IBM Master Data Management Collaborative Edition on Cloud User Guide
Version 1 Release 1

User Guide
(Last udpated: 2018-06-18)

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 1, modification 0 of IBM Master Data Management Collaborative Edition on Cloud User Guide and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. About IBM Master Data Management Collaborative Edition (MDM CE) on Cloud

IBM® InfoSphere® Master Data Management Collaboration Server - Collaborative Edition on Cloud for Bluemix® offers the rich features of an on-premises InfoSphere Master Data Management Collaboration Server - Collaborative Edition deployment without the cost, complexity, and risk of managing your own infrastructure. IBM InfoSphere Master Data Management Collaboration Server - Collaborative Edition provides pre-installed InfoSphere Master Data Management Collaboration Server - Collaborative Edition configurations for production and development environments in an IBM SoftLayer® cloud-hosted environment.

Chapter 2. Overview of IBM MDM CE on Cloud

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

IBM MDM CE on Cloud is a multi-domain solution that comes pre-installed and ready to run in small, medium, and large server configuration. IBM MDM CE on Cloud provides a cost-effective entry point to InfoSphere MDM CE and a path to easily add new environments. It supports the following use cases:

- Quickly deploy development or test environments for new InfoSphere MDM CE projects.
- Move all or part of your InfoSphere MDM CE 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 CE 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 CE 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 CE on Cloud services, you must:

- Actively monitor and report any issues that you encounter with IBM MDM CE on Cloud
- Maintain the software platform, InfoSphere MDM CE 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 CE on Cloud.

- Provide user access to IBM MDM CE 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 CE on Cloud environment and operating system.
- Create and maintain regular backups of data.
- Setup and manage the encryption of IBM MDM CE on Cloud according to your security policy and the service terms.

Default Values for MDM CE on cloud instances

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

Application Language

The default MDM CE Application language is English.

Time Zone

IBM MDM CE 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.

Company

By default, the MDM CE Application comes with the default company Trigo.

To create new company:

1. Go to MDM Install location

   /home/wasadmin/11.6/MDM
2. Run the script

   ./preSetup.sh
3. Stop all Services

   ./bin/go/stop_local.sh
4. Stop WebSphere Application Server Cluster.

   ```
   Refer to section IBM MDM CE on Cloud Administration -> WebSphere Application Server -> Stoping WebSphere
   Application Server
   ```
5. Run script to create new Company

   ./bin/db/create_cmp.sh
6. Start All Services

   ./bin/go/start_local.sh
7. Start WebSphere Application Server Cluster.

   ```
   Refer to section IBM MDM CE on Cloud Administration -> WebSphere Application Server -> Starting WebSphere
   Application Server
   ```

Chapter 3. IBM MDM CE on Cloud High Availability Plans

IBM MDM CE on cloud offering comes with preinstalled MDM CE HA configurations for Production and Staging MDM CE environments, along with standalone deployment environment for Dev and QA, all in easy to select size of Small, Medium, and Large configurations required to manage a line of business through to enterprise application.

MDM CE in HA Architecture

This section describes the high availability features supported.

Technologies and Concepts

The technologies used in MDM CE high availability: **Pacemaker** This component detects machine heartbeat and does cluster management. Portable IP is assigned by the pacemaker to do available machine. Pacemaker status can be found by running the command

```
Ubuntu:
   crm status
```

Portable IP A special IP provided by Softlayer which is portable across machines. It will be assigned by Pacemaker to available machines. The enduser should use the portable IP for accessing UI applications.

HADR This DB Component helps in configuring data replication across multiple database servers.

