Download Logs from Umbrella Log Management Using the AWS CLI

Contents

Introduction

This document describes how to download logs from Umbrella Log Management using the AWS CLI.

Overview

Once your Log Management in the Amazon S3 has been set up you might wish to test the log files are being written and are downloadable.

In order to do this, we outlined an approach using Amazon's 'AWS Command Line Interface'

For alternative methods, please see here.

Prerequisites

- Download and install the AWS CLI from https://aws.amazon.com/cli/
- Create your Cisco managed bucket as described here
- Alternatively, configure logging to use your own S3 bucket as described here

Configuring Your Security Credentials in AWS CLI

At the command line, enter:

```
aws configure
```

You are presented with these four questions. If you created a Cisco Managed Bucket, the first three were provided when you created the bucket. For Cisco Managed Buckets, the 'Default region name' is listed in your bucket name. For example, the region for "cisco-managed-us-west-2" is "us-west-2". For your own bucket, the region is set according to your S3 settings. For a full list of Amazon S3 regions please see here.

You can rerun this configuration at any time, and it shows a reduced version of your credentials, for example:

AWS Access Key ID [**********HVBA]:

AWS Secret Access Key [**********OuFw]:

Default region name [us-west-2]:

Default output format [None]:

Sync your bucket contents to local folder

Enter this command, replacing with "yourbucketname" and "prefix" with your bucket details.

```
aws s3 sync s3://<yourbucketname>/<prefix>/ <your local folder path>
```

Prefix is optional for admin owned buckets, and mandatory for Cisco Managed ones. For example:

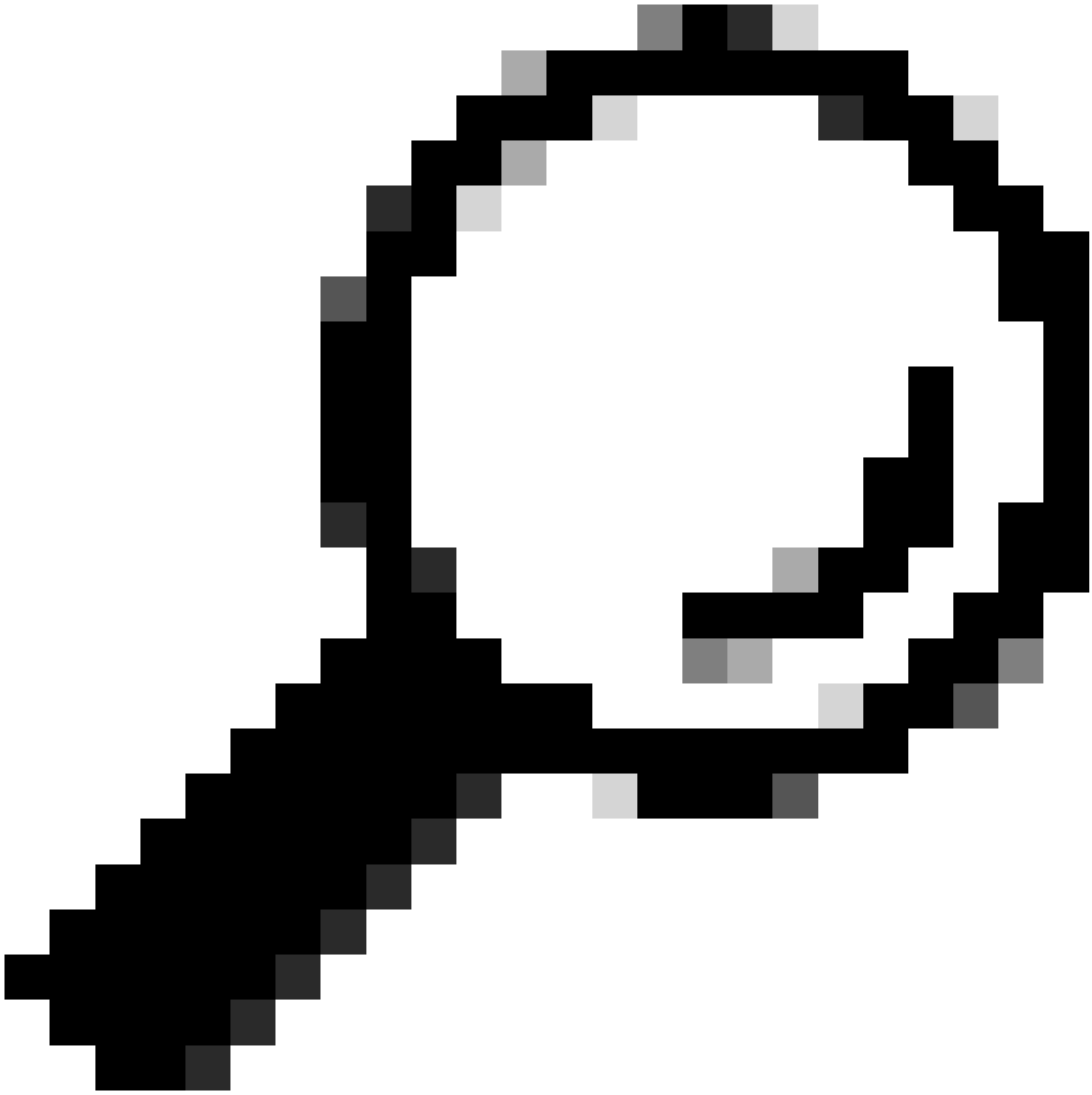
```
aws s3 sync s3://cisco-managed-us-west-2/2293370_96b88e0e21ac0136373b7009a340dc5f/ c:\temp\
```

