
Proxy component will ensure that load is shared between two MDM application server nodes.



Web Services Failover

Scenario

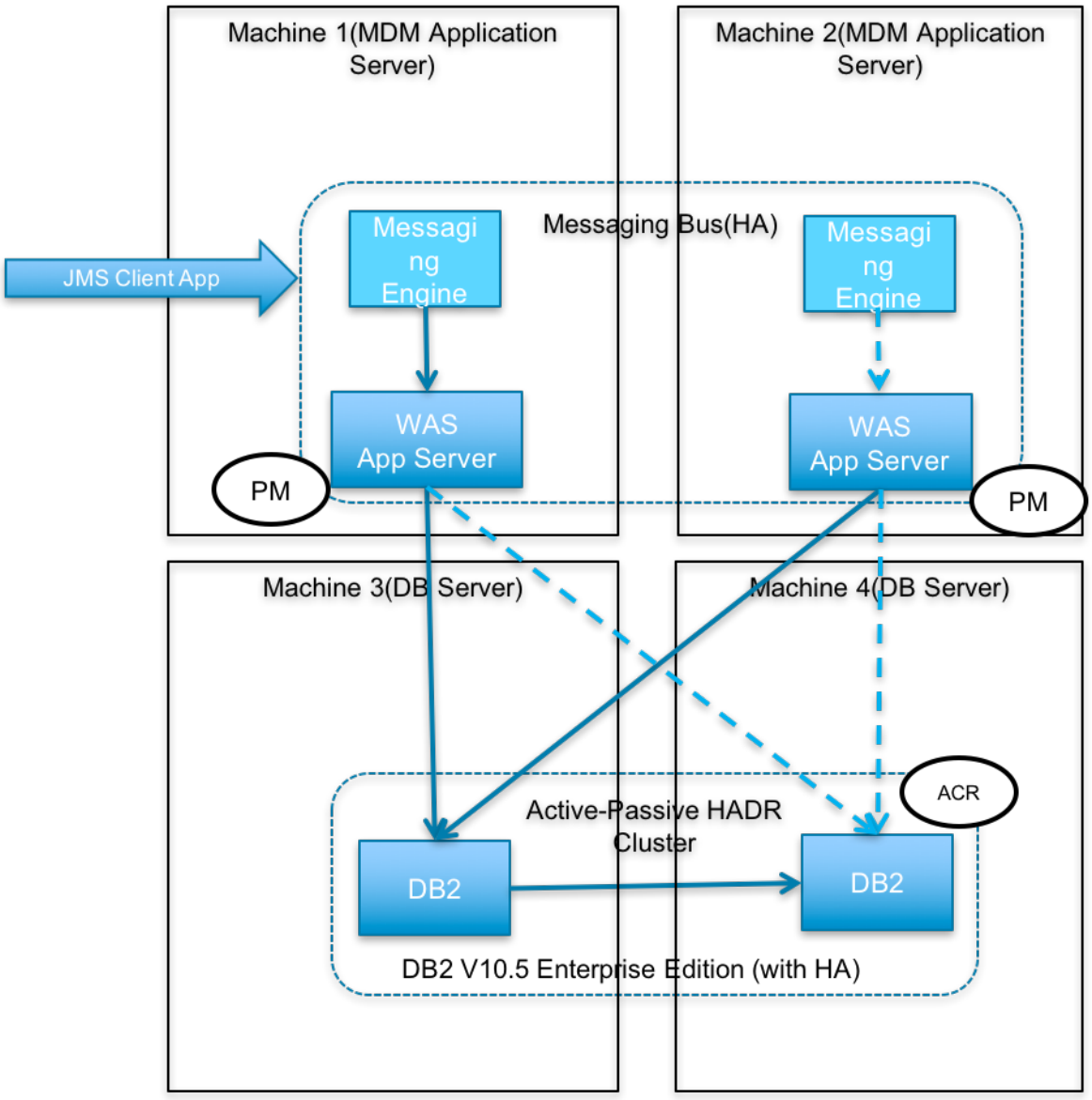
In case an application server fails, the requests will be routed to available application server



Messaging High Availability

Scenario

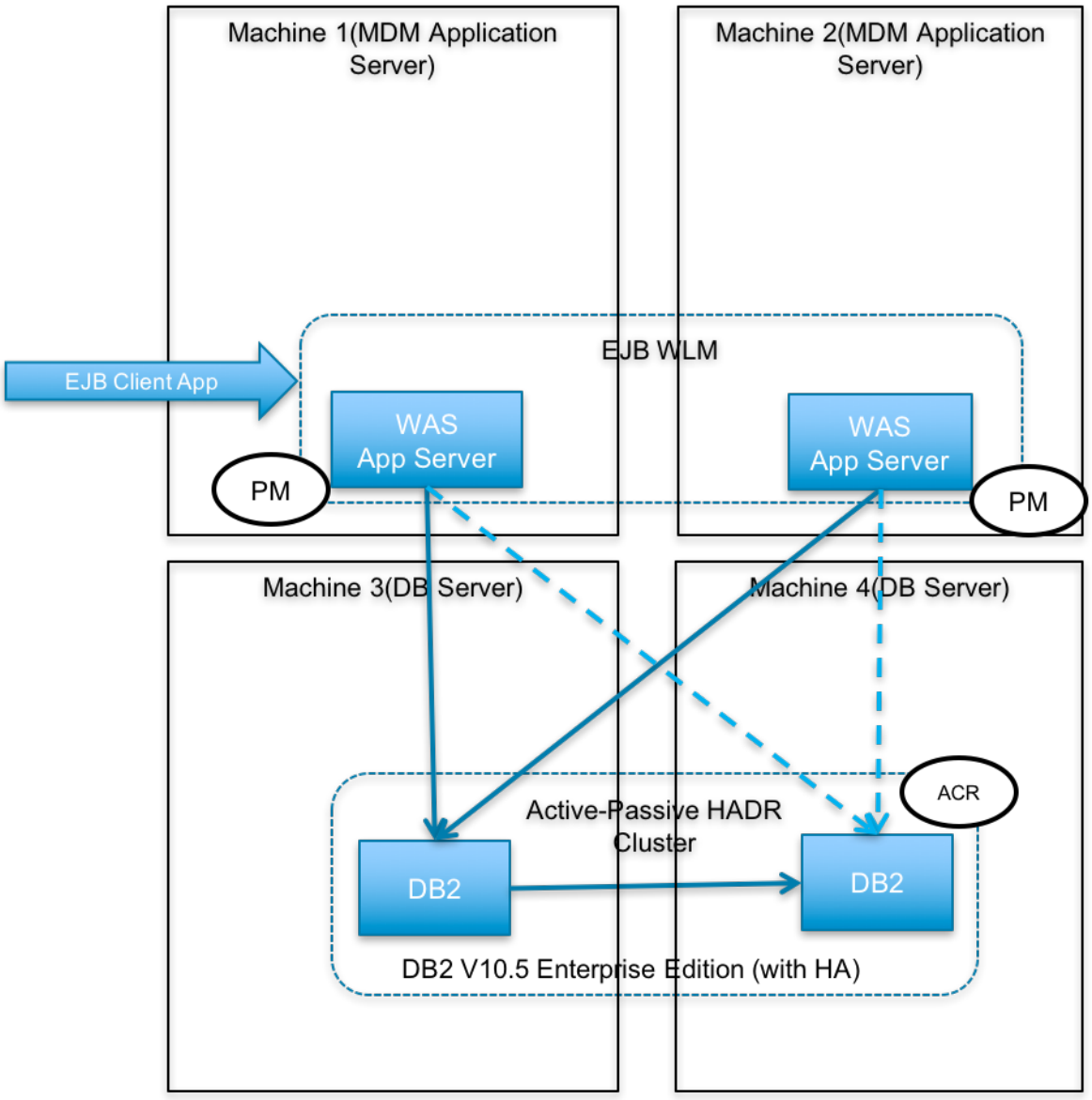
- A high availability configuration ensures there is always a messaging engine running in the cluster. When a server that is hosting a messaging engine fails, the messaging engine is activated and run on another server.
- This can be customized further in WebSphere console.



IIOP High Availability

Scenario

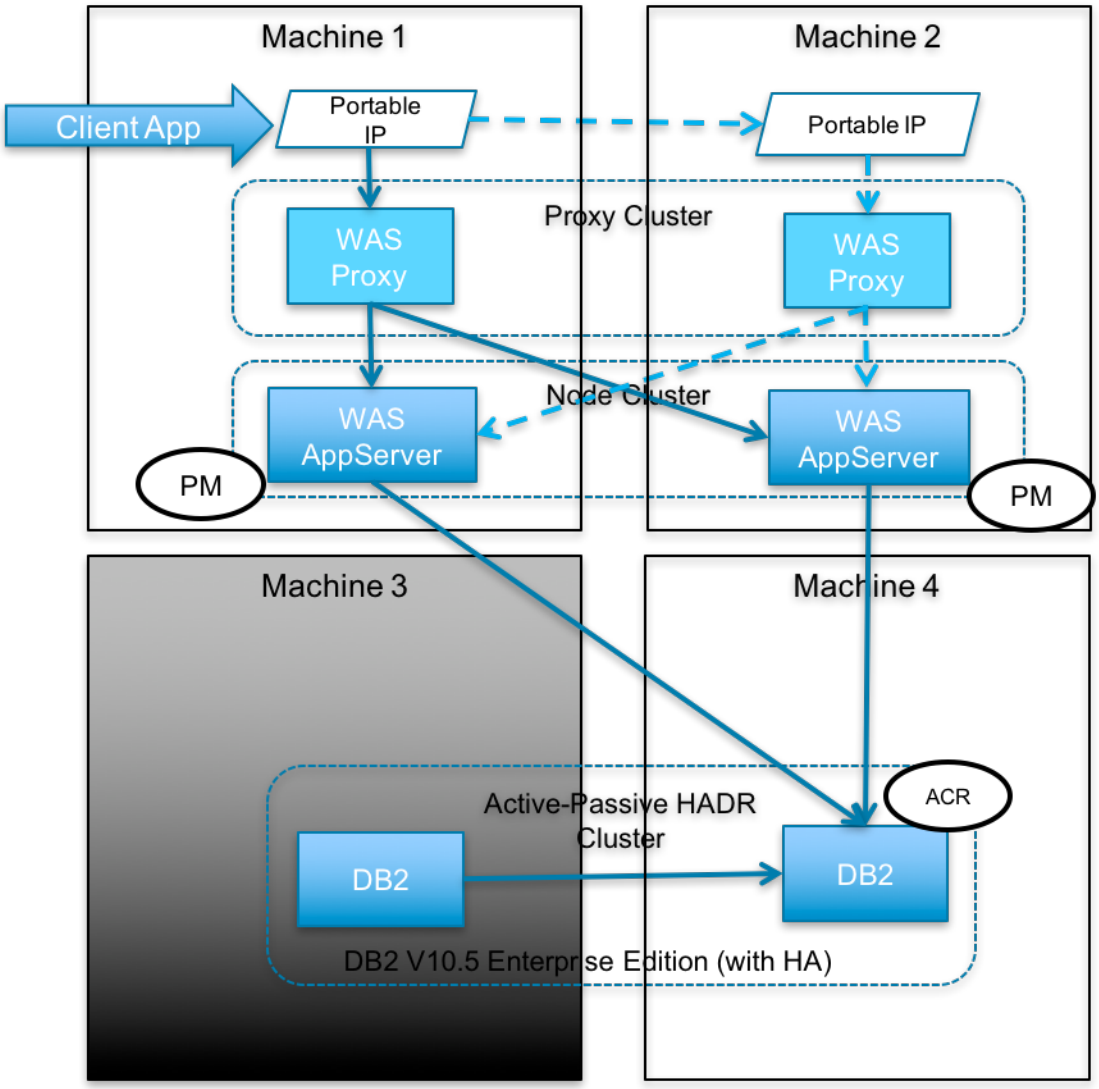
- EJB WLM does load balancing and fail-over



DB2 High Availability and Automatic Client Reroute

- Assume that the primary DB server – Machine 3, goes down.
- The transactions will start failing
- Administrator should run the db2 takeover command on db2 standby machine – Machine 4
- Automatic client reroute will redirect all transactions to machine 4.

Important - This solution do not archive db2 logs automatically. Database administrator should periodically perform db2 log archival.


Machine 1
Machine 2
Client App
Portable IP
Portable IP
Proxy Cluster
WAS Proxy
WAS Proxy
Node Cluster
WAS AppServer
WAS AppServer
PM
PM
Machine 3
Machine 4
ACR
Active-Passive HADR Cluster
DB2
DB2
DB2 V10.5 Enterprise Edition (with HA)

Chapter 6. IBM MDM on Cloud information roadmap

This roadmap outlines the information resources that are available for users of IBM® MDM on Cloud. These resources provide information about various subject areas, such as learning basic skills and troubleshooting.

Product overviews

- **InfoSphere® MDM product overview** IBM InfoSphere Master Data Management (InfoSphere MDM) manages master data for single or multiple domains-customers, patients, citizens, suppliers, locations, products, services offerings, accounts and more-for improving application and business process effectiveness. Learn about the features and benefits of InfoSphere MDM.
- **InfoSphere MDM product documentation** The InfoSphere MDM Knowledge Center provides you with InfoSphere MDM concepts and usage information to help you to prepare for using your system.
- **InfoSphere MDM developerWorks resources** Use the MDM developerWorks blogs, forums, and other resources to interact with other InfoSphere MDM users, stay posted on the latest MDM technical resources, learn how to get the most out of MDM tools, ask questions, and share tips and answers to technical problems.
- **IBM Business Process Manager product overview** IBM Business Process Manager Standard provides tooling and run time for process design, execution, monitoring and optimization-and basic system integration. It is designed for multi-project improvement programs that focus on workflow and productivity. Learn about the features and benefits of IBM Business Process Manager.
- **IBM® Business Process Manager product documentation** The IBM Business Process Manager Knowledge Center enables you to learn about the capabilities and features in IBM® Business Process Manager.
- **InfoSphere DataStage features** Learn about the features and benefits of InfoSphere DataStage.
- **InfoSphere DataStage product documentation** The InfoSphere Information Server Knowledge Center provides you with InfoSphere DataStage concepts and usage information to help new users prepare for using your new system.
- **InfoSphere DataStage developerWorks forum** Use this forum to interact with other InfoSphere DataStage users to better understand how to design, build, debug and deploy jobs for information collection, integration and transformation.

Getting started

- **Overview of InfoSphere MDM** This overview covers InfoSphere MDM concepts, technical features, architecture, scenarios, user roles, and more.

Customizing MDM solutions

- **Configuring and loading data** This section describes how to load data into your MDM solution and provides references such as data dictionaries and data models.
- **Developing additions and extensions** Detailed technical documentation about how to extend, tune, and configure your MDM solution using the MDM Workbench tooling or other methods.
- **Governing data** This documentation provides you with details about the InfoSphere MDM data governance capabilities and data stewardship tools. Data stewards can use these tools to enforce the governance standards that are defined by the data governance council.

- **Using MDM and BPM within the IBM Stewardship Center application** IBM Stewardship Center provides consistent visibility, collaboration, and governance of your master data by combining the strengths of IBM Business Process Manager and InfoSphere® MDM Application Toolkit.
- **Integrating InfoSphere MDM and InfoSphere Information Server** You can use the MDM Workbench to share metadata between your MDM solution and InfoSphere Information Server. Learn more about integrating InfoSphere Information Server features with InfoSphere MDM.

Troubleshooting and support

- **IBM Support Portal** Use the IBM Support Portal for InfoSphere MDM to search for known problems and APARs.
- **Troubleshooting documentation** This section of the InfoSphere MDM Knowledge Center provides information and links to common troubleshooting tools, issues, and concepts.

Chapter 7. Getting started and using IBM MDM on Cloud

You must set up your connection to IBM® MDM on Cloud. Then, you can work with IBM MDM on Cloud as you would with the on-premises product.

Prerequisite: You must know the IP addresses and the credentials of your accounts on the IBM MDM on Cloud servers and clients. This information is in the "Access Credentials and Initial Setup" section of the Welcome letter that you received from your IBM Sales Representative.

The IBM MDM on Cloud software is installed at the following locations on the corresponding provisioned servers, depending on the details of your plan:

- InfoSphere® MDM installation location: `/home/mdmcloud/IBM`
- IBM DB2® (MDM database) installation location: `/opt/ibm/DB2`
- IBM Business Process Manager installation location: `/bpm`
- IBM InfoSphere Information Server installation location: `/opt/IBM/InformationServer`

1. Connect to each of the virtual machines provisioned in your environment. Use the addresses and connection credentials listed in your Welcome letter. Depending on the plan described in your Welcome letter, you will be able to connect to some or all of the following:
   - IBM BPM Designer
   - IBM BPM Process Center
   - IBM InfoSphere Information Server
   - IBM InfoSphere Information Server client
   - InfoSphere MDM runtime operational servers
   - InfoSphere MDM developer instances

You can connect to the MDM developer instances using a tool such as VNC Viewer. IBM Rational Application Developer, including the MDM Workbench, is installed on each developer instance.

1. Install the locally installable components available to you depending on your plan:
   a. Install InfoSphere MDM, IBM DB2, and IBM WebSphere® Application Server components from `/home/mdmcloud/installables`.
   b. Install IBM Business Process Manager components from `/software`.
   c. Install IBM InfoSphere Information Server components from `/tmp`.
2. Move the keys for DB2 encryption and disk encryption for virtual machines to a secure location. The encryption keys for the servers that host InfoSphere MDM, InfoSphere Information Server, or IBM Business Process Manager are initially located in `/keystore`. For more information about encryption, see Disk partitions and encryption.
3. Set up your InfoSphere Information Server virtual machine:
   a. On your local system, use an SSH client to connect to the InfoSphere Information Server virtual machine. For example, you can use PuTTY to connect to the server. The user ID, password, and IP address of the server are in your Welcome letter.
   b. On the InfoSphere Information Server virtual machine, run the ISALite tool. The *IS_install_path* for the InfoSphere Information Server virtual machine is `/opt/IBM/InformationServer`.
   c. Connect the InfoSphere Information Server client to the server by doing these steps. (The user ID, password, and IP address of the client are in your Welcome letter.)
      1) On your local computer, go to the Start menu. Click **Accessories > Remote Desktop Connection**.

2) Enter the IP address of the Windows system that hosts your InfoSphere Information Server client. Click **Connect**.
3) In the Windows Security window of the InfoSphere Information Server client, enter the user name and password for the client. **Important:** Do not include the domain name with the user name.
4) In the InfoSphere Information Server client, open the file `C:\Windows\System32\drivers\etc\hosts`. Add an entry for the InfoSphere Information Server. The host entry is in the following format: `<public_IP_address> <host_name> <short_host_name>`

d. Verify the connection and installation on the InfoSphere Information Server client by doing the following steps.
   - Run the ISALite tool. The *IS_install_path* for the client computer is `C:\IBM\InformationServer`.
   - Test the installation of the IBM InfoSphere DataStage and QualityStage® Administrator and InfoSphere DataStage and QualityStage Designer clients.

e. Install anti-virus software on the client computer to increase security.
f. Enable multiple users to open remote sessions to the InfoSphere Information Server client:
   1) Create user accounts.
   2) Give users permission to do a remote desktop connection.
   3) Configure the Remote Desktop Session server to allow concurrent remote connections. The number of concurrent remote sessions to the client is based on the offering size of your IBM MDM on Cloud instance.
g. Reset the password for users on the InfoSphere Information Server client. Likewise, reset the password for administrators on the InfoSphere Information Server server.
h. Optional: Change and display firewall security for IBM MDM on Cloud.

4. Connect to the MDM on Cloud client using a remote desktop connection, and then open the client.
5. Continue working with IBM MDM on Cloud by completing the following tasks:
   - Connecting to an on-premises computer
   - Connecting to the database
   - Setting up a non-production environment

Whitelisting other computers

From any host in your MDM on Cloud, you can connect to computers that you trust by whitelisting them.

About this task

In-order to provide your trusted computers access to your MDM on Cloud virtual machines, you should open up the required ports that you want to access.

This task should be executed in all virtual machines you want to access externally.

A helper script is provided on all Linux MDM on Cloud machines.

This script will help to open up set of ports in that machine to the external trusted IP provided. Alternatively, you can modify the IPTables directly.

A property file ports.prop is also provided which lists the ports to be opened. You can edit the property file to add more ports which are required to be opened.

Each line in the property file should have one port.

Procedure

1. Edit the `/opt/iis/scripts/ports.prop` file and add the ports that you want to open.
2. Run the script that automates the IPTables changes for you.

```
sudo /opt/iis/scripts/enable_ports.sh <Trusted IP Address>
```

3. If you want to open separate set of ports to different trusted IPs, you need to execute the command multiple times with right set of ports and trusted IP

Connecting to an on-premises computer

You can connect to an on-premises system from the IBM® MDM on Cloud server or client systems.

Prerequisite: You must know the external IP address of the on-premise computer.

Your on-premise system might be a machine that is running in a UNIX or Microsoft Windows operating system environment.

1. Ensure that you whitelist the external IP of on-premise system Whitelist trusted IP
2. If the on-premise machine that you need to connect to is behind a firewall, do these steps before you connect for the first time:
   a. Log in to the IBM MDM on Cloud server machine that you want to connect from.
   b. On your server machine, ping the on-premise computer. This step verifies that the connection is valid. After the connection is available, you can connect to the on-premise machines.

Setting up a non-production environment

If you have the IBM® MDM on Cloud Non-Production offering plan, then there are some extra steps to complete to set up your non-production environment.

1. Connect to the following virtual machines using the addresses and credentials listed in your Welcome letter:
   - Windows CLients
   - IBM InfoSphere® Information Server
   - InfoSphere MDM developer and test machines.
   - BPM Process Center and Process Server machine.

   You can connect to the MDM developer virtual machines using a tool such as VNC Viewer. IBM Rational® Application Developer, including the MDM Workbench, is installed on each developer virtual machine.
2. For Microsoft Windows clients such as IBM BPM Designer and IBM InfoSphere Information Server client, connect the clients to the server by adding the IBM BPM Process Center and IBM InfoSphere Information Server IP addresses and host names to the hosts file.
   a. Log in to the Windows 2012 client machine as the administrator user.
   b. Open the hosts file located at `C:\Windows\System32\drivers\etc`.
   c. Add the IP address, fully qualified host name, and host name to the end of the file.
   d. Save the file.

   Example:

```
132.27.134.78 mdmwa30-d-bdpc.dal09.us-south.services.bluemix.net mdmwa30-d-bdpc
```

3. Link two InfoSphere MDM instances to a single IBM BPM Process Center instance. For details, see Connecting two InfoSphere MDM instances to a single BPM Process Center.

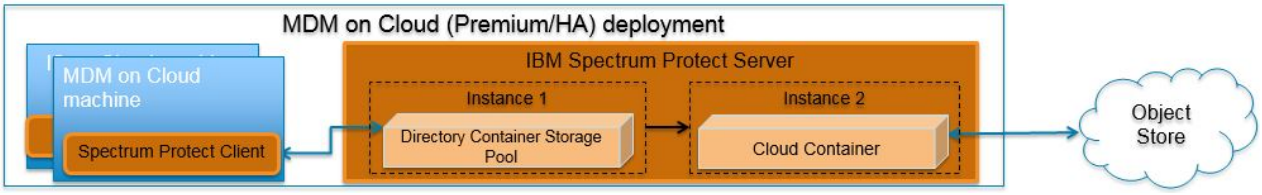
Chapter 8. Backing up IBM MDM on Cloud components

IBM MDM on Cloud Premium and High Availability services provides software and hardware infrastructure for taking backups. Backup capability is based on IBM Spectrum Protect version 8.1.5 product (formerly known as Tivoli Storage Manager). One dedicated server machine with an installation of IBM Spectrum Protect server version 8.1.5 is provided with each deployment of MDM on Cloud Premium and High Availablity service. Spectrum Protect Server version used is 8.1.5 and Spectrum Protect Client 8.1.4, CMS version used is 8.1.5

Sample configuration templates are also provided, you can create new configurations or customize the sample templates to take regular backups.

To learn about IBM Spectrum Protect, check IBM Spectrum Protect Knowledge Center.

Spectrum Protect setup



IBM Spectrum Protect Server installation

Two instances of IBM Spectrum Protect server are configured on a dedicated machine for each deployment of MDM on Cloud Premium and High Availablity service. To store backup data on the storage attached to the server machine, the first instance is configured with Directory Container Storage Pool. The second instance is configured with Cloud Container Storage Pool to store data in Object Store. For the description of different data pools types, check Storage pool types.

By default, operating system IP table rules allows communication only from those machines where IBM Spectrum Protect Client is installed. In order to use Spectrum Protect Operation Console (web application), you need to open 11090 port for specific IPs in the IP table firewall rules.

For small & medium plans, Directory Container Storage Pool is mapped to SAN storage and DB2 (which is used by IBM Spectrum Protect Server) is installed on Performance Storage. SAN storage is encrypted using operating system's LUKS encryption. IBM SoftLayer provides default encryption for Performance Storage in most of the data centers, for remaining data centers encryption is done at the operating system level using LUKS. For data center list you can check IBM SoftLayer documentation.

Directory Container Storage Pool (Instance 1)

A Directory Container Storage Pool is configured in Instance 1, this pool is used to store backup data locally. To know more about Directory Container Storage Pool, check Directory-container storage pools FAQs.

Domain configurations are created for all client machines; these domains are linked with Directory Container Storage pool. For details about policy domain configuration check Creating a policy domain.

Cloud Container Storage Pool (Instance 2)

The Cloud Container Storage Pool configured on Instance 2 is used to store data in cloud storage. The cloud-container storage pools that are provided by IBM Spectrum Protect can store data to cloud storage that is object-based. By storing data in cloud-container storage pools, you can exploit the cost per unit advantages that clouds offer along with the scaling capabilities that cloud storage provides. IBM Spectrum Protect manages the credentials, security, read and write I/Os, and the lifecycle of data that is

stored in the cloud. You can back up and restore data or archive and retrieve data directly from the cloud-container storage pool. To understand more, check Cloud-container storage pools FAQs and Configuring a cloud-container storage pool pages.

Before sending data to Object Store, Spectrum Protect server encrypts the data using an encryption key. For encryption configurations details, check (https://www.ibm.com/support/knowledgecenter/SSEQVQ_8.1.0/srv.admin/t_cloud_encryption.html).

Like Directory Container Storage Pool, policy domain configurations are created for all Client machines; these domains are linked with Cloud Container Storage pool.

Ports exposed

The following ports are opened to and from both the Spectrum Protect server and Spectrum Protect client machines:

- 1550
- 1552
- 1553
- 1650
- 1652
- 1653

Port 4362 is also opened to access Spectrum Protect Server from the Gateway machine.

Apart from these ports, all the other ports are blocked for communication in the Spectrum Protect Server.

You need to open port 11090 from Spectrum Protect Server machine to access the Operations Center.

Node replication

Replicating client data from a source server to another server helps to ensure that backed-up data is available for recovery if the source server is damaged. Replication incrementally copies data from the source server to the target server to provide failover and failback capability.

In the setup provided to you, replication is enabled for all clients and backed-up data is replicated from Spectrum Protect Server Instance 1 to Instance 2 at every hour. If required you can change replication settings by following instructions available at Replicating client data to another server.