HA Topology

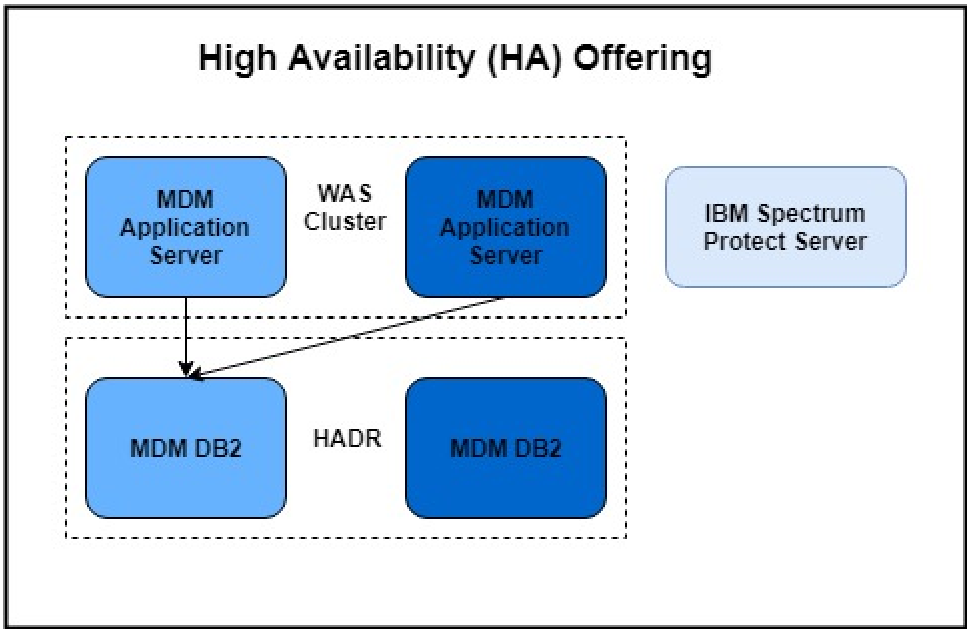


Figure 1: HA Topology

MDM HA Topology

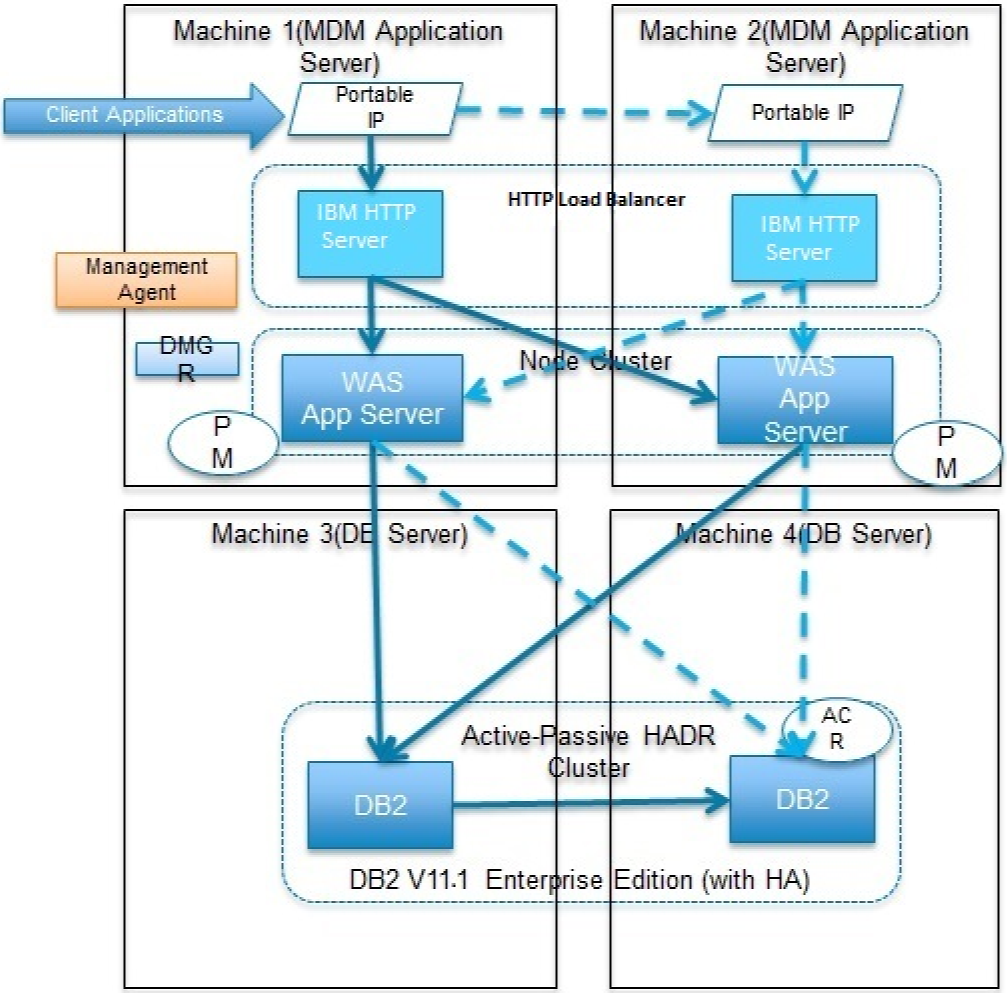


Figure 2: MDM HA Topology

Plans

IBM Master Data Management Collaborative Edition on Cloud Small

IBM Master Data Management Collaborative Edition on Cloud Medium

IBM Master Data Management Collaborative Edition on Cloud Large

IBM Master Data Management Collaborative Edition on Cloud Small

Production MDM CE Environment

All plans support Backup Infrastructure for production offerings. The production offerings include four machines with the following software:

- A primary MDM CE virtual machine with:
  - IBM MDM CE Edition
  - WebSphere Application Server Network Deployment V 9.0.0.0 (Deployment Manager & Node)
  - IBM Spectrum Protect Client v 8.1.4
- A secondary InfoSphere MDM CE virtual machine with:
  - IBM MDM CE Edition
  - WebSphere Application Server Network Deployment V 9.0.0.0 (Node)
  - IBM Spectrum Protect Client v 8.1.4
- A VM with MDM CE Database
  - IBM DB2 v 11.1
  - No HA for DB2 in-case of Small Tee Shirt offering
  - IBM Spectrum Protect Client v 8.1.4
- A backup infrastructure machine
  - IBM Spectrum Protect Server v 8.1.3

Host Names

Machine	Hostname
MDM CE primary operational server	`<orderID>-mdmce-mdmp.ibm.com`
MDM CE secondary operational server	`<orderID>-mdmce-mdms.ibm.com`
MDM CE Database Server	`<orderID>-mdmce-db2p.ibm.com`
Backup Server	`<orderID>-mdmce-backup.ibm.com`

Specifications

Machine	Hardware	Software
MDM CE primary/secondary operational server	2 nodes, 4 cores per node, 16GB memory per node, 2 disks 100GB + 200GB SAN Disk Virtual Machines and 100GB Shared Storage with rate 4 IOPS/GB	IBM MDM Collaborative Edition and IBM WebSphere Application Server
MDM CE Database Server	1 node, 4 cores per node, 16GB memory per node, 2 disks 100GB + 400GB SAN Disk Virtual Machine	IBM DB2 Enterprise Edition v11.1
Backup Server	1 node, 8 cores per node, 64GB memory per node, 100GB + 4TB SAN disk + 1TB Performance(4000 IOPS)	IBM Spectrum Protect Server, IBM DB2

Related Topics

- Common Specifications

Staging MDM Environment

The Staging environment is an exact clone of Production environment but with no backup server.

Host Names

Machine	Hostname
MDM CE primary operational server	`<orderID>-stage-mdmce-mdmp.ibm.com`
MDM CE secondary operational server	`<orderID>-stage-mdmce-mdms.ibm.com`
MDM CE Database Server	`<orderID>-stage-mdmce-db2p.ibm.com`

Specifications

Machine	Hardware	Software
MDM CE primary/secondary operational server	2 nodes, 4 cores per node, 16GB memory per node, 2 disks 100GB + 200GB SAN Disk Virtual Machines and 100GB Shared Storage with rate 4 IOPS/GB	IBM MDM Collaborative Edition and IBM WebSphere Application Server
MDM CE Database	1 node, 4 cores per node, 16GB memory per node, 2 disks 100GB + 400GB SAN Disk Virtual Machine	IBM DB2 Enterprise Edition v11.1

Related Topics

- Common Specifications

QA MDM Environment

The QA offering included one machine with a standalone deployment of IBM MDM Collaborative Edition.

Host Names

Machine	Hostname
MDM CE QA server	<orderID>-mdmce-qa.ibm.com

Specifications

Machine	Hardware	Software
MDM CE QA	1 node, 4 cores per node, 16GB memory per node, 2 disks 100GB + 300GB SAN Disk Virtual Machine	IBM MDM Collaborative Edition, IBM WebSphere Application Server, IBM DB2 EE v11.1

Related Topics

- Common Specifications

DEV MDM Environment

The DEV offering included one machine with a standalone deployment of IBM MDM Collaborative Edition.

Host Names

Machine	Hostname
MDM CE DEV Server	<orderID>-mdmce-dev.ibm.com

Specifications

Machine	Hardware	Software
MDM CE DEV	1 node, 4 cores per node, 16GB memory per node, 2 disks 100GB + 300GB SAN Disk Virtual Machine	IBM MDM Collaborative Edition, IBM WebSphere Application Server, IBM DB2 EE v11.1

IBM Master Data Management Collaborative Edition on Cloud Medium

Production MDM CE Environment

All plans support Backup Infrastructure for production offerings. The production offerings include five machines with the following software:

- A primary MDM CE virtual machine with:
  - IBM MDM CE Edition
  - WebSphere Application Server Network Deployment V 9.0.0.0 (Deployment Manager & Node)
  - IBM Spectrum Protect Client v 8.1.4
- A secondary InfoSphere MDM CE virtual machine with:
  - IBM MDM CE Edition
  - WebSphere Application Server Network Deployment V 9.0.0.0 (Node)
  - IBM Spectrum Protect Client v 8.1.4
- Two VM with MDM CE Database
  - IBM DB2 v 11.1
  - HA Configuration in Active – Passive mode
  - IBM Spectrum Protect Client v 8.1.4
- A backup infrastructure machine
  - IBM Spectrum Protect Server v 8.1.3

Host Names

Machine	Hostname
MDM CE primary operational server	`<orderID>-mdmce-mdmp.ibm.com`
MDM CE secondary operational server	`<orderID>-mdmce-mdms.ibm.com`
MDM CE Database Server	`<orderID>-mdmce-db2p.ibm.com`
MDM CE Database Server	`<orderID>-mdmce-db2s.ibm.com`
Backup Server	`<orderID>-mdmce-backup.ibm.com`

Specifications

Machine	Hardware	Software
MDM CE primary/secondary operational server	2 nodes, 8 cores per node, 32GB memory per node, 2 disks 100GB + 300GB SAN Disk Virtual Machines and 100GB Shared Storage with rate 4 IOPS/GB	IBM MDM Collaborative Edition and IBM WebSphere Application Server

Machine	Hardware	Software
MDM CE Database Server	2 nodes, 8 cores per node, 32GB memory per node, 2 disks 100GB + 750GB SAN Disk Virtual Machine	IBM DB2 Enterprise Edition v11.1
Backup Server	1 node, 8 cores per node, 64GB memory per node, 100GB + 8TB SAN disk + 1TB Performance(6000 IOPS)	IBM Spectrum Protect Server, IBM DB2

Related Topics

- Common Specifications

Staging MDM Environment

The Staging environment is an exact clone of Production environment but with no backup server.

