

Centers for Medicare & Medicaid Services

EDGE Server RHEL 6.7 Upgrade

Version 1.0

January 2016

1 Contents

Instructions 1
Run EDGE Local Backup Command 1
AWS Servers 1
On-Premise Servers 1
Pre-Step Checklist 1
Logging into PuTTY 2
Retrieving Your IP Address to Log in to PuTTY 2
Verifying the Schema Information 3
Executing the Backup Command for AWS Servers 3
Verifying the Backup for an AWS Server 4
Saving Your Backup Files from an AWS Server 5
Executing the Backup for On-Premise Servers 7
Verifying the Backup for On-Premise Servers 7
Saving Your Backup files from an On-Premise Server 8
Restoring Your Backup Files 8
Update from RHEL 6.5 to RHEL 6.7 9
Verify RHEL 6.7 Upgrade 10
Check Java Version 10
Check MySQL 11
Verifying the Schema Information 11
Verify EDGE Application Updates 11
Execute RA Local Command 12

Instructions

Migrating from Red Hat Enterprise Linux (RHEL) 6.5 to RHEL 6.7 involves the following major steps:

1. Run "**edge dbbackup"** to create a backup of MySQL database tables and all ingested files on the External Data Gathering Environment (EDGE) server, including all schemas that currently exist on the server.
2. Run **"yum update"**.
3. Post upgrade checks.

Run EDGE Local Backup Command

The purpose of the local **"edge dbbackup"** command is to create a backup of the MySQL database tables and all ingested files on the EDGE server, including all schemas that currently exist on the server (e.g. EDGE_SRVR_COMMON, EDGE_SRVR_PROD, and EDGE_SRVR_TEST) and any existing backup schemas that exist (e.g. EDGE_SRVR_COMMON_2014, EDGE_SRVR_PROD_2014 and EDGE_SRVR_TEST_2014). The backup will also include any new backup schemas created for the 2015 payment year and any archive or performance schemas created.

The command can be used by running from the command prompt in PuTTY by simply typing in the backup command "**edge dbbackup**". The command has no input parameters.

The **"edge dbbackup"** command will not backup any reports or output files generated as part of the ingest from the outbox folder.

The command will be used by issuers to generate the backup files. Once the backup file is generated, it is the issuer's responsibility to store the file in a secure location that meets their internal IT backup policies.

Issuers will also be responsible for backing up any output reports generated in a secure location that meets their internal IT backup policies.

AWS Servers

The command creates .SQL backup files in the issuer's Amazon Web Services (AWS) Simple Storage Service (S3) backup directory. These files contain a backup of all of the data on the EDGE server MySQL database, including all schemas.

On-Premise Servers

The command creates .SQL backup files in the issuer's EDGE backup directory (**cd /opt/edge/ingest/backup**) on the On-Premise server. These files contain a backup of all of the data on the EDGE server MySQL database, including all schemas.

Pre-Step Checklist

- ✓ Ensure there is a valid working server available.
- ✓ Ensure the server is running in AWS EC2.
- ✓ Download the PuTTY application from the Web.
- ✓ Download WINSCP or any FTP client of your choice.

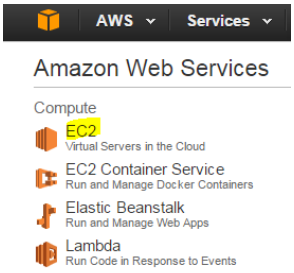
Logging into PuTTY

PuTTY will allow the issuer to successfully log in to their server once the server has been successfully provisioned. PuTTY will also allow the issuer to run the **"edge dbbackup"** to backup their files and schemas. PuTTY will allow the issuer to log into MySQL to query their database for reference data and files ingested in the PROD and TEST schemas.

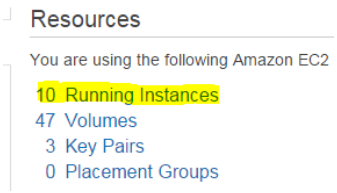
The below are steps to create a putty session and log in to the server.

Retrieving Your IP Address to Log in to PuTTY

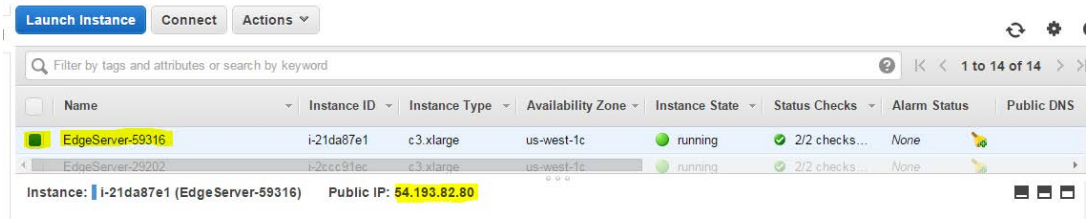
- Log in to your AWS account.
- Navigate to EC2.



- Click on Running Instances.

