



Centers for Medicare & Medicaid Services

Backup Policy and User Guide for AWS and On-Premise EDGE Servers

**Version 2.0
September 2016**

Contents

1	Introduction and Purpose of Local Backups	1
1.1	AWS Servers	1
1.2	On-Premise Servers	1
2	Backup Policy	2
3	Pre-Step Checklist	2
4	Executing the Backup Command for AWS Server.....	3
4.1	Logging into PuTTY	4
4.2	Verifying the Schema Information.....	5
4.3	Verifying the Backup for an AWS Server	6
4.4	Accessing your Backup files from an AWS Server	7
5	Executing the Backup for On-Premise Server.....	9
5.1	Verifying the Backup for an On-Premise Server	9
5.2	Saving your Backup Files from an On-Premise Server.....	10
6	Restoring your Backup Files	11
7	Acronyms and Abbreviations	12

Figures

Figure 1 – AWS Account	3
Figure 2 – Resources.....	3
Figure 3 – Instance State	3
Figure 4 – Public IP Address	4
Figure 5 – Logging into PuTTY	4
Figure 6 – DB Schemas.....	4
Figure 7 – Backup Command Prompt for AWS Server.....	5
Figure 8 – AWS S3 Folder	5
Figure 9 – S3 Folder Backup Folder	5
Figure 10 – Verify Creation of Backup Files	6
Figure 11 – S3 Folder Page	6
Figure 12 – Backup Folder Link.....	6
Figure 13 – Selecting Backup File	7
Figure 14 – On-Premise Backup Command Prompt	8
Figure 15 – On-Premise Backup Command Prompt	8
Figure 16 – Ingest Backup Command	8
Figure 17 – Confirming Creation of Backup File for On-Premise Extraction.....	9
Figure 18 – EDGE Server Version	9
Figure 19 – Log in to WINSCP	10
Figure 20 – Ingest Folder	10

Tables

Table 1 – Acronyms and Abbreviations.....	11
---	----

1 Introduction and Purpose of Local Backups

The purpose of this document is to outline the steps that are required to back up local and Amazon Web Services (AWS) External Data Gathering Environment (EDGE) servers. The backup process is a required procedure to restore EDGE servers during a disaster recovery process. These steps will focus on taking database backups, archiving to different physical locations and restoring the data.

The “**edge dbbackup**” command creates a backup of the MySQL database schemas on the EDGE server. The command can be executed by the issuer from the command line for both AWS and On-Premise (OP) EDGE servers.

In the command prompt in PuTTY, simply type in the backup command “**edge dbbackup**” without input parameters.

The backup command **will** include:

1. All production, common, and test database schemas that exist on the server for the current processing year.
 - a. e.g. EDGE_SRVR_COMMON, EDGE_SRVR_PROD, and EDGE_SRVR_TEST
2. Any backup database schemas that have been created for past years.
 - a. e.g. EDGE_SRVR_COMMON_2014, EDGE_SRVR_PROD_2014 and EDGE_SRVR_TEST_2014.

The backup command **will not** include:

1. Any eXtensible Markup Language (XML) ingest files submitted to the EDGE server for processing.
2. Any XML output reports generated by the EDGE server.

ISSUERS’ RESPONSIBILITIES:

1. The backup command will **not back up any XML ingest files submitted to the server or output XML files generated by the server**. The issuer is responsible for backing up the XML ingest files submitted to the server for processing and the XML output files generated.
2. Once the backup files are generated, it is the issuer’s responsibility to store the database tables and files in a secure location, off the EDGE server, in a manner that meets their internal IT backup policies.

1.1 AWS Servers

The command creates .SQL backup files in the issuer’s 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.

1.2 OP Servers

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

2 Backup Policy

EDGE server issuers are required to retain all original data stored in their MySQL data tables for a period of 10 years. Issuers must maintain their MySQL data on the EDGE server, in an active, queryable status for a period of three (3) years. CMS recommends issuers maintain the inbound and outbound files and reports on their servers for at least the entire reporting period for a coverage year and for the purpose of troubleshooting and to support the discrepancy and appeals process.