You see an output like this:

download: s3://cisco-managed-us-west-2/2293370_96b88e0e21ac0136373b7009a340dc5f/dnslogs/2018-05-01/2018-05-01-12-30-0e41.csv.gz to dnslogs\2018-05-01\2018-05-01-12-30-0e41.csv.gz

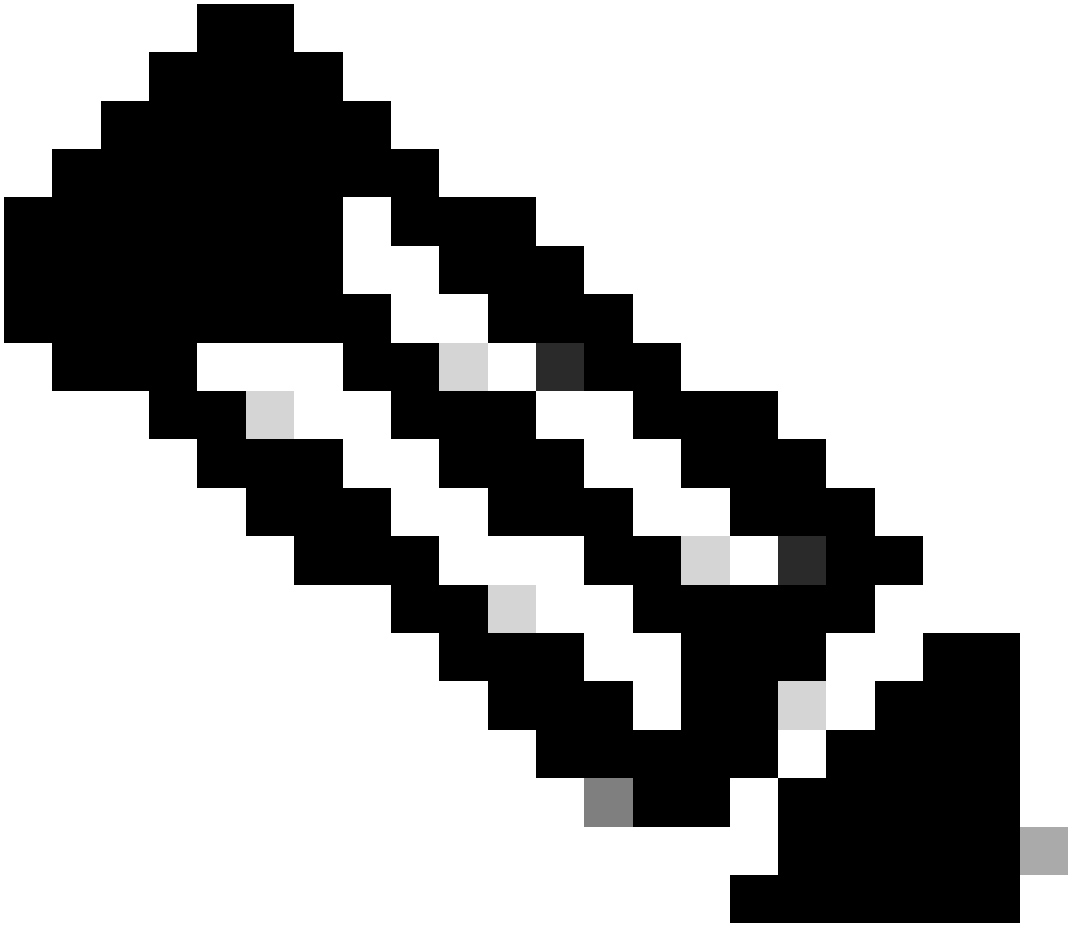
download: s3://ccisco-managed-us-west-2/2293370_96b88e0e21ac0136373b7009a340dc5f/dnslogs/2018-05-01/2018-05-01-12-40-0e41.csv.gz to dnslogs\2018-05-01\2018-05-01-12-40-0e41.csv.gz

download: s3://cisco-managed-us-west-2/2293370_96b88e0e21ac0136373b7009a340dc5f/dnslogs/2018-05-01/2018-05-01-12-30-b3ab.csv.gz to dnslogs\2018-05-01\2018-05-01-12-30-b3ab.csv.gz



Tip: Attempting to list the contents of a Cisco Managed bucket root generally results in an error as the access level provided does not have the rights to list bucket root contents. You can however list the contents of the prefix and folders within the bucket using a command similar to this:

```
aws s3 Is s3:////dnslogs
```



Note: The full command line interface documentation is available from Amazon here.