Data is replicated from Spectrum Protect instance 1 to Spectrum Protect instance 2 using node replication. The administrative schedule is configured for this purpose. There are two schedules replicate_nodes_weekend and replicate_nodes_weekday. schedule replicate_nodes_weekday replicates data from Spectrum Protect instance 1 to Spectrum Protect instance 2 for every 3 hours. schedule replicate_nodes_weekend replicates data from Spectrum Protect instance 1 to Spectrum Protect instance 2 for every 12 hours. By default, these schedules are stopped, run this.

```
update schedule replicate_nodes_weekday type=administrative expiration=never

update schedule replicate_nodes_weekend type=administrative expiration=never
```

Run above commands from the "Command Builder" of Spectrum protect operation center.

IBM Spectrum Protect client installation

IBM Spectrum Protect Client is installed on all the machines except the one on which IBM Spectrum Protect Server is installed. IBM Spectrum Protect Client is configured to send backup data/metadata/configuration files to Spectrum Protect Server over SSL. The client communicates with IBM Spectrum Protect server using server's private IP.

To learn about IBM Spectrum Protect Client, check IBM Spectrum Protect Knowledge Center

To enable access to IBM Spectrum Protect Client user interfaces, VNC server is installed on Client machines. By default, IP table firewall rules do not allow communication over 5901 port which is used by VNC server. To allow communication from the machine on which you want to access the user interfaces, you need to update IP Table firewall rules for port 5901. VNC server communication is not encrypted, if

your organization mandates this communication to be secure then use some other tool which supports encryption.

Getting started with IBM Spectrum Protect Operations Center console

IBM Spectrum Protect provides a web application called Operations Center for managing IBM Spectrum Protect environment. You can use the Operations Center to monitor multiple servers and to complete some administrative tasks. The Operations Center also provides web access to the IBM Spectrum Protect command line.

More details about Operations Center are available at Managing the Operations Center.

In the setup provided to you, Operations Center is accessible using port 11090. Default IP table firewall rules on the IBM Spectrum Protect server machine does not allow communication with port 11090 from the external machines which are not part of MDM on Cloud service deployment. You can follow below steps to enable Operations Center access from an external machine.

1. Connect to Spectrum Protect server machine using putty or terminal.
2. Go to scripts directory

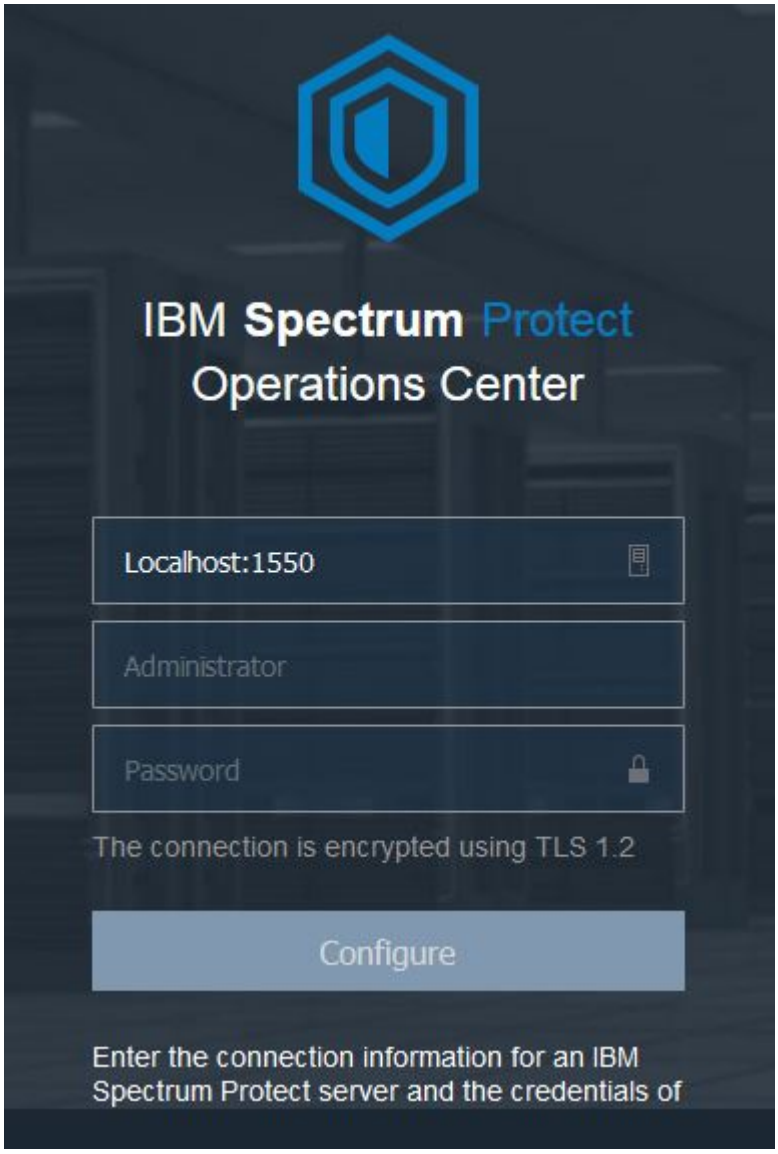
   ```
   cd /opt/iig/scripts
   ```
3. Execute below command after replacing <IP_ADDRESS> with IP address of the machine from where you want to access Operations Console.

   ```
   ./enable_ports.sh <IP_ADDRESS>
   ```

When Operations Center is opened for the first time, it asks for some inputs. You must follow below steps to provide inputs when you open Operations Center for the first time

1. Open following URL in browser after replacing <Spectrum_Protct_Server_IP_Address> with your Spectrum Protect server machine IP.

   ```
   https://<Spectrum_Protct_Server_IP_Address>:11090/oc
   ```
2. When you open Operations Console for the first time, it will ask for credentials.



3. Replace default details with correct values.

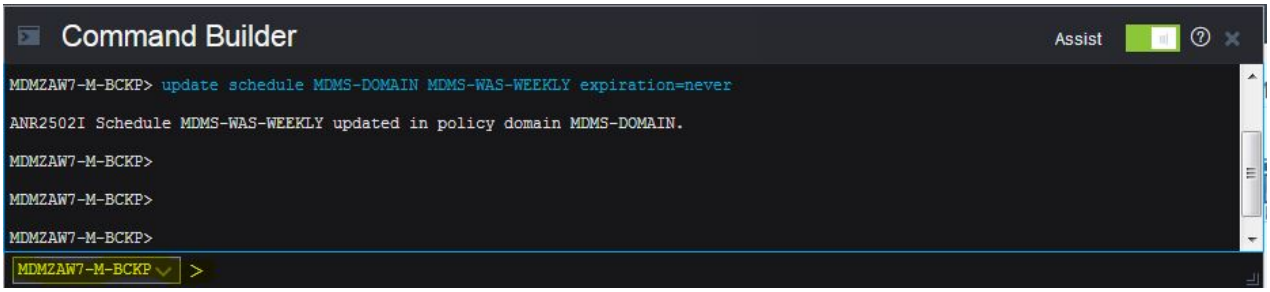
```
Localhost:1500          --   <Spectrum Protect server PUBLIC or PRIVATE IP>:1550
Administrator           --   tsminst
Password                --   Password for tsminst user is provided in welcome letter.
```

4. In the next page, you will be asked to provide password (two times) for "Administrator ID". Provide password.
5. After providing password details, on the next page, you need to specify how frequently you want to collect data. Depending on your requirement you can select 1 minute to 1 hour.
6. Follow instructions on the user interface to finish the wizard.

Note that "Instance 2" may be down and may take few minutes to start. You can check the status of both instances under Overview tab of Operations Center console.

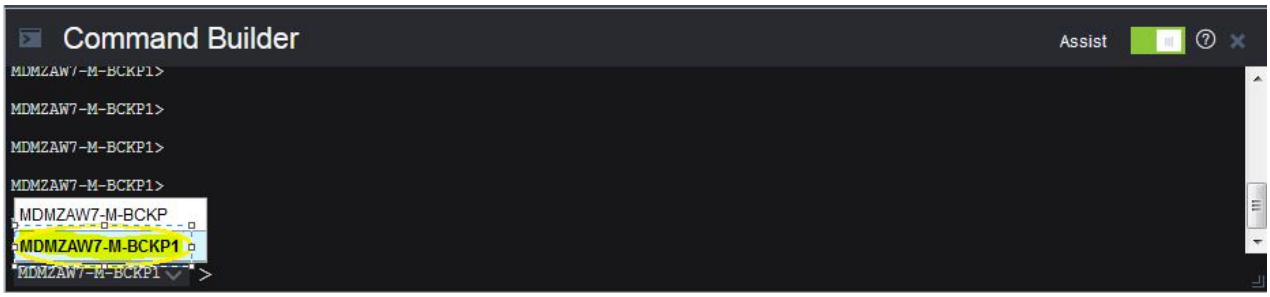
Starting Command Builder

Open following URL in browser `https://<Spectrum_Protct_Server_IP_Address>:11090/oc` to access Operation Center. To open the command-line interface, hover over the first icon from top right side in the Operations Center menu bar, and click Command Builder.



IBM Spectrum Protect processes administrator commands either in the foreground or in the background. Commands that process in the foreground must complete before you can issue another command. When commands are processing in the background, you can issue additional commands at any time. Most IBM Spectrum Protect commands process in the foreground.

Spectrum Protect server contains two instances of servers which are connected using node replication feature for the fail-over scenario. In Command builder left side down you can see both Spectrum Protect instance. By default first instance of Spectrum Protect server is selected. You need to select the second instance of Spectrum protect server if you need to execute any commands against the second instance of Spectrum protect server. In "Command Builder" you can select second instance which has name like <ORDER_ID>_/s/m/l_bckp1. Select drop down menu from left downside corner, as shown in the image.



Retention Policy

Life cycle of backup data objects

A backup object exists in three states, active, inactive, and expired before being purged from the Spectrum Protect server. The four steps involved in the life cycle of a backup data object are listed here.

1. A copy of the client data is sent to the Spectrum Protect server as a backup object. When a backup object is sent to the Spectrum Protect server, it becomes the active version.
2. It remains in an active state until the Spectrum Protect client program deletes the backup object manually, or a newer version of the backup object is sent. The backup object changes state from active to inactive.
3. The backup object remains inactive until it exceeds its retention settings. A backup object can exceed retention settings by either time or number of versions. The backup object changes state from inactive to expired.
4. The backup object remains in the expired state until expiration processing runs on the Spectrum Protect server. This process is invoked by a Spectrum Protect administrator with the expire inventory command. When expiration processing encounters a backup object in the expired state, it purges that object from the Spectrum Protect database and frees up the storage space where the backup object resided.

Spectrum Protect server sample domains for directory container storage pool (Spectrum Protect server local storage) are configured with backretention=30 archretention=30 Spectrum Protect server sample domains for cloud container storage pool (Object storage) are configured with backretention=365 archretention=365

BACKRETention :

Specifies the number of days (from the date the backup versions became inactive) to retain backup versions of files that are no longer on the client file system. This parameter is optional. You can specify an integer from 0 to 9999. The default value is 30. The server uses the backup retention value to manage inactive versions of files when any of the following conditions occur: - A file is rebound to a new management class, but the new management class and the default management class do not contain a backup copy group. - The management class to which a file is bound no longer exists. The default management class does not contain a backup copy group. - The backup copy group is deleted from the management class to which a file is bound. The default management class does not contain a backup copy group.

ARCHRETention :

Specifies the number of days (from the date of archive) to retain archive copies. This parameter is optional. You can specify an integer from 0 to 30000. The default value is 365. The server uses the archive retention value to manage archive copies of files when either of the following conditions occur: - The management class to which a file is bound no longer exists. The default management class does not contain an archive copy group. - The archive copy group is deleted from the management class to which a file is bound. The default management class does not contain an archive copy group.

More details about domain configuration details are here

Below copygroup is defined for directory container storage pool (Spectrum Protect server local storage) Spectrum Protect server sample copygroup defined with domain for backup is configured with VEREXISTS=NOLimit VERDEL=NOLimit RETEXTRA=30 RETONLY=30

Below copygroup is defined for cloud container storage pool (Object storage) Spectrum Protect server sample copygroup defined with domain for backup is configured with VEREXISTS=NOLimit VERDEL=NOLimit RETEXTRA=365 RETONLY=365

Domain and copygroup created for each Spectrum Protect client machine have same settings.

VERExists :

Specifies the maximum number of backup versions to retain for files that are currently on the client file system. This parameter is optional. The default value is 2.

VEREXISTS=NOLimit Specifies that you want the server to retain all backup versions. The number of backup versions to retain is controlled by this parameter until versions exceed the retention time specified by the RETEXTRA parameter.

VERDeleted :

Specifies the maximum number of backup versions to retain for files that have been deleted from the client file system after being backed up using IBM Spectrum Protect. This parameter is optional. The default value is 1. If a user deletes a file from the client file system, the next incremental backup causes the server to expire the oldest versions of the file in excess of this number. The expiration date for the remaining versions is determined by the retention time specified by the RETEXTRA or RETONLY parameter.

VERDEL=NOLimit Specifies that you want the server to retain all backup versions for files that are deleted from the client file system after being backed up.

RETExtra :

Specifies the number of days to retain a backup version after that version becomes inactive. A version of a file becomes inactive when the client stores a more recent backup version, or when the client deletes the file from the workstation and then runs a full incremental backup. The server deletes inactive versions based on retention time even if the number of inactive versions does not exceed the number allowed by the VEREXISTS or VERDELETED parameters. This parameter is optional. The default value is 30 days.

RETOnly :

Specifies the number of days to retain the last backup version of a file that has been deleted from the client file system. This parameter is optional. The default value is 60.

You can change sample retention policy values according to your requirement, keeping Spectrum Protect server storage space in mind.

More details about copygroup configuration details are here

Configuring Object storage

You can store deduplicated data and non-deduplicated data in a cloud-container storage pool and restore the data as required. You can configure IBM Spectrum Protect to temporarily store data in one or more local storage pool directories during data ingestion. The data is then moved from local storage to the cloud. In this way, you can improve data backup and archive performance.

After you define a storage pool directory, the IBM Spectrum Protect server uses that directory as a temporary landing spot for the data that you are transferring to cloud object storage. The server uses an automated background process to transfer data from local storage in the directory to cloud object storage. You do not need to take any additional steps to start or manage this transfer process. After the server successfully moves the data from local storage to cloud object storage, the server deletes the data from the directory and releases space for more incoming data.

If storage pool directories contain no more free space, backup operations stop prematurely. To avoid this situation, you can allocate more storage pool directories. You can also wait for the data to be automatically removed from the local directories after the data moves to the cloud.

Spectrum Protect server supports these cloud service providers.

- Amazon S3
- IBM Cloud Object Storage
- IBM SoftLayer
- OpenStack Swift

Amazon S3 API object storage has been used for the sample domains, policies, and schedules. Object store is configured with dummy credentials and URL. Once the user has created an object storage with S3 API of their own, they can input the appropriate values for credentials and URLs and other necessities required to configure an object storage to Spectrum Protect server.

Bucket

A bucket is a logical unit of storage in object storage service, Simple Storage Solution S3. Buckets are used to store objects, which consist of data and metadata that describes the data.

A bucket is analogous to a subdirectory, where the object storage in the main directory and the buckets in the object storage can be seen as subdirectories. In the sample policy provided, each Spectrum Protect client has its own bucket, ie. its own subdirectory in the object storage. Bucket names and unique IDs (called "keys" in S3) are used to access data from object storage in Spectrum Protect.

Use Operation center in updating the details of Object store details or use "Command Center" in Operation center to update values.

In the sample policy provided, data retention policy for Object store is set to 365 days, which means data stored in Object store is available for 365 days. These are specified in the backretention and archretention parameters of a domain, as mentioned in the - Retention Policy section.

Each machine contains two cloud pools, one used for backup and another for archive, where dummy credentials are provided.

Use private URL instead of public URL, if it's private URL data transfer between Spectrum Protect server and Object store is very fast compared to the usage of public URL.

More details about SoftLayer Object store is here

More details about cloud object storage details are here

More details about configuring cloud-container storage pools for IBM SoftLayer is here

More details about encrypting data for cloud-container storage pools is here

Limitations and best practices

Spectrum Protect server setup and client installations are provided only with MDM on Cloud Premium and High Availability services. If you have also subscribed to following test & development offerings then you need to develop your own backup artifacts for these offerings. - Non-Production - Additional Virtual MDM Runtime - Additional MDM Developer - Additional BPM Developer

Spectrum Protect server installation which is provided with MDM on Cloud Premium and High Availability offerings can only be used for taking backups of applications and files which are part of MDM on Cloud deployment.

MDM on Cloud setup consists of many applications and components. When you configure different policies & schedules to take backup of different applications and components, backups are created at different timestamps. Hence after restoration of specific application backup, its data may not be in complete sync with related data elements in other applications or components.

Spectrum Protect server and Operation Center are installed in same system, so communication between Spectrum Protect server and Operation Center is through non-SSL. Spectrum Protect server has 2 instances which are connected through node replication. Both the instances are in same system, so communication between these 2 instances is through non-SSL.

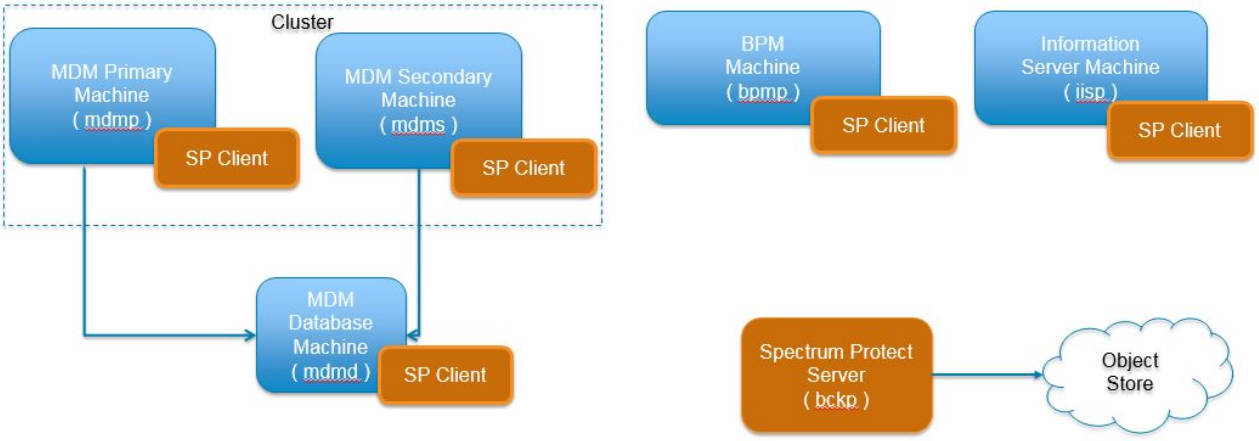
Cloud storage is connected to the 2nd instance of Spectrum Protect server, which acts as a fail-over server. There are some limitations in connecting to cloud storage from Spectrum Protect client. You can’t connect to Cloud storage and retrieve data when 1st instance of Spectrum Protect server is up and running. If the 1st instance of Spectrum Protect server is down, then you can connect to 2nd instance of Spectrum Protect server. You'll have only read only access, which means it’s used only to retrieve data, you can’t take backup and archive using this.

You should follow product or application specific documentation and best practices while developing artifacts to take backups, below are some examples. - IBM Information Server does not support hot backups. For details, check Backing up IBM InfoSphere Information Server components. - WebSphere Application Server documentation suggests that servers are stopped while taking backup of node configurations. For details, check backupConfig command

IMPORTANT

- Spectrum Protect server’s database backup files are not backed-up automatically. These files are mandatorily required to restore a SPectrum Protect Server in case of a failure scenario. Hence, it is recommended that the user backs the artifacts related to this to a secure location. Details about Spectrum Protect server database backup is available at "Spectrum Protect server database backup" section. - Spectrum Protect server database backup
- Spectrum Protect server master encryption key is stored in the server password file, dsmserv.pwd. This file takes care of encryption and decryption of data being transferred for backup and restore. Hence, it is recommended that the user backs the artifacts related to this to a secure location. Details about master key is available at "Protecting the master encryption key" section. - Protecting the master encryption key

IBM Spectrum Protect setup for MDM on Cloud Premium service



MDM on Cloud Premium service deployment consists of six machines. IBM Spectrum Protect Server is installed in one machine and Spectrum Protect Client is installed in rest of the machines.

By default, all the sample schedules are disabled by setting expiration value to -1. In order to use sample schedule, you need to enable them by setting an appropriate expiry date.

Backup files will be available only for 30 days, later they are removed from Spectrum Protect server directory storage pool. If cloud container is configured backup files will be available for 365 days, later they are removed from Spectrum Protect server cloud storage pool. You can change these settings according to your requirement, more details on modifying these settings are available in - Retention Policy section. Make sure storage in Spectrum Protect server is limited.

MDM Primary machine

To take backups of the artifacts which exists on MDM primary machine, a sample policy domain configuration named as MDMP-DOMAIN is created on Spectrum Protect Server.

Sample schedules are available to take backup of WAS profile, WAS profile configuration and other files which are located in MDM primary machine. These schedules when enabled notifies Spectrum Protect Client to execute specific scripts. Sample scripts which are available at Spectrum Protect Client machine execute commands to create backup archive files, copy files to the specific location and invoke Spectrum Protect commands to copy files to Spectrum Protect Server machine.

Configurations for taking backups of application server, deployment manager and proxy profiles

A sample schedule named as MDMP-WAS-WEEKLY is configured to take backups of WAS profiles. This schedule invokes WASProfileBackup_MDM.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Primary Machine. Before enabling MDMP-WAS-WEEKLY schedule, you must update WASProfileBackup_MDM.sh and provide value for PASSWORD field.

MDMP-WAS-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

WASProfileBackup_MDM.sh executes manageprofiles.sh utility provided by WAS to create profile backups named MDMP_AppServer_backup.zip, MDMP_Dmgr_backup.zip, MDMP_proxy_backup.zip which contains profile backups.

- WAS Dmgr01 profile folder : /home/mdmcloud/IBM/WebSphere/AppServer/profiles/Dmgr01
- WAS AppSrv01 profile folder : /home/mdmcloud/IBM/WebSphere/AppServer/profiles/AppSrv01
- WAS Proxy profile folder : /home/mdmcloud/IBM/WebSphere/AppServer/profiles/proxy

MDMP_Dmgr_backup.zip : Contains backup of Dmgr01 profile created using manageprofiles.sh utility where profile is located at /home/mdmcloud/IBM/WebSphere/AppServer/profiles/Dmgr01

MDMP_AppServer_backup.zip : Contains backup of AppSrv01 profile created using manageprofiles.sh utility where profile is located at /home/mdmcloud/IBM/WebSphere/AppServer/profiles/AppSrv01

MDMP_proxy_backup.zip : Contains backup of proxy profile created using manageprofiles.sh utility where profile is located at /home/mdmcloud/IBM/WebSphere/AppServer/profiles/proxy

Generated files are stored in /home/mdmcloud/WAS_Backup folder. WASProfileBackup_MDM.sh executes Spectrum Protect server selective backup command to take backup of MDMP_AppServer_backup.zip, MDMP_Dmgr_backup.zip, MDMP_proxy_backup.zip files.

IMPORTANT

WAS guidelines for backup of WAS profile mandates that the WAS services be stopped before the profile is being backed up. This schedule forces to stop servers related to that WAS profile.

As this schedule stop server related to WAS profile, it's up to you to take a decision on whether to run this schedule on weekly basis or run this when it's needed. It is recommended to take backup of profiles when there are changes to WAS like adding a new CBA or deleting a CBA etc..

If you want to run this schedule manually whenever it's needed instead of running weekly, a shell script named WASProfileBackup_MDM.sh is available at /opt/tivoli/tsm/client/ba/bin folder. Execute this script as a root user, it'll stop the profile and related servers, take the backup of profile and generated zip files are send to Spectrum Protect Server. If you are running this script manually make sure you run the similar script in MDM secondary box also as MDM is deployed in WAS cluster.

More information on the backup of WAS profiles is mentioned in the following links.

https://www.ibm.com/support/knowledgecenter/en/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/rxml_manageprofiles.html

Sample template used for taking backup of WAS profile :

```
su - mdmcloud -c "/home/mdmcloud/IBM/WebSphere/AppServer/profiles/<PROFILE_NAME>/bin/
stopServer.sh <SERVER_NAME> -username <WAS_USERNAME> -password <PASSWORD>"
su - mdmcloud -c "/home/mdmcloud/IBM/WebSphere/AppServer/profiles/<PROFILE_NAME>/bin/
stopNode.sh -username <WAS_USERNAME> -password <PASSWORD>"
su - mdmcloud -c "/home/mdmcloud/IBM/WebSphere/AppServer/bin/manageprofiles.sh -backupProfile -
profileName <PROFILE_NAME> -backupFile /home/mdmcloud/WAS_Backup/MDMP_AppServer_backup.zip -
username <WAS_USERNAME> -password <PASSWORD>"

su - mdmcloud -c "/home/mdmcloud/IBM/WebSphere/AppServer/profiles/<PROFILE_NAME>/bin/
startNode.sh"
su - mdmcloud -c "/home/mdmcloud/IBM/WebSphere/AppServer/profiles/<PROFILE_NAME>/bin/
startServer.sh <SERVER_NAME>"

dsmc sel "/home/mdmcloud/WAS_Backup/* " -subdir=yes
```

The server and nodeagent are stopped first, then the manageprofiles.sh command is used to take backup of the WAS profile and then the nodeagent, the server is started again. *dsmc* command is used to transfer the backup files from MDM Primary machine to the Spectrum Protect Server. In the case of Dmgr (deployment manager) profile, it'll stop deployment manager and start it back. There are no servers or node agents attached to it.

In order to enable MDMP-WAS-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

If you want to run this schedule weekly, execute below command.

```
update schedule MDMP-DOMAIN MDMP-WAS-WEEKLY expiration=never
```

Above command enable MDMP-WAS-WEEKLY schedule without the expiry date. After enabling MDMP-WAS-WEEKLY schedule, start 'dsmcad' service from MDM primary machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM primary machine and run `service dsmcad restart` using root user.

After running the MDMP-WAS-WEEKLY schedule or running WASProfileBackup_MDM.sh manually, make sure MDMP_AppServer_backup.zip, MDMP_Dmgr_backup.zip, MDMP_proxy_backup.zip files are created at /home/mdmcloud/WAS_Backup folder. If you didn't find these files, there might be an issue while running WASProfileBackup_MDM.sh which is available at /opt/tivoli/tsm/client/ba/bin folder. Run this script manually and fix the issues.

Configurations for taking backups of application server, deployment manager and proxy profile configuration

A sample schedule named as MDMP-WAS-DAILY is configured to take backups of WAS profile configuration. This schedule invokes WASProfileConfigBackup_MDM.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Primary Machine. Before enabling MDMP-WAS-DAILY schedule, you must update WASProfileConfigBackup_MDM.sh and provide value for PASSWORD field.

MDMP-WAS-DAILY schedule is configured to execute daily at midnight.

WASProfileConfigBackup_MDM.sh executes commands to create an archive files named MDMP_DmgrConfig.zip, MDMP_AppSrvConfig.zip, MDMP_proxyConfig.zip which contains all profile configurations.

- WAS Dmgr01 profile configuration folder : /home/mdmcloud/IBM/WebSphere/AppServer/profiles/Dmgr01
- WAS AppSrv01 profile configuration folder : /home/mdmcloud/IBM/WebSphere/AppServer/profiles/AppSrv01
- WAS Proxy profile configuration folder : /home/mdmcloud/IBM/WebSphere/AppServer/profiles/proxy

MDMP_DmgrConfig.zip : Contains Dmgr01 profile configuration which is generated by using backupConfig command MDMP_AppSrvConfig.zip : Contains AppSrv01 profile configuration which is generated by using backupConfig command MDMP_proxyConfig.zip : Contains proxy profile configuration which is generated by using backupConfig command

Archive files are stored in /home/mdmcloud/WAS_ConfigBackup folder.
WASProfileConfigBackup_MDM.sh executes Spectrum Protect server selective backup command to take backup of MDMP_DmgrConfig.zip, MDMP_AppSrvConfig.zip, MDMP_proxyConfig.zip files.