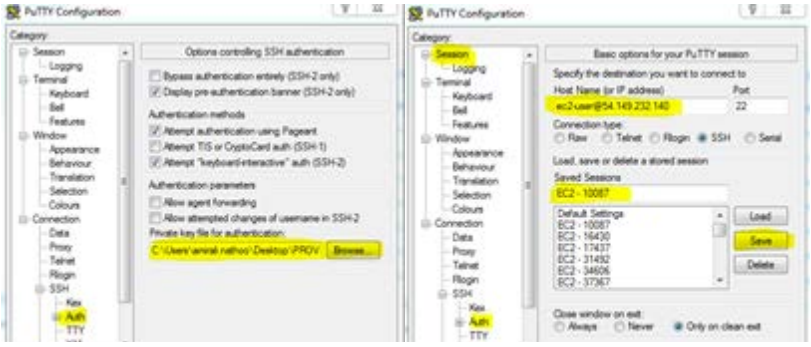


- Select your server and look at the instance below to retrieve your public IP for your server.



In the PuTTY screen under Host Name (or IP address) enter the IP address you retrieved from AWS.

- ✓ Enter the Host Name (or IP address) : ec2-user@xx.xxx.xxx.xxx.
- ✓ Enter any name for the server under “Saved Sessions”.
- ✓ Click on “Auth” under category in the left side panel.
- ✓ Click on “Browse” and select your .ppk key file.
- ✓ Click on “Session” under category in the left side panel.
- ✓ Click on “Save” to save your new PuTTY session.



Verifying the Schema Information

This step will verify all your schema information before you begin the backup process.

- ✓ Login to the server using the above PuTTY instructions.
- ✓ Login to MySQL.
- ✓ At the MySQL prompt, type: **show schemas;**

```
mysql> show schemas;
+----------------------+
| Database             |
+----------------------+
| information_schema   |
| EDGE_SRVR_COMMON     |
| EDGE_SRVR_COMMON_2015 |
| EDGE_SRVR_PROD       |
| EDGE_SRVR_PROD_2015  |
| EDGE_SRVR_TEST       |
| EDGE_SRVR_TEST_2015  |
| mysql                |
| test                 |
+----------------------+
9 rows in set (0.00 sec)
```

- ✓ Verify all your schemas are present.
- ✓ At the MySQL command prompt, type: **quit** to exit back to the UNIX command prompt.

Executing the Backup Command for AWS Servers

This step will guide you through executing the local backup command.

- ✓ At the command prompt, type the command: **edge dbbackup** and press “enter”**.**

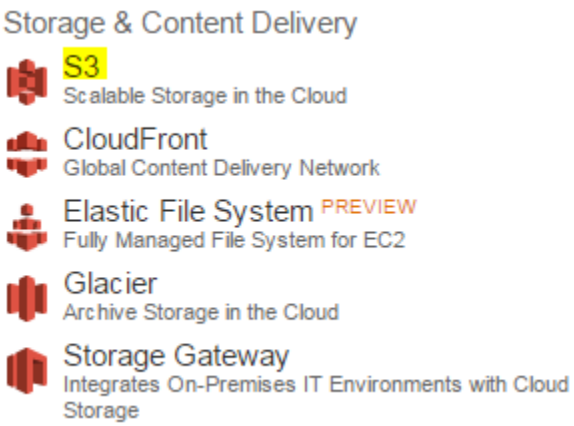
```
[ec2-user@edgeserver-2006380 ~]$ edge dbbackup
```

- ✓ Wait for the backup process to complete successfully.

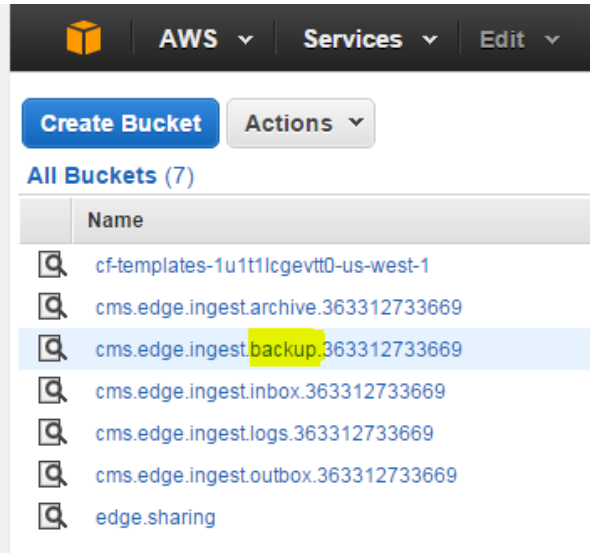
Verifying the Backup for an AWS Server

This step will verify that the backup was successfully created in the AWS backup bucket in the S3 bucket.

- ✓ Log in to AWS Website. The link will be the same one (1) used to ingest your eXtensible Markup Language (XML) files.
- ✓ Navigate to the S3 Folder on the home page.



- ✓ Inside the S3 Folder, navigate to the backup folder link.



- ✓ Select your Server ID and click on it to enter the folder.
- ✓ Verify that your backup is visible inside the folder.
  - o Verify the backup for all your schemas are created with *IssuerID.SchemaName.LOCAL_BACKUP.TodayDateandTime.sql*
  - o Verify the date the backup files created (Should be current date and time).

