



IBM MobileFirst Protect (MaaS360) Mobile Enterprise Gateway Upgrade Guide

Contents

Chapter 1. Introduction	1	Step 4: Configure the 2.3.0 IBM MaaS360 Virtual Appliance	7
Chapter 2. Prerequisites	3	Step 5: Restore Content into the 2.3.0 IBM MaaS360 Virtual Appliance.	8
Chapter 3. Upgrade Steps	5	Chapter 4. Rolling Back	9
Step 1: Back Up CDN Content	5		
Step 2: Perform the Database Upgrade.	6		
Step 3: Deploy the 2.3.0 IBM MaaS360 Virtual Appliance	7		

Chapter 1. Introduction

IBM MaaS360 On-Premises requires the administrator to perform the following steps to upgrade the installation to version 2.3.0.

Note:

Performing the upgrade will require downtime. All Portal, services and batch operations will be unavailable during the upgrade.

IBM MaaS360 agents for iOS, Android and Windows will continue to work, but device communication with IBM MaaS360 and policy updates will be affected. Emails will work if the email servers are operational.

Please plan for four hours of downtime, subject to the performance of the environment.

Chapter 2. Prerequisites

About this task

Before upgrading IBM MaaS360, ensure that the following has been done:

Procedure

1. Back up the IBM MaaS360 databases and the existing virtual appliance.
2. Make sure your environment is either at release level 2.1.1.x or 2.2.0.x.
3. The 2.1.1.x or 2.2.0.x virtual appliance must be shut down, with no application interacting with the IBM MaaS360 databases during the database upgrade. This is mandatory for a successful upgrade.
4. The **rsync** tool, used for backing up and restoring CDN content, must be installed on the backup server.

Chapter 3. Upgrade Steps

About this task

The backup process consists of five steps:

1. Back up the CDN content
2. Upgrade the IBM MaaS360 databases
3. Deploy the 2.3.0 IBM MaaS360 virtual appliance
4. Configure the 2.3.0 IBM MaaS360 virtual appliance
5. Restore the CDN content into the 2.3.0 virtual appliance

Step 1: Back Up CDN Content

About this task

The currently deployed IBM MaaS360 virtual appliance (2.1.1.x or 2.2.0.x) has content stored on the local CDN folder on the **op1svcapp1-0.op1.sysint.local** virtual machine that must be exported before the new virtual appliance is deployed. This content includes the following:

- Applications
- Documents
- Distribution requests
- IBM MaaS360 Cloud Extender configuration details

The CDN backup script is available for download from the following location:

https://<Configuration_VM_IP>:8443/static/cdnbackup.sh

For more information on using the CDN backup script, refer to CDN backup section of *IBM MaaS360 Installation Guide*.

To back up the content on the local CDN folder:

Procedure

1. Download the CDN backup script from the **Downloads** tab in the IBM MaaS360 Administration Console.
2. Copy and run the script on the destination server where the backed up data should be stored.

User: maas

Password: MaaS360_Console (default)

Note: *The default password is MaaS360_Console, but you should change it after your initial deployment. The recommended practice is to customize this password.*

The `cdnbackup.sh` script can be used according to the following parameters to back up the CDN content:

```
cdnbackup.sh [-b<backup_dir>] [-l <remote_user>] [-H <remote_host>] [-d <remote_dir>] [-D <dir>
```

Where:

-h: Help

- b: Directory to back up. This parameter can be omitted if the default value is used.
- l: User login name. This parameter can be omitted when you use the default CDN user.
- H: IP address of Service VM or host name, if a DNS entry can be added for the Service VM host name.
- d: Base directory to back up from. It can be omitted if the default value is used.
- D: List of directory names in the CDN to be backed up. It can be omitted if the default value is used.

The following example command backs up the entire CDN to the specified backup server:

```
./cdnbackup.sh -H <service_vm_ip_address>
```

Note: When prompted for a password, enter the IBM MaaS360 user password (MaaS360_Console is the default).

Step 2: Perform the Database Upgrade

About this task

Note: The 2.1.1.x or 2.2.0.x virtual appliance has been shut down, and no applications are interacting with the IBM MaaS360 databases during the database upgrade. This is mandatory for a successful upgrade.