In order to enable MDMP-WAS-DAILY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule MDMP-DOMAIN MDMP-WAS-DAILY expiration=never
```

Above command enable MDMP-WAS-DAILY schedule without the expiry date.

After enabling MDMP-WAS-DAILY schedule, start 'dsmcad' service from MDM primary machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM primary machine and run `service dsmcad restart` using root user.

Configurations for taking backups of files and folders

A sample schedule named as MDMP-FILES-WEEKLY is configured to take backups of files and folders. This schedule invokes mdmp_FilesWeekly.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Primary Machine.

MDMP-WAS-DAILY schedule is configured to execute weekly once, on Sundays at midnight.

mdmp_FilesWeekly.sh executes commands to take backup of below files and folders.

- /home/mdmcloud/DBCert.p12
- /home/mdmcloud/IBM/MDM/MDM115/properties/*
- /etc/sysconfig/iptables
- /keystore/*

mdmp_FilesWeekly.sh executes Spectrum Protect server selective backup command to take backup of files and folders as mentioned above.

In order to enable MDMP-FILES-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule MDMP-DOMAIN MDMP-FILES-WEEKLY expiration=never
```

Above command enable MDMP-FILES-WEEKLY schedule without the expiry date.

After enabling MDMP-FILES-WEEKLY schedule, start 'dsmcad' service from MDM primary machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM primary machine and run `service dsmcad restart` using root user.

You can modify existing files, folders or add new files, folders for backup by updating script /opt/tivoli/tsm/client/ba/bin/mdmp_FilesWeekly.sh available in MDM primary machine.

Object store configuration

Out of the box Object store in Spectrum protect server is configured with dummy credentials and URL. You need to update the details of Object store credentials, in cloud storage pools.

Bucket name used for MDM primary machine is mdmp.

Use Operation center in updating the details of Object store details.

Two cloud container storage pools are configured while replicating MDM primary machine data from instance 1 of Spectrum Protect server to instance 2 of Spectrum Protect server. Out of the box, these storage pools are configured with dummy credentials and URL. One used to store backup data and another used to store archive data.

Use private URL instead of public URL, if it's private URL data transfer between Spectrum Protect server and Object store is very fast compared to the usage of public URL.

Run below commands from "Command Builder" of Spectrum protect operation center. As these are cloud container pools client needs to run from the second instance of Spectrum Protect server. In "Command Builder" select second instance which has name like <ORDER_ID>_/s/m/l_bckp1. Select drop down menu from left downside corner, as shown in the image.

Details about Command Builder is available at - Starting Command Builder

```
update stgpool mdmp-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool mdmp-cloud-pool identity=<USERNAME>
update stgpool mdmp-cloud-pool password=<PASSWORD>

update stgpool mdmp-arc-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool mdmp-arc-cloud-pool identity=<USERNAME>
update stgpool mdmp-arc-cloud-pool password=<PASSWORD>
```

MDM Secondary machine

To take backups of the artifacts which exists on MDM secondary machine, a sample policy domain configuration named as MDMS-DOMAIN is created on Spectrum Protect Server.

Sample schedules are available to take backup of WAS profile, WAS profile configuration and other files which are located in MDM secondary machine. These schedules when enabled notifies Spectrum Protect Client to execute specific scripts. Sample scripts which are available at Spectrum Protect Client machine execute commands to create backup archive files, copy files to a specific location and invoke Spectrum Protect commands to copy files to Spectrum Protect Server machine.

Configurations for taking backups of custom server and proxy profiles

A sample schedule named as MDMS-WAS-WEEKLY is configured to take backups of WAS profiles. This schedule invokes WASProfileBackup_MDM.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Secondary Machine.Before enabling MDMS-WAS-WEEKLY schedule, you must update WASProfileBackup_MDM.sh and provide value for PASSWORD field.

MDMS-WAS-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

WASProfileBackup_MDM.sh executes manageprofiles.sh utility provided by WAS to create profile backups named MDMS_Custom_backup.zip, MDMS_proxy_backup.zip which contains profile backups.

- WAS Custom01 profile folder : /home/mdmcloud/IBM/WebSphere/AppServer/profiles/Custom01
- WAS Proxy profile folder : /home/mdmcloud/IBM/WebSphere/AppServer/profiles/proxy

MDMS_Custom_backup.zip : Contains backup of Custom01 profile created using manageprofiles.sh utility where profile is located at /home/mdmcloud/IBM/WebSphere/AppServer/profiles/Custom01
MDMS_proxy_backup.zip : Contains backup of proxy profile created using manageprofiles.sh utility where profile is located at /home/mdmcloud/IBM/WebSphere/AppServer/profiles/proxy

Generated files are stored in /home/mdmcloud/WAS_Backup folder. WASProfileBackup_MDM.sh executes Spectrum Protect server selective backup command to take backup of MDMS_Custom_backup.zip, MDMS_proxy_backup.zip files.

IMPORTANT

WAS guidelines for backup of WAS profile mandates that the WAS services be stopped before the profile is being backed up. This schedule forces to stop servers related to that WAS profile.

As this schedule stop server related to WAS profile, it's up to you to take a decision on whether to run this schedule on weekly basis or run this when it's needed. It is recommended to take backup of profiles when there are changes to WAS like adding a new CBA or deleting a CBA etc..

If you want to run this schedule manually whenever it's needed instead of running weekly, a shell script named WASProfileBackup_MDM.sh is available at /opt/tivoli/tsm/client/ba/bin folder. Execute this script as a root user, it'll stop the profile and related servers, take the backup of profile and generated zip files are send to Spectrum Protect Server. If you are running this script manually make sure you run similar script in MDM primary box also as MDM is deployed in WAS cluster.

More information on the backup of WAS profiles is mentioned in the following links.

https://www.ibm.com/support/knowledgecenter/en/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/rxml_manageprofiles.html

Sample template used for taking backup of WAS profile :

```
su - mdmcloud -c "/home/mdmcloud/IBM/WebSphere/AppServer/profiles/<PROFILE_NAME>/bin/
stopServer.sh <SERVER_NAME> -username <WAS_USERNAME> -password <PASSWORD>"
su - mdmcloud -c "/home/mdmcloud/IBM/WebSphere/AppServer/profiles/<PROFILE_NAME>/bin/
stopNode.sh -username <WAS_USERNAME> -password <PASSWORD>"
su - mdmcloud -c "/home/mdmcloud/IBM/WebSphere/AppServer/bin/manageprofiles.sh -backupProfile -
profileName <PROFILE_NAME> -backupFile /home/mdmcloud/WAS_Backup/MDMP_AppServer_backup.zip -
username <WAS_USERNAME> -password <PASSWORD>"

su - mdmcloud -c "/home/mdmcloud/IBM/WebSphere/AppServer/profiles/<PROFILE_NAME>/bin/
startNode.sh"
su - mdmcloud -c "/home/mdmcloud/IBM/WebSphere/AppServer/profiles/<PROFILE_NAME>/bin/
startServer.sh <SERVER_NAME>"

dsmc sel "/home/mdmcloud/WAS_Backup/* " -subdir=yes
```

The server and nodeagent are stopped first, then the manageprofiles.sh command is used to take backup of the WAS profile and then the nodeagent, the server is started again. *dsmc* command is used to transfer the backup files from MDM Secondary machine to the Spectrum Protect Server.

In order to enable MDMS-WAS-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule MDMS-DOMAIN MDMS-WAS-WEEKLY expiration=never
```

Above command enable MDMS-WAS-WEEKLY schedule without the expiry date. After enabling MDMS-WAS-WEEKLY schedule, start 'dsmcad' service from MDM secondary machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM secondary machine and run `service dsmcad restart` using root user.

After running the MDMS-WAS-WEEKLY schedule or running WASProfileBackup_MDM.sh manually, make sure MDMS_Custom_backup.zip, MDMS_proxy_backup.zip files are created at /home/mdmcloud/WAS_Backup folder. If you didn't find these files, there might be an issue while running WASProfileBackup_MDM.sh which is available at /opt/tivoli/tsm/client/ba/bin folder. Run this script manually and fix the issues.

Configurations for taking backups of custom server and proxy profile configuration

A sample schedule named as MDMS-WAS-DAILY is configured to take backups of WAS profile configuration. This schedule invokes WASProfileConfigBackup_MDM.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Secondary Machine. Before enabling MDMS-WAS-DAILY schedule, you must update WASProfileConfigBackup_MDM.sh and provide value for PASSWORD field.

MDMS-WAS-DAILY schedule is configured to execute daily at midnight.

WASProfileConfigBackup_MDM.sh executes commands to create an archive files named MDMS_CustomConfig.zip, MDMS_proxyConfig.zip which contains all profile configurations.

- WAS Custom01 profile configuration folder : /home/mdmcloud/IBM/WebSphere/AppServer/profiles/Custom01
- WAS Proxy profile configuration folder : /home/mdmcloud/IBM/WebSphere/AppServer/profiles/proxy

MDMS_CustomConfig.zip : Contains Custom01 profile configuration which is generated by using backupConfig command MDMS_proxyConfig.zip : Contains proxy profile configuration which is generated by using backupConfig command

Archive files are stored in /home/mdmcloud/WAS_ConfigBackup folder. WASProfileConfigBackup_MDM.sh executes Spectrum Protect server selective backup command to take backup of MDMS_CustomConfig.zip, MDMS_proxyConfig.zip files.

In order to enable MDMS-WAS-DAILY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule MDMS-DOMAIN MDMS-WAS-DAILY expiration=never
```

Above command enable MDMS-WAS-DAILY schedule without the expiry date.

After enabling MDMS-WAS-DAILY schedule, start 'dsmcad' service from MDM secondary machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM secondary machine and run `service dsmcad restart` using root user.

Configurations for taking backups of files and folders

A sample schedule named as MDMS-FILES-WEEKLY is configured to take backups of files and folders. This schedule invokes mdms_FilesWeekly.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Secondary Machine.

MDMS-FILES-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

mdms_FilesWeekly.sh executes commands to take backup of below files and folders.

- /home/mdmcloud/DBCert.p12
- /home/mdmcloud/IBM/MDM/MDM115/properties/*
- /etc/sysconfig/iptables
- /keystore/*

mdms_FilesWeekly.sh executes Spectrum Protect server selective backup command to take backup of files and folders as mentioned above.

In order to enable MDMS-FILES-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule MDMS-DOMAIN MDMS-FILES-WEEKLY expiration=never
```

Above command enable MDMS-FILES-WEEKLY schedule without the expiry date.

After enabling MDMS-FILES-WEEKLY schedule, start 'dsmcad' service from MDM secondary machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM secondary machine and run `service dsmcad restart` using root user.

You can modify existing files, folders or add new files, folders for backup by updating script /opt/tivoli/tsm/client/ba/bin/mdms_FilesWeekly.sh available in MDM secondary machine.

Object store configuration

Out of the box Object store in Spectrum protect server is configured with dummy credentials and URL. You need to update the details of Object store credentials, in cloud storage pools.

Bucket name used for MDM secondary machine is mdms.

Use Operation center in updating the details of Object store details.

Two cloud container storage pools are configured while replicating MDM secondary machine data from instance 1 of Spectrum Protect server to instance 2 of Spectrum Protect server. Out of the box, these storage pools are configured with dummy credentials and URL. One used to store backup data and another used to store archive data.

Use private URL instead of public URL, if it's private URL data transfer between Spectrum Protect server and Object store is very fast compared to the usage of public URL.

Run below commands from "Command Builder" of Spectrum protect operation center. As these are cloud container pools client needs to run from the second instance of Spectrum Protect server. In "Command Builder" select second instance which has name like <ORDER_ID>_/s/m/l_bckp1. Select drop down menu from left downside corner, as shown in the image.

Details about Command Builder is available at - Starting Command Builder

```
update stgpool mdms-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool mdms-cloud-pool identity=<USERNAME>
update stgpool mdms-cloud-pool password=<PASSWORD>

update stgpool mdms-arc-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool mdms-arc-cloud-pool identity=<USERNAME>
update stgpool mdms-arc-cloud-pool password=<PASSWORD>
```

MDM database machine

To take backups of the artifacts which exists on MDM database machine, a sample policy domain configuration named as MDM-DB-DOMAIN is created on Spectrum Protect Server.

Sample schedules are available to take backup of database full, database incremental online backups and other files which are located in MDM database machine. These schedules when enabled notifies Spectrum Protect Client to execute specific scripts. Sample scripts which are available at Spectrum Protect Client machine execute commands to take db2 full and incremental backups and invoke Spectrum Protect commands to copy files to Spectrum Protect Server machine.

Database configuration changes

The database is configured with linear logging, which means all the transaction (archive) logs of the database are stored on the MDM database machine. It is recommended that these logs should be stored in the Spectrum Protect server itself. In the case of a failover scenario, the logs are safe and secure in the Spectrum Protect server.

As transaction (archive) logs of the database are stored on the MDM database machine, it's your responsibility to clean up unused logs, as these logs are not cleared by default. Once you move transaction (archive) logs from local disk to Spectrum Protect server, it's the responsibility of Spectrum Protect server to clean unused logs. Use below commands in moving transaction (archive) logs from local disk to Spectrum Protect server:

Open Putty or terminal, switch to the db2inst1 user.

```
db2 update database configuration for mdmdb using LOGARCHMETH1 TSM:MDMDBMGMTCLASS
db2 stop db manager force
db2 start db manager
```

There are two kinds of database backups: full and incremental. It is required that a full backup of the database exists before any incremental backup is taken. Hence before the sample schedules are started,

you have to make sure that one full backup of the respective database is available. Verify available backups for a database by using `db2adutl query db <DATABASE_NAME>`. Open Putty or terminal, switch to the db2inst1 user to run this command. You have to execute the shell script db2FullBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Database Machine, incase there are no full backups available.

Before running db2FullBackup.sh decide, where to store database archive logs, whether in local disk or Spectrum protect server.

Configurations for taking online full database backups

A sample schedule named as MDM-DB-FULL-WEEKLY is configured to take backups of the online full database. This schedule invokes db2FullBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Database Machine.

MDM-DB-FULL-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

In order to enable MDM-DB-FULL-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule MDM-DB-DOMAIN MDM-DB-FULL-WEEKLY expiration=never
```

Above command enable MDM-DB-FULL-WEEKLY schedule without the expiry date. After enabling MDM-DB-FULL-WEEKLY schedule, start 'dsmcad' service from MDM database machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM database machine and run `service dsmcad restart` using root user.

Configurations for taking online incremental database backups

A sample schedule named as MDM-DB-INCREMENT-DAILY is configured to take online incremental database backups. This schedule invokes db2IncrementalBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Database Machine.

MDM-DB-INCREMENT-DAILY schedule is configured to execute from Monday to Saturday at midnights, except Sunday.

In order to enable MDM-DB-INCREMENT-DAILY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule MDM-DB-DOMAIN MDM-DB-INCREMENT-DAILY expiration=never
```

Above command enable MDM-DB-INCREMENT-DAILY schedule without the expiry date. After enabling MDM-DB-INCREMENT-DAILY schedule, start 'dsmcad' service from MDM database machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM database machine and run `service dsmcad restart` using root user.

Configurations for taking backups of files and folders

A sample schedule named as MDM-DB-FILES-WEEKLY is configured to take backups of files and folders. This schedule invokes mdmd_FilesWeekly.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Database Machine.

MDM-DB-FILES-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

mdmd_FilesWeekly.sh executes commands to take backup of below files and folders.

- /etc/sysconfig/iptables
- /keystore/*
- /keys/*

mdmd_FilesWeekly.sh executes Spectrum Protect server selective backup command to take backup of files and folders as mentioned above.

In order to enable MDM-DB-FILES-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule MDM-DB-DOMAIN MDM-DB-FILES-WEEKLY expiration=never
```

Above command enable MDM-DB-FILES-WEEKLY schedule without the expiry date.

After enabling MDM-DB-FILES-WEEKLY schedule, start 'dsmcad' service from MDM database machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM database machine and run `service dsmcad restart` using root user.

You can modify existing files, folders or add new files, folders for backup by updating script /opt/tivoli/tsm/client/ba/bin/mdmd_FilesWeekly.sh available in MDM database machine.

Object store configuration

Out of the box Object store in Spectrum protect server is configured with dummy credentials and URL. You need to update the details of Object store credentials, in cloud storage pools.

Bucket name used for MDM database machine is mdmd.

Use Operation center in updating the details of Object store details.

Two cloud container storage pools are configured while replicating MDM database machine data from instance 1 of Spectrum Protect server to instance 2 of Spectrum Protect server. Out of the box, these storage pools are configured with dummy credentials and URL. One used to store backup data and another used to store archive data.

Use private URL instead of public URL, if it's private URL data transfer between Spectrum Protect server and Object store is very fast compared to the usage of public URL.

Run below commands from "Command Builder" of Spectrum protect operation center. As these are cloud container pools client needs to run from the second instance of Spectrum Protect server. In "Command Builder" select second instance which has name like <ORDER_ID>_/s/m/l_bckp1. Select drop down menu from left downside corner, as shown in the image.

Details about Command Builder is available at - Starting Command Builder

```
update stgpool mdmdb-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool mdmdb-cloud-pool identity=<USERNAME>
update stgpool mdmdb-cloud-pool password=<PASSWORD>

update stgpool mdmdb-arc-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool mdmdb-arc-cloud-pool identity=<USERNAME>
update stgpool mdmdb-arc-cloud-pool password=<PASSWORD>
```

BPM machine

To take backups of the artifacts which exists on BPM machine, a sample policy domain configuration named as BPM-DOMAIN is created on Spectrum Protect Server.

Sample schedules are available to take backup of WAS profile directory, WAS profile configuration, database full, database incremental online backups and other files which are located in BPM machine. These schedules when enabled notifies Spectrum Protect Client to execute specific scripts. Sample scripts which are available at Spectrum Protect Client machine execute commands to create backup archive files, db2 full, db2 incremental backups and invoke Spectrum Protect commands to copy files to Spectrum Protect Server machine.

Database configuration changes

The database is configured with linear logging, which means all the transaction (archive) logs of the database are stored on the BPM machine. It is recommended that these logs should be stored in the Spectrum Protect server itself. In the case of a failover scenario, the logs are safe and secure in the Spectrum Protect server.

As transaction (archive) logs of the database are stored on the BPM machine, it's your responsibility to clean up unused logs, as these logs are not cleared by default. Once you move transaction (archive) logs from local disk to Spectrum Protect server, it's the responsibility of Spectrum Protect server to clean unused logs. Use below commands in moving transaction (archive) logs from local disk to Spectrum Protect server:

Open Putty or terminal, switch to the db2inst1 user.

```
db2 update database configuration for bpmdb using LOGARCHMETH1 TSM:BPMMGMTCLASS
db2 update database configuration for cmndb using LOGARCHMETH1 TSM:BPMMGMTCLASS
db2 update database configuration for pdwdb using LOGARCHMETH1 TSM:BPMMGMTCLASS
db2 stop db manager force
db2 start db manager
```

There are two kinds of database backups: full and incremental. It is required that a full backup of the database exists before any incremental backup is taken. Hence before the sample schedules are started, you have to make sure that one full backup of the respective database is available. Verify available backups for a database by using `db2adutl query db <DATABASE_NAME>`. Open Putty or terminal, switch to the db2inst1 user to run this command. You have to execute the shell script db2FullBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside BPM Machine, incase there are no full backups available.

Before running db2FullBackup.sh decide, where to store database archive logs, whether in local disk or Spectrum protect server.

Configurations for taking online full database backups

A sample schedule named as BPM-DB-FULL-WEEKLY is configured to take backups of online full database. This schedule invokes db2FullBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside BPM Machine.

BPM-DB-FULL-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight. db2FullBackup.sh executes commands to take online full backups for BPMDB, CMNDB and PDWDB databases.

In order to enable BPM-DB-FULL-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule BPM-DOMAIN BPM-DB-FULL-WEEKLY expiration=never
```

Above command enable BPM-DB-FULL-WEEKLY schedule without the expiry date. After enabling BPM-DB-FULL-WEEKLY schedule, start 'dsmcad' service from BPM machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in BPM machine and run `service dsmcad restart` using root user.

Configurations for taking online incremental database backups

A sample schedule named as BPM-DB-INCREMENT-DAILY is configured to take online incremental database backups. This schedule invokes db2IncrementalBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside BPM Machine.

BPM-DB-INCREMENT-DAILY schedule is configured to execute from Monday to Saturday at midnights, except Sunday. db2IncrementalBackup.sh executes commands to take online incremental backups for BPMDB, CMNDB and PDWDB databases.

In order to enable BPM-DB-INCREMENT-DAILY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule BPM-DOMAIN BPM-DB-INCREMENT-DAILY expiration=never
```

Above command enable BPM-DB-INCREMENT-DAILY schedule without the expiry date. After enabling BPM-DB-INCREMENT-DAILY schedule, start 'dsmcad' service from BPM machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in BPM machine and run `service dsmcad restart` using root user.

Configurations for taking backups of WAS and BPM configurations

Following actions are taken to take backup of BPM & WAS configurations 1. BPM configurations are backed up using bpmConfig command 2. WAS profile configurations are backed up using wasConfig command.

A sample scheduler named as BPM-WAS-DAILY is configured to take backups of BPM & WAS configurations. This scheduler invokes WASProfileConfigBackup_BPM.sh which is available at /opt/tivoli/tsm/client/ba/bin folder. Before enabling BPM-WAS-DAILY schedule, you must update WASProfileConfigBackup_BPM.sh and provide value for PASSWORD field.

BPM-WAS-DAILY schedule is configured to execute daily at midnight.

WASProfileConfigBackup_BPM.sh executes WAS backupconfig.sh command to create following archive files BPMP_DmgrConfig.zip : This file contains configurations of DmgrProfile profile BPMP_NodeConfig.zip : This file contains configurations of Node1Profile profile.

WASProfileConfigBackup_BPM.sh also executes /bpm/bin/BPMConfig.sh command which exports BPM configurations. Outcome of BPMConfig.sh command is stored in /bpm/WAS_ConfigBackup folder.

BPM-WAS-DAILY schedule is configured to take profile configuration backups using WAS utility backupconfig.sh and export BPM configuration using BPMConfig.sh export option.

In order to enable BPM-WAS-DAILY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule BPM-DOMAIN BPM-WAS-DAILY expiration=never
```

Above command enable BPM-WAS-DAILY schedule without the expiry date.

After enabling BPM-WAS-DAILY schedule, start 'dsmcad' service from BPM machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in BPM machine and run `service dsmcad restart` using root user.

Configurations for taking backups of application server and deployment manager profile folder

A sample schedule named as BPM-WAS-WEEKLY is configured to take backups of WAS profile directories. This schedule invokes WASProfileBackup_BPM.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside BPM Machine.

BPM-WAS-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

WASProfileBackup_BPM.sh executes Spectrum Protect server selective backup command to create following archive files inside /bpm/WAS_Backup folder.

BPMP_Dmgr_backup.tar : This file contains content of DmgrProfile profile directory which is located at /bpm/profiles/DmgrProfile. BPMP_Node1_backup.tar : This file contains content of Node1Profile profile directory which is located at /bpm/profiles/Node1Profile.

IMPORTANT As mentioned in IBM BPM documentation backupProfile option provided by manageprofile.sh is not available for BPM WAS profiles.

More information about BPM WAS profiles backup is available in following link https://www.ibm.com/support/knowledgecenter/SSFTDH_8.5.6/com.ibm.wbpm.ref.doc/topics/rins_manageprofiles.html

In order to enable BPM-WAS-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule BPM-DOMAIN BPM-WAS-WEEKLY expiration=never
```

Above command enable BPM-WAS-WEEKLY schedule without the expiry date. After enabling BPM-WAS-WEEKLY schedule, start 'dsmcad' service from BPM machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in BPM machine and run `service dsmcad restart` using root user.

Configurations for taking backups of files and folders

A sample schedule named as BPM-FILES-WEEKLY is configured to take backups of files and folders. This schedule invokes bpmp_FilesWeekly.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside BPM Machine.

BPM-FILES-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

bpmp_FilesWeekly.sh executes commands to take backup of below files and folders.

- /etc/sysconfig/iptables
- /keystore/*

bpmp_FilesWeekly.sh executes Spectrum Protect server selective backup command to take backup of files and folders as mentioned above.

In order to enable BPM-FILES-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule BPM-DOMAIN BPM-FILES-WEEKLY expiration=never
```

Above command enable BPM-FILES-WEEKLY schedule without the expiry date.

After enabling BPM-FILES-WEEKLY schedule, start 'dsmcad' service from BPM machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in BPM machine and run `service dsmcad restart` using root user.

You can modify existing files, folders or add new files, folders for backup by updating script /opt/tivoli/tsm/client/ba/bin/bpmp_FilesWeekly.sh available in BPM machine.

Object store configuration

Out of the box Object store in Spectrum protect server is configured with dummy credentials and URL. You need to update the details of Object store credentials, in cloud storage pools.

Bucket name used for BPM machine is bpmp.

Use Operation center in updating the details of Object store details.

Two cloud container storage pools are configured while replicating BPM machine data from instance 1 of Spectrum Protect server to instance 2 of Spectrum Protect server. Out of the box, these storage pools are configured with dummy credentials and URL. One used to store backup data and another used to store archive data.

Use private URL instead of public URL, if it’s private URL data transfer between Spectrum Protect server and Object store is very fast compared to the usage of public URL.

Run below commands from "Command Builder" of Spectrum protect operation center. As these are cloud container pools client needs to run from the second instance of Spectrum Protect server. In "Command Builder" select second instance which has name like <ORDER_ID>_/s/m/l_bckp1. Select drop down menu from left downside corner, as shown in the image.

Details about Command Builder is available at - Starting Command Builder

```
update stgpool bpm-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool bpm-cloud-pool identity=<USERNAME>
update stgpool bpm-cloud-pool password=<PASSWORD>

update stgpool bpm-arc-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool bpm-arc-cloud-pool identity=<USERNAME>
update stgpool bpm-arc-cloud-pool password=<PASSWORD>
```

IIS machine

To take backups of the artifacts which exists on IIS machine, a sample policy domain configuration named as IIS-DOMAIN is created on Spectrum Protect Server.

Sample schedules are available to take backup of WAS profile, WAS profile configuration, database full, database incremental online backups and other files which are located in IIS machine. These schedules

when enabled notifies Spectrum Protect Client to execute specific scripts. Sample scripts which are available at Spectrum Protect Client machine execute commands to create backup archive files, db2 full, db2 incremental backups and invoke Spectrum Protect commands to copy files to Spectrum Protect Server machine.

Database configuration changes

The database is configured with linear logging, which means all the transaction (archive) logs of the database are stored on the IIS machine. It is recommended that these logs should be stored in the Spectrum Protect server itself. In the case of a failover scenario, the logs are safe and secure in the Spectrum Protect server.

As transaction (archive) logs of the database are stored on the IIS machine, it's your responsibility to clean up unused logs, as these logs are not cleared by default. Once you move transaction (archive) logs from local disk to Spectrum Protect server, it's the responsibility of Spectrum Protect server to clean unused logs. Use below commands in moving transaction (archive) logs from local disk to Spectrum Protect server:

Open Putty or terminal, switch to the db2inst1 user.

