Cisco Workload Automation Amazon S3 Adapter Guide

Version 6.3

First Published: August, 2015
Last Updated: September 6, 2016

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

© 2016 Cisco Systems, Inc. All rights reserved.

Contents

Contents 3
Preface 5
- Audience 5
- Related Documentation 5
- Obtaining Documentation and Submitting a Service Request 5
- Document Change History 6

Introducing the Amazon S3 Adapter 7
- Overview 7
- Prerequisites 8

Configuring the Amazon S3 Adapter 9
- Overview 9
- Licensing an Adapter 9
- Securing the Adapter 10
  - Defining Runtime Users 10
  - Configuring Security Policies for Amazon S3 Adapter Jobs 11
  - Defining CWA Users 12
- Defining a Connection 14

Using the Amazon S3 Adapter 17
- Defining Amazon S3 Jobs 17
  - Create Bucket Operation 17
  - Update Bucket Operation 23
  - Delete Bucket Operation 27
  - Update Object(s) Operation 27
  - Rename/Restore Object Operation 31
  - Move, Copy, and Delete Object(s) Operations 33
- Monitoring Amazon S3 Job Activity 35
- Controlling Adapter and Agent Jobs 39
  - Holding a Job 39
  - Aborting a Job 40
  - Rerunning a Job 40
  - Making One Time Changes to an Adapter or Agent Job Instance 40
  - Deleting a Job Instance before It Has Run 40

Configuring service.props 41
- About Configuring service.props 41
- service.props Properties 41

Preface

This guide describes the installation, configuration, and usage of the Amazon S3 Adapter with Cisco Workload Automation (CWA).

Audience

This guide is for administrators who install and configure the Amazon S3 Adapter for use with Cisco Workload Automation, and who troubleshoot CWA installation and requirements issues.

Related Documentation

See the *Cisco Workload Automation Documentation Overview* for your release on cisco.com at:

http://www.cisco.com/c/en/us/support/cloud-systems-management/tidal-enterprise-scheduler/products-documentation-roadmaps-list.html

...for a list of all Cisco Workload Automation guides.

Note: We sometimes update the documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Document Change History

The table below provides the revision history for the Amazone S3 Adapter Guide.

Version Number	Issue Date	Reason for Change
6.1.0	October 2012	New Cisco version.
6.2.1	June 2014	Available in online Help only.
6.2.1 SP2	June 2015	Configuration provided in the *Cisco Tidal Enterprise Scheduler Installation Guide*; usage provided in online Help only.
6.2.1 SP3	May 2016	Consolidated all Amazon S3 Adapter documentation into one document.
6.3	August 2016	Rebranded “Cisco Tidal Enterprise Scheduler (TES)” to “Cisco Workload Automation (CWA)”. Miscellaneous edits for the 6.3 release.

1

Introducing the Amazon S3 Adapter

This chapter provides an overview of the Cisco Workload Automation Amazon S3 (Simple Storage Service) Adapter and its requirements:

- Overview, page 7
- Prerequisites, page 8

Overview

Amazon Simple Storage Service (S3) is persistent storage that provides a simple web service interface that customers use to store and retrieve any amount of data. Like a file system, Amazon S3 data is conceptualized into buckets (folders) and objects (files).

The Cisco Workload Automation (CWA) Amazon S3 Adapter automates the execution of Amazon S3 jobs as a part of Workload Automation's managed process. It is an API-level integration solution. As a platform independent solution, the Amazon S3 Adapter can run on any platform where the Cisco Workload Automation master runs.

An Amazon S3 Adapter job can be used to create buckets that can store large volumes of data. It also provides authentication mechanisms to ensure that data is kept secure from unauthorized access, objects can be made private or public, and rights can be granted to specific users.

The Adapter provides the following features.

- Connection/Availability – Reports the connectivity status.
- Data organization – Allows user to create a bucket, move/copy/rename/restore objects from one bucket to another bucket or within the same bucket.
- Data security for bucket – Allows user to configure ACL permission to a buck
- Data storage and retrieval – can be integrated with Data Mover Job to allow user to upload/download objects(s).
- Data protection – Allows you to specify server-side encryption while uploading/downloading object(s) from/to the Amazon S3 Bucket Amazon S3 service. APIs allow the Amazon S3 Adapter to make requests to Amazon S3 service.
- Data security for object – Allows user to configure ACL permission to an object. User can set ACL permission for an object.
- Free/cleanup data storage (objects) – Allows user to delete objects and bucket.

The Amazon S3 Adapter uses the AWS SDK, which is a set of application programming interfaces (APIs) that allow interaction with the Amazon S3 service. The APIs allow the AmazonsS3 Adapter to read, write and delete objects, manage lifecycle of buckets and objects, configure or update bucket and object properties, and manage files within Amazon S3 buckets.

Prerequisites

An Amazon S3 Adapter user must have an AWS Account or AMI user credentials (Access Key ID, Secret Access Key) to make requests to Amazon S3 service.

Generally, CWA supports the latest version of Amazon S3. See the *Cisco Workload Automation Compatibility Guide* for a complete list of support and requirements for all Workload Automation products.

2

Configuring the Amazon S3 Adapter

Overview

The Amazon S3 Adapter software is installed as part of a standard installation of Cisco Workload Automation. However, you must perform the following steps to license and configure the adapter before you can schedule and run Amazon S3 jobs:

- Licensing an Adapter, page 7 – Apply the license to the Adapter. You cannot define a Amazon S3 connection until you have applied the license from Cisco.
- Securing the Adapter, page 8 – Define Amazon S3 users that the adapter can use to establish authenticated sessions with the Amazon S3 service and permit requests to be made on behalf of the authenticated account.
- Defining a Connection, page 12 – Define a connection so the master can communicate with the Amazon S3 service.

See Configuring service.props, page 39 for details about configuring service.props to control such things as polling, output, and log gathering.

Licensing an Adapter

Each CWA Adapter must be separately licensed. You cannot use an Adapter until you apply the license file. If you purchase the Adapter after the original installation of CWA, you will receive a new license file authorizing the use of the Adapter.

You might have a Demo license which is good for 30 days, or you might have a Permanent license. The procedures to install these license files are described below.

To license an Adapter:

1. Stop the master:

   Windows:

   a. Click on **Start** and select **All Programs>Cisco Workload Automation>Scheduler>Service Control Manager**.

   b. Verify that the master is displayed in the **Service** list and click on the **Stop** button to stop the master.

   UNIX:

   Enter **tesm stop**

2. Create the license file:

   – For a Permanent license, rename your Permanent license file to *master.lic*.

- For a Demo license, create a file called *demo.lic*, then type the demo code into the *demo.lic* file.

3. Place the file in the **C:\Program Files\TIDAL\Scheduler\Master\config** directory.
4. Restart the master:

   Windows:

   Click **Start** in the Service Control Manager.

   UNIX:

   Enter **tesm start**

   The master will read and apply the license when it starts.
5. To validate that the license was applied, select **Registered License** from **Activities** main menu.

Securing the Adapter

There are two types of users associated with the Amazon S3 Adapter, **Runtime Users** and **Schedulers**. You maintain definitions for both types of users from the **Users** pane.

- Runtime Users

  Runtime users in the context of Amazon S3 jobs represent those users and passwords required for authentication. Amazon S3 operations require authentication against a valid Amazon S3 user as defined by a Amazon S3 administrator. You can also use runtime users to override data source logons used by your reports. See Defining Runtime Users, page 8.