Required:

Issuers are required to back up their EDGE servers in accordance with this user guide after each CMS-executed Risk Adjustment (RA) and Reinsurance (RI) run. Backups must also be moved to a secure external location off the server in order for the data to be retrievable and accessible in case of catastrophic system failure. Issuers must move backed-up final EDGE data SQL tables to an external source after the final RA and RI calculations are run in May. Storing a backup on the EDGE server is not sufficient. Storage of the EDGE data SQL tables is the minimum requirement to meet the data retention policy. Retention of inbound and outbound data files that contributed to the final calculations is a recommended best practice.

After the final RA and RI calculations are run each calendar year, CMS will require that issuers attest that they have performed the backup function to an external location. Additionally, issuers will need to attest that they have verified that their data has been backed-up and is available for future use if need be. Backups should be performed and moved to a secure external location other than the EDGE server, in order for the data to be retrievable in case of system disaster.

Recommendations:

CMS recommends that issuers back up the MySQL tables and all inbound and outbound reports frequently, such as after each data submission and whenever issuers are making Information Technology (IT) changes (e.g. software/hardware changes, migrations, etc.) to their EDGE server.

Note that the issuer is ultimately responsible for making sure files are appropriately backed-up off their server in a safe and accessible location. Issuers should ensure any contracted parties responsible for data submission and retention have the appropriate backup procedures in place.

Issuers who do not comply with backup requirements and experience a loss of data that is irretrievable, may receive adverse audit findings where applicable. CMS will not be extending file submission deadlines for issuers who have failed to back up their data in accordance with these instructions.

3 Pre-Step Checklist

Prior to executing the EDGE command to conduct the backup, complete the pre-step checklist below to ensure an environment suitable to conduct the backup exist.

1. Ensure there is a valid working server available.
2. Ensure the server is running in AWS EC2.
3. Download and install the PuTTY application from the web.
4. Download and install WINSCP or any File Transfer Protocol (FTP) client of your choice.

4 Executing the Backup Command for an AWS Server

This step will guide you through executing the local backup command for AWS servers for extraction of XML (input/output) files.

4.1 Logging into PuTTY

PuTTY will allow issuers to log into their server once the server has been provisioned. This will allow issuers to run the **“edge dbbackup”** command to back up their files and schemas and log into MySQL to query their database for reference data and files ingested in the PROD and TEST schemas.

Below are steps to retrieve the server Internet Protocol (IP) address, create a PuTTY session, and log in to the server.

1. Log in to your AWS account.
2. Navigate to EC2.

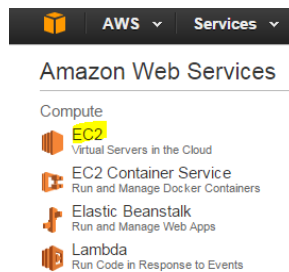


Figure 1 – AWS Account

3. Click on “Running Instances”.

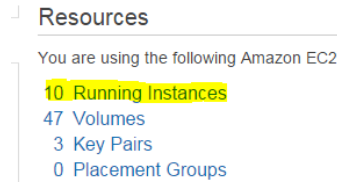


Figure 2 – Resources

4. Identify your server and confirm that the “Instance State” is “running”. If the “Instance State” is “stopped”, then you must first start the instance by right clicking on the instance row and selecting Instance State > Start as seen in the screenshot below:

Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
t2.micro	us-west-2c	stopped		None
c3.xlarge	us-west-2c	running		None
c3.xlarge	us-west-2c	running		None
c3.xlarge	us-west-2c	running		None
c3.xlarge	us-west-2c	running		None
c3.xlarge	us-west-2c	running		None
c3.xlarge	us-west-2c	stopped		None
c3.xlarge	us-west-2c	stopped		None