```
db2 update database configuration for xmeta using LOGARCHMETH1 TSM:IISMGMTCLASS
db2 update database configuration for iadb using LOGARCHMETH1 TSM:IISMGMTCLASS
db2 update database configuration for ESDBDB2 using LOGARCHMETH1 TSM:IISMGMTCLASS
db2 update database configuration for DSODB using LOGARCHMETH1 TSM:IISMGMTCLASS
db2 stop db manager force
db2 start db manager
```

There are two kinds of database backups: full and incremental. It is required that a full backup of the database exists before any incremental backup is taken. Hence before the sample schedules are started, you have to make sure that one full backup of the respective database is available. Verify available backups for a database by using `db2adutl query db <DATABASE_NAME>`. Open Putty or terminal, switch to the db2inst1 user to run this command. You have to execute the shell script db2FullBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside IIS Machine, incase there are no full backups available.

Before running db2FullBackup.sh decide, where to store database archive logs, whether in local disk or Spectrum protect server.

Configurations for taking online full database backups

A sample schedule named as IIS-DB-FULL-WEEKLY is configured to take backups of online full database. This schedule invokes db2FullBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside IIS Machine.

IIS-DB-FULL-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight. db2FullBackup.sh executes commands to take online full backups for XMETA, IADB, ESDBDB2 and DSODB databases.

In order to enable IIS-DB-FULL-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule IIS-DOMAIN IIS-DB-FULL-WEEKLY expiration=never
```

Above command enable IIS-DB-FULL-WEEKLY schedule without the expiry date. After enabling IIS-DB-FULL-WEEKLY schedule, start 'dsmcad' service from IIS machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in IIS machine and run `service dsmcad restart` using root user.

Configurations for taking online incremental database backups

A sample schedule named as IIS-DB-INCREMENT-DAILY is configured to take online incremental database backups. This schedule invokes db2IncrementalBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside IIS Machine.

IIS-DB-INCREMENT-DAILY schedule is configured to execute from Monday to Saturday at midnights, except Sunday. db2IncrementalBackup.sh executes commands to take online incremental backups for XMETA, IADB, ESDBDB2 and DSODB databases.

In order to enable IIS-DB-INCREMENT-DAILY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule IIS-DOMAIN IIS-DB-INCREMENT-DAILY expiration=never
```

Above command enable IIS-DB-INCREMENT-DAILY schedule without the expiry date. After enabling IIS-DB-INCREMENT-DAILY schedule, start 'dsmcad' service from IIS machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in IIS machine and run `service dsmcad restart` using root user.

Configurations for taking backups of WAS InfoSphere profiles

A sample schedule named as IIS-WAS-WEEKLY is configured to take backups of WAS profiles. This schedule invokes WASProfileBackup_IIS.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside IIS Machine. Before enabling IIS-WAS-WEEKLY schedule, you must update WASProfileBackup_IIS.sh and provide value for PASSWORD field.

IIS-WAS-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

WASProfileBackup_IIS.sh executes manageprofiles.sh utility provided by WAS to create profile backups named IIS_AppServer_backup.zip which contains profile backups.

- WAS InfoSphere profile folder : /opt/IBM/WebSphere/AppServer/profiles/InfoSphere

IIS_AppServer_backup.zip : Contains backup of InfoSphere profile created using manageprofiles.sh utility where profile is located at /opt/IBM/WebSphere/AppServer/profiles/InfoSphere

Generated files are stored in /opt/WAS_Backup folder. WASProfileBackup_IIS.sh executes Spectrum Protect server selective backup command to take backup of IIS_AppServer_backup.zip file.

IMPORTANT

WAS guidelines for backup of WAS profile mandates that the WAS services be stopped before the profile is being backed up. This schedule forces to stop servers related to that WAS profile.

As this schedule stop server related to WAS profile, it's up to you to take a decision on whether to run this schedule on weekly basis or run this when it's needed. It is recommended to take backup of profiles when there are changes to WAS like deploying an application or deleting an application etc..

If you want to run this schedule manually whenever it's needed instead of running weekly, a shell script named WASProfileBackup_IIS.sh is available at /opt/tivoli/tsm/client/ba/bin folder. Execute this script as a root user, it'll stop the profile and related servers, take the backup of profile and generated zip files are send to Spectrum Protect Server.

More information on the backup of WAS profiles is mentioned in the following links.

https://www.ibm.com/support/knowledgecenter/en/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/rxml_manageprofiles.html

Sample template used for taking backup of WAS profile :

```
/opt/IBM/WebSphere/AppServer/profiles/<PROFILE_NAME>/bin/stopServer.sh <SERVER_NAME> -username
wasadmin -password PASSWORD
/opt/IBM/WebSphere/AppServer/bin/manageprofiles.sh -backupProfile -profileName <PROFILE_NAME> -
backupFile /opt/WAS_Backup/IIS_AppServer_backup.zip

/opt/IBM/WebSphere/AppServer/profiles/<PROFILE_NAME>/bin/startServer.sh <SERVER_NAME>

dsmc sel "/opt/WAS_Backup/*" -subdir=yes
```

The server is stopped first, then the manageprofiles.sh command is used to take backup of the WAS profile and then the server is started again. *dsmc* command is used to transfer the backup files from IIS machine to the Spectrum Protect Server.

In order to enable IIS-WAS-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule IIS-DOMAIN IIS-WAS-WEEKLY expiration=never
```

Above command enable IIS-WAS-WEEKLY schedule without the expiry date. After enabling IIS-WAS-WEEKLY schedule, start 'dsmcad' service from IIS machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in IIS machine and run `service dsmcad restart` using root user.

After running the IIS-WAS-WEEKLY schedule or running WASProfileBackup_IIS.sh manually, make sure IIS_AppServer_backup.zip is created at /opt/WAS_Backup folder. If you didn't find these files, there might be an issue while running WASProfileBackup_IIS.sh which is available at /opt/tivoli/tsm/client/ba/bin folder. Run this script manually and fix the issues.

Configurations for taking backups of WAS InfoSphere profile configuration

A sample schedule named as IIS-WAS-DAILY is configured to take backups of WAS profile configuration. This schedule invokes WASProfileConfigBackup_IIS.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside IIS Machine. Before enabling IIS-WAS-DAILY schedule, you must update WASProfileConfigBackup_IIS.sh and provide value for PASSWORD field.

IIS-WAS-DAILY schedule is configured to execute daily at midnight.

WASProfileConfigBackup_IIS.sh executes commands to create an archive files named IIS_AppServerConfig.zip which contains all profile configurations.

- WAS Infosphere profile configuration folder : /opt/IBM/WebSphere/AppServer/profiles/InfoSphere

IIS_AppServerConfig.zip : Contains InfoSphere profile configuration which is generated by using backupConfig command

Archive file is stored in /opt/WAS_ConfigBackup folder. WASProfileConfigBackup_IIS.sh executes Spectrum Protect server selective backup command to take backup of IIS_AppServerConfig.zip file.

In order to enable IIS-WAS-DAILY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule IIS-DOMAIN IIS-WAS-DAILY expiration=never
```

Above command enable IIS-WAS-DAILY schedule without the expiry date.

After enabling IIS-WAS-DAILY schedule, start 'dsmcad' service from IIS machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in IIS machine and run `service dsmcad restart` using root user.

Configurations for taking backups of ISTool

A sample schedule named as IIS-ISTOOL-WEEKLY is configured to take backups of ISTool export configuration. This schedule invokes istool_assets.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside IIS Machine. Before enabling IIS-ISTOOL-WEEKLY schedule, you must update istool_assets.sh and provide value for PASSWORD field.

IIS-ISTOOL-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

istool_assets.sh executes commands to create an archive file which contains all ISTool export configurations.

- IIS istool.sh export backup : Using istool.sh export all configuration

Archive file generated by istool.sh is stored in /opt/ISTool folder. istool_assets.sh executes Spectrum Protect server selective backup command to take backup of istool generated file.

In order to enable IIS-ISTOOL-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule IIS-DOMAIN IIS-ISTOOL-WEEKLY expiration=never
```

Above command enable IIS-ISTOOL-WEEKLY schedule without the expiry date.

After enabling IIS-ISTOOL-WEEKLY schedule, start 'dsmcad' service from IIS machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in IIS machine and run `service dsmcad restart` using root user.

Configurations for taking backups of files and folders

A sample schedule named as IIS-FILES-WEEKLY is configured to take backups of files and folders. This schedule invokes iisp_FilesWeekly.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside IIS Machine.

IIS-FILES-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

iisp_FilesWeekly.sh executes commands to take backup of below files and folders.

- /opt/IBM/InformationServer/Server/Configurations/*
- /opt/IBM/InformationServer/Updates/*
- /opt/IBM/InformationServer/Server/DSODB/*.cfg
- /opt/IBM/InformationServer/Server/DSEngine/dsenv
- /etc/services
- /etc/inittab
- /opt/IBM/InformationServer/ASBServer/apps/lib/iis/15properties/*
- /opt/IBM/InformationServer/ASBServer/apps/lib/iis/classes/*

iisp_FilesWeekly.sh executes Spectrum Protect server selective backup command to take backup of files and folders as mentioned above.

In order to enable IIS-FILES-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule IIS-DOMAIN IIS-FILES-WEEKLY expiration=never
```

Above command enable IIS-FILES-WEEKLY schedule without the expiry date.

After enabling IIS-FILES-WEEKLY schedule, start 'dsmcad' service from IIS machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in IIS machine and run `service dsmcad restart` using root user.

You can modify existing files, folders or add new files, folders for backup by updating script /opt/tivoli/tsm/client/ba/bin/iisp_FilesWeekly.sh available in IIS machine.

Configurations for taking backups of files and folders

A sample schedule named as IIS-FILES-WEEKLY2 is configured to take backups of files and folders. This schedule invokes iisp_FilesWeekly2.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside IIS Machine.

IIS-FILES-WEEKLY2 schedule is configured to execute weekly once, on Sundays at midnight.

iisp_FilesWeekly2.sh executes commands to take backup of below files and folders.

- /keys/*
- /keystore/*
- /etc/sysconfig/iptables
- /opt/IBM/InformationServer/Server/MsgHandlers/*

iisp_FilesWeekly2.sh executes Spectrum Protect server selective backup command to take backup of files and folders as mentioned above.

In order to enable IIS-FILES-WEEKLY2 schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule IIS-DOMAIN IIS-FILES-WEEKLY2 expiration=never
```

Above command enable IIS-FILES-WEEKLY2 schedule without the expiry date.

After enabling IIS-FILES-WEEKLY2 schedule, start 'dsmcad' service from IIS machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in IIS machine and run `service dsmcad restart` using root user.

You can modify existing files, folders or add new files, folders for backup by updating script /opt/tivoli/tsm/client/ba/bin/iisp_FilesWeekly2.sh available in IIS machine.

Configurations for taking backups of files and folders

A sample schedule named as IIS-FILES-DAILY is configured to take backups of files and folders. This schedule invokes iisp_FilesDaily.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside IIS Machine.

IIS-FILES-DAILY schedule is configured to execute daily at midnight.

iisp_FilesDaily.sh executes commands to take backup of below files and folders.

- /opt/IBM/InformationServer/Version.xml
- /opt/IBM/InformationServer/Server/Projects/*

iisp_FilesDaily.sh executes Spectrum Protect server selective backup command to take backup of files and folders as mentioned above.

In order to enable IIS-FILES-DAILY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule IIS-DOMAIN IIS-FILES-DAILY expiration=never
```

Above command enable IIS-FILES-DAILY schedule without the expiry date.

After enabling IIS-FILES-DAILY schedule, start 'dsmcad' service from IIS machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in IIS machine and run `service dsmcad restart` using root user.

You can modify existing files, folders or add new files, folders for backup by updating script /opt/tivoli/tsm/client/ba/bin/iisp_FilesDaily.sh available in IIS machine.

Object store configuration

Out of the box Object store in Spectrum protect server is configured with dummy credentials and URL. You need to update the details of Object store credentials, in cloud storage pools.

Bucket name used for IIS machine is iisp.

Use Operation center in updating the details of Object store details.

Two cloud container storage pools are configured while replicating IIS machine data from instance 1 of Spectrum Protect server to instance 2 of Spectrum Protect server. Out of the box, these storage pools are configured with dummy credentials and URL. One used to store backup data and another used to store archive data.

Use private URL instead of public URL, if it’s private URL data transfer between Spectrum Protect server and Object store is very fast compared to the usage of public URL.

Run below commands from "Command Builder" of Spectrum protect operation center. As these are cloud container pools client needs to run from the second instance of Spectrum Protect server. In "Command

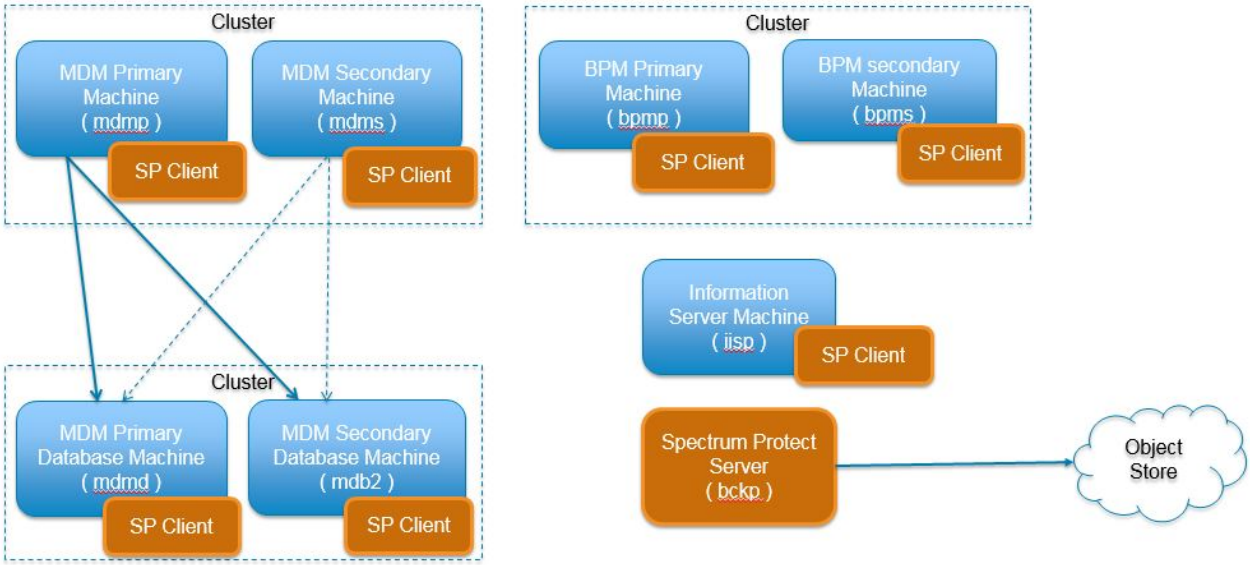
Builder" select second instance which has name like <ORDER_ID>_/s/m/l_bckp1. Select drop down menu from left downside corner, as shown in the image.

Details about Command Builder is available at - Starting Command Builder

```
update stgpool iis-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool iis-cloud-pool identity=<USERNAME>
update stgpool iis-cloud-pool password=<PASSWORD>

update stgpool iis-arc-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool iis-arc-cloud-pool identity=<USERNAME>
update stgpool iis-arc-cloud-pool password=<PASSWORD>
```

IBM Spectrum Protect setup for MDM on Cloud High Availability service



MDM on Cloud Premium service deployment consists of eight machines. IBM Spectrum Protect server is installed in one machine and IBM Spectrum Protect Client is installed in rest of the machines.

Backup files will be available only for 30 days, later they are removed from Spectrum Protect server directory storage pool. If cloud container is configured backup files will be available for 365 days, later they are removed from Spectrum Protect server cloud storage pool. You can change these settings according to your requirement, more details on modifying these settings are available in - Retention Policy section. Make sure storage in Spectrum Protect server is limited.

MDM Primary machine

To take backups of the artifacts which exists on MDM primary machine, a sample policy domain configuration named as MDMP-DOMAIN is created on Spectrum Protect Server.

Sample schedules are available to take backup of WAS profile, WAS profile configuration and other files which are located in MDM primary machine. These schedules when enabled notifies Spectrum Protect Client to execute specific scripts. Sample scripts which are available at Spectrum Protect Client machine execute commands to create backup archive files, copy files to a specific location and invoke Spectrum Protect commands to copy files to Spectrum Protect Server machine.

Configurations for taking backups of application server, deployment manager and proxy profiles

A sample schedule named as MDMP-WAS-WEEKLY is configured to take backups of WAS profiles. This schedule invokes WASProfileBackup_MDM.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Primary Machine. Before enabling MDMP-WAS-WEEKLY schedule, you must update WASProfileBackup_MDM.sh and provide value for PASSWORD field.

MDMP-WAS-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

WASProfileBackup_MDM.sh executes manageprofiles.sh utility provided by WAS to create profile backups named MDMP_AppServer_backup.zip, MDMP_Dmgr_backup.zip, MDMP_proxy_backup.zip which contains profile backups.

- WAS Dmgr01 profile folder : /home/mdmcloud/IBM/WebSphere/AppServer/profiles/Dmgr01
- WAS AppSrv01 profile folder : /home/mdmcloud/IBM/WebSphere/AppServer/profiles/AppSrv01
- WAS Proxy profile folder : /home/mdmcloud/IBM/WebSphere/AppServer/profiles/proxy

MDMP_Dmgr_backup.zip : Contains backup of Dmgr01 profile created using manageprofiles.sh utility where profile is located at /home/mdmcloud/IBM/WebSphere/AppServer/profiles/Dmgr01
MDMP_AppServer_backup.zip : Contains backup of AppSrv01 profile created using manageprofiles.sh utility where profile is located at /home/mdmcloud/IBM/WebSphere/AppServer/profiles/AppSrv01
MDMP_proxy_backup.zip : Contains backup of proxy profile created using manageprofiles.sh utility where profile is located at /home/mdmcloud/IBM/WebSphere/AppServer/profiles/proxy

Generated files are stored in /home/mdmcloud/WAS_Backup folder. WASProfileBackup_MDM.sh executes Spectrum Protect server selective backup command to take backup of MDMP_AppServer_backup.zip, MDMP_Dmgr_backup.zip, MDMP_proxy_backup.zip files.

IMPORTANT

WAS guidelines for backup of WAS profile mandates that the WAS services be stopped before the profile is being backed up. This schedule forces to stop servers related to that WAS profile.

As this schedule stop server related to WAS profile, it's up to you to take a decision on whether to run this schedule on weekly basis or run this when it's needed. It is recommended to take backup of profiles when there are changes to WAS like adding a new CBA or deleting a CBA etc..

If you want to run this schedule manually whenever it's needed instead of running weekly, a shell script named WASProfileBackup_MDM.sh is available at /opt/tivoli/tsm/client/ba/bin folder. Execute this script as a root user, it'll stop the profile and related servers, take the backup of profile and generated zip files are send to Spectrum Protect Server. If you are running this script manually make sure you run similar script in MDM secondary box also as MDM is deployed in WAS cluster.

More information on the backup of WAS profiles is mentioned in the following links.

https://www.ibm.com/support/knowledgecenter/en/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/rxml_manageprofiles.html

Sample template used for taking backup of WAS profile :

```
su - mdmcloud -c "/home/mdmcloud/IBM/WebSphere/AppServer/profiles/<PROFILE_NAME>/bin/
stopServer.sh <SERVER_NAME> -username <WAS_USERNAME> -password <PASSWORD>"
su - mdmcloud -c "/home/mdmcloud/IBM/WebSphere/AppServer/profiles/<PROFILE_NAME>/bin/
stopNode.sh -username <WAS_USERNAME> -password <PASSWORD>"
su - mdmcloud -c "/home/mdmcloud/IBM/WebSphere/AppServer/bin/manageprofiles.sh -backupProfile -
profileName <PROFILE_NAME> -backupFile /home/mdmcloud/WAS_Backup/MDMP_AppServer_backup.zip -
username <WAS_USERNAME> -password <PASSWORD>"

su - mdmcloud -c "/home/mdmcloud/IBM/WebSphere/AppServer/profiles/<PROFILE_NAME>/bin/
startNode.sh"
su - mdmcloud -c "/home/mdmcloud/IBM/WebSphere/AppServer/profiles/<PROFILE_NAME>/bin/
startServer.sh <SERVER_NAME>"

dsmc sel "/home/mdmcloud/WAS_Backup/* " -subdir=yes
```

The server and nodeagent are stopped first, then the manageprofiles.sh command is used to take backup of the WAS profile and then the nodeagent, the server is started again. *dsmc* command is used to transfer the backup files from MDM Primary machine to the Spectrum Protect Server. In the case of Dmgr (deployment manager) profile, it'll stop deployment manager and start it back. There are no servers or node agents attached to it.

In order to enable MDMP-WAS-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule MDMP-DOMAIN MDMP-WAS-WEEKLY expiration=never
```

Above command enable MDMP-WAS-WEEKLY schedule without the expiry date. After enabling MDMP-WAS-WEEKLY schedule, start 'dsmcad' service from MDM primary machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM primary machine and run `service dsmcad restart` using root user.

After running the MDMP-WAS-WEEKLY schedule or running WASProfileBackup_MDM.sh manually, make sure MDMP_AppServer_backup.zip, MDMP_Dmgr_backup.zip, MDMP_proxy_backup.zip files are created at /home/mdmcloud/WAS_Backup folder. If you didn't find these files, there might be an issue while running WASProfileBackup_MDM.sh which is available at /opt/tivoli/tsm/client/ba/bin folder. Run this script manually and fix the issues.

Configurations for taking backups of application server, deployment manager and proxy profile configuration

A sample schedule named as MDMP-WAS-DAILY is configured to take backups of WAS profile configuration. This schedule invokes WASProfileConfigBackup_MDM.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Primary Machine. Before enabling MDMP-WAS-DAILY schedule, you must update WASProfileConfigBackup_MDM.sh and provide value for PASSWORD field.

MDMP-WAS-DAILY schedule is configured to execute daily at midnight.

WASProfileConfigBackup_MDM.sh executes commands to create an archive files named MDMP_DmgrConfig.zip, MDMP_AppSrvConfig.zip, MDMP_proxyConfig.zip which contains all profile configurations.

- WAS Dmgr01 profile configuration folder : /home/mdmcloud/IBM/WebSphere/AppServer/profiles/Dmgr01
- WAS AppSrv01 profile configuration folder : /home/mdmcloud/IBM/WebSphere/AppServer/profiles/AppSrv01
- WAS Proxy profile configuration folder : /home/mdmcloud/IBM/WebSphere/AppServer/profiles/proxy

MDMP_DmgrConfig.zip : Contains Dmgr01 profile configuration which is generated by using backupConfig command MDMP_AppSrvConfig.zip : Contains AppSrv01 profile configuration which is generated by using backupConfig command MDMP_proxyConfig.zip : Contains proxy profile configuration which is generated by using backupConfig command

Archive files are stored in /home/mdmcloud/WAS_ConfigBackup folder.
WASProfileConfigBackup_MDM.sh executes Spectrum Protect server selective backup command to take backup of MDMP_DmgrConfig.zip, MDMP_AppSrvConfig.zip, MDMP_proxyConfig.zip files.

In order to enable MDMP-WAS-DAILY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule MDMP-DOMAIN MDMP-WAS-DAILY expiration=never
```

Above command enable MDMP-WAS-DAILY schedule without the expiry date.

After enabling MDMP-WAS-DAILY schedule, start 'dsmcad' service from MDM primary machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM primary machine and run `service dsmcad restart` using root user.

Configurations for taking backups of files and folders

A sample schedule named as MDMP-FILES-WEEKLY is configured to take backups of files and folders. This schedule invokes mdmp_FilesWeekly.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Primary Machine.

MDMP-WAS-DAILY schedule is configured to execute weekly once, on Sundays at midnight.

mdmp_FilesWeekly.sh executes commands to take backup of below files and folders.

- /home/mdmcloud/DBCert.p12
- /home/mdmcloud/IBM/MDM/MDM115/properties/*

- /etc/sysconfig/iptables
- /keystore/*

mdmp_FilesWeekly.sh executes Spectrum Protect server selective backup command to take backup of files and folders as mentioned above.

In order to enable MDMP-FILES-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule MDMP-DOMAIN MDMP-FILES-WEEKLY expiration=never
```

Above command enable MDMP-FILES-WEEKLY schedule without the expiry date.

After enabling MDMP-FILES-WEEKLY schedule, start 'dsmcad' service from MDM primary machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM primary machine and run `service dsmcad restart` using root user.

You can modify existing files, folders or add new files, folders for backup by updating script /opt/tivoli/tsm/client/ba/bin/mdmp_FilesWeekly.sh available in MDM primary machine.

Object store configuration

Out of the box Object store in Spectrum protect server is configured with dummy credentials and URL. You need to update the details of Object store credentials, in cloud storage pools.

Bucket name used for MDM primary machine is mdmp.

Use Operation center in updating the details of Object store details.

Two cloud container storage pools are configured while replicating MDM primary machine data from instance 1 of Spectrum Protect server to instance 2 of Spectrum Protect server. Out of the box, these storage pools are configured with dummy credentials and URL. One used to store backup data and another used to store archive data.

Use private URL instead of public URL, if it’s private URL data transfer between Spectrum Protect server and Object store is very fast compared to the usage of public URL.

Run below commands from "Command Builder" of Spectrum protect operation center. As these are cloud container pools client needs to run from the second instance of Spectrum Protect server. In "Command Builder" select second instance which has name like <ORDER_ID>_/s/m/l_bckp1. Select drop down menu from left downside corner, as shown in the image.

Details about Command Builder is available at - Starting Command Builder

```
update stgpool mdmp-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool mdmp-cloud-pool identity=<USERNAME>
update stgpool mdmp-cloud-pool password=<PASSWORD>

update stgpool mdmp-arc-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool mdmp-arc-cloud-pool identity=<USERNAME>
update stgpool mdmp-arc-cloud-pool password=<PASSWORD>
```

MDM Secondary machine

To take backups of the artifacts which exists on MDM secondary machine, a sample policy domain configuration named as MDMS-DOMAIN is created on Spectrum Protect Server.

Sample schedules are available to take backup of WAS profile, WAS profile configuration and other files which are located in MDM secondary machine. These schedules when enabled notifies Spectrum Protect Client to execute specific scripts. Sample scripts which are available at Spectrum Protect Client machine execute commands to create backup archive files, copy files to a specific location and invoke Spectrum Protect commands to copy files to Spectrum Protect Server machine.

Configurations for taking backups of custom server and proxy profiles

A sample schedule named as MDMS-WAS-WEEKLY is configured to take backups of WAS profiles. This schedule invokes WASProfileBackup_MDM.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Secondary Machine.Before enabling MDMS-WAS-WEEKLY schedule, you must update WASProfileBackup_MDM.sh and provide value for PASSWORD field.

MDMS-WAS-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

WASProfileBackup_MDM.sh executes manageprofiles.sh utility provided by WAS to create profile backups named MDMS_Custom_backup.zip, MDMS_proxy_backup.zip which contains profile backups.

- WAS Custom01 profile folder : /home/mdmcloud/IBM/WebSphere/AppServer/profiles/Custom01
- WAS Proxy profile folder : /home/mdmcloud/IBM/WebSphere/AppServer/profiles/proxy

MDMS_Custom_backup.zip : Contains backup of Custom01 profile created using manageprofiles.sh utility where profile is located at /home/mdmcloud/IBM/WebSphere/AppServer/profiles/Custom01
MDMS_proxy_backup.zip : Contains backup of proxy profile created using manageprofiles.sh utility where profile is located at /home/mdmcloud/IBM/WebSphere/AppServer/profiles/proxy

Generated files are stored in /home/mdmcloud/WAS_Backup folder. WASProfileBackup_MDM.sh executes Spectrum Protect server selective backup command to take backup of MDMS_Custom_backup.zip, MDMS_proxy_backup.zip files.