- Schedulers

  Schedulers are those users who will define and/or manage Amazon S3 jobs. There are three aspects of a user profile that grant and/or limit access to scheduling jobs that affect Amazon S3:

  - Security policy that grants or denies add, edit, delete and view capabilities for Amazon S3 jobs. See Configuring Security Policies for Amazon S3 Adapter Jobs, page 9.
  - Authorized runtime user list that grants or denies access to specific authentication accounts for use with Amazon S3 jobs. See Defining CWA Users, page 10.
  - Authorized agent list that grants or denies access to specific Amazon S3 Adapter connections for use when defining Amazon S3 jobs. See Defining CWA Users, page 10.

Defining Runtime Users

To define a runtime user:

1. From the **Navigator** pane, expand the **Administration** node and select **Runtime Users** to display the defined users.
2. Right-click **Runtime Users** and select **Add Runtime User** from the context menu (*Insert* mode).

   -or-

   Click the **Add** button on the CWA menu bar.

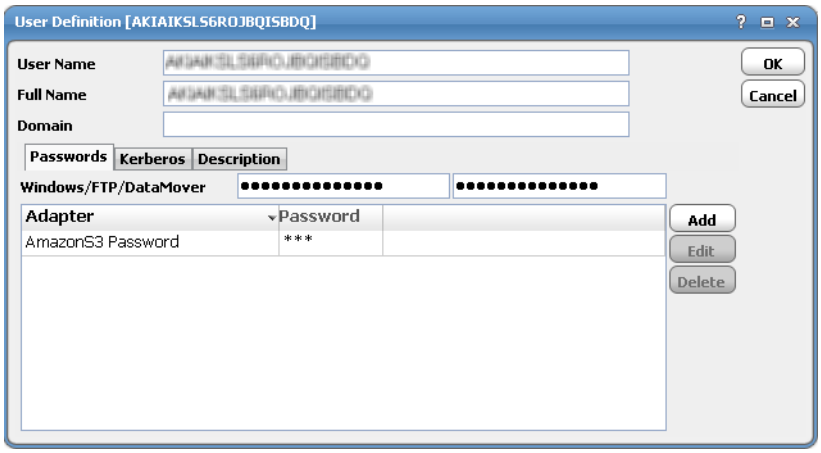
   The **User Definition** dialog displays.
3. Enter the new user name in the **User Name** field.

4. For documentation, enter the **Full Name** or description associated with this user.
5. In the **Domain** field, select a Windows domain associated with the user account required for authentication, if necessary.
6. To define this user as a runtime user for Amazon S3 Adapter jobs, click **Add** on the **Passwords** tab.

   The **Change Password** dialog displays.
7. Select **AmazonS3** from the **Password Type** list.
8. Enter a password (along with confirmation) in the **Password/Confirm Password** fields.

   Only those users with a password specified for Amazon S3 will be available for use with Amazon S3 jobs. The password might be the same as the one specified for Windows/FTP/DataMover jobs.
9. Click **OK** to return to the **User Definition** dialog.

   The new password record displays on the **Passwords** tab.



10. Click **OK** to add or save the user record in the CWA database.

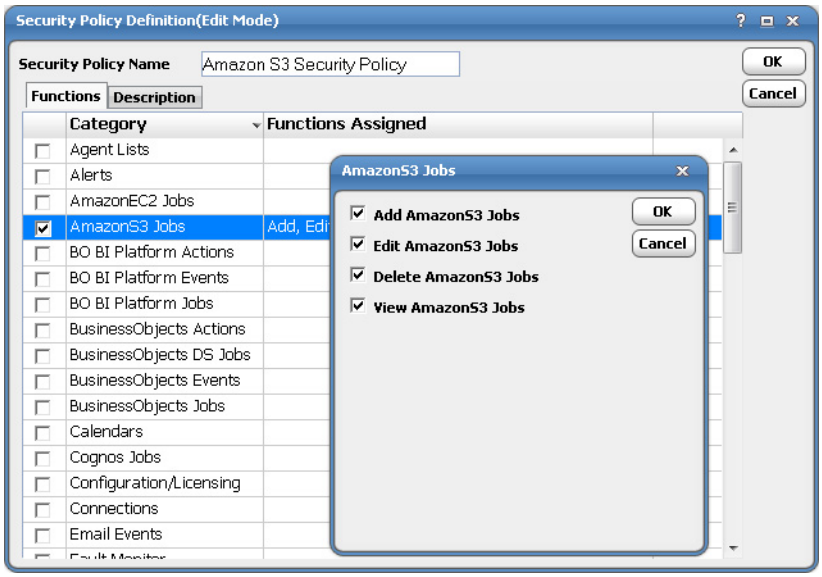
For further information about the **User Definition** dialog, see your *Cisco Workload Automation User Guide*.

Configuring Security Policies for Amazon S3 Adapter Jobs

To configure a security policy for Amazon S3 jobs:

1. From the **Navigator** pane, select **Administration>Security Policies** to display the **Security Policies** pane.

2. Right-click **Security Policies** and select **Add Security Policy** from the context menu. You can also right-click to select an existing security policy in the **Security Policies** pane and select **Edit Security Policy**.



3. In the **Security Policy Name** field, enter a name for the policy.
4. On the **Functions** page, scroll to the **AmazonS3 Jobs** category, click the ellipses on the right-hand side of the dialog and select the check boxes next to the functions that are to be authorized under this policy (**Add**, **Edit**, **Delete** and **View AmazonS3 Jobs**).
5. Click **Close** on the **Function** drop-down list.
6. Click **OK** to save the policy.

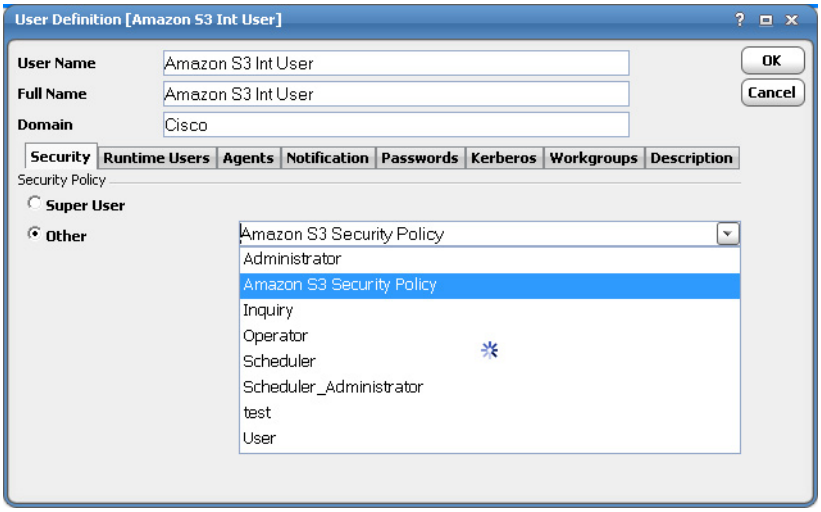
For further information about setting up security policies, see your *Cisco Workload Automation User Guide*.