Host Names

Machine	Hostname
MDM CE primary operational server	`<orderID>-stage-mdmce-mdmp.ibm.com`
MDM CE secondary operational server	`<orderID>-stage-mdmce-mdms.ibm.com`
MDM CE Database Primary Server	`<orderID>-stage-mdmce-db2p.ibm.com`
MDM CE Database Standby Server	`<orderID>-stage-mdmce-db2s.ibm.com`

Specifications

Machine	Hardware	Software
MDM CE primary/secondary operational server	2 nodes, 8 cores per node, 32GB memory per node, 2 disks 100GB + 300GB SAN Disk Virtual Machines and 100GB Shared Storage with rate 4 IOPS/GB	IBM MDM Collaborative Edition and IBM WebSphere Application Server
MDM CE Database Server	2 nodes, 8 cores per node, 32GB memory per node, 2 disks 100GB + 750GB SAN Disk Virtual Machine	IBM DB2 Enterprise Edition v11.1

Related Topics

- Common Specifications

QA MDM Environment

The QA offering included one machine with a standalone deployment of IBM MDM Collaborative Edition.

Host Names

Machine	Hostname
MDM CE QA Server	<orderID>-mdmce-qa.inm.com

Specifications

Machine	Hardware	Software
MDM CE QA	1 node, 8 cores per node, 16GB memory per node, 2 disks 100GB + 400GB SAN Disk Virtual Machine	IBM MDM Collaborative Edition, IBM WebSphere Application Server, IBM DB2 EE v11.1

Related Topics

- Common Specifications

DEV MDM Environment

The DEV offering included one machine with a standalone deployment of IBM MDM Collaborative Edition.

Host Names

Machine	Hostname
MDM CE DEV Server	<orderID>-mdmce-dev.ibm.com

Specifications

Machine	Hardware	Software
MDM CE DEV	1 node, 8 cores per node, 16GB memory per node, 2 disks 100GB + 400GB SAN Disk Virtual Machine	IBM MDM Collaborative Edition, IBM WebSphere Application Server, IBM DB2 EE v11.1

IBM Master Data Management Collaborative Edition on Cloud Large

Production MDM CE Environment

All plans support Backup Infrastructure for production offerings. The production offerings include six machines with the following software:

- A primary MDM CE virtual machine with:
  - IBM MDM CE Edition
  - WebSphere Application Server Network Deployment V 9.0.0.0 (Deployment Manager & Node)
  - IBM Spectrum Protect Client v 8.1.4
- A secondary InfoSphere MDM CE virtual machine with:
  - IBM MDM CE Edition
  - WebSphere Application Server Network Deployment V 9.0.0.0 (Node)
  - IBM Spectrum Protect Client v 8.1.4
- A tertiary InfoSphere MDM CE virtual machine with:
  - IBM MDM CE Edition
  - WebSphere Application Server Network Deployment V 9.0.0.0 (Node)
  - IBM Spectrum Protect Client v 8.1.4
- Two VM with MDM CE Database
  - IBM DB2 v 11.1
  - HA Configuration in Active – Passive mode

  - IBM Spectrum Protect Client v 8.1.4
- A backup infrastructure machine
  - IBM Spectrum Protect Server v 8.1.3

Host Names

Machine	Hostname
MDM CE primary operational server	`<orderID>-mdmce-mdmp.ibm.com`
MDM CE secondary operational server	`<orderID>-mdmce-mdms.ibm.com`
MDM CE tertiary operational server	`<orderID>-mdmce-mdmt.ibm.com`
MDM CE Database Server	`<orderID>-mdmce-db2p.ibm.com`
MDM CE Database Server	`<orderID>-mdmce-db2s.ibm.com`
Backup Server	`<orderID>-mdmce-backup.ibm.com`

Specifications

Machine	Hardware	Software
MDM CE primary/secondary/ tertiary operational server	3 nodes, 16 cores per node, 64GB memory per node, 2 disks 100GB + 500GB SAN Disk Virtual Machines and 250GB Shared Storage with rate 4 IOPS/GB	IBM MDM Collaborative Edition and IBM WebSphere Application Server
MDM CE Database Server	2 nodes, 16 cores per node, 64GB memory per node, 2 disks 100GB + 1TB SAN Disk Virtual Machine	IBM DB2 Enterprise Edition v11.1
Backup Server	1 node, 8 cores per node, 64GB memory per node, 100GB + 16TB SAN disk + 1TB Performance(6000 IOPS)	IBM Spectrum Protect Server, IBM DB2

Related Topics

- Common Specifications

Staging MDM Environment

The Staging environment is an exact clone of Production environment but with no backup server.

Host Names

Machine	Hostname
MDM CE primary operational server	`<orderID>-stage-mdmce-mdmp.ibm.com`
MDM CE secondary operational server	`<orderID>-stage-mdmce-mdms.ibm.com`
MDM CE tertiary operational server	`<orderID>-stage-mdmce-mdmt.ibm.com`
MDM CE Database Primary Server	`<orderID>-stage-mdmce-db2p.ibm.com`
MDM CE Database Standby Server	`<orderID>-stage-mdmce-db2s.ibm.com`

Specifications

Machine	Hardware	Software
MDM CE primary/secondary/ tertiary operational server	3 nodes, 16 cores per node, 64GB memory per node, 2 disks 100GB + 500GB SAN Disk Virtual Machines and 250GB Shared Storage with rate 4 IOPS/GB	IBM MDM Collaborative Edition and IBM WebSphere Application Server
MDM CE Database Server	2 nodes, 16 cores per node, 64GB memory per node, 2 disks 100GB + 1TB SAN Disk Virtual Machine	IBM DB2 Enterprise Edition v11.1

Related Topics

- Common Specifications

QA MDM Environment

The QA offering included one machine with a standalone deployment of IBM MDM Collaborative Edition.

Host Names

Machine	Hostname
MDM CE QA Server	<orderID>-mdmce-qa.persistent.com

Specifications

Machine	Hardware	Software
MDM CE QA	1 node, 16 cores per node, 32GB memory per node, 2 disks 100GB + 750GB SAN Disk Virtual Machine	IBM MDM Collaborative Edition, IBM WebSphere Application Server, IBM DB2 EE v11.1

Related Topics

- Common Specifications

DEV MDM Environment

The DEV offering included one machine with a standalone deployment of IBM MDM Collaborative Edition.

Host Names

Machine	Hostname
MDM CE DEV Server	<orderID>-mdmce-dev.persistent.com

Specifications

Machine	Hardware	Software
MDM CE DEV	1 node, 16 cores per node, 32GB memory per node, 2 disks 100GB + 750GB SAN Disk Virtual Machine	IBM MDM Collaborative Edition, IBM WebSphere Application Server, IBM DB2 EE v11.1

Common Specifications

Security

Users

Machine	SSH Users	Application Users
MDM primary/secondary/tertiary Server	{orderId}sshuser	db2inst1, wasadmin
DB2 primary/standby Server	{orderId}sshuser	db2inst1, db2fenc1, dbadmin
Backup Server	{orderId}sshuser	tsminst, tsminst1, tsminst2
DEV/QA	{orderId}sshuser	db2inst1,db2fenc1,dbadmin,was admin

Note: root user is disabled by default

Encryption

Machine	Encryption Type	Location	Keys Location
MDM Primay/ Secondary/Tertiary Server	Disk	/home	/keys/keyfile
DB2 Primary/Standby Server	Disk	/home	/keys/keyfile
DB2 Primary/Standby Server	Native		/home/db2inst1/keys/ db2keystore.p12
Backup Server	DISK	/home, /mnt1, /mnt2, / mnt3, /mnt4	/keys/keyfile
DEV/QA	Disk	/home	/keys/keyfile

Chapter 4. IBM MDM CE on Cloud Administration

Use this guide for administration of IBM MDM CE on Cloud.

DEV and QA instances are standalone deployments. The guide below explains administration for clustered deployment. Same is also applicable for DEV and QA instances.

First Steps

Logging into the machines for first time

MDM(Production and Staging), DB2(Production and Staging), DEV, QA Machines

1. Once the VPN tunnel is set, SSH into each machine using credentials for user *{orderId}sshuser*.
2. Change the password of the user.
3. su to user *dbadmin* and change the password.
4. su to user *wasadmin* and change the password.