IMPORTANT

WAS guidelines for backup of WAS profile mandates that the WAS services be stopped before the profile is being backed up. This schedule forces to stop servers related to that WAS profile.

As this schedule stop server related to WAS profile, it's up to you to take a decision on whether to run this schedule on weekly basis or run this when it's needed. It is recommended to take backup of profiles when there are changes to WAS like adding a new CBA or deleting a CBA etc..

If you want to run this schedule manually whenever it's needed instead of running weekly, a shell script named WASProfileBackup_MDM.sh is available at /opt/tivoli/tsm/client/ba/bin folder. Execute this script as a root user, it'll stop the profile and related servers, take the backup of profile and generated zip files are send to Spectrum Protect Server. If you are running this script manually make sure you run similar script in MDM primary box also as MDM is deployed in WAS cluster.

More information on the backup of WAS profiles is mentioned in the following links.

https://www.ibm.com/support/knowledgecenter/en/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/rxml_manageprofiles.html

Sample template used for taking backup of WAS profile :

```
su - mdmcloud -c "/home/mdmcloud/IBM/WebSphere/AppServer/profiles/<PROFILE_NAME>/bin/
stopServer.sh <SERVER_NAME> -username <WAS_USERNAME> -password <PASSWORD>"
su - mdmcloud -c "/home/mdmcloud/IBM/WebSphere/AppServer/profiles/<PROFILE_NAME>/bin/
stopNode.sh -username <WAS_USERNAME> -password <PASSWORD>"
su - mdmcloud -c "/home/mdmcloud/IBM/WebSphere/AppServer/bin/manageprofiles.sh -backupProfile -
profileName <PROFILE_NAME> -backupFile /home/mdmcloud/WAS_Backup/MDMP_AppServer_backup.zip -
username <WAS_USERNAME> -password <PASSWORD>"

su - mdmcloud -c "/home/mdmcloud/IBM/WebSphere/AppServer/profiles/<PROFILE_NAME>/bin/
startNode.sh"
su - mdmcloud -c "/home/mdmcloud/IBM/WebSphere/AppServer/profiles/<PROFILE_NAME>/bin/
startServer.sh <SERVER_NAME>"

dsmc sel "/home/mdmcloud/WAS_Backup/* " -subdir=yes
```

The server and nodeagent are stopped first, then the manageprofiles.sh command is used to take backup of the WAS profile and then the nodeagent, the server is started again. *dsmc* command is used to transfer the backup files from MDM Secondary machine to the Spectrum Protect Server.

In order to enable MDMS-WAS-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule MDMS-DOMAIN MDMS-WAS-WEEKLY expiration=never
```

Above command enable MDMS-WAS-WEEKLY schedule without the expiry date. After enabling MDMS-WAS-WEEKLY schedule, start 'dsmcad' service from MDM secondary machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM secondary machine and run `service dsmcad restart` using root user.

After running the MDMS-WAS-WEEKLY schedule or running WASProfileBackup_MDM.sh manually, make sure MDMS_Custom_backup.zip, MDMS_proxy_backup.zip files are created at /home/mdmcloud/WAS_Backup folder. If you didn't find these files, there might be an issue while running WASProfileBackup_MDM.sh which is available at /opt/tivoli/tsm/client/ba/bin folder. Run this script manually and fix the issues.

Configurations for taking backups of custom server and proxy profile configuration

A sample schedule named as MDMS-WAS-DAILY is configured to take backups of WAS profile configuration. This schedule invokes WASProfileConfigBackup_MDM.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Secondary Machine. Before enabling MDMS-WAS-DAILY schedule, you must update WASProfileConfigBackup_MDM.sh and provide value for PASSWORD field.

MDMS-WAS-DAILY schedule is configured to execute daily at midnight.

WASProfileConfigBackup_MDM.sh executes commands to create an archive files named MDMS_CustomConfig.zip, MDMS_proxyConfig.zip which contains all profile configurations.

- WAS Custom01 profile configuration folder : /home/mdmcloud/IBM/WebSphere/AppServer/profiles/Custom01
- WAS Proxy profile configuration folder : /home/mdmcloud/IBM/WebSphere/AppServer/profiles/proxy

MDMS_CustomConfig.zip : Contains Custom01 profile configuration which is generated by using backupConfig command MDMS_proxyConfig.zip : Contains proxy profile configuration which is generated by using backupConfig command

Archive files are stored in /home/mdmcloud/WAS_ConfigBackup folder. WASProfileConfigBackup_MDM.sh executes Spectrum Protect server selective backup command to take backup of MDMS_CustomConfig.zip, MDMS_proxyConfig.zip files.

In order to enable MDMS-WAS-DAILY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule MDMS-DOMAIN MDMS-WAS-DAILY expiration=never
```

Above command enable MDMS-WAS-DAILY schedule without the expiry date.

After enabling MDMS-WAS-DAILY schedule, start 'dsmcad' service from MDM secondary machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM secondary machine and run `service dsmcad restart` using root user.

Configurations for taking backups of files and folders

A sample schedule named as MDMS-FILES-WEEKLY is configured to take backups of files and folders. This schedule invokes mdms_FilesWeekly.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Secondary Machine.

MDMS-FILES-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

mdms_FilesWeekly.sh executes commands to take backup of below files and folders.

- /home/mdmcloud/DBCert.p12
- /home/mdmcloud/IBM/MDM/MDM115/properties/*
- /etc/sysconfig/iptables
- /keystore/*

mdms_FilesWeekly.sh executes Spectrum Protect server selective backup command to take backup of files and folders as mentioned above.

In order to enable MDMS-FILES-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule MDMS-DOMAIN MDMS-FILES-WEEKLY expiration=never
```

Above command enable MDMS-FILES-WEEKLY schedule without the expiry date.

After enabling MDMS-FILES-WEEKLY schedule, start 'dsmcad' service from MDM secondary machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM secondary machine and run `service dsmcad restart` using root user.

You can modify existing files, folders or add new files, folders for backup by updating script /opt/tivoli/tsm/client/ba/bin/mdms_FilesWeekly.sh available in MDM secondary machine.

Object store configuration

Out of the box Object store in Spectrum protect server is configured with dummy credentials and URL. You need to update the details of Object store credentials, in cloud storage pools.

Bucket name used for MDM secondary machine is mdms.

Use Operation center in updating the details of Object store details.

Two cloud container storage pools are configured while replicating MDM secondary machine data from instance 1 of Spectrum Protect server to instance 2 of Spectrum Protect server. Out of the box, these storage pools are configured with dummy credentials and URL. One used to store backup data and another used to store archive data.

Use private URL instead of public URL, if it's private URL data transfer between Spectrum Protect server and Object store is very fast compared to the usage of public URL.

Run below commands from "Command Builder" of Spectrum protect operation center. As these are cloud container pools client needs to run from the second instance of Spectrum Protect server. In "Command Builder" select second instance which has name like <ORDER_ID>_/s/m/l_bckp1. Select drop down menu from left downside corner, as shown in the image.

Details about Command Builder is available at - Starting Command Builder

```
    update stgpool mdms-cloud-pool cloudurl=https://<PRIVATE_URL>
    update stgpool mdms-cloud-pool identity=<USERNAME>
    update stgpool mdms-cloud-pool password=<PASSWORD>

    update stgpool mdms-arc-cloud-pool cloudurl=https://<PRIVATE_URL>
    update stgpool mdms-arc-cloud-pool identity=<USERNAME>
    update stgpool mdms-arc-cloud-pool password=<PASSWORD>
```

MDM primary database machine

To take backups of the artifacts which exists on MDM primary database machine, a sample policy domain configuration named as MDM-DB-DOMAIN is created on Spectrum Protect Server.

Sample schedules are available to take backup of database full, database incremental online backups and other files which are located in MDM primary database machine. These schedules when enabled notifies Spectrum Protect Client to execute specific scripts. Sample scripts which are available at Spectrum Protect Client machine execute commands to take db2 full and incremental backups and invoke Spectrum Protect commands to copy files to Spectrum Protect Server machine.

Database configuration changes

The database is configured with linear logging, which means all the transaction (archive) logs of the database are stored on the MDM database machine. It is recommended that these logs should be stored

in the Spectrum Protect server itself. In the case of a failover scenario, the logs are safe and secure in the Spectrum Protect server.

As transaction (archive) logs of the database are stored on the MDM database machine, it's your responsibility to clean up unused logs, as these logs are not cleared by default. Once you move transaction (archive) logs from local disk to Spectrum Protect server, it's the responsibility of Spectrum Protect server to clean unused logs. Use below commands in moving transaction (archive) logs from local disk to Spectrum Protect server:

The database is configured with HADR scenario, verify HADR status before applying any database configuration changes.

Open Putty or terminal, switch to the db2inst1 user. Check database HADR status. `db2pd -db mdmdb -hadr` If it's proper then follow these steps.

```
db2 update database configuration for mdmdb using LOGARCHMETH1 TSM:MDMDBMGMTCLASS
db2 stop db manager force
db2 start db manager
```

Wait for few minutes and check HADR status. `db2pd -db mdmdb -hadr`

There are two kinds of database backups: full and incremental. It is required that a full backup of the database exists before any incremental backup is taken. Hence before the sample schedules are started, you have to make sure that one full backup of the respective database is available. Verify available backups for a database by using `db2adutl query db <DATABASE_NAME>`. Open Putty or terminal, switch to the db2inst1 user to run this command. You have to execute the shell script db2FullBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Database Machine, incase there are no full backups available.

Before running db2FullBackup.sh decide, where to store database archive logs, whether in local disk or Spectrum protect server.

Configurations for taking online full database backups

A sample schedule named as MDM-DB-FULL-WEEKLY is configured to take backups of the online full database. This schedule invokes db2FullBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Primary Database Machine.

MDM-DB-FULL-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

In order to enable MDM-DB-FULL-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule MDM-DB-DOMAIN MDM-DB-FULL-WEEKLY expiration=never
```

Above command enable MDM-DB-FULL-WEEKLY schedule without the expiry date. After enabling MDM-DB-FULL-WEEKLY schedule, start 'dsmcad' service from MDM primary database machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM primary database machine and run `service dsmcad restart` using root user.

Configurations for taking online incremental database backups

A sample schedule named as MDM-DB-INCREMENT-DAILY is configured to take online incremental database backups. This schedule invokes db2IncrementalBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Primary Database Machine.

MDM-DB-INCREMENT-DAILY schedule is configured to execute from Monday to Saturday at midnights, except Sunday.

In order to enable MDM-DB-INCREMENT-DAILY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule MDM-DB-DOMAIN MDM-DB-INCREMENT-DAILY expiration=never
```

Above command enable MDM-DB-INCREMENT-DAILY schedule without the expiry date. After enabling MDM-DB-INCREMENT-DAILY schedule, start 'dsmcad' service from MDM primary database machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM primary database machine and run `service dsmcad restart` using root user.

Configurations for taking backups of files and folders

A sample schedule named as MDM-DB-FILES-WEEKLY is configured to take backups of files and folders. This schedule invokes mdmd_FilesWeekly.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Primary Database Machine.

MDM-DB-FILES-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

mdmd_FilesWeekly.sh executes commands to take backup of below files and folders.

- /etc/sysconfig/iptables
- /keystore/*
- /keys/*

mdmd_FilesWeekly.sh executes Spectrum Protect server selective backup command to take backup of files and folders as mentioned above.

In order to enable MDM-DB-FILES-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule MDM-DB-DOMAIN MDM-DB-FILES-WEEKLY expiration=never
```

Above command enable MDM-DB-FILES-WEEKLY schedule without the expiry date.

After enabling MDM-DB-FILES-WEEKLY schedule, start 'dsmcad' service from MDM primary database machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM primary database machine and run `service dsmcad restart` using root user.

You can modify existing files, folders or add new files, folders for backup by updating script /opt/tivoli/tsm/client/ba/bin/mdmd_FilesWeekly.sh available in MDM database machine.

Object store configuration

Out of the box Object store in Spectrum protect server is configured with dummy credentials and URL. You need to update the details of Object store credentials, in cloud storage pools.

Bucket name used for MDM primary database machine is mdmd.

Use Operation center in updating the details of Object store details.

Two cloud container storage pools are configured while replicating MDM primary database machine data from instance 1 of Spectrum Protect server to instance 2 of Spectrum Protect server. Out of the box, these storage pools are configured with dummy credentials and URL. One used to store backup data and another used to store archive data.

Use private URL instead of public URL, if it’s private URL data transfer between Spectrum Protect server and Object store is very fast compared to the usage of public URL.

Run below commands from "Command Builder" of Spectrum protect operation center. As these are cloud container pools client needs to run from the second instance of Spectrum Protect server. In "Command Builder" select second instance which has name like <ORDER_ID>_/s/m/l_bckp1. Select drop down menu from left downside corner, as shown in the image.

Details about Command Builder is available at - Starting Command Builder

```
update stgpool mdmdb-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool mdmdb-cloud-pool identity=<USERNAME>
update stgpool mdmdb-cloud-pool password=<PASSWORD>

update stgpool mdmdb-arc-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool mdmdb-arc-cloud-pool identity=<USERNAME>
update stgpool mdmdb-arc-cloud-pool password=<PASSWORD>
```

MDM secondary database machine

To take backups of the artifacts which exists on MDM secondary database machine, a sample policy domain configuration named as MDM-DBS-DOMAIN is created on Spectrum Protect Server.

Sample schedules are available to take backup of database full, database incremental online backups and other files which are located in MDM secondary database machine. These schedules when enabled notifies Spectrum Protect Client to execute specific scripts. Sample scripts which are available at Spectrum Protect Client machine execute commands to take db2 full and incremental backups and invoke Spectrum Protect commands to copy files to Spectrum Protect Server machine.

Database configuration changes

IMPORTANT As this database acts as passive, don't run any database schedules or configuration changes at the starting. Start these database schedules or configuration changes only if this database takeover as a primary database.

The database is configured with linear logging, which means all the transaction (archive) logs of the database are stored on the MDM database machine. It is recommended that these logs should be stored in the Spectrum Protect server itself. In the case of a failover scenario, the logs are safe and secure in the Spectrum Protect server.

As transaction (archive) logs of the database are stored on the MDM database machine, it's your responsibility to clean up unused logs, as these logs are not cleared by default. Once you move transaction (archive) logs from local disk to Spectrum Protect server, it's the responsibility of Spectrum Protect server to clean unused logs. Use below commands in moving transaction (archive) logs from local disk to Spectrum Protect server:

The database is configured with HADR scenario, verify HADR status before applying any database configuration changes.

Open Putty or terminal, switch to the db2inst1 user. Check database HADR status. `db2pd -db mdmdb -hadr` If it's proper then follow these steps.

```
db2 update database configuration for mdmdb using LOGARCHMETH1 TSM:MDMDBMGMTCLASS
db2 stop db manager force
db2 start db manager
```

Wait for few minutes and check HADR status. `db2pd -db mdmdb -hadr`

There are two kinds of database backups: full and incremental. It is required that a full backup of the database exists before any incremental backup is taken. Hence before the sample schedules are started, you have to make sure that one full backup of the respective database is available. Verify available backups for a database by using `db2adutl query db <DATABASE_NAME>`. Open Putty or terminal, switch to the db2inst1 user to run this command. You have to execute the shell script db2FullBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Database Machine, incase there are no full backups available.

Before running db2FullBackup.sh decide, where to store database archive logs, whether in local disk or Spectrum protect server.

Configurations for taking online full database backups

A sample schedule named as MDM-DBS-FULL-WEEKLY is configured to take backups of online full database. This schedule invokes db2FullBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Secondary Database Machine.

MDM-DBS-FULL-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

IMPORTANT As this database acts as passive, don't run any database schedules provided for this machine. Start these database schedules only if this database takeover as a primary database.

In order to enable MDM-DBS-FULL-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule MDM-DBS-DOMAIN MDM-DBS-FULL-WEEKLY expiration=never
```

Above command enable MDM-DBS-FULL-WEEKLY schedule without the expiry date. After enabling MDM-DBS-FULL-WEEKLY schedule, start 'dsmcad' service from MDM secondary database machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM secondary database machine and run `service dsmcad restart` using root user.

Configurations for taking online incremental database backups

A sample schedule named as MDM-DBS-INCREMENT-DAILY is configured to take online incremental database backups. This schedule invokes db2IncrementalBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Secondary Database Machine.

MDM-DBS-INCREMENT-DAILY schedule is configured to execute from Monday to Saturday at midnights, except Sunday.

IMPORTANT As this database acts as passive, don't run any database schedules provided for this machine. Start these database schedules only if this database takeover as a primary database.

In order to enable MDM-DBS-INCREMENT-DAILY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule MDM-DBS-DOMAIN MDM-DBS-INCREMENT-DAILY expiration=never
```

Above command enable MDM-DBS-INCREMENT-DAILY schedule without the expiry date. After enabling MDM-DBS-INCREMENT-DAILY schedule, start 'dsmcad' service from MDM secondary database machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM secondary database machine and run `service dsmcad restart` using root user.

Configurations for taking backups of files and folders

A sample schedule named as MDM-DBS-FILES-WEEKLY is configured to take backups of files and folders. This schedule invokes mdmd_FilesWeekly.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside MDM Secondary Database Machine.

MDM-DBS-FILES-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

mdmd_FilesWeekly.sh executes commands to take backup of below files and folders.

- /etc/sysconfig/iptables
- /keystore/*
- /keys/*

mdmd_FilesWeekly.sh executes Spectrum Protect server selective backup command to take backup of files and folders as mentioned above.

In order to enable MDM-DBS-FILES-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule MDM-DBS-DOMAIN MDM-DBS-FILES-WEEKLY expiration=never
```

Above command enable MDM-DBS-FILES-WEEKLY schedule without the expiry date.

After enabling MDM-DBS-FILES-WEEKLY schedule, start 'dsmcad' service from MDM secondary database machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in MDM secondary database machine and run `service dsmcad restart` using root user.

You can modify existing files, folders or add new files, folders for backup by updating script /opt/tivoli/tsm/client/ba/bin/mdmd_FilesWeekly.sh available in MDM database machine.

Object store configuration

Out of the box Object store in Spectrum protect server is configured with dummy credentials and URL. You need to update the details of Object store credentials, in cloud storage pools.

Bucket name used for MDM secondary database machine is mdmds.

Use Operation center in updating the details of Object store details.

Two cloud container storage pools are configured while replicating MDM secondary database machine data from instance 1 of Spectrum Protect server to instance 2 of Spectrum Protect server. Out of the box, these storage pools are configured with dummy credentials and URL. One used to store backup data and another used to store archive data.

Use private URL instead of public URL, if it's private URL data transfer between Spectrum Protect server and Object store is very fast compared to the usage of public URL.

Run below commands from "Command Builder" of Spectrum protect operation center. As these are cloud container pools client needs to run from the second instance of Spectrum Protect server. In "Command Builder" select second instance which has name like <ORDER_ID>_/s/m/l_bckp1. Select drop down menu from left downside corner, as shown in the image.

Details about Command Builder is available at - Starting Command Builder

```
update stgpool mdmdbs-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool mdmdbs-cloud-pool identity=<USERNAME>
update stgpool mdmdbs-cloud-pool password=<PASSWORD>

update stgpool mdmdbs-arc-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool mdmdbs-arc-cloud-pool identity=<USERNAME>
update stgpool mdmdbs-arc-cloud-pool password=<PASSWORD>
```

BPM primary machine

To take backups of the artifacts which exists on BPM machine, a sample policy domain configuration named as BPM-DOMAIN is created on Spectrum Protect Server.

Sample schedules are available to take backup of WAS profile directory, WAS profile configuration, database full, database incremental online backups and other files which are located in BPM machine. These schedules when enabled notifies Spectrum Protect Client to execute specific scripts. Sample scripts which are available at Spectrum Protect Client machine execute commands to create backup archive files, db2 full, db2 incremental backups and invoke Spectrum Protect commands to copy files to Spectrum Protect Server machine.

Database configuration changes

The database is configured with linear logging, which means all the transaction (archive) logs of the database are stored on the BPM machine. It is recommended that these logs should be stored in the Spectrum Protect server itself. In the case of a failover scenario, the logs are safe and secure in the Spectrum Protect server.

As transaction (archive) logs of the database are stored on the BPM machine, it's your responsibility to clean up unused logs, as these logs are not cleared by default. Once you move transaction (archive) logs from local disk to Spectrum Protect server, it's the responsibility of Spectrum Protect server to clean unused logs. Use below commands in moving transaction (archive) logs from local disk to Spectrum Protect server:

The database is configured with HADR scenario, follow these steps.

Open Putty or terminal, switch to the db2inst1 user. Check database HADR status. `db2pd -db bpmdb -hadr` `db2pd -db cmndb -hadr` `db2pd -db pdwdb -hadr` If it's proper then follow these steps.

```
db2 update database configuration for bpmdb using LOGARCHMETH1 TSM:BPMMGMTCLASS
db2 update database configuration for cmndb using LOGARCHMETH1 TSM:BPMMGMTCLASS
db2 update database configuration for pdwdb using LOGARCHMETH1 TSM:BPMMGMTCLASS
db2 stop db manager force
db2 start db manager
```

Wait for few minutes and check HADR status. `db2pd -db bpmdb -hadr` `db2pd -db cmndb -hadr` `db2pd -db pdwdb -hadr`

There are two kinds of database backups: full and incremental. It is required that a full backup of the database exists before any incremental backup is taken. Hence before the sample schedules are started, you have to make sure that one full backup of the respective database is available. Verify available backups for a database by using `db2adutl query db <DATABASE_NAME>`. Open Putty or terminal, switch to the db2inst1 user to run this command. You have to execute the shell script db2FullBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside BPM Machine, incase there are no full backups available.

Before running db2FullBackup.sh decide, where to store database archive logs, whether in local disk or Spectrum protect server.

Configurations for taking online full database backups

A sample schedule named as BPM-DB-FULL-WEEKLY is configured to take backups of online full database. This schedule invokes db2FullBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside BPM Machine.

BPM-DB-FULL-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight. db2FullBackup.sh executes commands to take online full backups for BPMDB, CMNDB and PDWDB databases.

In order to enable BPM-DB-FULL-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule BPM-DOMAIN BPM-DB-FULL-WEEKLY expiration=never
```

Above command enable BPM-DB-FULL-WEEKLY schedule without the expiry date. After enabling BPM-DB-FULL-WEEKLY schedule, start 'dsmcad' service from BPM machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in BPM machine and run `service dsmcad restart` using root user.

Configurations for taking online incremental database backups

A sample schedule named as BPM-DB-INCREMENT-DAILY is configured to take online incremental database backups. This schedule invokes db2IncrementalBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside BPM Machine.

BPM-DB-INCREMENT-DAILY schedule is configured to execute from Monday to Saturday at midnights, except Sunday. db2IncrementalBackup.sh executes commands to take online incremental backups for BPMDB, CMNDB and PDWDB databases.

In order to enable BPM-DB-INCREMENT-DAILY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule BPM-DOMAIN BPM-DB-INCREMENT-DAILY expiration=never
```

Above command enable BPM-DB-INCREMENT-DAILY schedule without the expiry date. After enabling BPM-DB-INCREMENT-DAILY schedule, start 'dsmcad' service from BPM machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in BPM machine and run `service dsmcad restart` using root user.

Configurations for taking backups of WAS and BPM configurations

Following actions are taken to take backup of BPM & WAS configurations 1. BPM configurations are backed up using bpmConfig command 2. WAS profile configurations are backed up using wasConfig command.

A sample scheduler named as BPM-WAS-DAILY is configured to take backups of BPM & WAS configurations. This scheduler invokes WASProfileConfigBackup_BPM.sh which is available at /opt/tivoli/tsm/client/ba/bin folder. Before enabling BPM-WAS-DAILY schedule, you must update WASProfileConfigBackup_BPM.sh and provide value for PASSWORD field.

BPM-WAS-DAILY schedule is configured to execute daily at midnight.

WASProfileConfigBackup_BPM.sh executes WAS backupconfig.sh command to create following archive files BPMP_DmgrConfig.zip : This file contains configurations of DmgrProfile profile BPMP_NodeConfig.zip : This file contains configurations of Node1Profile profile.

WASProfileConfigBackup_BPM.sh also executes /bpm/bin/BPMConfig.sh command which exports BPM configurations. Outcome of BPMConfig.sh command is stored in /bpm/WAS_ConfigBackup folder.

BPM-WAS-DAILY schedule is configured to take profile configuration backups using WAS utility backupconfig.sh and export BPM configuration using BPMConfig.sh export option.

In order to enable BPM-WAS-DAILY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule BPM-DOMAIN BPM-WAS-DAILY expiration=never
```

Above command enable BPM-WAS-DAILY schedule without the expiry date.

After enabling BPM-WAS-DAILY schedule, start 'dsmcad' service from BPM machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in BPM machine and run `service dsmcad restart` using root user.

Configurations for taking backups of application server and deployment manager profiles folder

A sample scheduler named as BPM-WAS-WEEKLY is configured to take backups of WAS profile directories. This scheduler invokes WASProfileBackup_BPM.sh which is available at /opt/tivoli/tsm/client/ba/bin folder.

BPM-WAS-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

WASProfileBackup_BPM.sh executes Spectrum Protect server selective backup command to create following archive files inside /bpm/WAS_Backup folder.

BPMP_Dmgr_backup.tar : This file contains content of DmgrProfile profile directory which is located at /bpm/profiles/DmgrProfile. BPMP_Node1_backup.tar : This file contains content of Node1Profile profile directory which is located at /bpm/profiles/Node1Profile.

IMPORTANT As mentioned in IBM BPM documentation backupProfile option provided by manageprofile.sh is not available for BPM WAS profiles.

More information about BPM WAS profiles backup is available in following link https://www.ibm.com/support/knowledgecenter/SSFTDH_8.5.6/com.ibm.wbpm.ref.doc/topics/rins_manageprofiles.html

In order to enable BPM-WAS-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule BPM-DOMAIN BPM-WAS-WEEKLY expiration=never
```

Above command enable BPM-WAS-WEEKLY schedule without the expiry date. After enabling BPM-WAS-WEEKLY schedule, start 'dsmcad' service from BPM machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in BPM machine and run `service dsmcad restart` using root user.

Configurations for taking backups of files and folders

A sample schedule named as BPM-FILES-WEEKLY is configured to take backups of files and folders. This schedule invokes bpmp_FilesWeekly.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside BPM Machine.

BPM-FILES-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

bpmp_FilesWeekly.sh executes commands to take backup of below files and folders.

- /etc/sysconfig/iptables
- /keystore/*

bpmp_FilesWeekly.sh executes Spectrum Protect server selective backup command to take backup of files and folders as mentioned above.

In order to enable BPM-FILES-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule BPM-DOMAIN BPM-FILES-WEEKLY expiration=never
```

Above command enable BPM-FILES-WEEKLY schedule without the expiry date.

After enabling BPM-FILES-WEEKLY schedule, start 'dsmcad' service from BPM machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in BPM machine and run `service dsmcad restart` using root user.

You can modify existing files, folders or add new files, folders for backup by updating script /opt/tivoli/tsm/client/ba/bin/bpmp_FilesWeekly.sh available in BPM primary machine.