Defining CWA Users

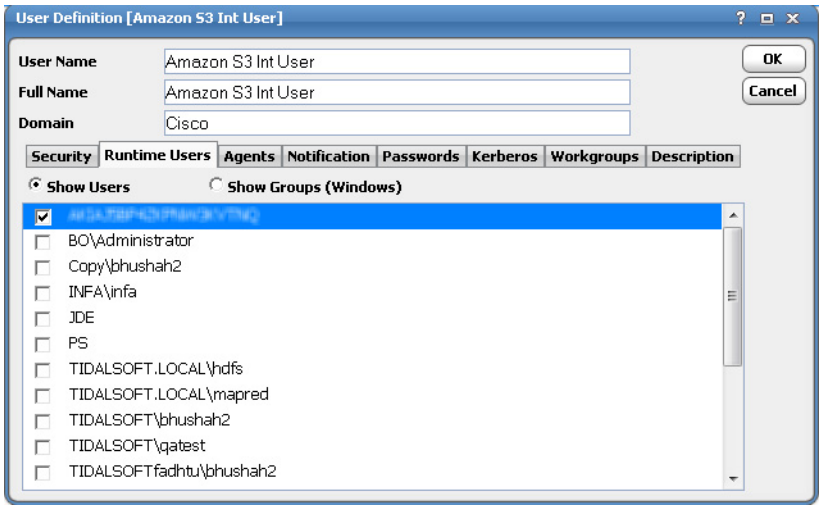
To define a CWA user to work with Amazon S3 Adapter jobs:

1. From the **Navigator** pane, expand the **Administrative** node and select **Interactive Users** to display the defined users.
2. Right-click **Interactive Users** and select **Add Interactive User** from the context menu (*Insert* mode). You can also right-click a user in the **Interactive Users** pane and select **Edit Interactive User** from the shortcut menu (*Edit* mode).

The **User Definition** dialog displays.



3. If this is a new user definition, enter the new user name in the **User/Group Name** field.
4. For documentation, enter the **Full Name** or description associated with this user.
5. In the **Domain** field, select a Windows domain associated with the user account required for authentication, if necessary.
6. On the **Security** page, select the **Other** option and then select the security policy that includes authorization for Amazon S3 Adapter jobs.
7. Click the **Runtime Users** tab.



8. Select the Amazon S3 Adapter users that this scheduling user can use for Amazon S3 Adapter authentication from Amazon S3 Adapter jobs.
9. Click the **Agents** tab.
10. Select the check boxes for the Amazon S3 Adapter connections that this scheduling user can access when scheduling jobs.

11. Click **OK** to save the user definition.

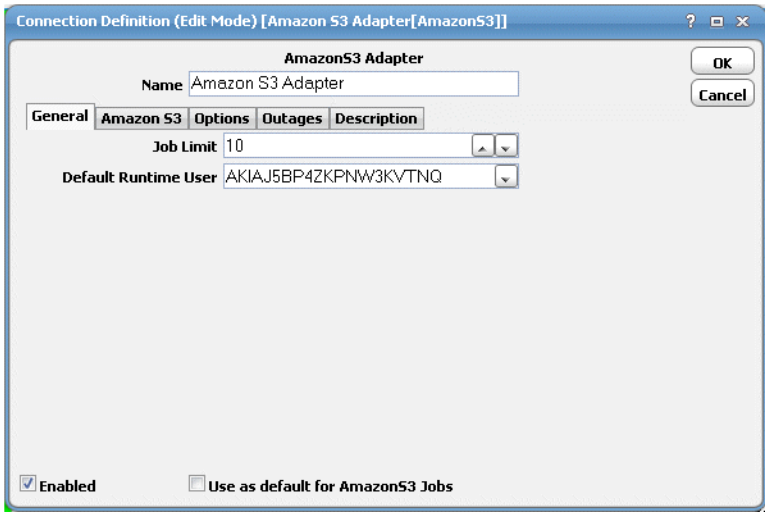
Defining a Connection

You must create one or more Amazon S3 connections before CWA can run your Amazon S3 Adapter jobs. These connections also must be licensed before CWA can use them. A connection is created using the **Connection Definition** dialog.

To define an Amazon S3 connection:

1. From the **Navigator** pane, navigate to **Administration>Connections** to display the **Connections** pane.
2. Right-click **Connections** and select **Add Connection>AmazonS3 Adapter** from the context menu.

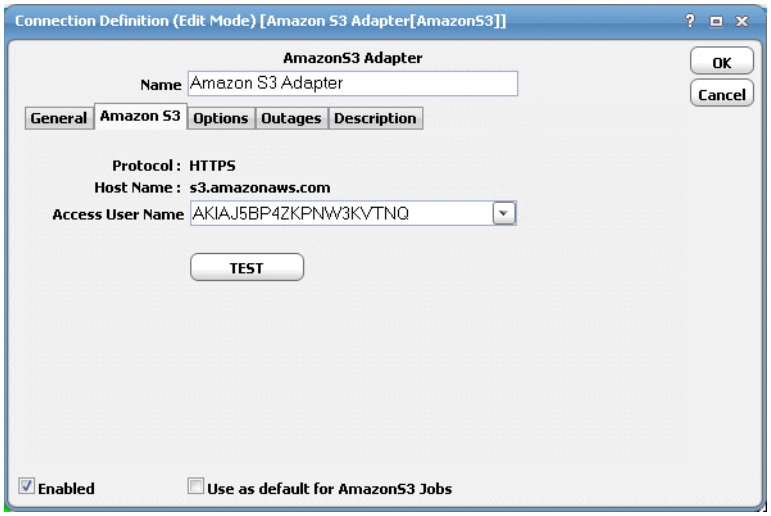
   The **Amazon S3 Adapter Connection Definition** dialog displays.



3. On the **General** page, enter a name for the new connection in the **Name** field.
4. In the **Job Limit** field, select the maximum number of concurrent active processes that CWA should submit to the Amazon S3 server at one time.
5. From the **Default Runtime User** drop-down list, you have the option to select the name of a default user for Amazon S3 Adapter jobs. The runtime user is auto-selected when defining Amazon S3 Adapter jobs.

   Only authorized users that have been defined with Amazon S3 passwords display in this list. The selected user is automatically supplied as the default runtime user in a new CWA Amazon S3 Adapter job definition.

6. Click the **Amazon S3** connection tab.



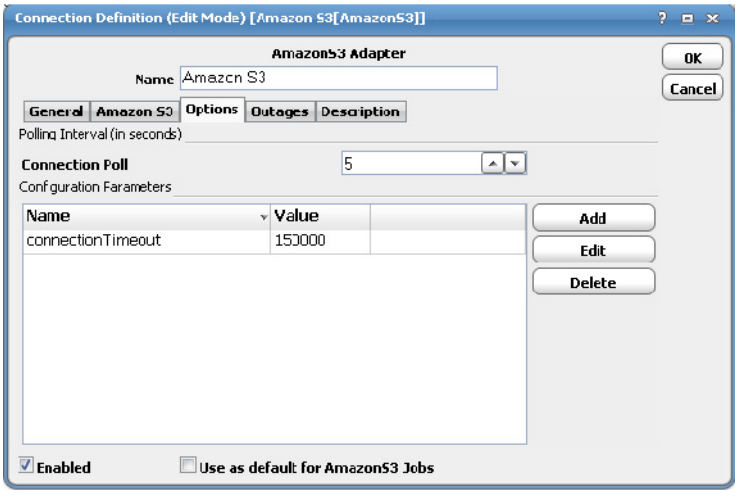
The connection **Protocol** is **HTTPS** and **Host Name** is **s3.amazonaws.com**.

7. From the **Access User Name** list, select the S3 user name.

Note: The Access User will be used for to interact with Amazon S3 and request needed information. The connection availability pings Amazon S3 without actually logging in to Amazon S3. Click Test to verify that your access credentials are valid.

8. (*Optionally*) Click the **Test** button to verify connectivity.