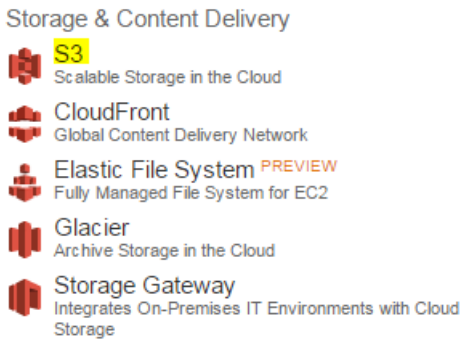


Saving Your Backup Files from an AWS Server

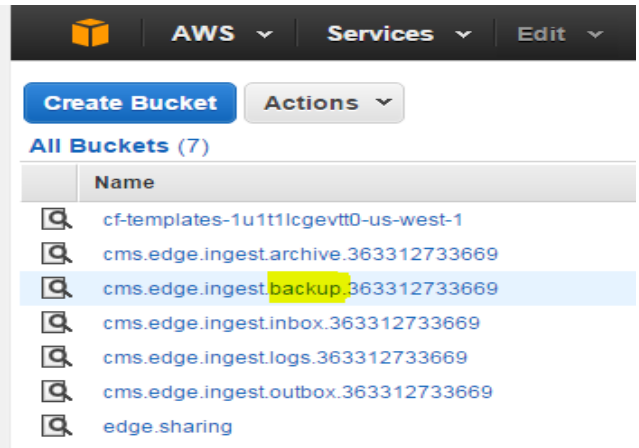
Note: It is important that issuers download and store the backup that is generated and any reports not saved by the backup command in a secure location that meets the issuers internal IT backup policies.

To save the backup files that are generated, please follow the below steps.

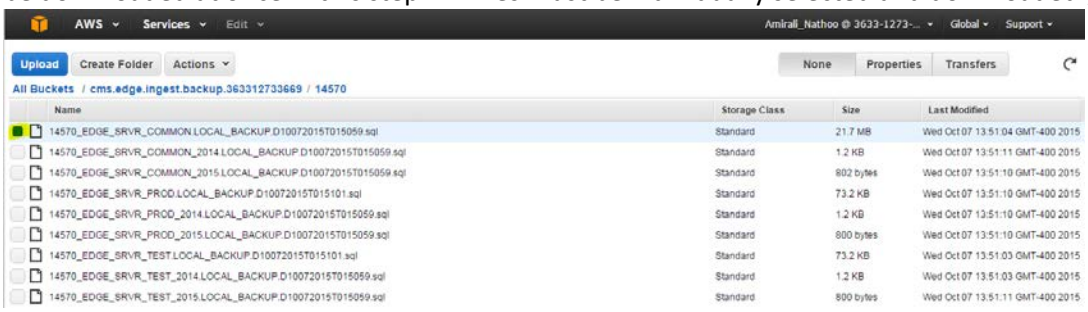
- ✓ Log in to AWS Website. The link will be the same one (1) used to ingest your XML files.
- ✓ Navigate to the S3 Folder on the home page.



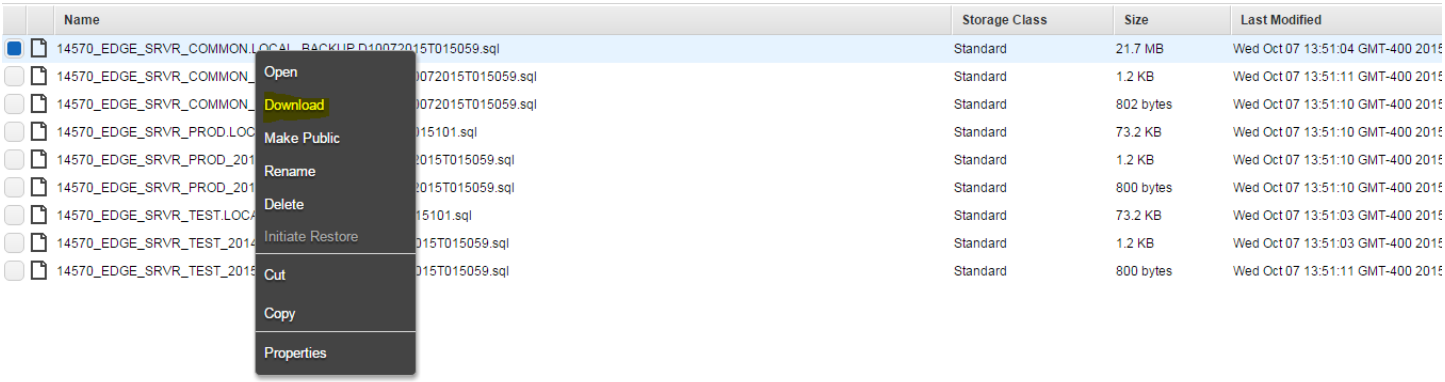
- ✓ Inside the S3 Folder, navigate to the backup folder link.