Object store configuration

Out of the box Object store in Spectrum protect server is configured with dummy credentials and URL. You need to update the details of Object store credentials, in cloud storage pools.

Bucket name used for BPM machine is bpmp.

Use Operation center in updating the details of Object store details.

Two cloud container storage pools are configured while replicating BPM primary machine data from instance 1 of Spectrum Protect server to instance 2 of Spectrum Protect server. Out of the box, these storage pools are configured with dummy credentials and URL. One used to store backup data and another used to store archive data.

Use private URL instead of public URL, if it’s private URL data transfer between Spectrum Protect server and Object store is very fast compared to the usage of public URL.

Run below commands from "Command Builder" of Spectrum protect operation center. As these are cloud container pools client needs to run from the second instance of Spectrum Protect server. In "Command Builder" select second instance which has name like <ORDER_ID>_/s/m/l_bckp1. Select drop down menu from left downside corner, as shown in the image.

Details about Command Builder is available at - Starting Command Builder

```
update stgpool bpm-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool bpm-cloud-pool identity=<USERNAME>
update stgpool bpm-cloud-pool password=<PASSWORD>

update stgpool bpm-arc-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool bpm-arc-cloud-pool identity=<USERNAME>
update stgpool bpm-arc-cloud-pool password=<PASSWORD>
```

BPM secondary machine

To take backups of the artifacts which exists on BPM machine, a sample policy domain configuration named as BPM-DOMAIN is created on Spectrum Protect Server.

Sample schedules are available to take backup of WAS profile directory, WAS profile configuration, database full, database incremental online backups and other files which are located in BPM machine.

These schedules when enabled notifies Spectrum Protect Client to execute specific scripts. Sample scripts which are available at Spectrum Protect Client machine execute commands to create backup archive files, db2 full, db2 incremental backups and invoke Spectrum Protect commands to copy files to Spectrum Protect Server machine.

Database configuration changes

IMPORTANT As this database acts as passive, don't run any database schedules or configuration changes at the starting. Start these database schedules or configuration changes only if this database takeover as a primary database.

The database is configured with linear logging, which means all the transaction (archive) logs of the database are stored on the BPM machine. It is recommended that these logs should be stored in the Spectrum Protect server itself. In the case of a failover scenario, the logs are safe and secure in the Spectrum Protect server.

As transaction (archive) logs of the database are stored on the BPM machine, it's your responsibility to clean up unused logs, as these logs are not cleared by default. Once you move transaction (archive) logs from local disk to Spectrum Protect server, it's the responsibility of Spectrum Protect server to clean unused logs. Use below commands in moving transaction (archive) logs from local disk to Spectrum Protect server:

The database is configured with HADR scenario, follow these steps.

Open Putty or terminal, switch to the db2inst1 user. Check database HADR status. `db2pd -db bpmdb -hadr` `db2pd -db cmndb -hadr` `db2pd -db pdwdb -hadr` If it's proper then follow these steps.

```
db2 update database configuration for bpmdb using LOGARCHMETH1 TSM:BPMMGMTCLASS
db2 update database configuration for cmndb using LOGARCHMETH1 TSM:BPMMGMTCLASS
db2 update database configuration for pdwdb using LOGARCHMETH1 TSM:BPMMGMTCLASS
db2 stop db manager force
db2 start db manager
```

Wait for few minutes and check HADR status. `db2pd -db bpmdb -hadr` `db2pd -db cmndb -hadr` `db2pd -db pdwdb -hadr`

There are two kinds of database backups: full and incremental. It is required that a full backup of the database exists before any incremental backup is taken. Hence before the sample schedules are started, you have to make sure that one full backup of the respective database is available. Verify available backups for a database by using `db2adutl query db <DATABASE_NAME>`. Open Putty or terminal, switch to the db2inst1 user to run this command. You have to execute the shell script db2FullBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside BPM Machine, incase there are no full backups available.

Before running db2FullBackup.sh decide, where to store database archive logs, whether in local disk or Spectrum protect server.

Configurations for taking online full database backups

A sample schedule named as BPMS-DB-FULL-WEEKLY is configured to take backups of online full database. This schedule invokes db2FullBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside BPM Machine.

BPMS-DB-FULL-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight. db2FullBackup.sh executes commands to take online full backups for BPMDB, CMNDB and PDWDB databases.

In order to enable BPMS-DB-FULL-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule BPMS-DOMAIN BPMS-DB-FULL-WEEKLY expiration=never
```

Above command enable BPMS-DB-FULL-WEEKLY schedule without the expiry date. After enabling BPMS-DB-FULL-WEEKLY schedule, start 'dsmcad' service from BPM machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in BPM machine and run `service dsmcad restart` using root user.

Configurations for taking online incremental database backups

A sample schedule named as BPMS-DB-INCREMENT-DAILY is configured to take online incremental database backups. This schedule invokes db2IncrementalBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside BPM Machine.

BPMS-DB-INCREMENT-DAILY schedule is configured to execute from Monday to Saturday at midnights, except Sunday. db2IncrementalBackup.sh executes commands to take online incremental backups for BPMDB, CMNDB and PDWDB databases.

In order to enable BPMS-DB-INCREMENT-DAILY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule BPMS-DOMAIN BPMS-DB-INCREMENT-DAILY expiration=never
```

Above command enable BPMS-DB-INCREMENT-DAILY schedule without the expiry date. After enabling BPMS-DB-INCREMENT-DAILY schedule, start 'dsmcad' service from BPM machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in BPM machine and run `service dsmcad restart` using root user.

Configurations for taking backups of application server and deployment manager configuration

A sample schedule named as BPMS-WAS-DAILY is configured to take backups of WAS profile configuration. This schedule invokes WASProfileConfigBackup_BPM.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside BPM Machine. Before enabling BPM-WAS-DAILY schedule, you must update WASProfileConfigBackup_BPM.sh and provide value for PASSWORD field.

BPMS-WAS-DAILY schedule is configured to execute daily at midnight.

WASProfileConfigBackup_BPM.sh executes commands to create an archive files named BPMS_NodeConfig.zip, BPMS_ProxyConfig.zip which contains all profile configurations.

- WAS Node02 profile configuration folder : /bpm/profiles/Node2Profile
- WAS proxy profile configuration folder : /bpm/profiles/proxy

BPMS_NodeConfig.zip : Contains Node2Profile profile configuration which is generated by using backupConfig command BPMS_ProxyConfig.zip : Contains proxy profile configuration which is generated by using backupConfig command

Archive files, BPMConfig export files are stored in /bpm/WAS_ConfigBackup folder. WASProfileConfigBackup_BPM.sh executes Spectrum Protect server selective backup command to take backup of BPMS_NodeConfig.zip, BPMS_ProxyConfig.zip files.

BPMS-WAS-DAILY schedule is configured to take profile configuration backups using WAS utility backupconfig.sh and export BPM configuration using BPMConfig.sh export option.

In order to enable BPMS-WAS-DAILY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule BPMS-DOMAIN BPMS-WAS-DAILY expiration=never
```

Above command enable BPMS-WAS-DAILY schedule without the expiry date.

After enabling BPM-WAS-DAILY schedule, start 'dsmcad' service from BPM machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in BPM machine and run `service dsmcad restart` using root user.

Configurations for taking backups of application server and deployment manager profiles folder

A sample schedule named as BPMS-WAS-WEEKLY is configured to take backups of WAS profile directories. This schedule invokes WASProfileBackup_BPM.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside BPM Machine.

BPMS-WAS-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

WASProfileBackup_BPM.sh executes commands to create an archive files named BPMS_Node2_backup.tar, BPMS_proxy_backup.tar which contains all the files from following directories.

- WAS Node02 profile folder : /bpm/profiles/Node2Profile
- WAS proxy profile folder : /bpm/profiles/proxy

BPMS_Node2_backup.tar : Contains content of Node2Profile profile directory which is located at /bpm/profiles/Node2Profile BPMS_proxy_backup.tar : Contains content of proxy profile directory which is located at /bpm/profiles/proxy

Archive files are stored in /bpm/WAS_Backup folder. WASProfileBackup_BPM.sh executes Spectrum Protect server selective backup command to take backup of BPMS_Node2_backup.tar, BPMS_proxy_backup.tar files.

IMPORTANT

BPM knowledge center claims manageprofile.sh option backupProfile is not available for BPM WAS profiles.

More information on the backup of BPM WAS profiles is mentioned in the following links.

https://www.ibm.com/support/knowledgecenter/SSFTDH_8.5.6/com.ibm.wbpm.ref.doc/topics/rins_manageprofiles.html

BPMS-WAS-WEEKLY schedule takes profile folder backup and store it in Spectrum Protect Server. You can use these tar files to replace any files or folders which are deleted mistakenly.

In order to enable BPMS-WAS-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule BPMS-DOMAIN BPMS-WAS-WEEKLY expiration=never
```

Above command enable BPMS-WAS-WEEKLY schedule without the expiry date. After enabling BPMS-WAS-WEEKLY schedule, start 'dsmcad' service from BPM machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in BPM machine and run `service dsmcad restart` using root user.

Configurations for taking backups of files and folders

A sample schedule named as BPMS-FILES-WEEKLY is configured to take backups of files and folders. This schedule invokes bpmp_FilesWeekly.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside BPM Machine.

BPMS-FILES-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

bpmp_FilesWeekly.sh executes commands to take backup of below files and folders.

- /etc/sysconfig/iptables
- /keystore/*

bpmp_FilesWeekly.sh executes Spectrum Protect server selective backup command to take backup of files and folders as mentioned above.

In order to enable BPMS-FILES-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule BPMS-DOMAIN BPMS-FILES-WEEKLY expiration=never
```

Above command enable BPMS-FILES-WEEKLY schedule without the expiry date.

After enabling BPMS-FILES-WEEKLY schedule, start 'dsmcad' service from BPM machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in BPM machine and run `service dsmcad restart` using root user.

You can modify existing files, folders or add new files, folders for backup by updating script /opt/tivoli/tsm/client/ba/bin/bpmp_FilesWeekly.sh available in BPM primary machine.

Object store configuration

Out of the box Object store in Spectrum protect server is configured with dummy credentials and URL. You need to update the details of Object store credentials, in cloud storage pools.

Bucket name used for BPM machine is bpms.

Use Operation center in updating the details of Object store details.

Two cloud container storage pools are configured while replicating BPM secondary machine data from instance 1 of Spectrum Protect server to instance 2 of Spectrum Protect server. Out of the box, these storage pools are configured with dummy credentials and URL. One used to store backup data and another used to store archive data.

Use private URL instead of public URL, if it's private URL data transfer between Spectrum Protect server and Object store is very fast compared to the usage of public URL.

Run below commands from "Command Builder" of Spectrum protect operation center. As these are cloud container pools client needs to run from the second instance of Spectrum Protect server. In "Command Builder" select second instance which has name like <ORDER_ID>_/s/m/l_bckp1. Select drop down menu from left downside corner, as shown in the image.

Details about Command Builder is available at - Starting Command Builder

```
update stgpool bpms-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool bpms-cloud-pool identity=<USERNAME>
update stgpool bpms-cloud-pool password=<PASSWORD>

update stgpool bpms-arc-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool bpms-arc-cloud-pool identity=<USERNAME>
update stgpool bpms-arc-cloud-pool password=<PASSWORD>
```

IIS machine

To take backups of the artifacts which exists on IIS machine, a sample policy domain configuration named as IIS-DOMAIN is created on Spectrum Protect Server.

Sample schedules are available to take backup of WAS profile, WAS profile configuration, database full, database incremental online backups and other files which are located in IIS machine. These schedules when enabled notifies Spectrum Protect Client to execute specific scripts. Sample scripts which are available at Spectrum Protect Client machine execute commands to create backup archive files, db2 full, db2 incremental backups and invoke Spectrum Protect commands to copy files to Spectrum Protect Server machine.

Database configuration changes

The database is configured with linear logging, which means all the transaction (archive) logs of the database are stored on the IIS machine. It is recommended that these logs should be stored in the Spectrum Protect server itself. In the case of a failover scenario, the logs are safe and secure in the Spectrum Protect server.

As transaction (archive) logs of the database are stored on the IIS machine, it's your responsibility to clean up unused logs, as these logs are not cleared by default. Once you move transaction (archive) logs from local disk to Spectrum Protect server, it's the responsibility of Spectrum Protect server to clean unused logs. Use below commands in moving transaction (archive) logs from local disk to Spectrum Protect server:

Open Putty or terminal, switch to the db2inst1 user.

```
db2 update database configuration for xmeta using LOGARCHMETH1 TSM:IISMGMTCLASS
db2 update database configuration for iadb using LOGARCHMETH1 TSM:IISMGMTCLASS
db2 update database configuration for ESDBDB2 using LOGARCHMETH1 TSM:IISMGMTCLASS
db2 update database configuration for DSODB using LOGARCHMETH1 TSM:IISMGMTCLASS
```

```
db2 stop db manager force
db2 start db manager
```

There are two kinds of database backups: full and incremental. It is required that a full backup of the database exists before any incremental backup is taken. Hence before the sample schedules are started, you have to make sure that one full backup of the respective database is available. Verify available backups for a database by using `db2adutl query db <DATABASE_NAME>`. Open Putty or terminal, switch to the db2inst1 user to run this command. You have to execute the shell script db2FullBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside IIS Machine, incase there are no full backups available.

Before running db2FullBackup.sh decide, where to store database archive logs, whether in local disk or Spectrum protect server.

Configurations for taking online full database backups

A sample schedule named as IIS-DB-FULL-WEEKLY is configured to take backups of online full database. This schedule invokes db2FullBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside IIS Machine.

IIS-DB-FULL-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight. db2FullBackup.sh executes commands to take online full backups for XMETA, IADB, ESDBDB2 and DSODB databases.

In order to enable IIS-DB-FULL-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule IIS-DOMAIN IIS-DB-FULL-WEEKLY expiration=never
```

Above command enable IIS-DB-FULL-WEEKLY schedule without the expiry date. After enabling IIS-DB-FULL-WEEKLY schedule, start 'dsmcad' service from IIS machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in IIS machine and run `service dsmcad restart` using root user.

Configurations for taking online incremental database backups

A sample schedule named as IIS-DB-INCREMENT-DAILY is configured to take online incremental database backups. This schedule invokes db2IncrementalBackup.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside IIS Machine.

IIS-DB-INCREMENT-DAILY schedule is configured to execute from Monday to Saturday at midnights, except Sunday. db2IncrementalBackup.sh executes commands to take online incremental backups for XMETA, IADB, ESDBDB2 and DSODB databases.

In order to enable IIS-DB-INCREMENT-DAILY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule IIS-DOMAIN IIS-DB-INCREMENT-DAILY expiration=never
```

Above command enable IIS-DB-INCREMENT-DAILY schedule without the expiry date. After enabling IIS-DB-INCREMENT-DAILY schedule, start 'dsmcad' service from IIS machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in IIS machine and run `service dsmcad restart` using root user.

Configurations for taking backups of WAS InfoSphere profiles

A sample schedule named as IIS-WAS-WEEKLY is configured to take backups of WAS profiles. This schedule invokes WASProfileBackup_IIS.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside IIS Machine. Before enabling IIS-WAS-WEEKLY schedule, you must update WASProfileBackup_IIS.sh and provide value for PASSWORD field.

IIS-WAS-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

WASProfileBackup_IIS.sh executes manageprofiles.sh utility provided by WAS to create profile backups named IIS_AppServer_backup.zip which contains profile backups.

- WAS InfoSphere profile folder : /opt/IBM/WebSphere/AppServer/profiles/InfoSphere

IIS_AppServer_backup.zip : Contains backup of InfoSphere profile created using manageprofiles.sh utility where profile is located at /opt/IBM/WebSphere/AppServer/profiles/InfoSphere

Generated files are stored in /opt/WAS_Backup folder. WASProfileBackup_IIS.sh executes Spectrum Protect server selective backup command to take backup of IIS_AppServer_backup.zip file.

IMPORTANT

WAS guidelines for backup of WAS profile mandates that the WAS services be stopped before the profile is being backed up. This schedule forces to stop servers related to that WAS profile.

As this schedule stop server related to WAS profile, it's up to you to take a decision on whether to run this schedule on weekly basis or run this when it's needed. It is recommended to take backup of profiles when there are changes to WAS like deploying an application or deleting an application etc..

If you want to run this schedule manually whenever it's needed instead of running weekly, a shell script named WASProfileBackup_IIS.sh is available at /opt/tivoli/tsm/client/ba/bin folder. Execute this script as a root user, it'll stop the profile and related servers, take the backup of profile and generated zip files are send to Spectrum Protect Server.

More information on the backup of WAS profiles is mentioned in the following links.

https://www.ibm.com/support/knowledgecenter/en/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/rxml_manageprofiles.html

Sample template used for taking backup of WAS profile :

```
/opt/IBM/WebSphere/AppServer/profiles/<PROFILE_NAME>/bin/stopServer.sh <SERVER_NAME> -username
wasadmin -password PASSWORD
/opt/IBM/WebSphere/AppServer/bin/manageprofiles.sh -backupProfile -profileName <PROFILE_NAME> -
backupFile /opt/WAS_Backup/IIS_AppServer_backup.zip

/opt/IBM/WebSphere/AppServer/profiles/<PROFILE_NAME>/bin/startServer.sh <SERVER_NAME>

dsmc sel "/home2/WAS_Backup/*" -subdir=yes
```

The server is stopped first, then the manageprofiles.sh command is used to take backup of the WAS profile and then the server is started again. *dsmc* command is used to transfer the backup files from IIS machine to the Spectrum Protect Server.

In order to enable IIS-WAS-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule IIS-DOMAIN IIS-WAS-WEEKLY expiration=never
```

Above command enable IIS-WAS-WEEKLY schedule without the expiry date. After enabling IIS-WAS-WEEKLY schedule, start 'dsmcad' service from IIS machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in IIS machine and run `service dsmcad restart` using root user.

After running the IIS-WAS-WEEKLY schedule or running WASProfileBackup_IIS.sh manually, make sure IIS_AppServer_backup.zip is created at /opt/WAS_Backup folder. If you didn't find these files, there might be an issue while running WASProfileBackup_IIS.sh which is available at /opt/tivoli/tsm/client/ba/bin folder. Run this script manually and fix the issues.

Configurations for taking backups of WAS InfoSphere profile configuration

A sample schedule named as IIS-WAS-DAILY is configured to take backups of WAS profile configuration. This schedule invokes WASProfileConfigBackup_IIS.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside IIS Machine. Before enabling IIS-WAS-DAILY schedule, you must update WASProfileConfigBackup_IIS.sh and provide value for PASSWORD field.

IIS-WAS-DAILY schedule is configured to execute daily at midnight.

WASProfileConfigBackup_IIS.sh executes commands to create an archive files named IIS_AppServerConfig.zip which contains all profile configurations.

- WAS Infosphere profile configuration folder : /opt/IBM/WebSphere/AppServer/profiles/InfoSphere

IIS_AppServerConfig.zip : Contains InfoSphere profile configuration which is generated by using backupConfig command

Archive file is stored in /opt/WAS_ConfigBackup folder. WASProfileConfigBackup_IIS.sh executes Spectrum Protect server selective backup command to take backup of IIS_AppServerConfig.zip file.

In order to enable IIS-WAS-DAILY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule IIS-DOMAIN IIS-WAS-DAILY expiration=never
```

Above command enable IIS-WAS-DAILY schedule without the expiry date.

After enabling IIS-WAS-DAILY schedule, start 'dsmcad' service from IIS machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in IIS machine and run `service dsmcad restart` using root user.

Configurations for taking backups of ISTool

A sample schedule named as IIS-ISTOOL-WEEKLY is configured to take backups of ISTool export configuration. This schedule invokes istool_assets.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside IIS Machine. Before enabling IIS-ISTOOL-WEEKLY schedule, you must update istool_assets.sh and provide value for PASSWORD field.

IIS-ISTOOL-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

istool_assets.sh executes commands to create an archive file which contains all ISTool export configurations.

- IIS istool.sh export backup : Using istool.sh export all configuration

Archive file generated by istool.sh is stored in /opt/ISTool folder. istool_assets.sh executes Spectrum Protect server selective backup command to take backup of istool generated file.

In order to enable IIS-ISTOOL-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule IIS-DOMAIN IIS-ISTOOL-WEEKLY expiration=never
```

Above command enable IIS-ISTOOL-WEEKLY schedule without the expiry date.

After enabling IIS-ISTOOL-WEEKLY schedule, start 'dsmcad' service from IIS machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in IIS machine and run `service dsmcad restart` using root user.

Configurations for taking backups of files and folders

A sample schedule named as IIS-FILES-WEEKLY is configured to take backups of files and folders. This schedule invokes iisp_FilesWeekly.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside IIS Machine.

IIS-FILES-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight.

iisp_FilesWeekly.sh executes commands to take backup of below files and folders.

- /opt/IBM/InformationServer/Server/Configurations/*
- /opt/IBM/InformationServer/Updates/*
- /opt/IBM/InformationServer/Server/DSODB/*.cfg
- /opt/IBM/InformationServer/Server/DSEngine/dsenv

- /etc/services
- /etc/inittab
- /opt/IBM/InformationServer/ASBServer/apps/lib/iis/15properties/*
- /opt/IBM/InformationServer/ASBServer/apps/lib/iis/classes/*

iisp_FilesWeekly.sh executes Spectrum Protect server selective backup command to take backup of files and folders as mentioned above.

In order to enable IIS-FILES-WEEKLY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule IIS-DOMAIN IIS-FILES-WEEKLY expiration=never
```

Above command enable IIS-FILES-WEEKLY schedule without the expiry date.

After enabling IIS-FILES-WEEKLY schedule, start 'dsmcad' service from IIS machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in IIS machine and run `service dsmcad restart` using root user.

You can modify existing files, folders or add new files, folders for backup by updating script /opt/tivoli/tsm/client/ba/bin/iisp_FilesWeekly.sh available in IIS machine.

Configurations for taking backups of files and folders

A sample schedule named as IIS-FILES-WEEKLY2 is configured to take backups of files and folders. This schedule invokes iisp_FilesWeekly2.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside IIS Machine.

IIS-FILES-WEEKLY2 schedule is configured to execute weekly once, on Sundays at midnight.

iisp_FilesWeekly2.sh executes commands to take backup of below files and folders.

- /keys/*
- /keystore/*
- /etc/sysconfig/iptables
- /opt/IBM/InformationServer/Server/MsgHandlers/*

iisp_FilesWeekly2.sh executes Spectrum Protect server selective backup command to take backup of files and folders as mentioned above.

In order to enable IIS-FILES-WEEKLY2 schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule IIS-DOMAIN IIS-FILES-WEEKLY2 expiration=never
```

Above command enable IIS-FILES-WEEKLY2 schedule without the expiry date.

After enabling IIS-FILES-WEEKLY2 schedule, start 'dsmcad' service from IIS machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in IIS machine and run `service dsmcad restart` using root user.

You can modify existing files, folders or add new files, folders for backup by updating script /opt/tivoli/tsm/client/ba/bin/iisp_FilesWeekly2.sh available in IIS machine.

Configurations for taking backups of files and folders

A sample schedule named as IIS-FILES-DAILY is configured to take backups of files and folders. This schedule invokes iisp_FilesDaily.sh which is available at /opt/tivoli/tsm/client/ba/bin folder inside IIS Machine.

IIS-FILES-DAILY schedule is configured to execute daily at midnight.

iisp_FilesDaily.sh executes commands to take backup of below files and folders.

- /opt/IBM/InformationServer/Version.xml
- /opt/IBM/InformationServer/Server/Projects/*

iisp_FilesDaily.sh executes Spectrum Protect server selective backup command to take backup of files and folders as mentioned above.

In order to enable IIS-FILES-DAILY schedule, you need to execute the following command using "Command Builder". Details about Command Builder is available at - Starting Command Builder

```
update schedule IIS-DOMAIN IIS-FILES-DAILY expiration=never
```

Above command enable IIS-FILES-DAILY schedule without the expiry date.

After enabling IIS-FILES-DAILY schedule, start 'dsmcad' service from IIS machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed.

Open Putty or terminal in IIS machine and run `service dsmcad restart` using root user.

You can modify existing files, folders or add new files, folders for backup by updating script /opt/tivoli/tsm/client/ba/bin/iisp_FilesDaily.sh available in IIS machine.

Object store configuration

Out of the box Object store in Spectrum protect server is configured with dummy credentials and URL. You need to update the details of Object store credentials, in cloud storage pools.

Bucket name used for IIS machine is iisp.

Use Operation center in updating the details of Object store details.

Two cloud container storage pools are configured while replicating IIS machine data from instance 1 of Spectrum Protect server to instance 2 of Spectrum Protect server. Out of the box, these storage pools are configured with dummy credentials and URL. One used to store backup data and another used to store archive data.

Use private URL instead of public URL, if it's private URL data transfer between Spectrum Protect server and Object store is very fast compared to the usage of public URL.

Run below commands from "Command Builder" of Spectrum protect operation center. As these are cloud container pools client needs to run from the second instance of Spectrum Protect server. In "Command Builder" select second instance which has name like <ORDER_ID>_/s/m/l_bckp1. Select drop down menu from left downside corner, as shown in the image.

Details about Command Builder is available at - Starting Command Builder

```
update stgpool iis-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool iis-cloud-pool identity=<USERNAME>
update stgpool iis-cloud-pool password=<PASSWORD>

update stgpool iis-arc-cloud-pool cloudurl=https://<PRIVATE_URL>
update stgpool iis-arc-cloud-pool identity=<USERNAME>
update stgpool iis-arc-cloud-pool password=<PASSWORD>
```

Adding new schedules

Spectrum protect server is configured with sample schedules and you can create new schedules based on your requirement.

More information on creating new schedules is available here

Updating existing schedules

Spectrum protect server is configured with sample schedules and you can change existing schedules according to your requirement or you can create a new schedule.

You can update starting time of schedule or when to execute schedule or disable schedule based on your requirements.

More information on updating schedules is available here

Creating new policies and domain

Spectrum protect server is configured with sample policies and domain for each machine. You can create new policies and domains based on your requirement.

More information about adding new policies and domain is available here

You can specify your own rules on when to take backup, archive, and data retention requirements. More information about these are available here

Starting Spectrum Protect Server

Follow these steps to start both Spectrum Protect instances and Operation center.

Connect to Spectrum Protect server using putty or terminal using root user. Executed below commands.

```
cd /bckp/opt/tivoli/tsm/server/bin/
. /bckp/tsminst1/sqllib/db2profile
./dsmserv -u tsminst1 -i /bckp/tsminst1  -q &
```

This will start TSM server 1.

```
. /bckp/tsminst2/sqllib/db2profile
./dsmserv -u tsminst2 -i /bckp/tsminst2  -q &
```

This will start TSM server 2.

Starting Operation center

```
cd /bckp/opt/tivoli/tsm/ui/Liberty/bin
service opscenter.rc status
service opscenter.rc start
```

Initially, Spectrum Protect server second instance will be down, it'll take 5 to 10 minutes to come up. You can check if both instances are up, under overview tab in operation center console.

`https://<PUBLIC_IP>:11090/oc` or `https://<PRIVATE_IP>:11090/oc`

If any of Spectrum protect client (like MDM primary machine or BPM or IIS machine) is restarted run dsmcad service. Open Putty or terminal in Spectrum protect client machine which is restarted and run `service dsmcad restart` using root user.

Spectrum Protect server inventory expire

As mentioned in the - Retention Policy section, a file can be present in 3 states: active, inactive and expired. Once the file has reached the "expired" mode, it has to be manually deleted from the Spectrum Protect server. Inventory Expiration enables us to delete these expired artifacts.