Connect

Get Windows Password

Launch More Like This

Instance State

Instance Settings

Image

Networking

CloudWatch Monitoring

Start

Stop

Reboot

Terminate

Figure 3 – Instance State

- After confirming the server is running, retrieve the public IP address for your server as seen below:

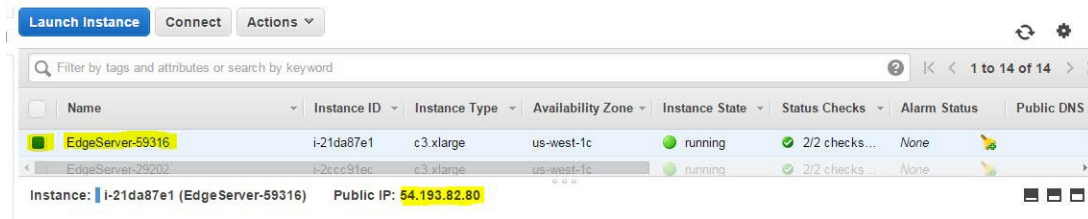


Figure 4 – Public IP Address

- 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.

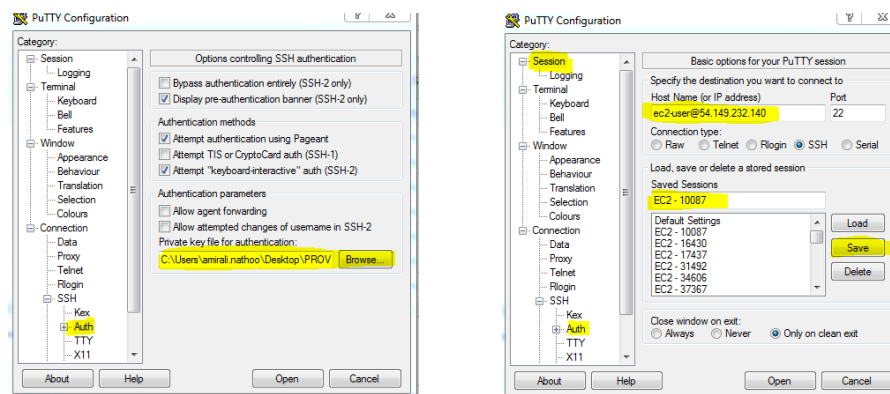


Figure 5 – Logging into PuTTY

4.2 Verifying the Schema Information

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

- Log in to your server using the above PuTTY instructions.
- Log in 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)
```

Figure 6 – DB Schemas

4. Verify all your schemas are present.
5. At the MySQL command prompt, type: **“quit”** to exit back to the UNIX command prompt.
6. At the command prompt, type the command: **“edge dbbackup”** and press **“enter”**.

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

Figure 7 – Backup Command Prompt for AWS Server

7. Wait for the backup process to complete successfully.

4.3 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.

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