9. Click the **Options** tab to specify Global Job Parameters that are applicable to all jobs using the connection. If the job definition specifies the same job parameters, the values defined in the job definition will override the corresponding connection values. The Configuration Parameters are general connection parameter options. Currently, there are no connection level parameters for the Amazon S3 Adapter.



10. To add a parameter, click **Add** to display the **Parameter Definition** dialog.

11. Click **OK** to save the new Amazon S3 connection. The configured connection displays in the **Connections** pane.

The status light next to the connection indicates whether the CWA Master is connected to the Amazon S3 service. If the light is green, the Amazon S3 service is connected.

A red light indicates that the master cannot connect to the Amazon S3 service. Amazon S3 jobs will not be submitted without a connection to the Amazon S3 service. You can only define jobs from the Client if the connection light is green.

If the light is red, you can test the connection to determine the problem. Right-click the connection and select **Test** from the shortcut menu. A message displays on the **Test Amazon S3 Connection** dialog describing the problem. Or go to **Operator>Logs** to look for error messages associated with this connection.

3

Using the Amazon S3 Adapter

This chapter covers these topics:

- Defining Amazon S3 Jobs, page 17
- Monitoring Amazon S3 Job Activity, page 35
- Controlling Adapter and Agent Jobs, page 39

Defining Amazon S3 Jobs

This section provides instructions for defining an Amazon S3 job in CWA and descriptions of the various operation types that can be defined:

- Create Bucket Operation, page 17 – Allows you to create a new bucket, define region, configure bucket Access Control Lists (ACL) and user permission objects security policy, and enable versioning.

  To apply parameter value into the supported field, user use ":" as an indication for a parameter variable. The parameter is defined on the Parameters tab and the parameter variable's value will be substituted during runtime.

- Update Bucket Operation, page 23– Allows you to update a selected bucket configuration. You can modify user permissions and bucket policies, website, lifecycle, and versioning.

- Delete Bucket Operation, page 27 – Allows you to delete a bucket. When deleting a bucket, all objects and all versions, only if versioning is enabled, will be deleted including previously deleted markers.

- Update Object(s) Operation, page 27 – Allows you to modify the objects' configuration including user permissions, storage, and metadata.

- Rename/Restore Object Operation, page 31 – Allows you to rename an object within the same bucket or retrieve/restore a specified version of object. Renaming an object across buckets involves the **Copy** and **Delete** operations. Restoring an object from a specific version into a different bucket involves the **Copy** operation only.

- Move, Copy, and Delete Object(s) Operations, page 33:

  - **Move objects** – You can move one or more objects to a different bucket. The move operation involves the **Copy** and **Delete** operations.

  - **Copy objects** – You can copy one or more objects from one bucket to another. Additionally, you can copy all versions of a given object(s).

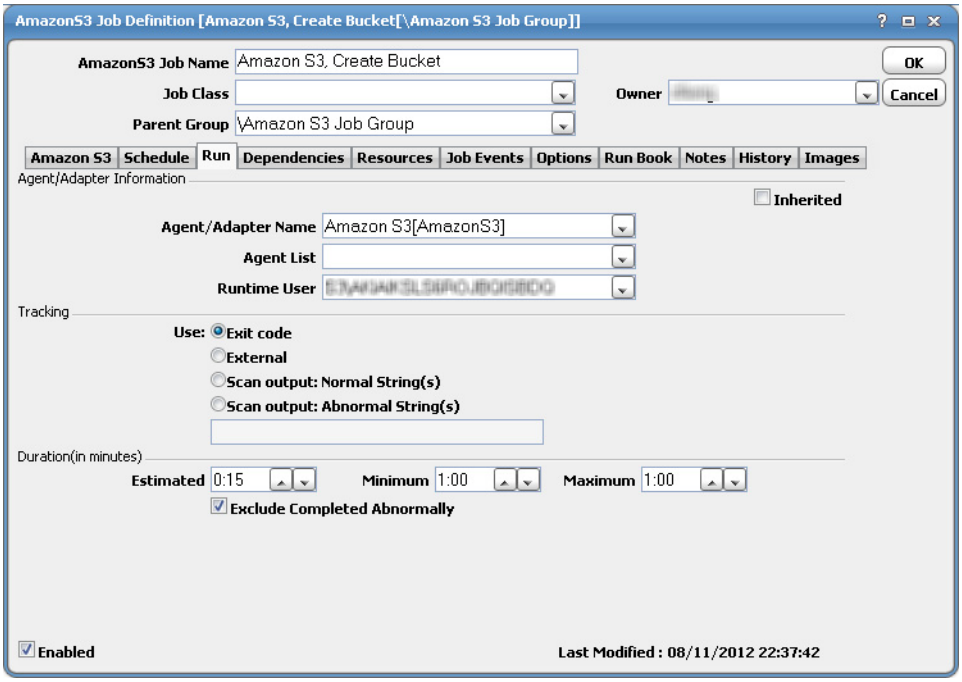
  - **Delete objects** – You can delete one or more objects.

Create Bucket Operation

This section describes the basic steps for defining an Amazon S3 job for creating a bucket.

To define an Amazon S3 job that creates a bucket:

1. In the **Navigator** pane, select **Definitions>Jobs** to display the **Jobs** pane.
2. Right-click **Jobs** and select **Add Job>AmazonS3 Job** from the context menu. The **Amazon S3 Job Definition** dialog displays.



The **Run** tab is selected by default. You must first specify a name for the job, the Amazon S3 Adapter connection that will be used for the job and a valid runtime user who has the appropriate Amazon S3 authority for the job being scheduled.

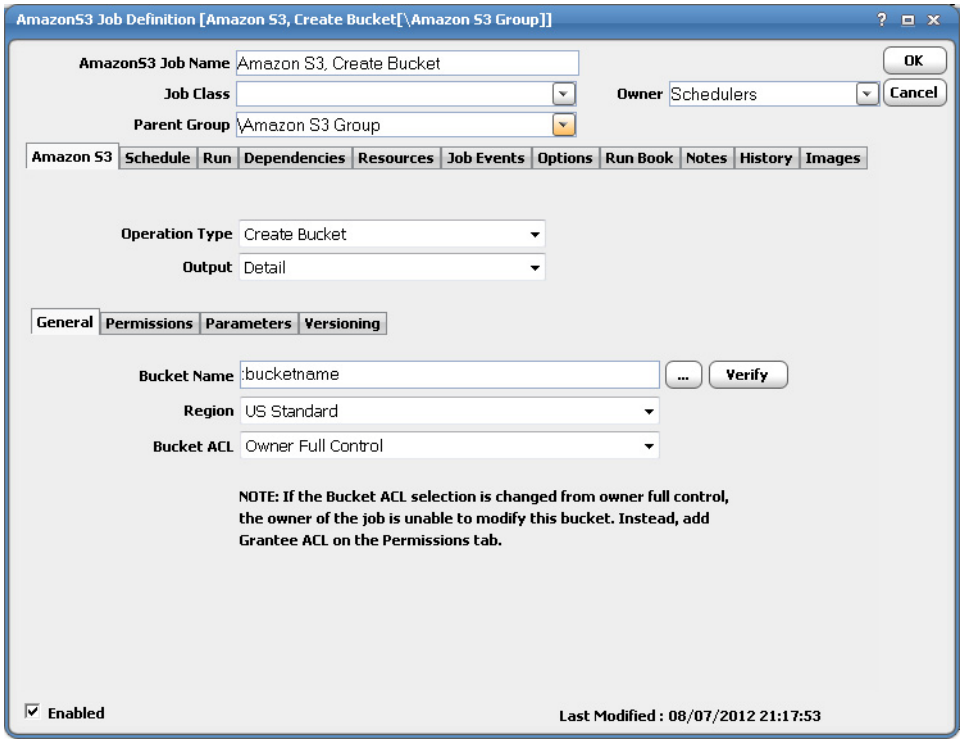
3. In the upper portion of the dialog, specify the following information to describe the job:
   - **Job Name** – Enter a name that describes the job.
   - **Job Class** – If you want to assign a defined job class to this job, select it from the drop-down list. This field is optional.
   - **Owner** – Select the Amazon S3 owner of the selected report/ Web Intelligence. The user must have the appropriate Amazon S3 authority for the operation.
   - **Parent Group** – If this job exists under a parent group, select the name of the parent group from the drop-down list. All properties in the **Agent Information** section are inherited from its parent job group.
4. Specify the following connection information in the **Agent/Adapter Information** section:
   - **Agent/Adapter Name** – Select the Amazon S3 Adapter connection to be used for this job from the drop-down list.