Expire Inventory command might take several minutes to hours some times which results in performance degrade of the Spectrum Protect Server. This command should be scheduled to run only when the Spectrum Protect server is busy.

Schecules have been created for both the Spectrum Protect server instances, which call scripts to execute the Inventory Expiration command. Information on these scripts and schedules have been given below.

First instance

An administrative schedule named *EXPIRES* is used to call the script, *EXPIRES*, every day at 07:00:00. It can be queried by using the following command in the command builder.

```
query script EXPIRES format=lines
```

Second instance

An administrative schedule named *EXPIRET* is used to call the script, *EXPIRET*, every day at 07:00:00. It can be queried by using the following command in the command builder.

```
query script EXPIRET format=lines
```

More details about expire inventory is here

Protecting the master encryption key

Data encryption and decryption is handled automatically by the Spectrum Protect server and does not require any user action apart from some initial configuration. To encrypt data for cloud-container storage pools, the server uses a master encryption key, which is created when the server password is set. The master encryption key is itself encrypted, and is stored as part of the server password file.

The master encryption key is stored in the server password file, /bckp/tsminst1/dsmkeydb.kdb for the first server instance and /bckp/tsminst2/dsmkeydb.kdb for the second server instance in the Spectrum Protect server machine. The master encryption key is encrypted by a different key, so the master encryption key is itself protected. The master encryption key is re-encrypted whenever the server password is set by the SET SERVERPASSWORD command, so the user can issue this command periodically to further protect the key.

To decrypt data that was sent to encrypted cloud-container storage pools, the master encryption key is required. For this reason, it is important that the server password file is protected. If the server password file is lost or corrupted, the server cannot decrypt the data.

It is recommended that you copy these files to Object Store or some secure location.

More details about master key is here

Spectrum Protect server database backup

In case of a scenario, where the Spectrum Protect server is no longer accessible, the Spectrum Protect server can be restored back to its latest state. To recover or restore any Spectrum Protect server, the following artifacts pertaining to that are required:

- Database used by Spectrum Protect for its functionality (.dbv)
- Metadata volume history file (volhist.out)
- Device configuration file (devconfig.out)

Since there are two Spectrum Protect server instances used in this offering, we need to backup two sets of the above mentioned artifacts. Scripts have been created to store these artifacts in a specfic location locally. These artifacts are mandatorily required in the scenario where the Spectrum Protect server has to be restored. Hence, **it is recommended that the user should back transfer these files to a secure place.**

Scripts have been created within the Spectrum Protect server to take backup of these artifacts. Administrative schedules are used to run these scripts. The details of these scripts and their relation to the two server instances can be found below.

Spectrum protect server admin scheduled is configured for this purpose, which takes daily full backup of Spectrum Protect server DB, metadata file (volume history) & configurations (devconfig). Only a full database backup clears the archive log.

```
def sch tsminst1db t=a cmd="run backuptsms" t=a ACTIVE=y startdate=today starttime=18:00:00
duration=1 durunits=h period=1 perunits=D day=ANY expiration=never
def sch tsminst1db t=a cmd="run backuptsmt" t=a ACTIVE=y startdate=today starttime=19:00:00
duration=1 durunits=h period=1 perunits=D day=ANY expiration=never
```

These schedules are enabled and if you want to change the start time of these schedules you can update accordingly. These scripts also clears the Spectrum Protect database archive logs.

First instance

An administrative schedule named *tsminst1db*, created in the first instance, is used to call this script named *backuptsms*. The schedule calls this script everyday at 18:00:00. The script, *backuptsms*, creates the artifacts required to restore the Spectrum Protect Server in the */bckp/tsmdbbckps/* location in the Spectrum Protect server. The script also deletes the old backup artifacts and maintains only the latest two versions at any point of time. The script can be queried by using the following command in the command builder.

```
query script backuptsms format=lines
```

Second instance

An administrative schedule named *tsminst1db*, created in the second instance, is used to call this script named *backuptsmt*. The schedule calls this script everyday at 19:00:00. The script, *backuptsmt*, creates the artifacts required to restore the Spectrum Protect Server in the */bckp/tsmdbbckpt/* location in the Spectrum Protect server. The script also deletes the old backup artifacts and maintains only the latest two versions at any point of time. The script can be queried by using the following command in the command builder.

```
query script backuptsmt format=lines
```

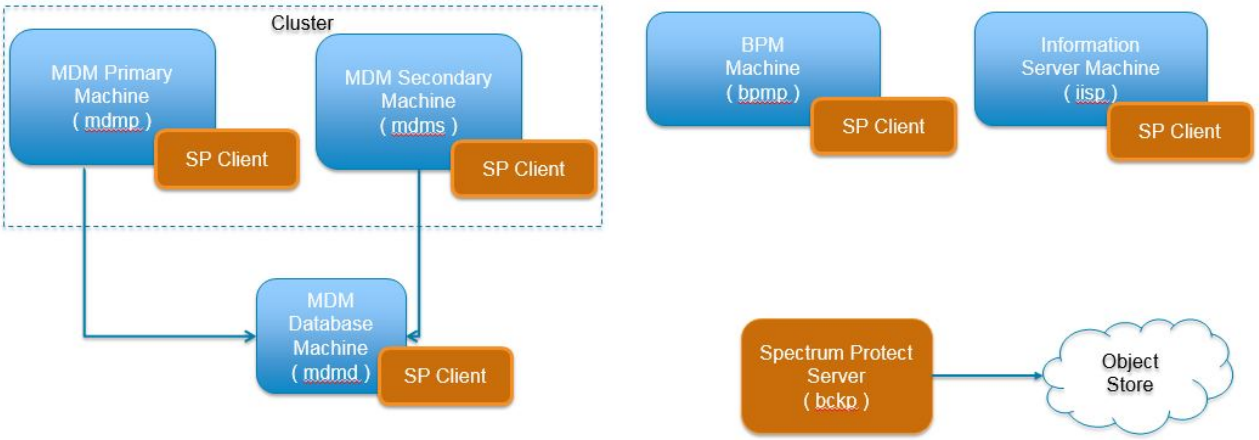
It's your responsibility to copy these artifacts to Object Store or some other machine. Without these artifacts it's not possible to restore Spectrum Protect server in case of failure.

More details about backup commands are here

More details about Spectrum Protect server database backup are here

Restoring Backups

Restore option in Spectrum Protect is used to restore files, directories and database using Spectrum Protect client. Restoring process a manual process. You have to follow this document while restoring artifacts. The Spectrum Protect client GUI can restore data from the server. You can use the GUI to restore individual files or folders from the IBM Spectrum Protect™ server.



Restoring MDM Database

Steps while restoring MDM database.

1. Drop existing MDMDB database.
2. Restore MDMDB database.
3. Verify if database is restored.

Drop existing MDMDB database

1. Open terminal for MDM database machine, switch to db2inst1 user using command `su - db2inst1`
2. `db2 LIST APPLICATIONS` , to check if any applications are connected to this database.
3. Using `db2adutl` command , check available full or incremental backups. Note down timestamp which you are going to restore. Once database is dropped you can't see available full or incremental backups.
4. Drop the database using `db2 drop db MDMDB` , if you face any issues that means database is connected to applications , we need to close all connections to database before dropping it.

```
db2 connect to mdmdb user db2inst1 using <PASSWORD>
db2 quiesce db immediate force connections
db2 connect reset;
db2 LIST APPLICATIONS
db2 terminate
db2 force application all
db2 drop database mdmdb
```

5. In order to make sure , there is no database named MDMDB , execute list command. `db2 list db directory`

Restore MDMDB database

1. Select full or incremental backup timestamp which needs to be restored.
2. `db2 restore db MDMDB use tsm taken at 20170526063832 ENCRYPT` 1. In above statement '20170526063832' is timestamp when the DB backup was taken. 1. "use TSM" is used which means , we are restoring a database which is stored in Spectrum Protect server. 1. "ENCRYPT" is used as existing database is db2 native encrypted. 1. While taking backup "include logs" is used , so if needed you can use "include logs" option, when there is a need to extract transaction logs needed in restore scenario.
3. Select incremental backup timestamp if you want to restore till that date.

   `db2 restore db MDMDB incremental automatic use tsm taken at 20170605134603` 1. On top of full backup , we are restoring incremental backup .
4. `db2 rollforward db MDMDB to end of logs and complete`.

   a. Used to rollforward database till end of logs.

Verify database

1. Connect to MDMDB database using following command. `db2 connect to mdmdb user mdmdbusr using <PASSWORD>`
2. Verify any table to check restore process is done and expected data is available.
3. Terminate database using command, db2 terminate
4. Verify id db2 native encryption is available.

   `db2 connect to MDMDB user db2inst1 using <PASSWORD>`

   `db2 "SELECT * FROM TABLE (SYSPROC.ADMIN_GET_ENCRYPTION_INFO())"`
5. Verify if AES is available in the output.

Restoring Application Server Machine Artifacts

In MDM primary and secondary machines we can restore WebSphere Application server artifacts.

Restore option is available to restore entire profile, this option is useful, in case some of the WAS profile files are corrupted or deleted mistakenly.

Restore option is available to restore profile configuration, where you want to restore WAS profile configuration to old state as some of changes to WAS data sources are giving issues. Before restoring stop all servers, nodes and deployment manager in WebSphere application server.

Before starting any of these steps make sure WebSphere application server is stopped.

Here are the high level steps, and detailed description is available following.

1. Restore WAS artifacts in MDM primary machine, detailed description is provided following.
    a. Restore WAS artifacts from backup server to MDM primary machine
    b. Restore entire WAS profile in MDM primary machine
    c. Restore WAS profile configuration in MDM primary machine
2. Restore WAS artifacts in MDM secondary machine, detailed description is provided following.
    a. Restore WAS artifacts from backup server to MDM secondary machine
    b. Restore WAS profile configuration in MDM secondary machine
    c. Restore entire WAS profile in MDM secondary machine

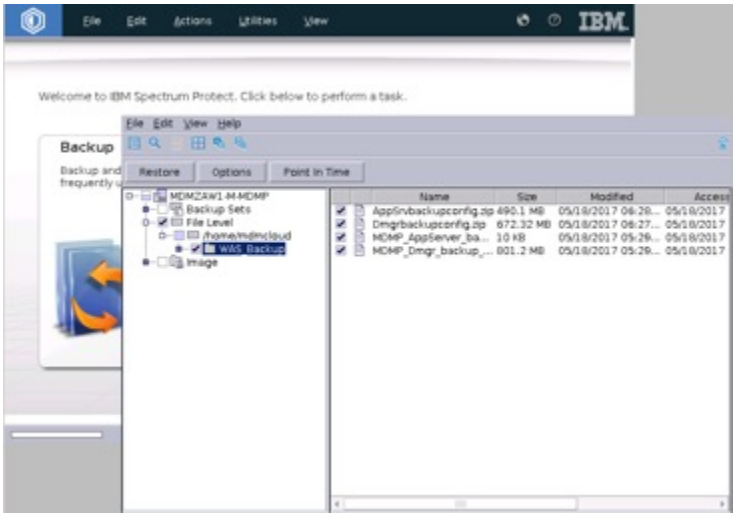
Following verification steps are common for any of above restore scenario.

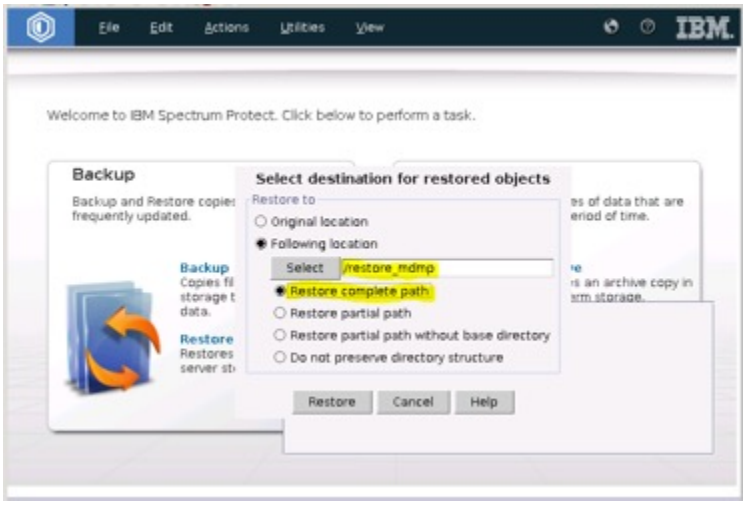
1. Verification steps for any of above scenarios.
    a. Verify if WebSphere Application server is restored.
    b. Verify if connectivity happens from WAS admin console.
    c. Verify IVT
    d. MDM-BPM integration
    e. Verify MDM-BPM integration

Default WAS username is wasadmin, in case if this user is changed by you, use the same while restoring also.

Restore WAS artifacts from Backup server to MDM primary machine

1. Open terminal for MDM primary machine using root user.
2. Start vncserver , if it's first time, it'll ask for password.
3. Open vncserver viewer and connect to MDM primary machine.
4. Once you login open terminal and go to /opt/tivoli/tsm/client/ba/bin
5. Start Spectrum Protect client by executing ./dsmj in terminal.
6. Enter credentials as tsminst and common password provided in welcome letter.
7. Select "Restore" option as we need to restore WAS artifacts.
8. In MDM primary machine create a folder named /restore_mdmp under / (root directory)
9. Restore WAS artifacts to /restore_mdmp folder.
10. In Spectrum Protect server select "Restore", this will pop-up a window.
11. Select /home/mdmcloud/WAS_Backup folder , you can find lot of files based on date. Select the files for which date , you want to restore and press "Restore" button.





1. Here select "Following location" and give location as /restore_mdmp folder.
2. Open the `/restore_mdmp` folder to see the following files.

- If profile full restore is needed, then use these files based on the profile: MDMP_AppServer_backup.zip, MDMP_Dmgr_backup.zip, MDMP_proxy_backup.zip
- If profile configuration restore is needed, then use below files based on the profile: MDMP_DmgrConfig.zip, MDMP_AppSrvConfig.zip, MDMP_proxyConfig.zip

Restore entire WAS profile in MDM primary machine

IMPORTANT

WAS guidelines for restore of WAS profile mandates that the WAS services be stopped before the profile is being restored. You need to stop servers related to that WAS profile.

1. Open terminal for MDM primary machine using root user.
2. Go to `/restore_mdmp` folder and rename zip file which you want to restore. MDMP_AppServer_backup.zip is used to restore AppServer full profile. MDMP_Dmgr_backup.zip is used to restore Deployment manager full profile. MDMP_proxy_backup.zip is used to restore proxy full profile.
3. Select the zip file which you want to replace and change the permission of the file to mdmcloud user. For example, if you want to replace AppServer profile use following commands. chown mdmcloud / restore_mdmp/WAS_Backup/MDMP_AppServer_backup.zip chown :mdmcloud /restore_mdmp/ WAS_Backup/MDMP_AppServer_backup.zip
4. Switch the user to mdmcloud user using command `su - db2inst1` .
5. WAS full profile restore uses WAS utility manageprofiles.sh
6. Stop all servers related to this profile before restoring.
7. Rename existing Dmgr01 or AppSrv01 or proxy profile which you want to restore from /home/ mdmcloud/IBM/WebSphere/AppServer/profiles
8. Choose which profile you want to restore. Commands are provided for all profiles , you can choose which ever profile you want to restore.

   cd /home/mdmcloud/IBM/WebSphere/AppServer/bin

   ./manageprofiles.sh -validateAndUpdateRegistry ./manageprofiles.sh -restoreProfile -backupFile / restore_mdmp/WAS_Backup/MDMP_Dmgr_backup.zip

   ./manageprofiles.sh -validateAndUpdateRegistry ./manageprofiles.sh -restoreProfile -backupFile / restore_mdmp/WAS_Backup/MDMP_AppServer_backup.zip

   ./manageprofiles.sh -validateAndUpdateRegistry ./manageprofiles.sh -restoreProfile -backupFile / restore_mdmp/WAS_Backup/MDMP_proxy_backup.zip

9. Verify if restored profile has same permissions as old.

Follow these steps to verify if restore Profile process. - Verification Process

Restore WAS profile configuration in MDM primary machine

1. Restore WAS profile configuration in MDM primary machine.
2. Open terminal for MDM primary machine using root user. Switch the user to mdmcloud user using command `su - db2inst1.cd /home/mdmcloud/IBM/WebSphere/AppServer/bin`
3. Choose which profiles you needs to replace configuration. Here are commands.

```
./restoreConfig.sh /restore_mdmp/WAS_Backup/MDMP_AppSrvConfig.zip -nostop -
username wasadmin -password <PASSWORD> -profileName AppSrv01
```

```
./restoreConfig.sh /restore_mdmp/WAS_Backup/MDMP_DmgrConfig.zip -nostop -
username wasadmin -password <PASSWORD> -profileName Dmgr01
```

```
./restoreConfig.sh /restore_mdmp/WAS_Backup/MDMP_proxyConfig.zip -nostop -
username wasadmin -password <PASSWORD> -profileName Proxy
```

Restore WAS artifacts from Backup server to MDM secondary machine

1. Open terminal for MDM secondary machine using root user.
2. Start vncserver , if It's first time, It'll ask for password.
3. Open vncserver viewer and connect to MDM secondary machine.
4. Once you login open terminal and go to /opt/tivoli/tsm/client/ba/bin
5. Start Spectrum Protect client by executing "./dsmj" in terminal.
6. Enter credentials as tsminst and common password provided in welcome letter.
7. Select "Restore" option as we need to restore WAS artifacts.
8. In MDM primary machine create a folder named /restore_mdms under / (root directory)
9. Restore WAS artifacts to /restore_mdms folder.
10. In Spectrum Protect server select "Restore", this will pop-up a window.
11. Select /home/mdmcloud/WAS_Backup folder , you can find lot of files based on date. Select the files for which date , you want to restore and press "Restore" button.
12. Here select "Following location" and give location as /restore_mdms folder.
13. Open the `/restore_mdms` folder to see the following files.
    - If profile full restore is needed, then use following files based on profile. MDMS_Custom_backup.zip, MDMS_proxy_backup.zip
    - If profile configuration restore is needed, then use following files based on profile. MDMS_CustomConfig.zip, MDMS_proxyConfig.zip

Restore entire WAS profile in MDM secondary machine

IMPORTANT

WAS guidelines for restore of WAS profile mandates that the WAS services be stopped before the profile is being restored. You need to stop servers related to that WAS profile.

1. Open terminal for MDM secondary machine using root user.
2. Go to `/restore_mdms` folder and rename zip file which you want to restore. MDMS_Custom_backup.zip is used to restore Custom full profile. MDMS_proxy_backup.zip is used to restore proxy full profile.
3. Select the zip file which you want to replace and change the permission of the file to mdmcloud user. For example, if you want to replace Custom profile use following commands. chown mdmcloud / restore_mdms/WAS_Backup/MDMS_Custom_backup.zip chown :mdmcloud /restore_mdms/ WAS_Backup/MDMS_Custom_backup.zip
4. Switch the user to mdmcloud user using command `su - db2inst1` .

5. WAS full profile restore uses WAS utility manageprofiles.sh
6. Stop all servers related to this profile before restoring.
7. Rename existing Custom01 or proxy profile which you want to restore from /home/mdmcloud/IBM/WebSphere/AppServer/profiles
8. Choose which profile you want to restore. Commands are provided for all profiles , you can choose which ever profile you want to restore.

   cd /home/mdmcloud/IBM/WebSphere/AppServer/bin

   ./manageprofiles.sh -validateAndUpdateRegistry ./manageprofiles.sh -restoreProfile -backupFile /restore_mdms/WAS_Backup/MDMS_Custom_backup.zip

   ./manageprofiles.sh -validateAndUpdateRegistry ./manageprofiles.sh -restoreProfile -backupFile /restore_mdms/WAS_Backup/MDMS_proxy_backup.zip
9. Verify if restored profile has same permissions as old.

Follow these steps to verify if restore Profile process. - Verification Process

Restore WAS profile configuration in MDM secondary machine

1. Restore WAS profile configuration in MDM secondary machine.
2. Open terminal for MDM secondary machine using root user. Switch the user to mdmcloud user using command `su - db2inst1.cd /home/mdmcloud/IBM/WebSphere/AppServer/bin`
3. Choose which profiles you needs to replace configuration. Here are commands.

```
./restoreConfig.sh /restore_mdms/WAS_Backup/MDMS_CustomConfig.zip -nostop -username wasadmin -password <PASSWORD> -profileName Custom01
```

```
./restoreConfig.sh /restore_mdms/WAS_Backup/MDMS_proxyConfig.zip -nostop -username wasadmin -password <PASSWORD> -profileName Proxy
```

Restoring files and directories

As has been discussed in the Backup Section of Master Data Management, sample policies and schedules are created to backup specific files and directories to the Spectrum Protect Server from individual machines like the MDM Primary machine, MDM Secondary machine, MDM database machine, BPM machine and IIS machine.

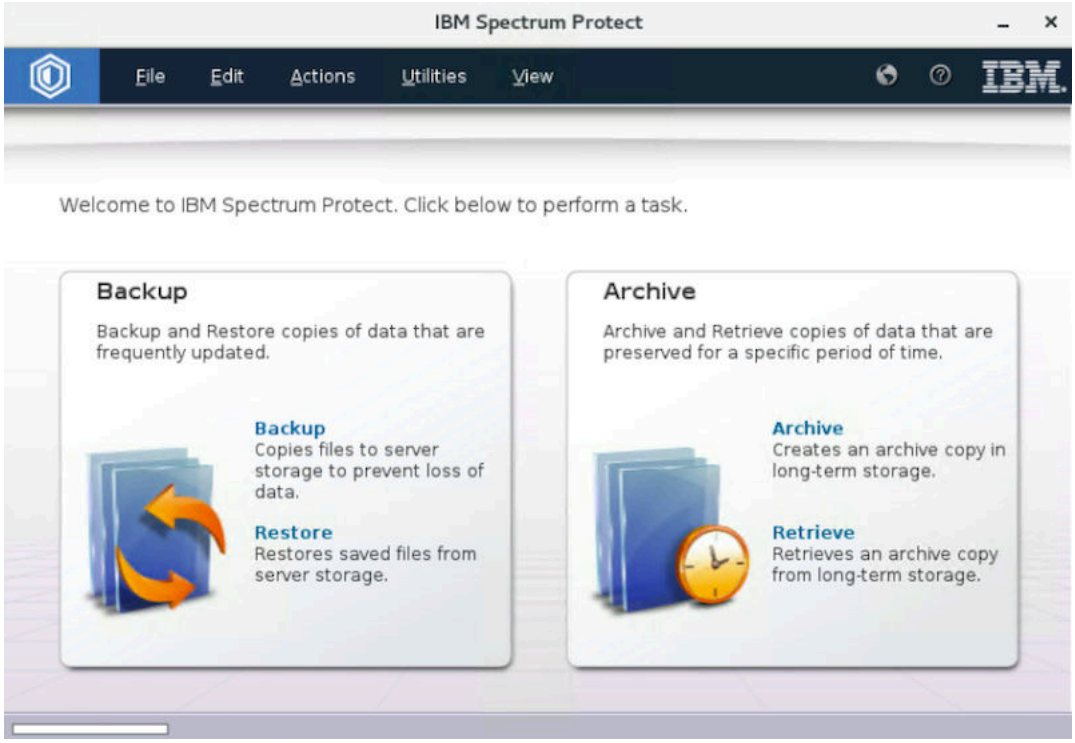
There are two things to be particular about when a file/directory is being restored

- Whichever file/directory is being restored, make sure that a copy of the same is created as a temporary file.
- The user privileges of the file/directory must be noted before restore. After restore, if there are any discrepancies, the user privileges must be set by the user for the restored files/directories so that they match with the ones of the current file/directory.

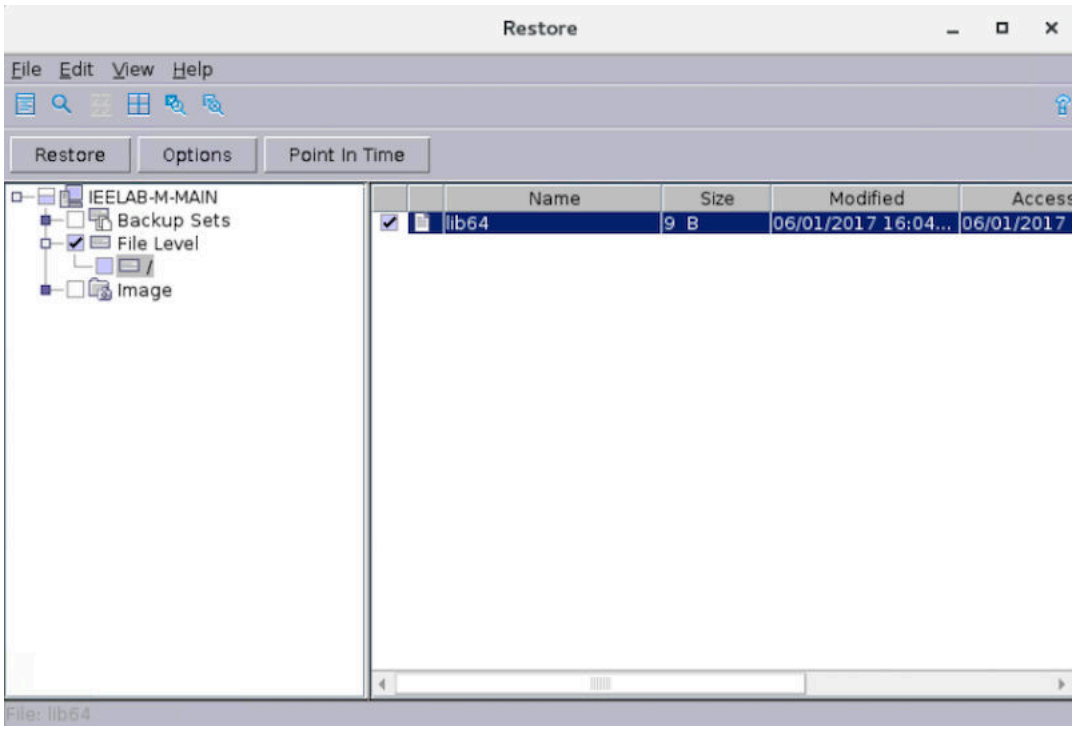
The method to restored has been explained for the MDM Primary machine. The procedure is the same for all other machines as well where Spectrum Protect Client is installed. The files/directories can be restored in the following way:

1. Log into the MDM Primary machine as root in a GUI session.

2. Execute the following command: /opt/tivoli/tsm/client/ba/bin/dsmj



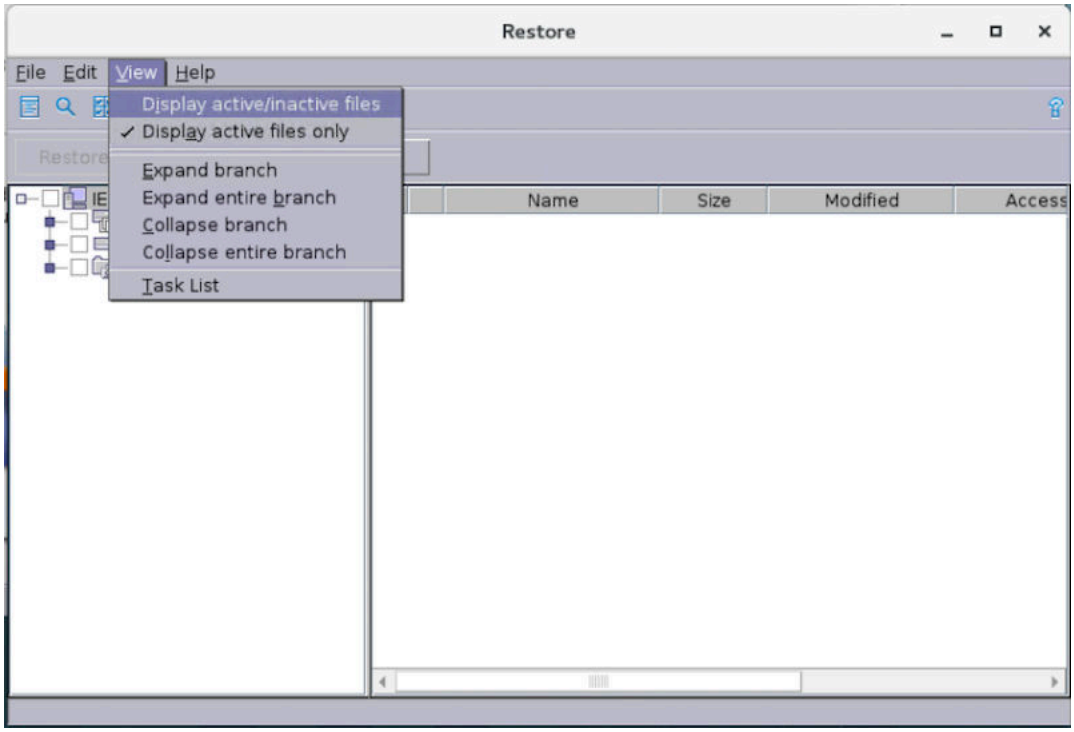
3. Under the "Restore" section, all the files and directories which have been backed up will be available to be selected for restore.