Figure 8 – AWS S3 Folder

3. Inside the S3 Folder, navigate to the backup folder link.

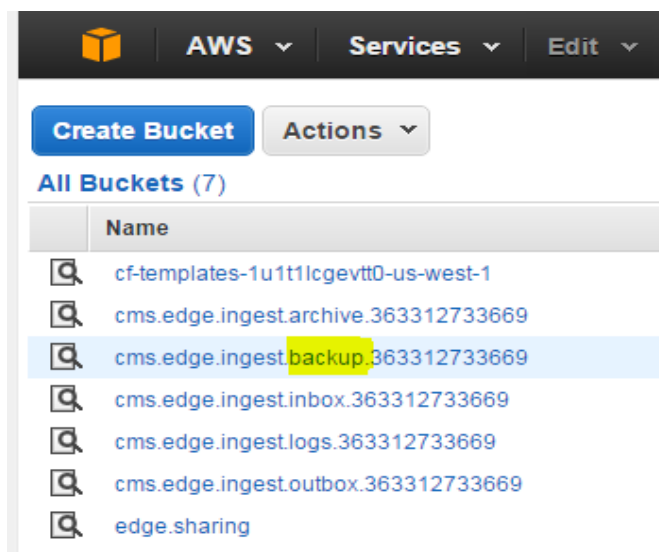
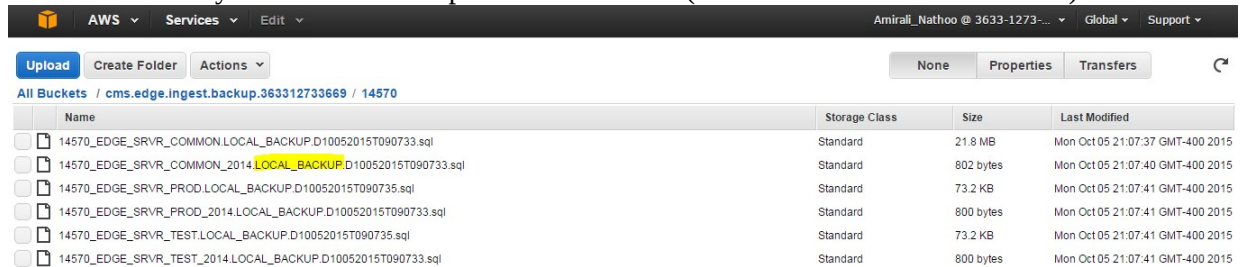


Figure 9 – S3 Folder Back up Folder

4. Select your server ID and click on it to enter the folder.
5. Verify that your backup is visible inside the folder.
 - a. Verify the backup for all your schemas are created with
IssuerID.SchemaName.LOCAL_BACKUP.TodayDateandTime.sql
 - b. Verify the date the backup files were created (Should be current date and time).



The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with 'AWS', 'Services', and 'Edit' dropdowns. Below that, a breadcrumb trail shows 'All Buckets / cms.edge.ingest.backup.363312733669 / 14570'. A table lists the files in the bucket:

Name	Storage Class	Size	Last Modified
14570_EDGE_SRVR_COMMON.LOCAL_BACKUP.D10052015T090733.sql	Standard	21.8 MB	Mon Oct 05 21:07:37 GMT-400 2015
14570_EDGE_SRVR_COMMON_2014.LOCAL_BACKUP.D10052015T090733.sql	Standard	802 bytes	Mon Oct 05 21:07:40 GMT-400 2015
14570_EDGE_SRVR_PROD.LOCAL_BACKUP.D10052015T090735.sql	Standard	73.2 KB	Mon Oct 05 21:07:41 GMT-400 2015
14570_EDGE_SRVR_PROD_2014.LOCAL_BACKUP.D10052015T090733.sql	Standard	800 bytes	Mon Oct 05 21:07:41 GMT-400 2015