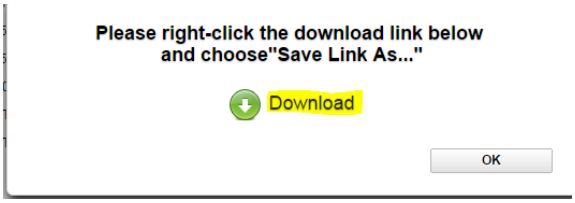
- ✓ Select your Server ID and click on it to enter the folder.
- ✓ Select the backup file by selecting the square box on the left hand corner in front of the files (All the files cannot be downloaded at once in this step. All files must be individually selected and downloaded.)



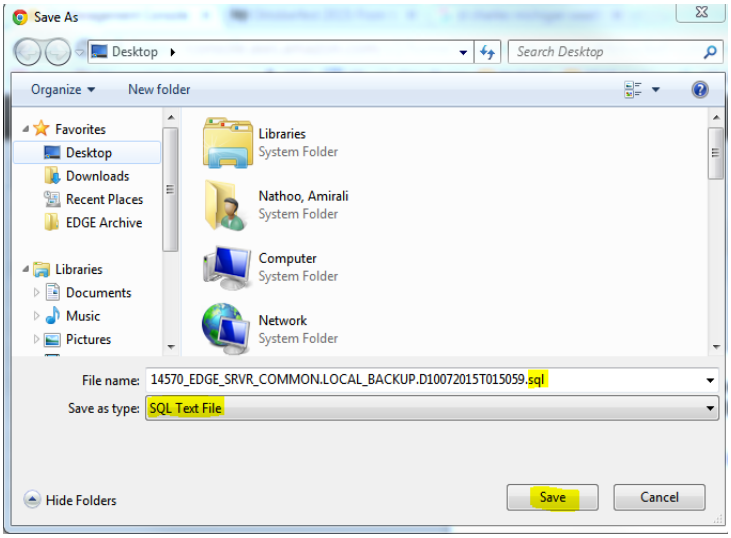
- ✓ Right click on the selected file and click on the “Download” link.



- ✓ Right click on the “Download” link displayed and click “Save Link As...”



- ✓ A window prompt will be displayed to save your file in the secure location of your choice. Select the location and click “Save”. Make sure the file is saved as a .SQL type.



Executing the Backup for On-Premise Servers

This step will guide you through executing the local backup command.

- ✓ Navigate to **cd /opt/edge/bin** folder.
- ✓ At the command prompt, type the command: **./edge dbbackup** and press enter.

```
[ec2-user@HPT1_OP_80991 bin]$ ./edge dbbackup
```

- ✓ Wait for the backup process to complete successfully.

Verifying the Backup for On-Premise Servers

This step will verify that the backup was successfully created in the AWS backup bucket in the S3 bucket.

- ✓ Log in to the On-Premise server.
- ✓ Navigate to **cd /opt/edge/ingest/backup**

```
[ec2-user@HPT1_OP_80991 backup]$ cd opt/edge/ingest/backup
-bash: cd: opt/edge/ingest/backup: No such file or directory
You have mail in /var/spool/mail/ec2-user
[ec2-user@HPT1_OP_80991 backup]$
```

- ✓ Verify that your backup is visible inside the folder.
  - o Verify the backup for all your schemas are created with *IssuerID.SchemaName.LOCAL_BACKUP.TodayDateandTime.sql*
  - o Verify the date the backup files created (Should be current date and time.)