Note: root user has been disabled by default. User *{orderId}sshuser* has sudo privileges.

WebSphere Application Server

The Production and Staging environment comes with WebSphere Application Server(WAS) configuration for High Availability whereas DEV and QA environment is standalone deployment. The WebSphere Application cluster runs on the each node. Each primary operational server hosts the Deployment Manager(dmgr) as well as a cluster node.

WAS is installed with the user *wasadmin* at the location:

```
/home/wasadmin/IBM/WebSphere/AppServer
```

Application Server logs directory:

```
/home/wasadmin/IBM/WebSphere/profiles/wasnode_{machine hostname}/logs/MDM_{machine hostname}
```

Starting WebSphere Application Server

1. First start DMGR by running script on MDM CE primary operational server:

   /home/wasadmin/IBM/WebSphere/AppServer/profiles/cellmanager01/bin/startManager.sh
2. Once DMGR is started, Start each WAS node by running this script on all MDM CE machines:

   /home/wasadmin/IBM/WebSphere/AppServer/profiles/wasnode_{machine hostname}/bin/startNode.sh
3. After starting all cluster nodes, open the WAS console in browser at:

   https://<ip of primary operational server>:9043/ibm/console
4. Login with the credentials for user *wasadmin*.
5. In the left pane of WAS UI, expand Servers tab, expand clusters and do following:
   a. Select WebSphere Application Server clusters.
   b. Issue *Start* on *wascluster*.

Stoping WebSphere Application Server

1. Open the WAS console in browser at:

   https://<ip of primary operational server>:9043/ibm/console
2. In the left pane of WAS UI, expand Servers tab, expand clusters and do following:
   a. Select WebSphere Application Server clusters.
   b. Issue *Stop* on *wascluster*.

IBM HTTP Server (IHS)

The Production and Staging environment comes with IBM HTTP Server. The server acts as a front-end and load balancer to the client request. All the client request are intelligently routed among the WebSphere Application Server in a WAS cluster. IHS is installed across all nodes in a cluster.

IBM HTTP Server is installed with the user *wasadmin* at the location:

```
/home/wasadmin/IBM/WebSphere/HTTPServer
```

HTTP Server logs directory:

```
/home/wasadmin/IBM/WebSphere/HTTPServer/logs/access_log
/home/wasadmin/IBM/WebSphere/HTTPServer/logs/error_log
```

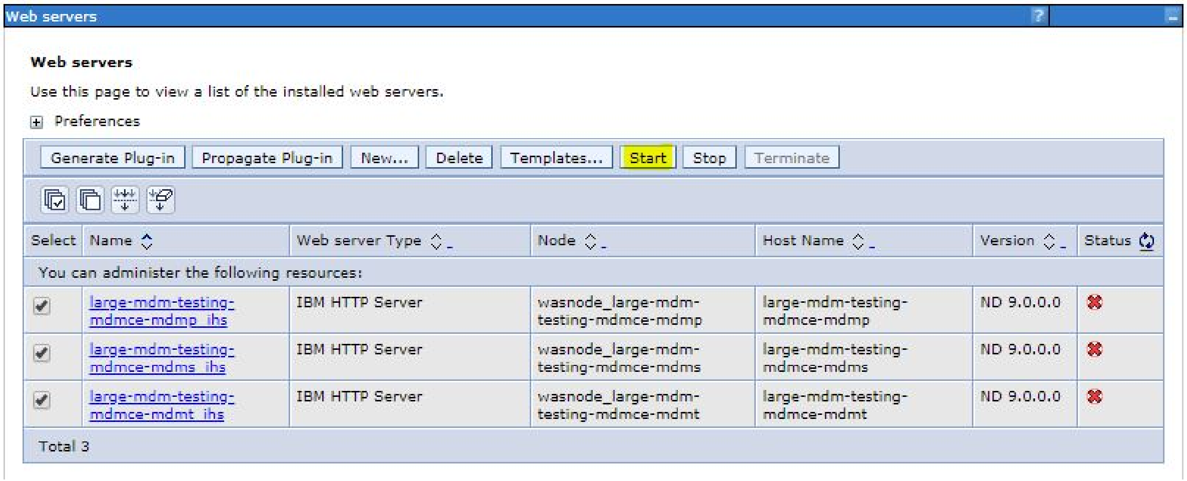
Starting IBM HTTP Server

Once DMGR is started.

1. Open the WAS administration console at:

```
https://<ip of primary operational server>:9043/ibm/console
```

2. Login with the credentials for user *wasadmin*.
3. In the left pane of WAS UI, expand **Servers** tab, expand **Server Types** and do following:
   a. Select *Web Servers*
   b. Check all the server from the right-hand side section.



Web servers

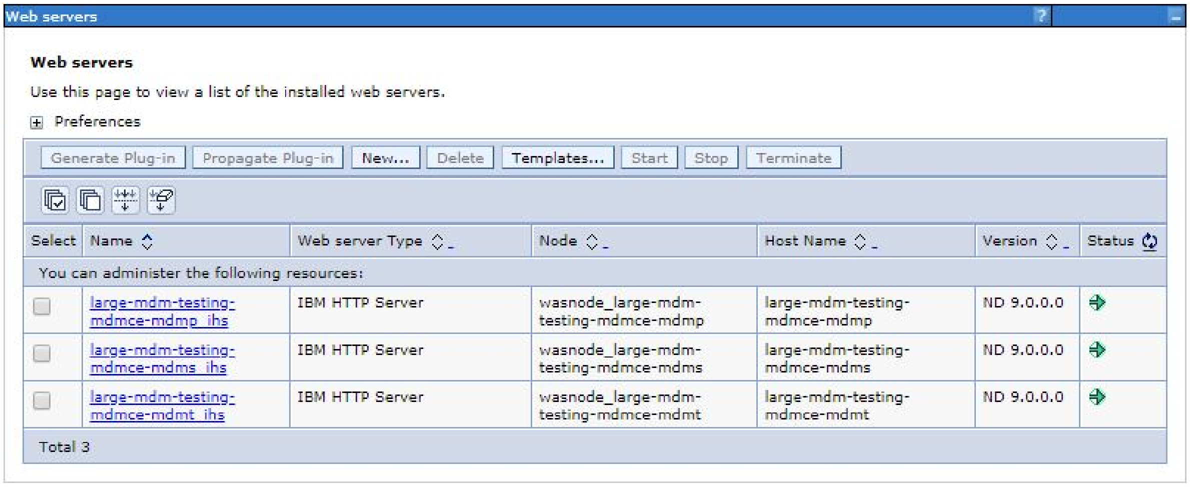
Use this page to view a list of the installed web servers.

⊞ Preferences

Select	Name	Web server Type	Node	Host Name	Version	Status
You can administer the following resources:						
☑	large-mdm-testing-mdmce-mdmp_ihs	IBM HTTP Server	wasnode_large-mdm-testing-mdmce-mdmp	large-mdm-testing-mdmce-mdmp	ND 9.0.0.0	✖
☑	large-mdm-testing-mdmce-mdms_ihs	IBM HTTP Server	wasnode_large-mdm-testing-mdmce-mdms	large-mdm-testing-mdmce-mdms	ND 9.0.0.0	✖
☑	large-mdm-testing-mdmce-mdmt_ihs	IBM HTTP Server	wasnode_large-mdm-testing-mdmce-mdmt	large-mdm-testing-mdmce-mdmt	ND 9.0.0.0	✖
Total 3						

Figure 3: Web Server Stop

   c. Click on the *Start* button from the right-hand side section.



Web servers

Use this page to view a list of the installed web servers.