   -or-

   Agent List Name – Select a list for broadcasting the job to multiple servers.
   - **Runtime User** – Select a valid runtime user with the appropriate Amazon S3 authority for the job from the drop-down list.

Note: Verify the runtime user who will have required permission rights for the above operations to avoid a failed job.

5. Specify the appropriate Tracking and Duration information for the job. Refer to the *Cisco Workload Automation User Guide* for information on these options.
6. Click the **Amazon S3** tab.
7. On the **General** tab, select the **Create Bucket** operation from the **Operation Type** list.



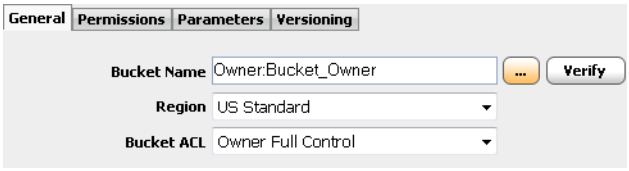
Except for **US Standard**, use the following guidelines when naming a bucket to remain DNS compliant.

- Bucket names must be between 3 and 63 characters long
- Bucket name must be a series of one or more labels separated by a period (.), where each label:
  - Must start with a lowercase letter or a number
  - Must end with a lowercase letter or a number
  - Can contain lowercase letters, numbers and dashes
- Bucket names must not be formatted as an IP address (e.g., 192.168.5.4)

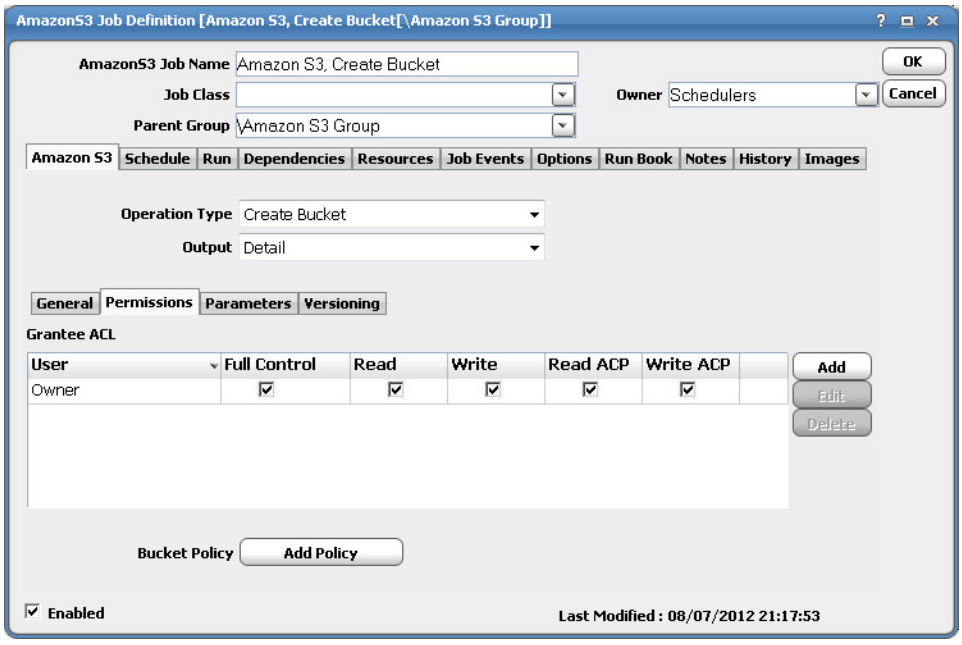
  In the **US Standard** region, you can optionally name a bucket using the following less restrictive rules:
  - Bucket names can be longer, between 3 and 255 characters long
  - Bucket names can contain any combination of uppercase letters, lowercase letters, numbers, periods (.), dashes (-) and an underscores (_)

  Additionally, you can use a parameter variable in the **Bucket Name** field by specifying ":" in front of the field value.

For example:

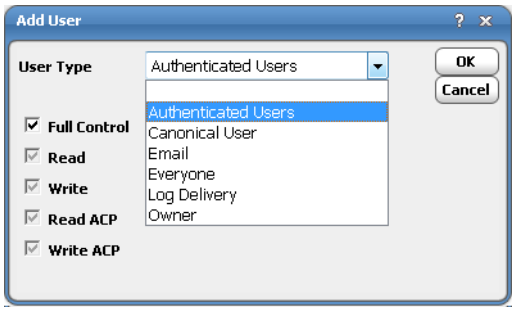


8. From the **Output** list, select one of the following output types:
   - **Simple** – will only return bucket name which allows bucket name to as input for another job, such as data mover job.
   - **Detail** – will return create bucket operation detail.
9. In the **Bucket Name** field, enter a name for the new bucket.
10. Click **Verify** to verify that the entered bucket name is available. A verification message displays.
11. From the **Region** list, select one of the following bucket locations.
    - **US Standard** – This is the default region. The US Standard Region automatically routes requests to facilities in Northern Virginia or the Pacific Northwest.
    - **US West Region**–Uses Amazon S3 servers in Oregon and Northern California.
    - **EU Region**–Uses Amazon S3 servers in Ireland.
    - **Asia Pacific Region**–Uses Amazon S3 servers in Singapore and Tokyo.
    - **South America Region**–Uses Amazon S3 servers in Sao Paulo.
12. From the **Bucket ACL** list, assign the bucket permission during creation. The default permission is Owner Full Control.
13. Click the **Permissions** tab to add, edit, or delete Grantee ACL Users and assign them permissions.



Amazon S3 stores objects in buckets. All buckets and objects are associated with access control policies. ACL is a mechanism which decides who can access what and consists of a set of permissions of read, write and update on Object as well as Bucket on the basis of these ACLs. Bucket ACLs are completely independent of Object ACLs. Meaning, ACLs set on a bucket can be different of ACLs set on any object, contained in bucket.

To add a grantee, click **Add** to display the **Add User** dialog.



From the **User Type** list, select one of the following types for an ACL:

- **Owner** – By default, an owner has full permission. An owner can create access and delete objects. The owner can also view and modify ACLs of each and every owner owned Bucket and its object(s).
- **Email** – If an owner wants to share or allow another Amazon S3 user to access a bucket, then the owner should know the email address of the invitee. This will only work if the invitee has registered his/her Amazon s3 account with that email address.
- **Authenticated Users** – This group represents all Amazon AWS accounts. Access permission to this group allows any Amazon AWS account to access the resource.
- **Canonical User** – Access permission to this group allows anyone with a Canonical User Id access to buckets and objects within your Amazon S3 account. The canonical user id is specific to S3 and is a 64 character long hex string.
- **Everyone** – Access permission to this group allows anyone to access the resource. The requests can be signed (authenticated) or unsigned (anonymous).
- **Log Delivery** – WRITE permission on a bucket enables this group to write server access logs to the bucket.