14570_EDGE_SRVR_TEST.LOCAL_BACKUP.D10052015T090735.sql	Standard	73.2 KB	Mon Oct 05 21:07:41 GMT-400 2015
14570_EDGE_SRVR_TEST_2014.LOCAL_BACKUP.D10052015T090733.sql	Standard	800 bytes	Mon Oct 05 21:07:41 GMT-400 2015

Figure 10 – Verify Creation of Backup Files

4.4 Accessing your Backup files from an AWS Server

Note: It is important that issuers download and store the backup that is generated and any ingest files under /opt/edge/ingest/archives/ and any reports not saved by the backup command, in a secure location that meets Issuers' internal IT backup policies.

To access the backup files that are generated, please follow the steps below:

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

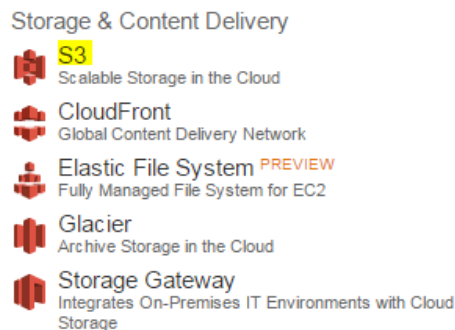


Figure 11 – S3 Folder Page

3. Inside the S3 Folder, navigate to the backup folder link.

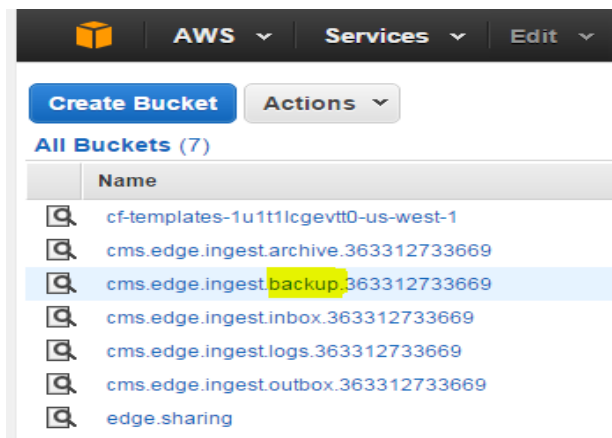


Figure 12– Backup Folder Link

4. Select your Server ID and click on it to enter the folder.
5. 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.)



Figure 13 – Selecting Backup File (Image 1 of 3)

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

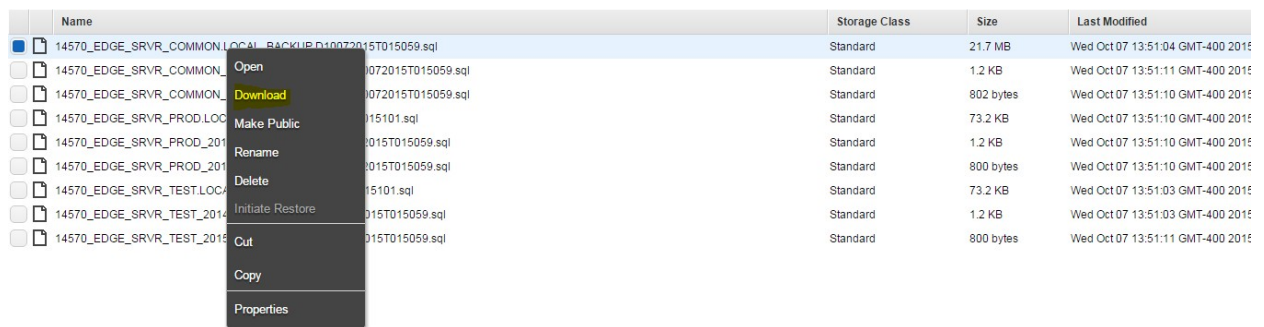