⊞ Preferences

Select	Name	Web server Type	Node	Host Name	Version	Status
You can administer the following resources:						
□	large-mdm-testing-mdmce-mdmp_ihs	IBM HTTP Server	wasnode_large-mdm-testing-mdmce-mdmp	large-mdm-testing-mdmce-mdmp	ND 9.0.0.0	➔
□	large-mdm-testing-mdmce-mdms_ihs	IBM HTTP Server	wasnode_large-mdm-testing-mdmce-mdms	large-mdm-testing-mdmce-mdms	ND 9.0.0.0	➔
□	large-mdm-testing-mdmce-mdmt_ihs	IBM HTTP Server	wasnode_large-mdm-testing-mdmce-mdmt	large-mdm-testing-mdmce-mdmt	ND 9.0.0.0	➔
Total 3						

Figure 4: Web Server Start

MDM CE Application

MDM CE Application is installed with user *wasadmin* at the location:

```
$TOP=/home/wasadmin/11.6/MDM
```

MDM CE Application uses shared network storage to synchronize files across nodes. The mount address could be found in the welcome letter provided. This storage should be mounted at mount point:

```
/mdmnfs
```

Before starting Application and its Services, ensure this storage is mounted and accessible. To mount shared storage use command:

```
mount {mountAddress} /mdmnfs
```

Note: This shared storage could be mounted only on MDM CE operational servers.

Start/Stop Application Services

Follow these steps to Start Application Services:

1. su to user *wasadmin*.
2. Change directory to $TOP.
3. Run *source preSetup.sh*
4. Run script *$TOP/bin/go/start_local.sh*.

To Stop MDM CE Services

1. su to user *wasadmin*.
2. Change directory to $TOP.
3. Run *source preSetup.sh*
4. Run script *$TOP/bin/go/stop_local.sh*.

The MDM CE Application offers 2 different UIs and it could be accessed over below URLs:

Old UI:

```
https://{mdmce portable ip}:5061/
```

New UI:

```
https://{mdmce portable ip}:5061/mdm_ce_ui
```

Portable IP

A special IP provided by SoftLayer which is portable across the machines. MDM CE machines are assigned a portable IP using Pacemaker. Pacemaker detects machine heartbeat and assigns IP to one of the VMs in its cluster.

View pacemaker cluster

```
pcs resource show mdmcecluster
```

Check status of the cluster

```
crm status
```

Manual switching of Portable IP

To switch portable IP manually across machines, restart pacemaker service on the machine it is currently assigned to.

```
service pacemaker stop
service pacemaker start
```

Pacemaker will automatically switch the portable IP to one of the machines available in its cluster.

DB2

MDM CE Application connects to DB2 v11.1 EE which is setup in HADR mode (Except for Small Plan where DB2 runs in standalone mode).

The DB2 HADR for MDM CE comprises of 2 DB2 instances running as Primary and Standby. At a time, application always connects to the primary instance.

Managing DB2 HADR

Starting DB2 in HADR mode

SSH into both DB2 machines and follow steps below:

1. su to user *db2inst1*.
2. Run *db2start* to start the Database Manager on both the machines.
3. Verify if DBs are in **CONNECTED** sate:

   db2pd -hadr -db PIMDB

DB2 Failure Management

The DB2 machines in HADR run in Active/Passive mode. In case of failure, the DB2 instance has to be switched manually for Standby to become Primary.

Follow these steps for switchover:

1. SSH into DB2 standby machine and switch to user *db2inst1*
2. Issue command

   DB2 TAKEOVER HADR ON DB PIMDB
3. In case above command fails issue:

   DB2 TAKEOVER HADR ON DB PIMDB BY FORCE

4. Verify the status of Portable and make a manual switchover if the Portable IP still points to failed DB2 node.

** Portable IP Status**

```
    crm status
```

Refer Section Manual switching of Portable IP described above.

LUKS Keys Management

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.

One LUKS key is specified in the Specifications section of Chapter 3. This key file is used from /etc/crypttab file to unlock the partition when the IBM MDM CE 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 -d <keyfile_path> luksAddKey <partition_name>
```

The parameter <partition_name> is the partition that is encrypted. For example, the partition for virtual servers is /dev/xvdc. The parameter <keyfile_path> is the absolute path of current key file.

Type in the existing key. When prompted, enter the name of the new key.

Remove existing LUKS keys

```
cryptsetup  -d <keyfile_path> luksRemoveKey <partition_name>
```

When prompted, enter the name of the specific key that you want to remove.

Add a key from a file

```
cryptsetup  -d <keyfile_path> 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.

Backup Server

MDM CE on Cloud provides software and hardware infrastructure for taking backups. Backup capability is based on IBM Spectrum Protect version 8.1.3 product. One dedicated server machine with an installation of IBM Spectrum Protect server version 8.1.3 is provided with each deployment of MDM CE on Cloud. Spectrum Protect Server version used is 8.1.3 and Spectrum Protect Client, CMS version used is 8.1.4.

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 Server Setup

Two instances of IBM Spectrum Protect server are configured on a dedicated machine for each deployment of MDM CE on Cloud. 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.

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. IBM Spectrum Protect manages the credentials, security, read and write I/Os, and the life-cycle 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. To understand check encryption configurations for details. Like Directory Container Storage Pool, policy domain configurations are created for all Client machines, these domains are linked with Cloud Container Storage pool.

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.

Getting started with IBM Spectrum Protect Operations Center console

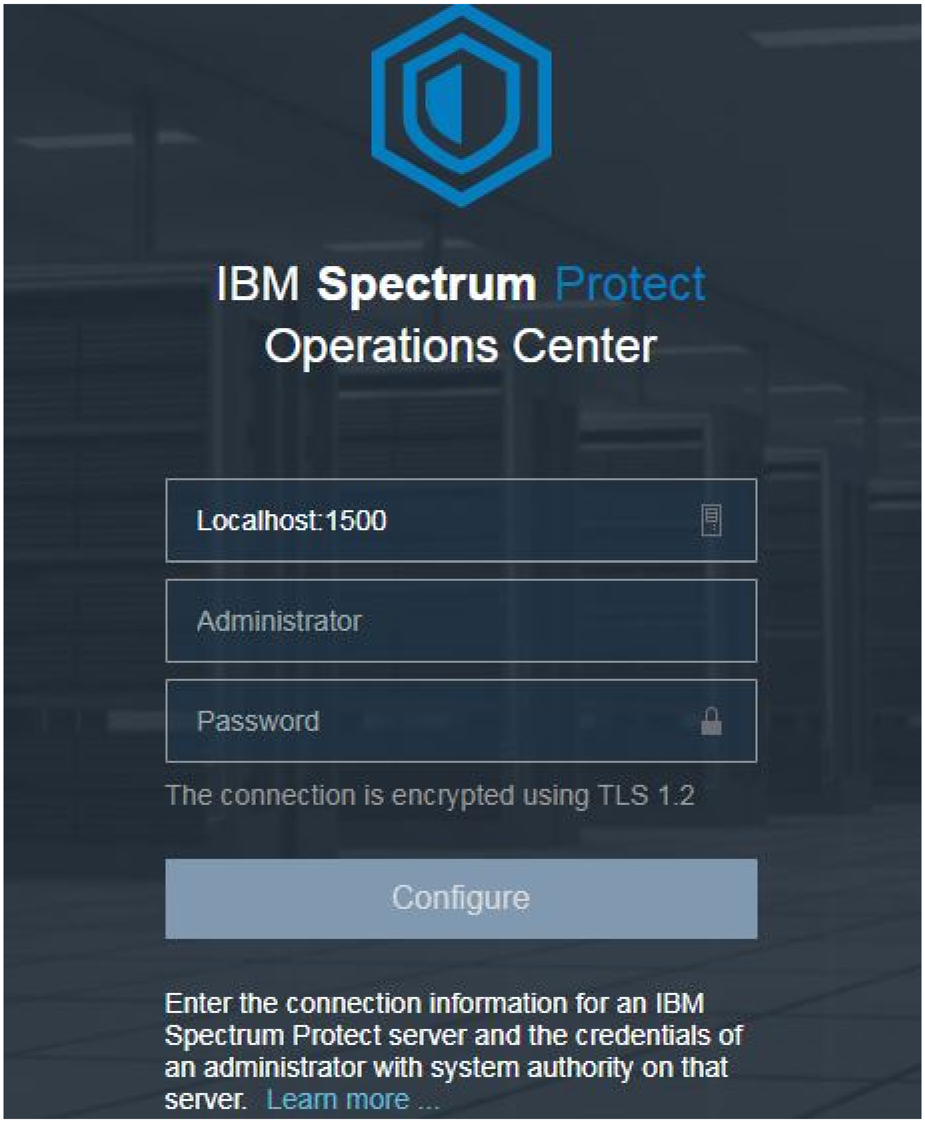
IBM Spectrum Protect provides a web application called Operations Center for managing IBM Spectrum Protect environment. You can use the Operations Center to monitor multiple servers and to complete some administrative tasks. The Operations Center also provides web access to the IBM Spectrum Protect command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