Select the ACL type for the selected permission.The following type of ACL are provided by Amazon S3:

With reference to Bucket:

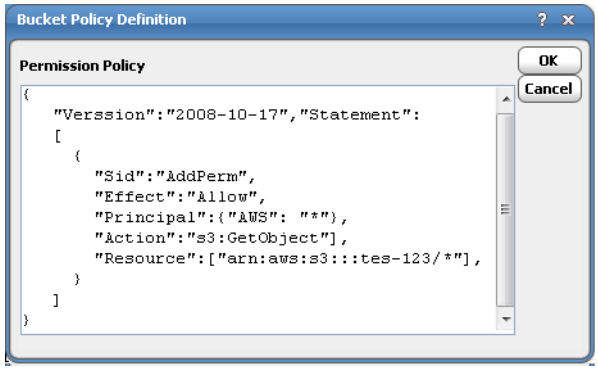
- **Read** – Authorized user can list the file names, their size and last modified date from a bucket.
- **Write** – Authorized user can upload new files in your bucket. They can also delete files on which they don't have permission. Someone with write permission on a bucket can delete files even if they do not have read permission to those files.
- **Read ACP** – Authorized users can check ACL of a bucket.
- **Write ACP** – Authorized user can update ACL of the bucket.

With reference to Object:

- **Read** – Authorized user can download the file.
- **Write** – Authorized user can replace the file or delete it.
- **Read ACP** – Authorized user can list ACL of that file.

- **Write ACP** – Authorized user can modify the ACL of the file.

Optionally, on the **General** tab, you can click **Add Policy** to add a permission policy via the **Bucket Policy Definition** dialog.

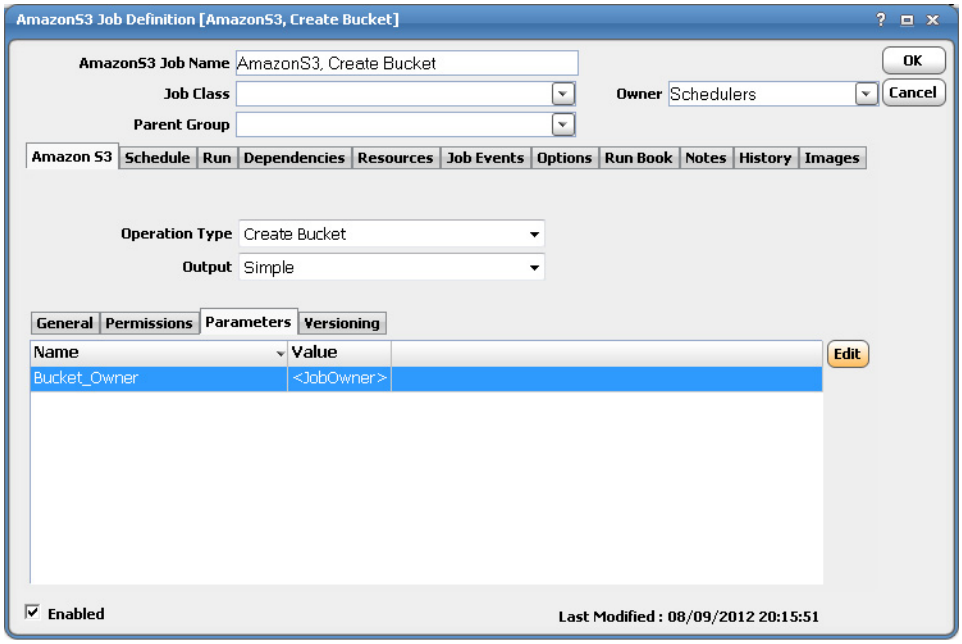


A permission policy is a JSON string containing the policy contents and statements. The policy can have granular control of the object, but is controlled at the bucket level. A policy includes:

- Optional policy-wide information (at the top of the document)
- One or more individual statements

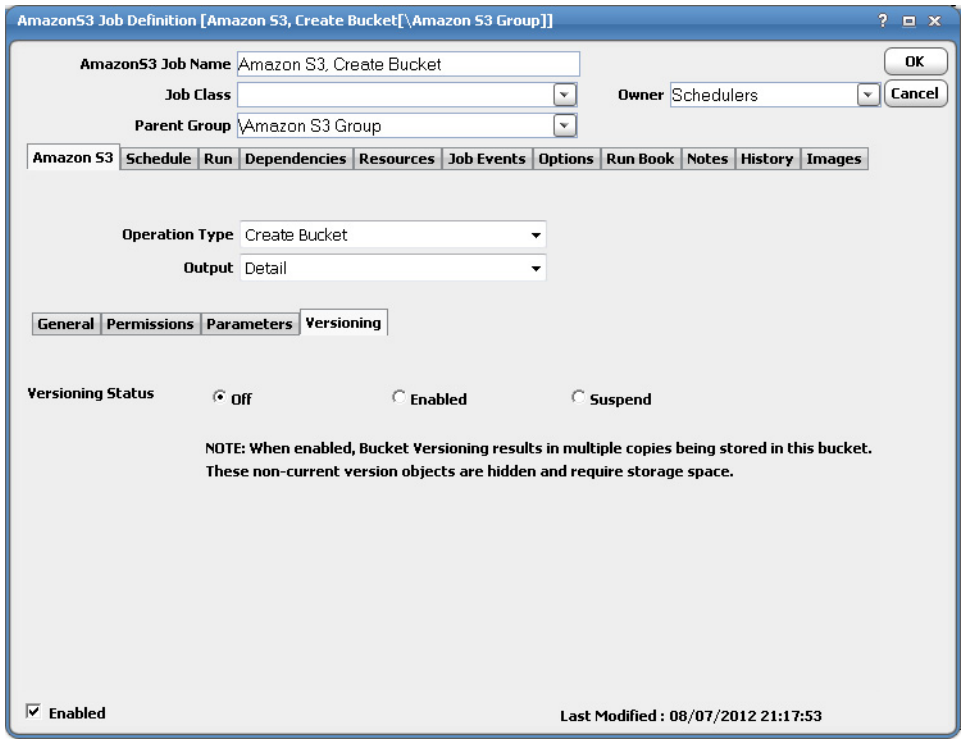
Each statement includes the core information about a single permission.

14. Click the **Parameters** tab to view or edit a list of parameters specified on the **General** tab. The parameter value is resolved during runtime.



To edit a parameter, select the parameter, then click **Edit** to display the **Parameter Definition** dialog.

15. Click the **Versioning** tab to set the versioning status and behavior.



Versioning enables you to keep multiple versions of an object in one bucket. You must explicitly enable versioning on your bucket. By default, versioning is disabled. Regardless of whether you have enabled versioning on your bucket or not, each object has a version ID. If you have not enabled versioning on your bucket, then Amazon S3 sets the version ID value to null. If you have enabled versioning on your bucket, Amazon S3 assigns a unique version ID value for the object.