Figure 13 – Selecting Backup File (Image 2 of 3)

7. Right click on the “Download” link displayed and click “Save link as...”

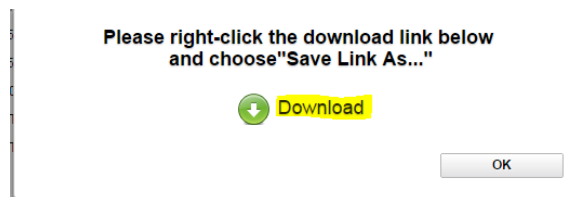


Figure 13 – Selecting Back up File (Image 3 of 3)

8. 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.

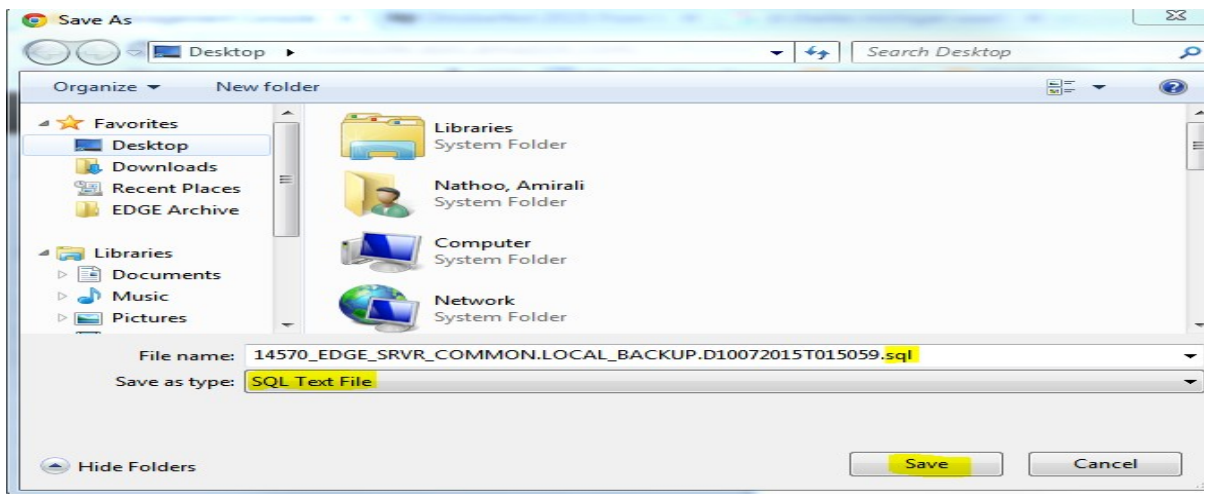


Figure 14 – OP Backup Command Prompt

5 Executing the Backup Command for an OP Server

This step will guide you through executing the local backup command for OP servers. These command prompts will assist issuers in extracting their XML (output/input) files not covered to be moved to their local backup tool for disaster recovery purposes.

1. Connect to the OP EDGE server using PuTTY or your preferred Secure Shell (SSH) client.
2. Navigate to the **cd /opt/edge/bin** folder.
3. At the command prompt, type the command: **./edge dbbackup** and press enter .

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

Figure 15 – OP Backup Command Prompt

4. Wait for the back-up process to complete successfully.

5.1 Verifying the Backup for an OP Server

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

1. Log in to the OP server.
2. 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]$
```