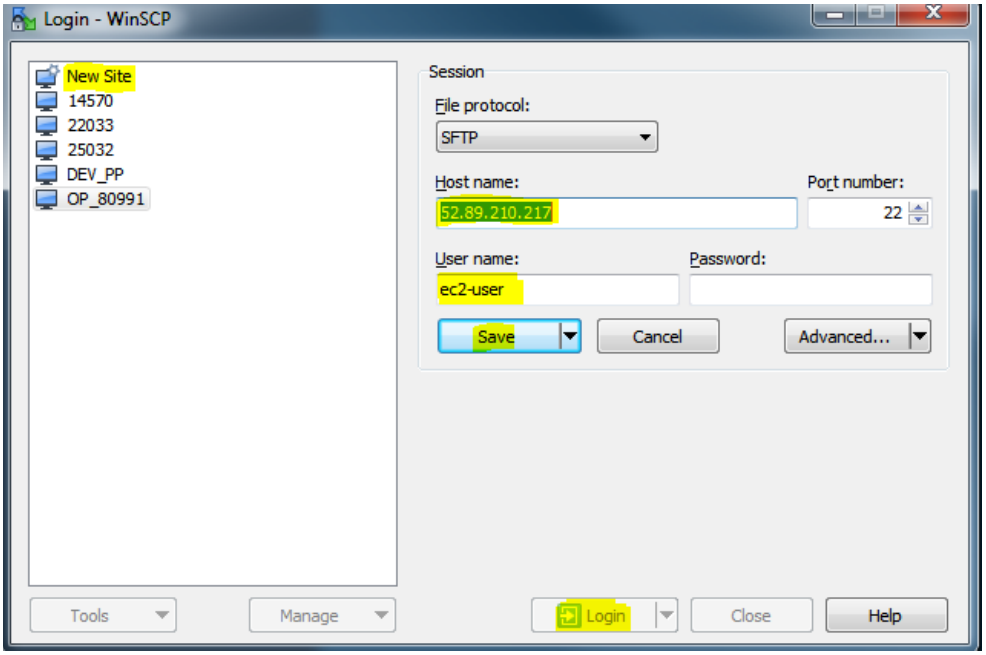
```
[ec2-user@HPT1_OP_80991 backup]$ ll
total 64396
-rw-rw-r--. 1 ec2-user ec2-user      791 Oct  6 13:17 80991_EDGE_SRVR_COMMON_2014.LOCAL_BACKUP.D10062015T011738.sql
-rw-rw-r--. 1 ec2-user ec2-user 22914528 Oct  6 13:17 80991_EDGE_SRVR_COMMON.LOCAL_BACKUP.D10062015T011738.sql
-rw-rw-r--. 1 ec2-user ec2-user      789 Oct  6 13:17 80991_EDGE_SRVR_PROD_2014.LOCAL_BACKUP.D10062015T011738.sql
-rw-rw-r--. 1 ec2-user ec2-user    78009 Oct  6 13:17 80991_EDGE_SRVR_PROD.LOCAL_BACKUP.D10062015T011742.sql
-rw-rw-r--. 1 ec2-user ec2-user      789 Oct  6 13:17 80991_EDGE_SRVR_TEST_2014.LOCAL_BACKUP.D10062015T011738.sql
-rw-rw-r--. 1 ec2-user ec2-user    78009 Oct  6 13:17 80991_EDGE_SRVR_TEST.LOCAL_BACKUP.D10062015T011741.sql
```

Saving Your Backup files from an On-Premise Server

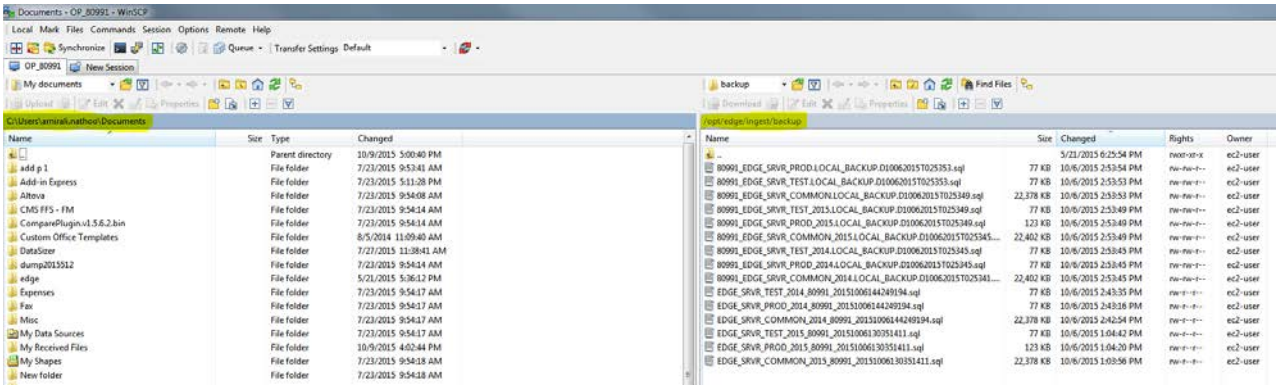
Note: It is important that issuers download and store the backup that is generated and any reports not saved by the backup command in a secure location that meets issuers internal IT backup policies.

To save the backup files that are generated, please follow the below steps.

- ✓ Retrieve your IP address.
- ✓ Log in to WinSCP.



- ✓ Click on the right hand panel to highlight it. Navigate to **/opt/edge/ingest/backup**.



- ✓ Click on the left hand panel to highlight the window. Navigate to the location you want to save your files. Drag the files from the right window to the location on the left.