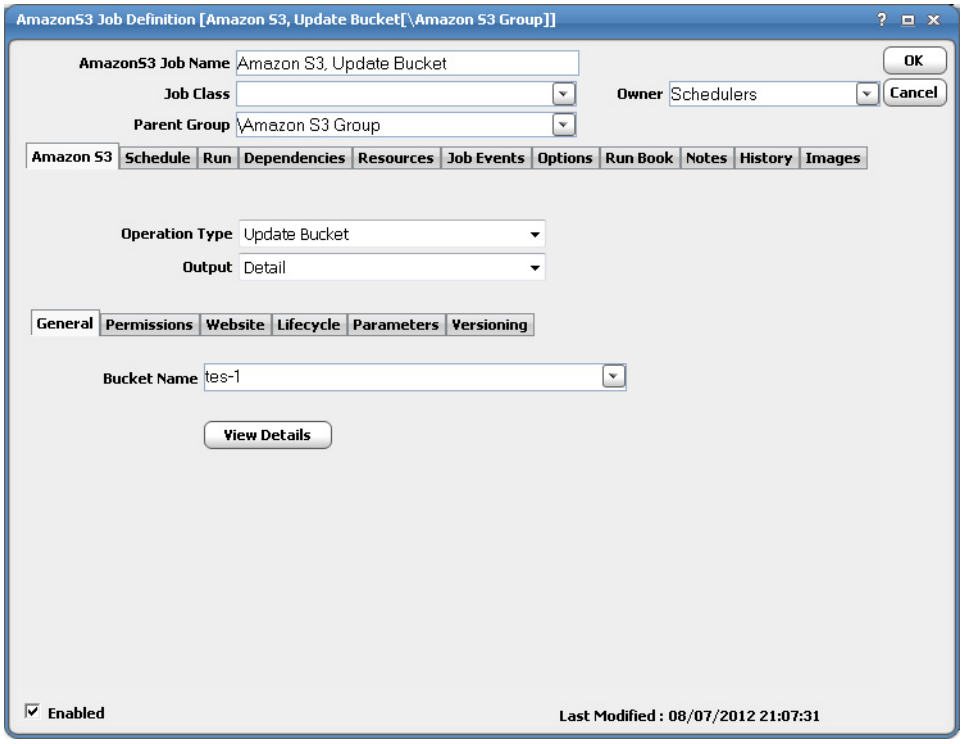
16. Click **OK** to save the job.

Update Bucket Operation

This section describes the basic steps for defining an Amazon S3 job for updating a bucket.

To define an Amazon S3 job that updates a bucket:

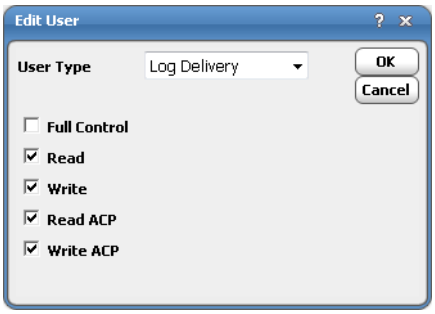
1. From the **Amazon S3** tab, and select **Update Bucket** from the **Operation Type** list.



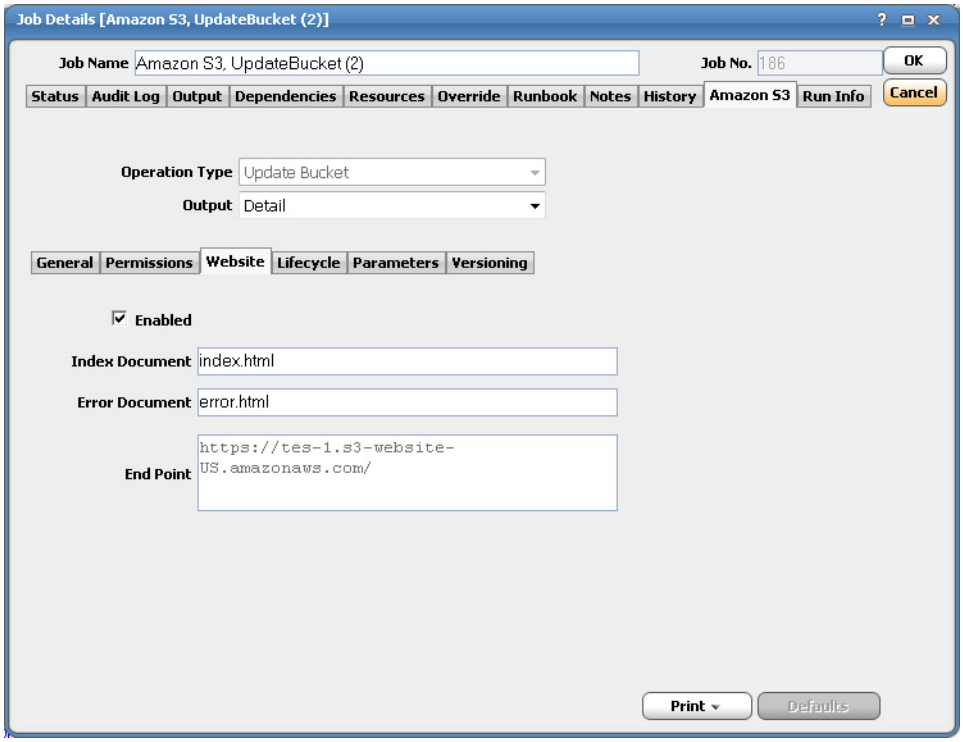
2. From the **Output** list, select one of the following output types:
   - **Simple** – will only return the updated bucket name.
   - **Detail** – will return updated bucket operation detail.
3. From the **Bucket Name** list, select the bucket you want to update.
4. Optionally, click **View Details** to display the **Bucket Details** dialog.

   This dialog contains the following elements:
   - **Region** – the location of the bucket.
   - **Creation Date** – the timestamp when this selected bucket was created.
   - **Owner** – the owner of bucket.
5. Click the **Permissions** tab to add, edit, or delete Grantee ACL Users and assign them permissions.

To edit a grantee, click **Edit** to display the **Edit User** dialog.



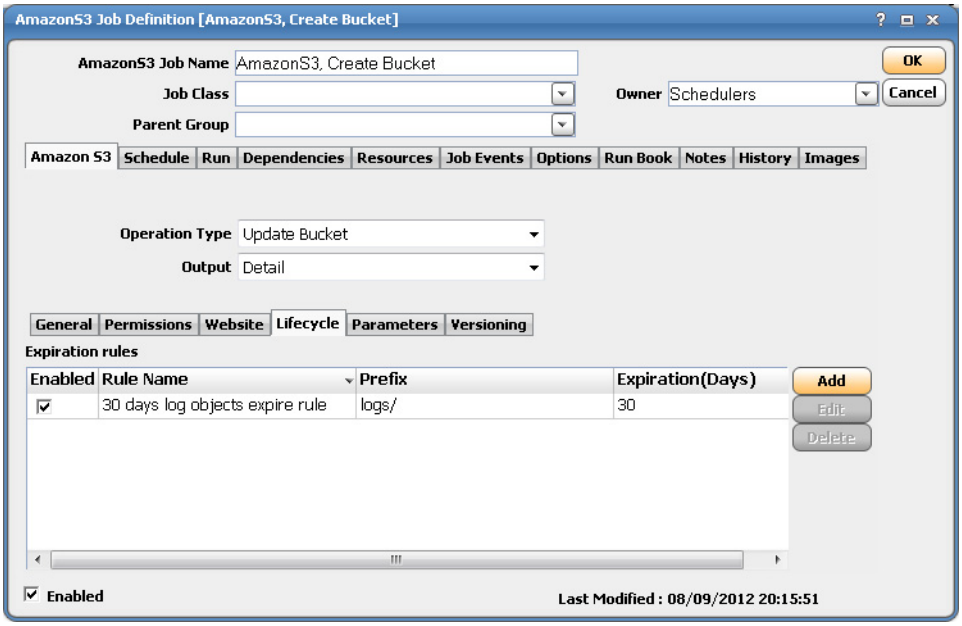
6. Click the **Website** tab to enable and configure an Amazon S3 website using the corresponding bucket as the content source. The website will have one default domain name associated with it, which is the bucket name.