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
   ```



IBM Spectrum Protect
Operations Center

Localhost:1500

Administrator

Password

The connection is encrypted using TLS 1.2

Enter the connection information for an IBM Spectrum Protect server and the credentials of an administrator with system authority on that server. Learn more ...

Figure 5: Spectum Protect Login

1. When you open Operations Console for the first time, it will ask for credentials.
2. Replace default details with correct values.

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

3. In the next page, you will be asked to provide password (two times) for "Administrator ID". Provide password.
4. 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.

5. 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

Operation Center console provides Command Builder tool, to run administrative command. 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. Since 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 from the drop down menu, if you need to execute any commands against the second instance of Spectrum protect server.

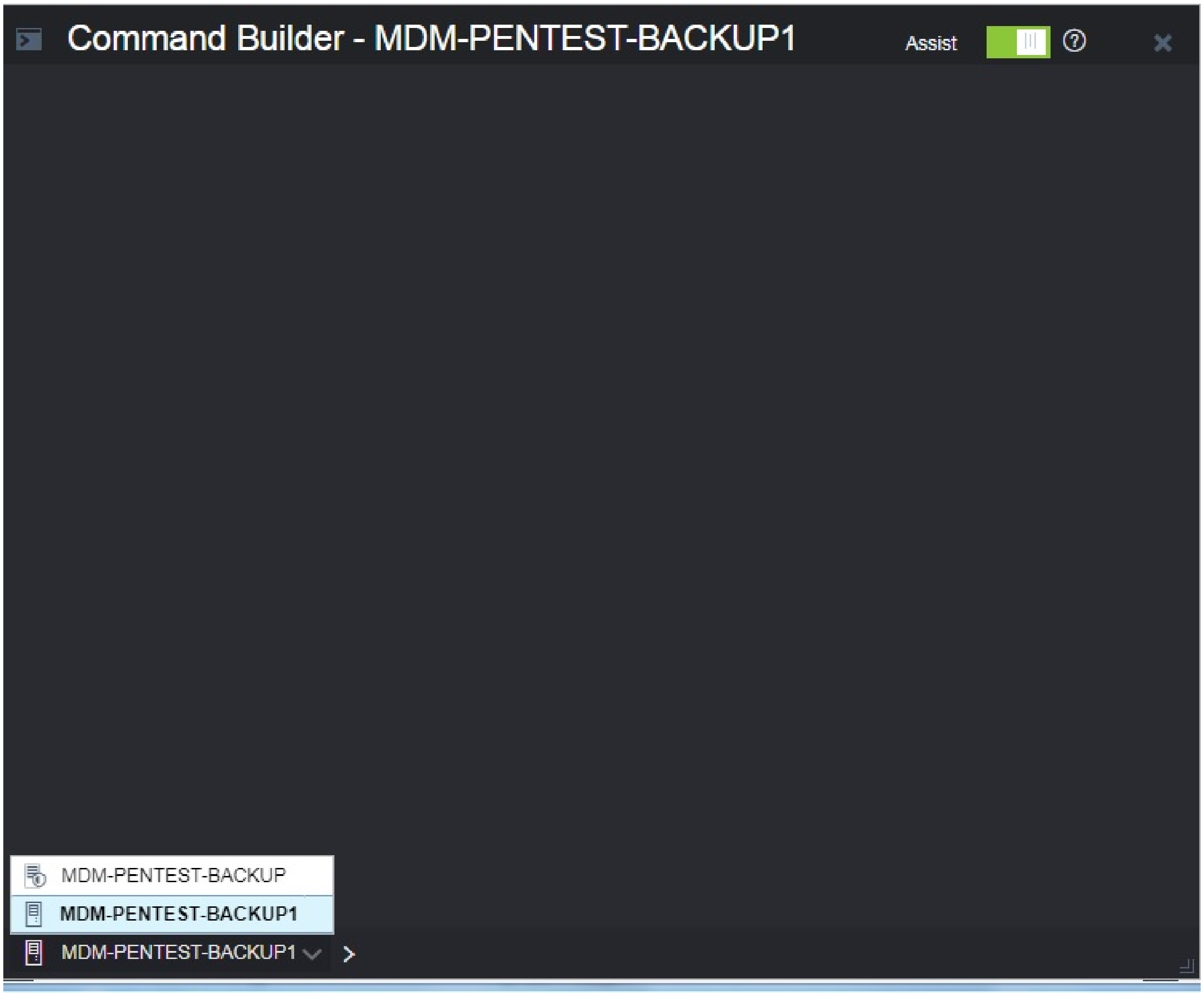


Figure 6: Start Command Builder

Retention Policy

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:

1. 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.
2. 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:

1. The management class to which a file is bound no longer exists. The default management class does not contain an archive copy group.
2. 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. 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.

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

MDM Primary machine

Profile Backup

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.

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. The PASSWORD is the Websphere administration password, which you have received in Welcome Letter. WASProfileBackup_MDM.sh executes manageprofiles.sh utility provided by WebSphere to create profile backups named MDMP_Dmgr_backup.zip, MDMP_WasNode_backup.zip which contains profile backups.

- WAS Dmgr Profile - /home/wasadmin/IBM/WebSphere/AppServer/profiles/cellmanager01

- WAS Node Profile - /home/wasadmin/IBM/WebSphere/AppServer/profiles/wasnode_{Host Name}

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

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_9.0.0/com.ibm.WebSphere.installation.nd.doc/ae/rxml_manageprofiles.html

In order to enable MDMP-WAS-WEEKLY schedule, you need to execute the following command using "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 lightweight 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.

Configuration file backup

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. The PASSWORD is the WebSphere administration password, which you have received in Welcome Letter. 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_WASNodeConfig.zip, MDMP_HttpServerConfig.zip, MDMP_HttpPluignConfig.zip which contains all profile configurations and IBM HTTP Server and Plugin configuration.

- WAS Dmgr Profile configuration folder - /home/wasadmin/IBM/WebSphere/AppServer/profiles/cellmanager01
- WAS Node Profile configuration folder - /home/wasadmin/IBM/WebSphere/AppServer/profiles/wasnode_{Host name}
- IBM HTTP Server configuration folder - /home/wasadmin/IBM/WebSphere/HTTPServer/conf
- IBM HTTP Plugin configuration folder - /home/wasadmin/IBM/WebSphere/Plugins/config

Archive files are stored in /home/wasadmin/WAS_ConfigBackup folder. In order to enable MDMP-WAS-DAILY schedule, you need to execute the following command using "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.

MDM files and folder backup

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/wasadmin/11.6/MDM
- /key/keyfile

In order to enable MDMP-FILES-WEEKLY schedule, you need to execute the following command using "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

The 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 mdm-p. Use Operation center in updating the details of Object store details.

```
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

Profile Backup

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 the specific location and invoke Spectrum Protect commands to copy files to Spectrum Protect Server machine.

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. The PASSWORD is the WebSphere administration password, which you have received in Welcome Letter. WASProfileBackup_MDM.sh executes manageprofiles.sh utility provided by WebSphere to create profile backups named MDMS_WasNode_backup.zip which contains profile backups.