Figure 16 – Ingest Backup Command

3. Verify that your backup is visible inside the folder.
 - a. Verify the backup for all your schemas are created with *IssuerID.SchemaName.LOCAL_BACKUP.TodayDateandTime.sql*
 - b. Verify the date the backup files were 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
```

Figure 17 – Confirming Creation of Backup File for OP Extraction

Issuers should install MySQL Community Server 5.5.43:

Note: Issuers who want to install a different version of MySQL should first contact their Financial Management Coordination Center (FMCC) representative to ensure it complies with current CMS guidelines and EDGE software.

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 29417
Server version: 5.5.43 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>
```

Figure 18 – EDGE Server Version

5.2 Saving your Backup Files from an OP 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.

1. Retrieve your IP Address.
2. Log in to WinSCP.

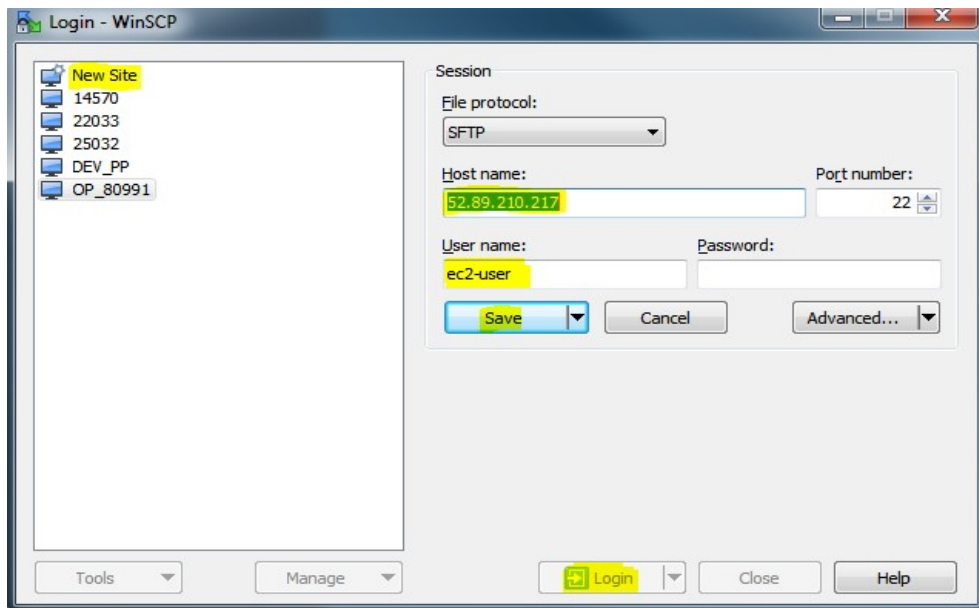


Figure 19 – Log in to WinSCP

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

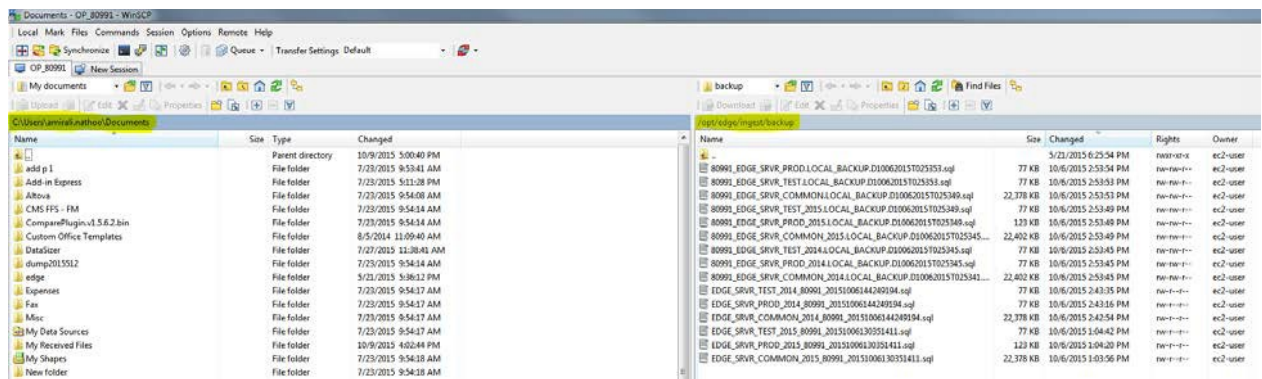


Figure 20 – Ingest Folder

- 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.

6 Restoring your Backup Files

Issuers must notify CMS immediately upon becoming aware of any issues with files, either stored or lost, which can create an access or retrieval problem. CMS would like to note that issuers must contact their FMCC Service Representatives for technical assistance. CMS encourages issuers to report issuer-based problems as soon as possible so that, to the extent feasible, CMS can provide assistance to issuers to resolve those problems before the final data submission deadline.

CMS also asks that issuers always review their data and their EDGE server reports during the data submission process. Issuers must submit accurate and complete data for a benefit year by April 30th of the subsequent benefit year.

AWS issuers should not contact Amazon for assistance in restoring their files until they have been instructed to do so by CMS.

7 Acronyms and Abbreviations

Table 1 provides a list of acronyms used in this document.

Table 1 – Acronyms and Abbreviations

Acronym / Abbreviation	Literal Translation
AWS	Amazon Web Services
DB	Database
EDGE	External Data Gathering Environment
OP	On Premise

8 Technical Assistance

FMCC representatives are available to answer any questions or assist issuers with this procedure. To reach an FMCC representative send an email to EDGE_Server_Data@cms.hhs.gov.