Restoring Your Backup Files

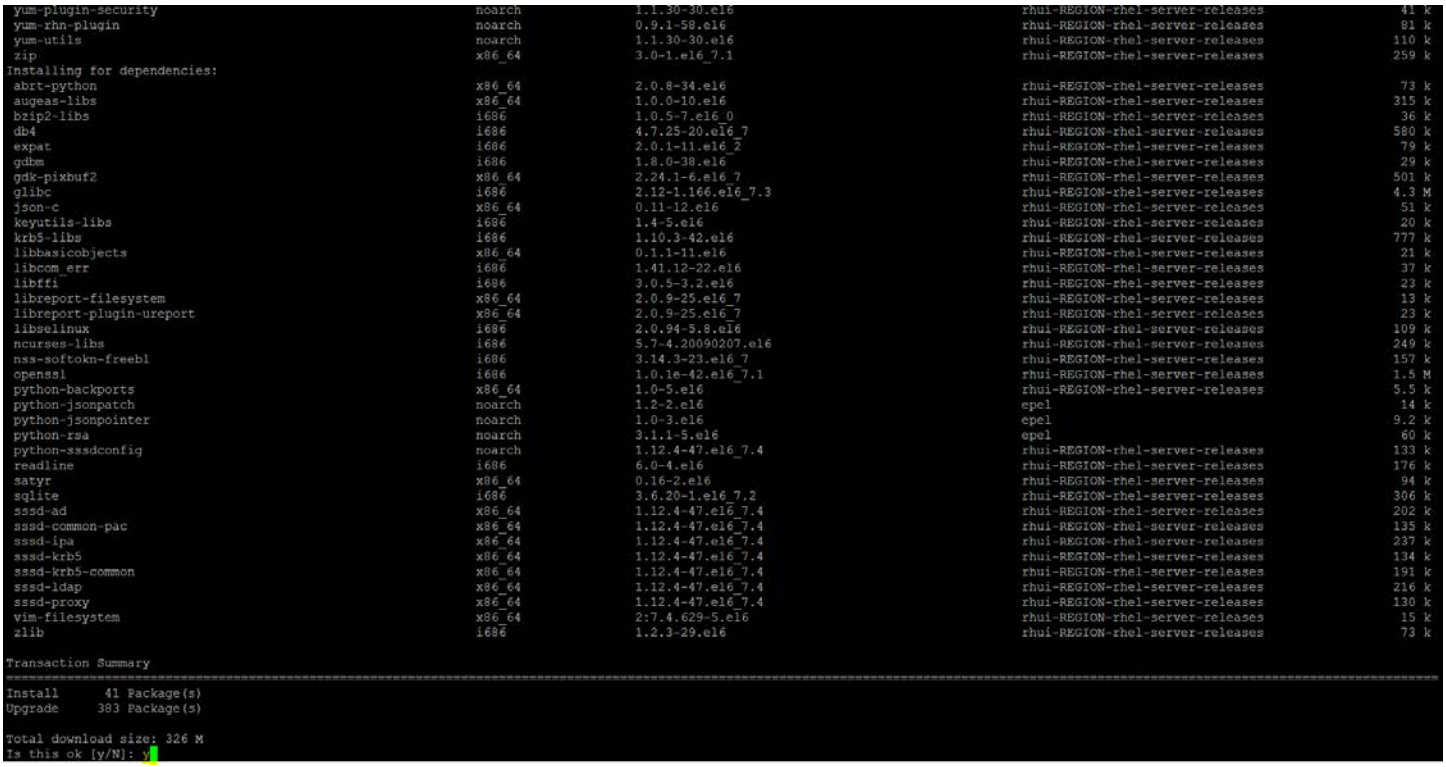
To restore the data backup, issuers need to reach out to their assigned Financial Management Coordinating Center (FMCC) Service Representative for coordination and instructions for restoring the backup.

Update from RHEL 6.5 to RHEL 6.7

Run **“yum update”** after login as root or **“sudo yum update”** with user who has root privileges.

```
Using username "ec2-user".
Authenticating with public key "imported-openssh-key"
Last login: Tue Jan  5 22:03:22 2016 from ip68-100-9-226.dc.dc.cox.net
[ec2-user@edgeserver-31492 ~]$ sudo yum update
```