- WAS Node Profile - /home/wasadmin/IBM/WebSphere/AppServer/profiles/wasnode_{Host name}

Generated files are stored in /home/wasadmin/WAS_Backup folder. WASProfileBackup_MDM.sh executes Spectrum Protect server selective backup command to take backup of MDMS_WasNode_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.

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_9.0.0/com.ibm.WebSphere.installation.nd.doc/ae/rxml_manageprofiles.html

In order to enable MDMS-WAS-WEEKLY schedule, you need to execute the following command using "Command Builder".

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

```
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 lightweight 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.

Configuration file backup

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. The PASSWORD is the WebSphere administration password, which you have received in Welcome Letter. MDMS-WAS-DAILY schedule is configured to execute daily at midnight. WASProfileConfigBackup_MDM.sh executes commands to create an archive files named MDMS_WASNodeConfig.zip, MDMS_HttpServerConfig.zip, MDMS_HttpPluignConfig.zip which contains all profile configurations and IBM HTTP Server and Plugin configuration.

- WAS Node Profile configuration folder - /home/wasadmin/IBM/WebSphere/AppServer/profiles/wasnode_{Host name}
- IBM HTTP Server configuration folder - /home/wasadmin/IBM/WebSphere/HTTPServer
- IBM HTTP Plugin configuration folder - /home/wasadmin/IBM/WebSphere/Plugins/config

Archive files are stored in /home/wasadmin/WAS_ConfigBackup folder. In order to enable MDMS-WAS-DAILY schedule, you need to execute the following command using "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.

MDM files and folder backup

A sample schedule named as MDMS-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 Secondary Machine. MDMS-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/wasadmin/11.6/MDM
- /key/keyfile

In order to enable MDMS-FILES-WEEKLY schedule, you need to execute the following command using "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/mdmp_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 mdm-s. Use Operation center in updating the details of Object store details.

```
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 tertiary machine (Only for Large Offering)

Profile Backup

To take backups of the artifacts which exists on MDM tertiary machine, a sample policy domain configuration named as MDMT-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 tertiary 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.

A sample schedule named as MDMT-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 tertiary Machine. Before enabling MDMT-WAS-WEEKLY schedule, you must update WASProfileBackup_MDM.sh and provide value for PASSWORD field. The PASSWORD is the WebSphere administration password, which you have received in Welcome Letter. WASProfileBackup_MDM.sh executes manageprofiles.sh utility provided by WebSphere to create profile backups named MDMT_WasNode_backup.zip which contains profile backups.

- WAS Node Profile - /home/wasadmin/IBM/WebSphere/AppServer/profiles/wasnode_{Host name}

Generated files are stored in /home/wasadmin/WAS_Backup folder. WASProfileBackup_MDM.sh executes Spectrum Protect server selective backup command to take backup of MDMT_WasNode_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.

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 tertiary 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_9.0.0/com.ibm.WebSphere.installation.nd.doc/ae/rxml_manageprofiles.html

In order to enable MDMT-WAS-WEEKLY schedule, you need to execute the following command using "Command Builder".

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

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

Above command enable MDMT-WAS-WEEKLY schedule without the expiry date. After enabling MDMT-WAS-WEEKLY schedule, start *dsmcad* service from MDM tertiary machine. dsmcad provides a lightweight timer which automatically starts and stops the scheduling process as needed. Open Putty or terminal in MDM tertiary machine and run service dsmcad restart using root user.

Configuration file backup

A sample schedule named as MDMT-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 tertiary Machine. Before enabling MDMT-WAS-DAILY schedule, you must update WASProfileConfigBackup_MDM.sh and provide value for PASSWORD field. The PASSWORD is the WebSphere administration password, which you have received in Welcome Letter. MDMT-WAS-DAILY schedule is configured to execute daily at midnight. WASProfileConfigBackup_MDM.sh executes commands to create an archive files named MDMT_WASNodeConfig.zip, MDMT_HttpServerConfig.zip, MDMT_HttpPluignConfig.zip which contains all profile configurations and IBM HTTP Server and Plugin configuration.

- WAS Node Profile configuration folder - /home/wasadmin/IBM/WebSphere/AppServer/profiles/wasnode_{Host name}
- IBM HTTP Server configuration folder - /home/wasadmin/IBM/WebSphere/HTTPServer
- IBM HTTP Plugin configuration folder - /home/wasadmin/IBM/WebSphere/Plugins/config

Archive files are stored in /home/wasadmin/WAS_ConfigBackup folder. In order to enable MDMT-WAS-DAILY schedule, you need to execute the following command using "Command Builder".

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

Above command enable MDMT-WAS-DAILY schedule without the expiry date. After enabling MDMT-WAS-DAILY schedule, start *dsmcad* service from MDM tertiary machine. dsmcad provides a light-weight timer which automatically starts and stops the scheduling process as needed. Open Putty or terminal in MDM tertiary machine and run service dsmcad restart using root user.

MDM files and folder backup

A sample schedule named as MDMT-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 tertiary Machine. MDMT-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/wasadmin/11.6/MDM
- /key/keyfile

In order to enable MDMT-FILES-WEEKLY schedule, you need to execute the following command using "Command Builder".

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

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

Open Putty or terminal in MDM tertiary 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 tertiary 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 tertiary machine is mdm-t. Use Operation center in updating the details of Object store details.

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

MDM primary 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.

If 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.

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

Wait for few minutes and check HADR status.

```
db2pd -db PIMDB -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 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".

```
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 MDMDB-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".

```
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.

Database VM files and folder backup

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.

- /home/db2inst1/keystore/*
- /key/keyfile

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".

```
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 secondary machine is mdm-d. Use Operation center in updating the details of Object store details.

```
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 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 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 fail-over 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.

If 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.

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

Wait for few minutes and check HADR status. db2pd -db PIMDB -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 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-DBS-FULL-WEEKLY schedule is configured to execute weekly once, on Sundays at midnight. In order to enable MDM-DBS-FULL-WEEKLY schedule, you need to execute the following command using "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 MDMDB-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-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 Database Machine.

MDM-DBS-INCREMENT-DAILY schedule is configured to execute from Monday to Saturday at midnights, except Sunday. In order to enable MDM-DBS-INCREMENT-DAILY schedule, you need to execute the following command using "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 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.

Database VM files and folder backup

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-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.

- /home/db2inst1/keystore/*

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".

```
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 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 secondary machine is mdm-ds. Use Operation center in updating the details of Object store details.

```
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>
```

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.

```
su - tsminst1
dsmserv -q &
```

This will start TSM server 1.

```
su - tsminst2
dsmserv -q &
```

This will start TSM server 2.

Starting Operation center Connect to Spectrum Protect server using putty or terminal using root user. Issue the below command:

```
service opscenter.rc status
service opscenter.rc start // For starting the service
service opscenter.rc stop // For stopping the service
```

Restoring backup

Restoring Database

1. Drop existing PIMDB database
    - Open terminal for MDM database machine, switch to db2inst1 user using command *su - db2inst1*
    - *db2 LIST APPLICATIONS*, to check if any applications are connected to this database.
    - 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.
    - Drop the database using *db2 drop db PIMDB*, 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 PIMDB 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 PIMDB
      ```

    - In order to make sure, there is no database named PIMDB, execute list command *db2 list db directory*
2. Restore PIMDB database
    - Select full or incremental backup timestamp which needs to be restored.
    - *db2 restore db PIMDB* use tsm taken at 20170526063832 ENCRYPT
        - In above statement '20170526063832' is timestamp when the DB backup was taken.

    - "use TSM" is used which means, we are restoring a database which is stored in Spectrum Protect server.
    - "ENCRYPT" is used as existing database is db2 native encrypted.
    - 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.
  - Select incremental backup timestamp if you want to restore till that date. *db2 restore db PIMDB* incremental automatic use tsm taken at 20170605134603 1. On top of full backup, we are restoring incremental backup.
  - *db2 rollforward db PIMDB* to end of logs and complete. Used to rollforward database till end of logs.