4. Select the files to be restored and click on the restore button.

Viewing and restoring multiple versions of a specific file

Spectrum Protect enables the user to restore not just the latest version of the file backup but older versions as well, if they are available in the Spectrum Protect server. In order to view the available versions, you can toggle the "Display active/inactive files" option in the "View" tab of Restore window.



The versions available in this option will not be more that 30 days old. If an older version is required, the user can use the cloud object storage to restore backup versions which are older that 30 days but not more than 365 days.

Restoring BPM Artifacts

Business Process Management contains database, WAS artifacts and BPMConfig artifacts. You can restore any of above artifacts based on your need.

BPM contains 3 databases BPMDB, CMNDB and PDWDB. Restoring approach for database is similar to MDM database machine restore scenario. Follow the same steps and restore any BPM database based on your need.

BPM contains WAS deployment manager and Node, based on your need you can restore WAS profile configuration using restoreconfig.sh provided by WAS. Follow MDM primary machine steps while restoring WAS profile configuration artifacts.

Using BPMConfig utility we are exporting Dmgr profile,in case needed , you can use BPMConfig utility to create new profiles.

Restoring Information Server Artifacts

Information server contains database and WAS artifacts. You can restore both artifacts based on your need.

IIS contains XMETA and IADB databases. Restoring approach for database is similar to MDM database machine restore scenario. Follow the same steps and restore any IIS database based on your need.

IIS contains WAS based on your need you can restore entire profile or restore profile configuration only. Follow MDM primary machine steps while restoring WAS artifacts.

Restoring ISTOOL asset

InfoSphere Information Server provides a backup utility called "ISTOOL" which enable us to backup assets related to Information Governance Catalog, Information Anaylzer etc. If these components are to be restored, restore istool related files from Spectrum Protect server using dsmj.

Follow the procedure to restore these assets from the .isx archive file

```
cd /home2/opt/IBM/InformationServer/Clients/istools/cli
import –dom <URL_IIS_MACHINE>:9443 –u isadmin –p <PASSWORD> -archive "<ISTOOL_RESTORE_PATH>/
istool.isx" -all
```

Restoring MDM Database when database is in HADR scenario

Steps while restoring MDM database.

1. Drop existing MDMDB database.
2. Restore MDMDB database.
3. Verify if database is restored.

Drop existing MDMDB database

1. Open terminal for MDM primary and secondary database machines, switch to db2inst1 user using command `su - db2inst1`
2. Using `db2adutl` command , check available full or incremental backups. Note down timestamp which you are going to restore. Once database is dropped you can't see available full or incremental backups.
3. Execute command `db2 STOP HADR ON DATABASE MDMDB` in both primary database and secondary database machine terminals.
4. Open terminal for MDM primary database machine, switch to db2inst1 user.
5. Run `db2 LIST APPLICATIONS` , to check if any applications are connected to this database.
6. Run following commands to restart and drop the database.

```
db2 stop db manager force
db2 start db manager
db2 drop db MDMDB
```

7. If you face any issues while dropping database, that means database is connected to applications, we need to close all connections to database before dropping it.

Restore MDMDB database

1. Open terminal for MDM primary database machine, switch to db2inst1 user.
2. Using `db2adutl` command , check available full or incremental backups.
3. Select full or incremental backup timestamp which needs to be restored.
4. `db2 restore db MDMDB use tsm taken at 20170526063832 ENCRYPT` 1. In above statement '20170526063832' is timestamp when the DB backup was taken. 1. "use TSM" is used which means , we are restoring a database which is stored in Spectrum Protect server. 1. "ENCRYPT" is used as existing database is db2 native encrypted. 1. While taking backup "include logs" is used , so if needed you can use "include logs" option, when there is a need to extract transaction logs needed in restore scenario.
5. Select incremental backup timestamp if you want to restore till that date.

   `db2 restore db MDMDB incremental automatic use tsm taken at 20170605134603` 1. On top of full backup , we are restoring incremental backup .
6. `db2 rollforward db MDMDB to end of logs and complete`.

   a. Used to rollforward database till end of logs.
7. Create a offline backup (db2 backup database MDMDB) in primary database machine and send it to /home/db2inst1/backup folder in secondary database machine.
8. Open terminal for MDM secondary database machine, switch to db2inst1 user. Run following commands to restart and drop the database.

```
db2 stop db manager force
db2 start db manager
db2 drop db MDMDB
```

9. Go to /home/db2inst1/backup folder, check if all backup files are available in this folder, which is copied from MDM primary database machine.
10. Run following commands to restore the database.

```
db2 restore database MDMDB encrypt
db2 update database configuration for MDMDB using LOGARCHMETH1 disk:/home/db2inst1/archive
db2 update database configuration for MDMDB using LOGINDEXBUILD ON

db2 update db cfg for MDMDB using HADR_LOCAL_HOST  <order_ID>-s/m/l-mdb2
db2 update db cfg for MDMDB using HADR_LOCAL_SVC 60666
db2 update db cfg for MDMDB using HADR_REMOTE_HOST <order_ID>-s/m/l-mdmd
db2 update db cfg for MDMDB using HADR_REMOTE_SVC 60666

db2 deactivate database MDMDB
db2 start hadr on database MDMDB as standby
```

11. Open terminal for MDM primary database machine, switch to db2inst1 user. Run following commands to start database in HADR mode.

```
db2 deactivate database MDMDB
db2 start hadr on database MDMDB as primary
```

Verify database

1. Connect to MDMDB database using following command. `db2 connect to mdmdb user mdmdbusr using <PASSWORD>`
2. Verify any table to check restore process is done and expected data is available.
3. Terminate database using command, db2 terminate
4. Verify id db2 native encryption is available.

   `db2 connect to MDMDB user db2inst1 using <PASSWORD>`

   `db2 "SELECT * FROM TABLE (SYSPROC.ADMIN_GET_ENCRYPTION_INFO())"`
5. Verify if AES is available in the output.

Restoring from Cloud Object Storage

As mentioned in the Spectrum Protect Setup, there are two Spectrum Protect Server instances. First instance is connected to local storage with the Spectrum Protect server and the second instance uses the Object Storage for storing backup.

Cloud Object storage stores backup of artifacts which are up to 365 days old. In order to restore the from the cloud object storage, follow the procedure.

Halt the first instance of the Spectrum Protect Server

Shut down the first instance of Spectrum Protect Server (tsminst1), so that the Spectrum Protect client can connect to the second instance of the Spectrum Protect server. The second instance of Spectrum Protect server is connected to the Cloud Object Storage.

1. Connect to the Operations Center. Start the command builder.
2. Execute the following commands.

```
DISABLE SESSIONS
QUERY SESSIONS
CANCEL SESSIONS
HALT
```

This stops the first server instance (tsminst1) and connects the Spectrum Protect Clients to the second server instance (tsminst2).

Change the SSL Certificate to connect to second instance of Spectrum Protect server

Certificate files of first instance of spectrum protect must be deleted so that the client machine can connect to the second instance. These files are located at the /opt/tivoli/tsm/client/ba/bin/ location of the Spectrum Protect client machine.

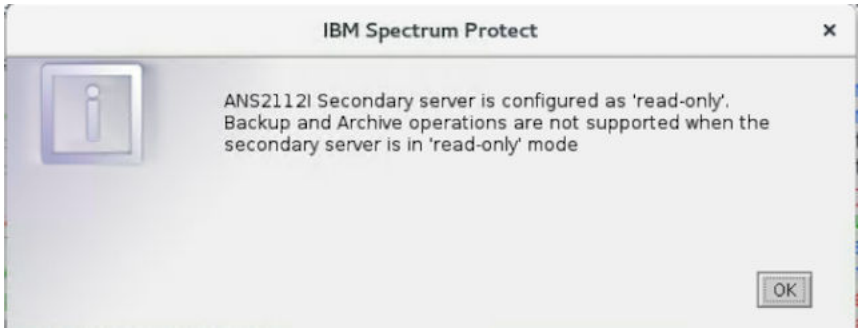
```
    dsmcert.crl
    dsmcert.kdb
    dsmcert.rdb
    dsmcert.sth
```

Rename cert256.arm file located at /opt/tivoli/tsm/client/ba/bin/ to cert256_tsminst1.arm Rename cert256_tsminst2.arm file located at /opt/tivoli/tsm/client/ba/bin/ to cert256.arm

Execute the following commands to create the ssl certificate key.

```
    cd /opt/tivoli/tsm/client/ba/bin/
    gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw
<Spectrum_Protect_Server_Password> -stash
    gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "<description>" -file /opt/
tivoli/tsm/client/ba/bin/cert256.arm -format ascii
    chmod 777 dsmcert.*
```

Use the /opt/tivoli/tsm/client/ba/bin/dsmj in the client machine to restore the required files/directories. The GUI will be opened in read only format. This implies we can only restore the files that have already been backed up.



After the restoration is completed, to revert back to the original configuration (ie. connecting back to first instance of Spectrum Protect Server), follow the procedure in the next sub-section.

Connecting back to first instance of Spectrum Protect server

The first server instance (tsminst1) has to be started to revert back to the original configuration of backup and its schedules. Execute the following commands in Spectrum Protect server.

```
    cd /bckp/opt/tivoli/tsm/server/bin/
    . /bckp/tsminst1/sqllib/db2profile
    ./dsmserv -u tsminst1 -i /bckp/tsminst1
```

The above mentioned commands starts the first server instance. Next, the SSL certificates in the Spectrum Protect client machine has to be made compliant to the first server instance.

In the Spectrum Protect client machines, execute the following steps.

1. Delete the following files in /opt/tivoli/tsm/client/ba/bin/

```
dsmcert.crl
dsmcert.kdb
dsmcert.rdb
dsmcert.sth
```

Rename cert256.arm file located at /opt/tivoli/tsm/client/ba/bin/ to cert256_tsminst2.arm Rename cert256_tsminst1.arm file located at /opt/tivoli/tsm/client/ba/bin/ to cert256.arm

1. Execute the following commands to change the ssl certificate key.

```
cd /opt/tivoli/tsm/client/ba/bin/
gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw
```

```
<Spectrum_Protect_Server_Password> -stash
gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "<description>" -file /opt/
tivoli/tsm/client/ba/bin/cert256.arm -format ascii
chmod 777 dsmcert.*
```

Verify if WebSphere Application server is restored.

1. Open terminal for MDM primary machine using mdmcloud user.
2. Go to /home/mdmcloud/IBM/WebSphere/AppServer/profiles/Dmgr01/bin `./startManager.sh`
3. Go to /home/mdmcloud/IBM/WebSphere/AppServer/profiles/AppSrv01/bin

   ./startNode.sh ./startServer.sh ClustMem1
4. Go to /home/mdmcloud/IBM/WebSphere/AppServer/profiles/proxy/bin

   ./startNode.sh ./startServer.sh proxy
5. Open terminal for MDM secondary machine using mdmcloud user.
6. Go to /home/mdmcloud/IBM/WebSphere/AppServer/profiles/Custom01/bin

   ./startNode.sh ./startServer.sh ClustMem2
7. Go to /home/mdmcloud/IBM/WebSphere/AppServer/profiles/proxy/bin

   ./startNode.sh ./startServer.sh proxy
8. Check if everything starts without any errors.

Verify if connectivity happens from WAS admin console. 1. Open Websphere admin console , https://<MDM_PRIMARY_MACHINE_IP>:9043/admin 1. Open this URL from the machine where access is provisioned. 1. Go to Resources JDBC Data sources 1. Select checkboxes before MDM data sources and press "Test Connection" button. 1. Makes sure all data sources are connecting to database without any errors.

1. Update plug-in configuration

- Open Websphere admin console , https://<MDM_PRIMARY_MACHINE_IP>:9043/admin
- Expand Environment and press "Update global Web server plug-in configuration", Press "Overwrite" and later press "ok" button.

1. Verify IVT and User Interfaces.

- Open terminal for MDM primary machine using mdmcloud user.
- Go to /home/mdmcloud/IBM/MDM/MDM115/IVT folder.
- Run verify.sh `verify.sh mdmdbusr <PASSWORD> wasadmin <PASSWORD> true /home/mdmcloud/DBCert.p12 <PASSWORD>`
- Replace PASSWORD with actual common password mentioned in welcome letter.

1. Verify SIB bus connection in MDM WAS admin console.
   a. Open MDM WAS admin console using https://<IP_ADDRESS>:9043/admin
   b. Expand "Service integration" and click "Buses". Select "MDM.SIB.CLUSTER1". Under "Topology", click "Foreign bus connections".
   c. Select "BPM.De1.Bus" and click "Test connection". Make sure connection is success.
2. In case if, SIB bus connection is not working follow these steps.

   As WAS profile is restored, you might need to exchange certificate between MDM and BPM. 1. Log into the MDM WebSphere application server administrative console using https://<IP_ADDRESS>:9043/admin 1. Expand Security and click SSL certificate and key management. Under Configuration settings, click Manage endpoint security configurations. 1. Select the appropriate outbound configuration to get to the (cell):<order_ID>-s/m/l-mdmpCell01 management scope. 1. Under Related Items, click Key stores and certificates and click the CellDefaultTrustStore key store. 1. Under Additional Properties, click "Signer certificates" and in next page click "Retrieve From Port" button. 1. In the Host field, enter

<order_ID>-s/m/l-bpmp in the host name field, enter 7286 in the Port field, and <order_ID>-s/m/l -bpmp_cert in the Alias field. 1. Click "Retrieve Signer Information" button. 1. Verify that the certificate information is for a certificate that you can trust. 1. Click Apply and Save.

After doing this, Go to BPM WAS admin console, test SIB bus connection, check if it's success. Go to MDM WAS admin console, test SIB bus connection, check if it's success. Restart WAS deployment manager, Application Server and proxy profiles and servers.

- Verify all User Interfaces.

  https://<MDM_PRIMARY_IP>:9443/CustomerBusinessAdminWeb/faces/login.jsp https://<MDM_PRIMARY_IP>:9443/inspector https://<MDM_PRIMARY_IP>:9443/accessweb https://<MDM_PRIMARY_IP>:9443/webreports

  https://<MDM_SECONDARY_IP>:9443/CustomerBusinessAdminWeb/faces/login.jsp https://<MDM_SECONDARY_IP>:9443/inspector https://<MDM_SECONDARY_IP>:9443/accessweb https://<MDM_SECONDARY_IP>:9443/webreports

- Verify all User Interfaces using proxy port, default port is 1025. Make sure this port is exposed to machine, where you are accessing these User Interfaces.

  https://<MDM_PRIMARY_IP>:1025/CustomerBusinessAdminWeb/faces/login.jsp https://<MDM_PRIMARY_IP>:1025/inspector https://<MDM_PRIMARY_IP>:1025/accessweb https://<MDM_PRIMARY_IP>:1025/webreports

  https://<MDM_SECONDARY_IP>:1025/CustomerBusinessAdminWeb/faces/login.jsp https://<MDM_SECONDARY_IP>:1025/inspector https://<MDM_SECONDARY_IP>:1025/accessweb https://<MDM_SECONDARY_IP>:1025/webreports

Stop WAS artifacts

1. Open terminal for MDM primary machine using mdmcloud user.
2. Go to /home/mdmcloud/IBM/WebSphere/AppServer/profiles/AppSrv01/bin

   ```
   ./stopServer.sh ClustMem1 -username wasadmin -password <PASSWORD> ./stopNode.sh -username wasadmin -password <PASSWORD>
   ```

3. Go to /home/mdmcloud/IBM/WebSphere/AppServer/profiles/proxy/bin

   ```
   ./stopServer.sh proxy -username wasadmin -password <PASSWORD> ./stopNode.sh -username wasadmin -password <PASSWORD>
   ```

4. Open terminal for MDM secondary machine using mdmcloud user.
5. Go to /home/mdmcloud/IBM/WebSphere/AppServer/profiles/Custom01/bin

   ```
   ./stopServer.sh ClustMem2 -username wasadmin -password <PASSWORD> ./stopNode.sh -username wasadmin -password <PASSWORD>
   ```

6. Go to /home/mdmcloud/IBM/WebSphere/AppServer/profiles/proxy/bin

   ```
   ./stopServer.sh proxy -username wasadmin -password <PASSWORD> ./stopNode.sh -username wasadmin -password <PASSWORD>
   ```

7. Open terminal for MDM primary machine using mdmcloud user.
8. Go to /home/mdmcloud/IBM/WebSphere/AppServer/profiles/Dmgr01/bin

```
./stopManager.sh -username wasadmin -password <PASSWORD>
```

Chapter 9. Administering IBM MDM on Cloud

You administer IBM® MDM on Cloud with the same utilities and tools that you use for your on-premises systems.

See Administering for detailed information about administering your system.

To encrypt DB2® database with native encryption (on production machines only) see DB2 native encryption.

Small/Medium/Large offerings

MDM Administrative UI

NON-HA :

https://< MDM Application Server Machine Public IP>:9043/ibm.console

https://< MDM Application Server Machine Public IP>:1025/CustomerBusinessAdminWeb/faces/login.jsp

https://< MDM Application Server Machine Public IP>:1025/inspector

https://< MDM Application Server Machine Public IP>:1025/webreports

https://< MDM Application Server Machine Public IP>:1025/accessweb

https://< MDM Application Server Machine Public IP>:1025/mdmconsent

HA :

https://< MDM Application Server Machine Public IP>:9043/ibm/console

https://< MDM Application Server Machine Public Portable IP>:1025/CustomerBusinessAdminWeb/faces/login.jsp

https://< MDM Application Server Machine Public Portable IP>:1025/inspector

https://< MDM Application Server Machine Public Portable IP>:1025/webreports

https://< MDM Application Server Machine Public Portable IP>:1025/accessweb

https://< MDM Application Server Machine Public Portable IP>:1025/mdmconsent

BPM

Non-HA

https://< BPM Server Machine Public IP>:9043/ibm/console

Process Server Admin UI : https://< BPM Server Machine Public IP>:9443/ProcessAdmin

Process Portal : https://< BPM Server Machine Public IP>:9443/ProcessPortal

HA

https://< BPM Server Machine Public IP>:9043/ibm/console

Process Server Admin UI : https://< BPM Server Machine Portable Public IP>:1025/ProcessAdmin

Process Portal : https://< BPM Server Machine Portable Public IP>:1025/ProcessPortal

IS Launchpad

https://< MDM IS Machine IP>:9446/ibm/console

https://< MDM IS Machine IP>:9446/ibm/iis/launchpad

Connecting to the database

You must establish a connection with the IBM® MDM on Cloud server to be able to access the MDM database.

Prerequisite: You must know the IP address or host name, port number, and credentials for the IBM MDM on Cloud server.

A database connection URL is a string that the JDBC driver uses to connect to the DB2 database in your instance of IBM MDM on Cloud. The URL contains connection information such as where to search for the database, the name of the database to connect to, and credentials.

1. Download the installation package from IBM Passport Advantage.
2. Add `ds.jar` to the CLASSPATH environment variable on your local computer. A Microsoft® Windows example:

   ```
   set CLASSPATH=ds.jar;classpath2;classpath3
   ```

3. Create the JDBC URL to connect to your IBM MDM on Cloud instance with your connection information. For example:

   ```
   jdbc:db2://169.21.34.4:50000/MYDB:user=admin;password=mypass
   ```

4. Load an IBM MDM on Cloud instance, and then create a connection by using your JDBC URL.

Changing and displaying firewall security

You can change the security level of your IBM® MDM on Cloud server by configuring the iptables firewall. On the client, you can use the netsh command from Microsoft Windows to show the firewall profile and to list open ports.

Prerequisite: You must know the credentials of a user and the IP address of the IBM MDM on Cloud client and server machines. This information is in the "Access Credentials and Initial Setup" section of the Welcome letter that you received from your IBM® Sales Representative.

When the IBM MDM on Cloud server and client are delivered, the network access to the Linux server and the Microsoft Windows client is secured.

If you need to access ports of the IBM MDM on Cloud server from your on premise instances, you must modify the iptables rules.

On the client, you can show the firewall profile, list the open ports, and close an open port.

To change the security level or to manage rules for the IBM MDM on Cloud server firewall

1. Log in to the root account of the IBM MDM on Cloud server.
2. Open a command-line window, and then type the command `sudo`.
3. Do any of following commands from the prompt.

List the rules in iptables

You can print the rules with the line numbers. This command is useful when you need to insert a rule at a specific location in iptables.

```
iptables -L --line-numbers
```

Restrict access to the server from a range of IP addresses

You can restrict access to a subnet so that only those IP addresses can use **ssh** to access your cloud server.

```
iptables -A INPUT -i eth0 -p tcp -s <ip_subnet_address> --dport 22 -m state --state
NEW,ESTABLISHED -j ACCEPT
```

where <ip_subnet_address> is the range of IP addresses in the subnet. For example, the following rule allows incoming ssh connections from only the 192.168.100.X subnet:

```
iptables –A INPUT –i eth0 –p tcp –s 192.168.100.0/24 ––dport 22 –m state ––state
NEW,ESTABLISHED –j ACCEPT
```

Restrict access to the server from a single IP address

This restriction is the most stringent.

```
iptables -A INPUT -i eth0 -p tcp -s <ip_address> --dport 22 -m state --state NEW,ESTABLISHED -j
ACCEPT
```

where <ip_address> is the single IP address that is permitted to access the server. For example, the following rule allows incoming ssh connections from a single port on 192.168.100.11:

```
iptables –A INPUT –i eth0 –p tcp –s 192.168.100.11 ––dport 22 –m state ––state NEW,ESTABLISHED –
j ACCEPT
```

Open a port from another machine

To connect to the IBM MDM on Cloud server from any other machine, you must open the MDM ports.

```
iptables -A INPUT -p tcp --dport <port_number> -j ACCEPT
```

where <port_number> is the IBM MDM on Cloud port that you want to open. For example, the following rule opens port 9446 on the server for incoming traffic from port 9446 of other machines:

```
iptables –A INPUT –p tcp ––dport 9446 –j ACCEPT
```

Add a rule at a specific line in the iptables

The order of the rules is important. Rules are appended to the end of existing rules. For example, if the rule that you added follows a DROP rule that matches incoming traffic, the DROP rule is considered before the newly added rule. You can add a rule at a specific line in the iptables to push subsequent rules down in the list.

```
iptables -I INPUT line_number -p tcp -s <ip_address> --dport 22 -j ACCEPT
```

For example, the following rule adds a rule at line 6 to accept incoming traffic on port 22 from 192.168.100.11:

```
iptables –I INPUT 6 –p tcp –s 192.168.100.11 ––dport 22 –j ACCEPT
```

Delete all rules in iptables

Important: Before you remove all rules, be sure that the default INPUT policy is ACCEPT. Otherwise, you cannot connect to the Information Server on Cloud server from anywhere.

```
iptables -F
```

To show the Microsoft Windows firewall profiles on the IBM MDM on Cloud client

1. Access the IBM MDM on Cloud client by using Microsoft Remote Desktop Connection.

2. Open a command-line window on the client.
3. Run the command `netsh advfirewall show allprofiles`.

To show a list of all open ports on the IBM MDM on Cloud client

1. Access the IBM MDM on Cloud client by using Microsoft Remote Desktop Connection.
2. On the client, click **Start > Administrative Tools > Server Manager**.
3. In the upper-right corner of the Server Manager window, click **Tools**. From the list, select **Windows Firewall with Advanced Security**.
4. In the left pane, click **Inbound Rules** to see which ports are open for incoming network traffic.

To block an open port on the IBM MDM on Cloud client

Do the previous task. Right-click the port number, and then select the appropriate action.

Managing LUKS keys on the server machine

Any partition that is encrypted by using Linux Unified Key Setup (LUKS) can have eight different keys. You can use any of the keys to open the encrypted partition. In addition, you can add new keys or remove existing ones according to your needs.

Prerequisite: You must know the credentials of the root user and the IP address of the IBM® MDM on Cloud server machine. This information is in the "Access Credentials and Initial Setup" section of the Welcome letter that you received from your IBM Sales Representative.

One LUKS key is specified in the "Encryption Details" section of the Welcome letter that you received from your IBM Sales Representative. This key file is used from `/etc/crypttab` file to unlock the partition when the IBM MDM on Cloud server reboots. For details about encrypted partitions on the IBM MDM on Cloud server, see Disk partitions and encryption.

Procedure

1. On the IBM MDM on Cloud server, open a command-line window.
2. Do any of the following tasks to manage your keys. The commands can be run from any directory.

Add new LUKS key

```
cryptsetup luksAddKey <partition_name>
```

The parameter `<partition_name>` is the partition that is encrypted.

For example, the partition for virtual servers is `/dev/xvdc1`. For bare metal servers, the partition is `/dev/sda5`.

Type in the existing key that is given in the Welcome letter. When prompted, enter the name of the new key.

Remove existing LUKS keys

```
cryptsetup luksRemoveKey <partition_name>
```

When prompted, enter the name of the specific key that you want to remove.

Add a key from a file

```
cryptsetup luksRemoveKey <partition_name> <keyfile_name>
```

The parameter `<keyfile_name>` must include the full file path of the file.

The command asks for an existing key and then reads the new key from the file.

Chapter 10. Security compliance: HIPAA

MDM on Cloud, when hosted on IBM SoftLayer, meets the required IBM controls that are commensurate with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security and Privacy Rule requirements. The controls include appropriate administrative, physical, and technical safeguards required of Business Associates in 45 CFR Part 160 and Subparts A and C of Part 164.

For information about how to order a HIPAA-ready MDM on Cloud system, contact your IBM Cloud Data Services sales representative.

Notices

Notices

This information was developed for products and services offered in the U.S.A.

IBM® may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Privacy Policy Considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session and persistent cookies that collect each user’s name, user name, password, profile name, or other personally identifiable information for purposes of session management, authentication, enhanced user usability, single sign-on configuration, or web page identification that the user tried to load prior to login. These cookies can be disabled, but disabling them will also likely eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek

your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at www.ibm.com/privacy and IBM's Online Privacy Statement at www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at www.ibm.com/software/info/product-privacy.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

The following terms are trademarks or registered trademarks of other companies:

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.