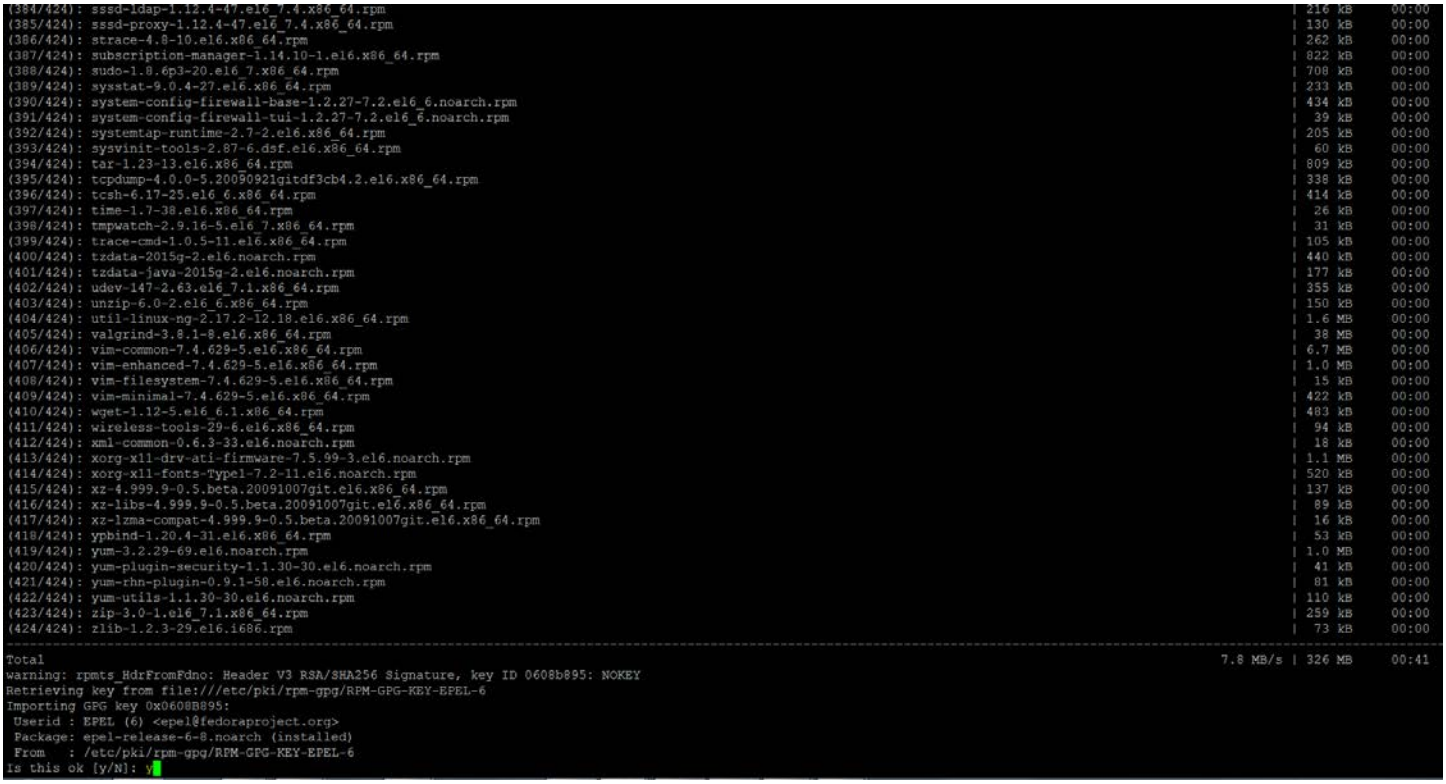
Type ‘y’ to install the downloaded update packages to start download and start upgrade process.



```
 yum-plugin-security                noarch          1.1.30-30.el6                  rhui-REGION-rhel-server-releases   41 k
 yum-rhn-plugin                     noarch          0.9.1-58.el6                   rhui-REGION-rhel-server-releases   81 k
 yum-utils                          noarch          1.1.30-30.el6                  rhui-REGION-rhel-server-releases  110 k
 zip                                x86_64          3.0-1.el6_7.1                  rhui-REGION-rhel-server-releases  259 k
Installing for dependencies:
 abrt-python                        x86_64          2.0.8-34.el6                   rhui-REGION-rhel-server-releases   73 k
 augeas-libs                        x86_64          1.0.0-10.el6                   rhui-REGION-rhel-server-releases  315 k
 bzip2-libs                         i686            1.0.5-7.el6_0                  rhui-REGION-rhel-server-releases   36 k
 db4                                i686            4.7.25-20.el6_7                rhui-REGION-rhel-server-releases  580 k
 expat                              i686            2.0.1-11.el6_2                 rhui-REGION-rhel-server-releases   79 k
 gdbm                               i686            1.8.0-38.el6                   rhui-REGION-rhel-server-releases   29 k
 gdk-pixbuf2                        x86_64          2.24.1-6.el6_7                 rhui-REGION-rhel-server-releases  501 k
 glibc                              i686            2.12-1.166.el6_7.3             rhui-REGION-rhel-server-releases  4.3 M
 json-c                             x86_64          0.11-12.el6                    rhui-REGION-rhel-server-releases   51 k
 keyutils-libs                      i686            1.4-5.el6                      rhui-REGION-rhel-server-releases   20 k
 krb5-libs                          i686            1.10.3-42.el6                  rhui-REGION-rhel-server-releases  777 k
 libbasicobjects                    x86_64          0.1.1-11.el6                   rhui-REGION-rhel-server-releases   21 k
 libcom_err                         i686            1.41.12-22.el6                 rhui-REGION-rhel-server-releases   37 k
 libffi                             i686            3.0.5-3.2.el6                  rhui-REGION-rhel-server-releases   23 k
 libreport-filesystem               x86_64          2.0.9-25.el6_7                 rhui-REGION-rhel-server-releases   13 k
 libreport-plugin-ureport           x86_64          2.0.9-25.el6_7                 rhui-REGION-rhel-server-releases   23 k
 libselinux                         i686            2.0.94-5.8.el6                 rhui-REGION-rhel-server-releases  109 k
 ncurses-libs                       i686            5.7-4.20090207.el6             rhui-REGION-rhel-server-releases  249 k
 nss-softokn-freebl                 i686            3.14.3-23.el6_7                rhui-REGION-rhel-server-releases  157 k
 openssl                            i686            1.0.1e-42.el6_7.1              rhui-REGION-rhel-server-releases  1.5 M
 python-backports                   x86_64          1.0-5.el6                      rhui-REGION-rhel-server-releases  5.5 k
 python-jsonpatch                   noarch          1.2-2.el6                      epel                              14 k
 python-jsonpointer                 noarch          1.0-3.el6                      epel                             9.2 k
 python-rsa                         noarch          3.1.1-5.el6                    epel                              60 k
 python-sssdconfig                  noarch          1.12.4-47.el6_7.4              rhui-REGION-rhel-server-releases  133 k
 readline                           i686            6.0-4.el6                      rhui-REGION-rhel-server-releases  176 k
 satyr                              x86_64          0.16-2.el6                     rhui-REGION-rhel-server-releases   94 k
 sqlite                             i686            3.6.20-1.el6_7.2               rhui-REGION-rhel-server-releases  306 k
 sssd-ad                            x86_64          1.12.4-47.el6_7.4              rhui-REGION-rhel-server-releases  202 k
 sssd-common-pac                    x86_64          1.12.4-47.el6_7.4              rhui-REGION-rhel-server-releases  135 k
 sssd-ipa                           x86_64          1.12.4-47.el6_7.4              rhui-REGION-rhel-server-releases  237 k
 sssd-krb5                          x86_64          1.12.4-47.el6_7.4              rhui-REGION-rhel-server-releases  134 k
 sssd-krb5-common                   x86_64          1.12.4-47.el6_7.4              rhui-REGION-rhel-server-releases  191 k
 sssd-ldap                          x86_64          1.12.4-47.el6_7.4              rhui-REGION-rhel-server-releases  216 k
 sssd-proxy                         x86_64          1.12.4-47.el6_7.4              rhui-REGION-rhel-server-releases  130 k
 vim-filesystem                     x86_64          2:7.4.629-5.el6                rhui-REGION-rhel-server-releases   15 k
 zlib                               i686            1.2.3-29.el6                   rhui-REGION-rhel-server-releases   73 k

Transaction Summary
================================================================================
Install      41 Package(s)
Upgrade     383 Package(s)

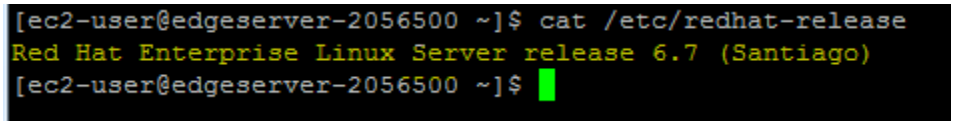
Total download size: 326 M
Is this ok [y/N]: y
```