3. Verify if database is restored
   - Connect to PIMDB database using following command. db2 connect to PIMDB user db2inst1 using <PASSWORD>
   - Verify any table to check restore process is done and expected data is available.
   - Terminate database using command, db2 terminate
   - Verify id db2 native encryption is available.
   - *db2 connect to PIMDB user db2inst1 using <PASSWORD>*
   - *db2 "SELECT * FROM TABLE (SYSPROC.ADMIN_GET_ENCRYPTION_INFO())"*

Restoring MDM Database when database is in HADR scenario

1. Drop existing PIMDB database
   - Open terminal for MDM primary and secondary database machines, switch to db2inst1 user using command *su - db2inst1*.
   - 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.
   - Execute command *db2 STOP HADR ON DATABASE PIMDB* in both primary database and secondary database machine terminals.
   - Run *db2 LIST APPLICATIONS*, to check if any applications are connected to this database.
   - Run following commands to restart and drop the database.

   ```
   db2 stop db manager force;
   db2 start db manager;
   db2 drop db PIMDB
   ```

2. Restore PIMDB database
   - Open terminal for MDM primary database machine, switch to db2inst1 user.
   - Using *db2adutl* command, check available full or incremental backups.
   - Select full or incremental backup timestamp which needs to be restored.
   - *db2 restore db PIMDB use tsm taken at 20170526063832 ENCRYPT*
     - In above statement *20170526063832* is timestamp when the DB backup was taken.
     - "use TSM" is used which means, we are restoring a database which is stored in Spectrum Protect server.
     - "ENCRYPT" is used as existing database is db2 native encrypted.
     - 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.
   - Select incremental backup timestamp if you want to restore till that date. db2 restore db PIMDB incremental automatic use tsm taken at 20170605134603 1. On top of full backup, we are restoring incremental backup.
   - *db2 rollforward db PIMDB* to end of logs and complete. Used to rollforward database till end of logs.

- Run the below command to enable HADR on primary database

```
db2 UPDATE DB CFG FOR PIMDB USING LOGINDEXBUILD ON LOGARCHMETH1 DISK:/home/db2inst1/archive_logs
db2 update db cfg for PIMDB using HADR_LOCAL_HOST <Private IP of DB2 VM1>
db2 update db cfg for PIMDB using HADR_LOCAL_SVC 51012
db2 update db cfg for PIMDB using HADR_REMOTE_HOST <Private IP of DB2 VM2>
db2 update db cfg for PIMDB using HADR_REMOTE_SVC 51013
db2 update db cfg for PIMDB using HADR_REMOTE_INST db2inst1
db2 UPDATE DB CFG FOR PIMDB USING HADR_TIMEOUT 120
db2 UPDATE DB CFG FOR PIMDB USING HADR_SYNCMODE NEARSYNC
db2 terminate
db2set DB2_HADR_PEER_WAIT_LIMIT=30
db2start
db2 start hadr on database PIMDB as primary
```

- Create an offline backup (*db2 backup database PIMDB*) in primary database machine and send it to */home/db2inst1/backup folder* in secondary database machine.
- 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 PIMDB
```

- Go to */home/db2inst1/backup* folder, check if all backup files are available in this folder, which is copied from MDM primary database machine.
- Run following commands to restore the database.

```
db2 restore database PIMDB encrypt
db2 restore db PIMDB continue
db2 rollforward db PIMDB query status
db2 UPDATE DB CFG FOR PIMDB USING LOGINDEXBUILD ON LOGARCHMETH1 DISK:/home/db2inst1/archive_logs
db2 update db cfg for PIMDB using HADR_LOCAL_HOST <Private IP of DB2 VM2>
db2 update db cfg for PIMDB using HADR_LOCAL_SVC 51013
db2 update db cfg for PIMDB using HADR_REMOTE_HOST <Private IP of DB2 VM1>
db2 update db cfg for PIMDB using HADR_REMOTE_SVC 51012
db2 update db cfg for PIMDB using HADR_REMOTE_INST db2inst1
db2 UPDATE DB CFG FOR PIMDB USING HADR_TIMEOUT 120
db2 UPDATE DB CFG FOR PIMDB USING HADR_SYNCMODE NEARSYNC
db2 terminate
db2start
db2 start hadr on database PIMDB as standby
```

3. Verify if database is restored

   - Connect to PIMDB database using following command. db2 connect to PIMDB user db2inst1 using <PASSWORD>
   - Verify any table to check restore process is done and expected data is available.
   - Terminate database using command, db2 terminate
   - Verify id db2 native encryption is available.
   - db2 connect to PIMDB user db2inst1 using <PASSWORD>
   - db2 "SELECT * FROM TABLE (SYSPROC.ADMIN_GET_ENCRYPTION_INFO())"

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.

- Restore WAS artifacts in MDM primary machine, detailed description is provided following.
- Restore WAS artifacts from backup server to MDM primary machine
- Restore entire WAS profile in MDM primary machine

- Restore WAS profile configuration in MDM primary machine
- Restore WAS artifacts in MDM secondary machine, detailed description is provided following.
- Restore WAS artifacts from backup server to MDM secondary machine
- Restore WAS profile configuration in MDM secondary machine
- Restore entire WAS profile in MDM secondary machine

As a pre-requisite, VNC Server should be installed on all the client machines

- Restore WAS artifacts from Backup server to MDM primary machine
- Open terminal for MDM primary machine using root user.
- Start vncserver , if it's first time, it'll ask for password.
- Open vncserver viewer and connect to MDM primary machine. This should be done from windows/Unix machine with UI interface.
- Login and go to */opt/tivoli/tsm/client/ba/bin*
- Start Spectrum Protect client by executing *./dsmj* in terminal.
- Enter credentials as tsminst and common password provided in welcome letter.
- Select "Restore" option as we need to restore WAS artifacts.
- In MDM primary machine create a folder named */restore_mdmp*.
- Restore WAS artifacts to */restore_mdmp* folder.
- In Spectrum Protect Server select the restore options to restore the files.
- In the Spectrum Protect Server interface, you can find lot of files based on date under */home/wasadmin/WAS_Backup* folder. Select the files for which date, you want to restore and press "Restore" button.
- Select */restore_mdmp* folder as restoration folder.
- Open the */restore_mdmp* folder to see the following files.

Similarly, you can restore WAS configuration file for all profile.

Using the WebSphere *manageprofile.sh* you can restore the profile. The *manageprofile.sh* is located */home/wasadmin/IBM/WebSphere/AppServer/bin*. Run the below command to restore the profile

```
manageprofiles.sh -restoreProfile -backupFile <profile backup file location>
```

Using the WebSphere *restoreConfig.sh* you can restore the profile configuration. The restoreConfig.sh is located */home/wasadmin/IBM/WebSphere/AppServer/bin*. Run the below command to restore the profile configuration

```
restoreConfig.sh <profile configuration file location>
```

Restoring MDM application, i.e. $TOP folder

To restore MDM application artifacts, launch the IBM Spectrum Protect Client application from respective WAS VM's. Identify the restore point and perform restore. You can follow the similar process as mentioned above. The restore operation will restore file on specific folder on respective VM's. Verify all the MDM related configuration is in place, like DB IP address, DB port, etc. The restoration folder should be */home/wasadmin/11.6/MDM*, i.e. $TOP folder. To verify, below are the steps to be followed - Login to MDM CE and verify the version displayed

Restoring Client custom data folders

Since the client related data is already on NFS file system, you need to mount NFS folder on all WAS VM and create a softlink under MDM $TOP/public_html folders.

```
mount {mountAddress} /mdmnfs
cd /home/wasadmin/11.6/MDM
ln -s /mdmnfs/public_html public_html
```

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.

IBM®