Log in to the database server as the user with permission to administer **IBM MaaS360 databases**, and then perform the following steps:

Procedure

1. Create an upgrade root directory: `mkdir upgrade_root`
2. Navigate to that `upgrade_root` directory: `cd upgrade_root`
3. Download the database artifact from PPA to the upgrade directory. The database artifact will be IBM MobileFirst Protect 2.3 Data Installation Model Package for Oracle on Multiplatforms (Little Endian) and IBM MobileFirst Protect 2.3 Data Installation Model Package for Oracle on Multiplatforms (Big Endian).
4. Unzip the database artifact you downloaded in Step #3.
5. Navigate to **upgrade** directory under `upgrade_root` and execute the following command to initiate the database upgrade.

Note: Perform the following steps before executing the master wrapper to suit your environment's configuration:

- a. Edit the `master_wrapper.sh` file.
- b. Modify the following values to match with SID of the instance that is running on the node from which upgrade is going to be executed:

```
VPN2_SID="<SID for VPN2>"
EDW_SID="<SID for EDW>"
AGILINK_SID="<SID for AGILINK>"
P03_SID="<SID for P03>"
```

Important: SIDs are case sensitive in most of the operating systems. Modify the values in the script above based on your environment's configuration.

- c. Modify the following parameter to match with database schema password that is configured as part of the IBM MaaS360 Administrative Console:

```
APP_PASS="<Application Schema Password>"
```

All installations should perform the following to initiate the database upgrade:

```
sh ./master_wrapper.sh --vpn2=system/<system_user_password>
--edw=system/<system_user_password>
--agilink=system/<system_user_password>
--p03=system/<system_user_password> --list_file=listfile.txt
```

6. Check the logs using the following command:

```
sh ./check_logs.sh
```

7. If you find any errors do not proceed with the next steps. Follow the instructions in the Chapter 4, "Rolling Back," on page 9 section to return to the original state.

Note: Upgrade scripts have one error with compilation of a database object. Ignore it. This error will be fixed when the application logic first accesses this object.

8. Execute the following SQL on vpn2 database as the SYSTEM user and commit if there are no issues:

```
update boms.cust_mf_state
set mf_stale_time = sysdate
where mf_type = 1
and cust_id in (select customerid from boms.customer );
```

Step 3: Deploy the 2.3.0 IBM MaaS360 Virtual Appliance

Procedure

Refer to *IBM MaaS360 Installation Guide* for instructions on how to deploy the 2.3.0 IBM MaaS360 virtual appliance.

Results

Note: If you encounter any errors do not proceed with the next steps. Follow the instructions in the Chapter 4, "Rolling Back," on page 9 section to return to the original state.

Step 4: Configure the 2.3.0 IBM MaaS360 Virtual Appliance

Procedure

1. Log in to the IBM MaaS360 Administrative Console.
2. Configure the vApp deployment properties and deploy the virtual appliance into the virtual server infrastructure. Refer to the *IBM MaaS360 2.3.0 Installation Guide* for more details.
3. Verify the configuration across different pages.
4. Navigate to the **Configure Instance** tab and initiate the configuration process for the IBM MaaS360 instance (either High Availability or non-High Availability).

5. Validate the deployment using the **Troubleshooting** tab.

Results

Note: If you find any errors do not proceed with the next steps. Follow the instructions in the Chapter 4, “Rolling Back,” on page 9 section to return to the original state.

After the upgrade is successful, deploy the 2.3.0.1 fix pack. Download it from <http://www-933.ibm.com/support/fixcentral/swg/selectFixes?product=ibm/Tivoli/IBM+MaaS360&release=All&platform=VMware&function=all>

Step 5: Restore Content into the 2.3.0 IBM MaaS360 Virtual Appliance

About this task

Note:

During the CDN restore process, you can ignore any errors that begin with the following text:

```
rsync : delete_file : unlink  
rsync : failed to set time on
```

Procedure

1. Remove the ssh key for the services virtual machine name or virtual machine i/p that is used for backups. This is required to avoid errors where rsynch fails with an rsync 255=>0 error
2. Execute the CDN restore command: `./cdnbackup.sh -b <backup_directory_to_copy_files> -r -l cdn`
3. When prompted for a password, enter the Service VM OS *cdn* user password.

Results

Note: If you find any errors do not proceed with the next steps. Follow the instructions in the Chapter 4, “Rolling Back,” on page 9 section to return to the original state.

Chapter 4. Rolling Back

About this task

To restore IBM MaaS360 databases to their pre-upgrade state from a backup, perform the following steps:

Procedure

1. Restore the database to the 2.1.1.x or 2.2.0.x version from backup.
2. Restart the 2.1.1.x or 2.2.0.x virtual appliance. Ensure that 2.3.0.x IBM MaaS360 virtual appliance is not up and running before you start the previous version of the virtual appliance.