Verify RHEL 6.7 Upgrade

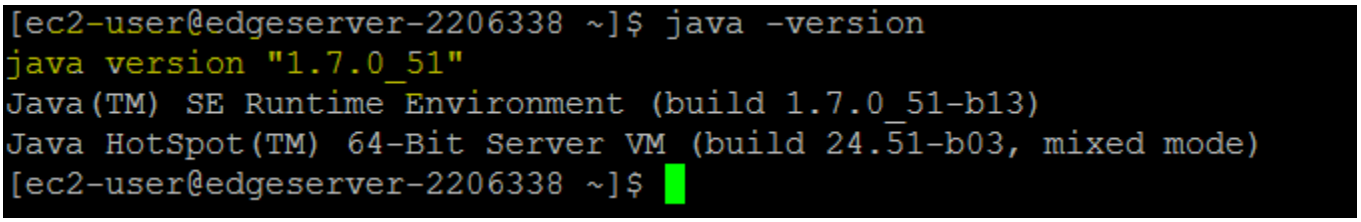
After running the upgrade successfully, verify upgraded RHEL version by executing the following:

1. cat /etc/redhat-release



Check Java Version

1. Run the command: **java -version.**
2. It will reflect the existing running Java version. The recommended version is **Java 1.7u_51.**



Check MySQL

1. Run the command to open MySQL shell: **mysql --host=localhost --user=edgedbuser --password=xxxxxxx**
2. Check all the schemas are available.

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 101
Server version: 5.5.46 MySQL Community Server (GPL) by Remi

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Verifying the Schema Information

This step will verify all your schema information after the RHEL 6.7 upgrade.

1. Log in to the server using the above PuTTY instructions.
2. Log in to MySQL.
3. At the MySQL prompt, type: **show schemas;**

```
mysql> show schemas;
+----------------------+
| Database             |
+----------------------+
| information_schema   |
| EDGE_SRVR_COMMON     |
| EDGE_SRVR_COMMON_2015 |
| EDGE_SRVR_PROD       |
| EDGE_SRVR_PROD_2015  |
| EDGE_SRVR_TEST       |
| EDGE_SRVR_TEST_2015  |
| mysql                |
| test                 |
+----------------------+
9 rows in set (0.00 sec)
```

4. Verify all your **prior** schemas are present.
5. At the MySQL command prompt, type: **quit** to exit back to the UNIX command prompt.

Verify EDGE Application Updates

1. Run the command: **edge update** to install any latest edge application updates**.**
2. Run the command: **edge version** to check the build version**.**
3. Verify the below build version is displayed.

   Edge version is EDGEServer_4.07_01_b0182

Execute RA Local Command

1. Run the command : **edge report RA_RS_Transfer_Prelim 2015**
2. Run the RA local command and share the Risk Adjustment Risk Score Summary Report (RARSS) and Risk Adjustment Transfer Elements Extract (RATEE) Reports for verification.