This dialog contains the following elements:

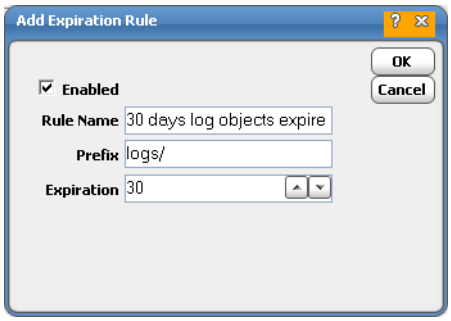
- **Enabled** – select to enable website configuration.
- **Index Document** – index document/page for the website if the bucket is associated with the website domain.
- **Error Document** – error document/page for accessing the website if the bucket is associated with the website domain.
- **End Point** – display URL assigned by Amazon S3 while creating a bucket.

7. Click the **Lifecycle** tab to set a lifecycle configuration on your bucket. The lifecycle configuration describes the lifetime of various objects in your bucket.



A lifecycle configuration contains rules, which identify an object prefix and a lifetime for objects that begin with this prefix. The lifetime is the number of days after creation that you want the object removed.

To add an expiration rule for an object, click **Add** to display the **Add Expiration Rule** dialog.



This dialog contains the following elements:

- **Enabled** – check to enable the expiration rule
- **Rule Name** – name of the expiration rule
- **Prefix** – specify a key prefix. The expiration rule applies to all objects whose key names begin with this prefix.
- **Expiration** – the number of days after creation that you want the object removed.

8. Click the **Parameters** tab to view or edit a list of parameters specified on the **General** tab. The parameter value is resolved during runtime.

   To edit a parameter, select the parameter, then click **Edit** to display the **Parameter Definition** dialog.

9. Click the **Versioning** tab to set the versioning status and behavior.

Versioning enables you to keep multiple versions of an object in one bucket. You must explicitly enable versioning on your bucket. By default, versioning is disabled. Regardless of whether you have enabled versioning on your bucket or not, each object has a version ID. If you have not enabled versioning on your bucket, then Amazon S3 sets the version ID value to null. If you have enabled versioning on your bucket, Amazon S3 assigns a unique version ID value for the object.

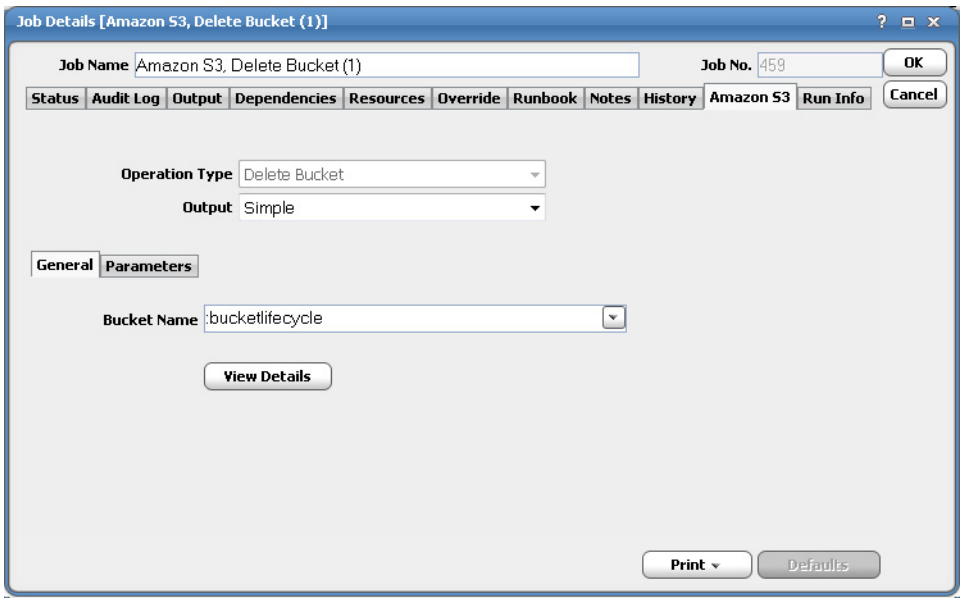
10. Click **OK** to save the job.

Delete Bucket Operation

This section describes the basic steps for defining an Amazon S3 job for deleting a bucket.

To define an Amazon S3 job that deletes a bucket:

1. From the **Amazon S3** tab, and select the **Delete Bucket** operation from the **Operation Type** list.



2. From the **Output** list, select one of the following output types:
   - **Simple** – will only return the deleted bucket name.
   - **Detail** – will return deleted bucket operation detail.
3. From the **Bucket Name** list, select the bucket you want to delete.
4. Optionally, click **View Details** to display the **Bucket Details** dialog.
5. Click the **Parameters** tab to view or edit a list of parameters specified on the **General** tab. The parameter value is resolved during runtime.

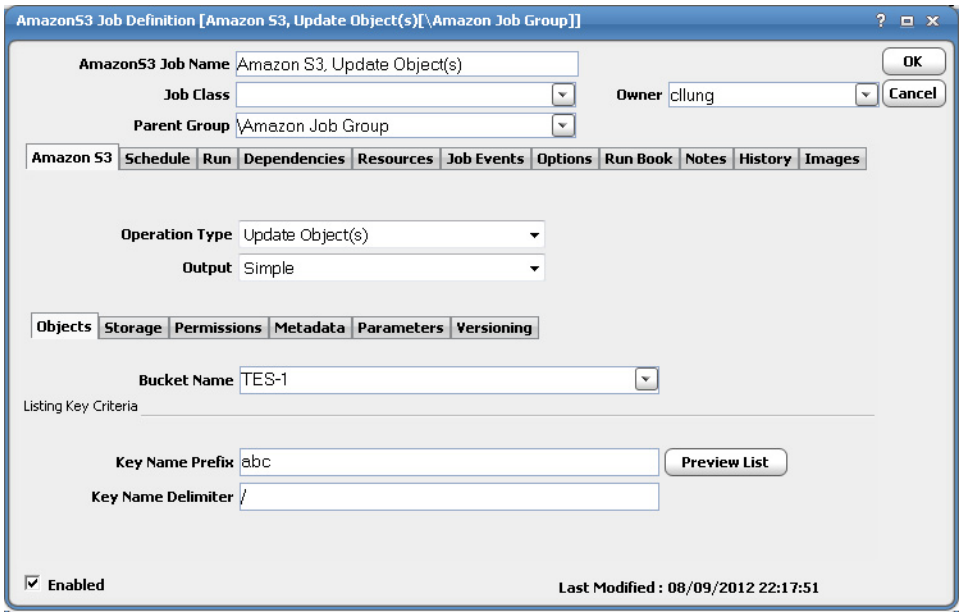
   To edit a parameter, select the parameter, then click **Edit** to display the **Parameter Definition** dialog.
6. Click **OK** to save the job.

Update Object(s) Operation

This section describes the basic steps for defining an Amazon S3 job for updating objects.

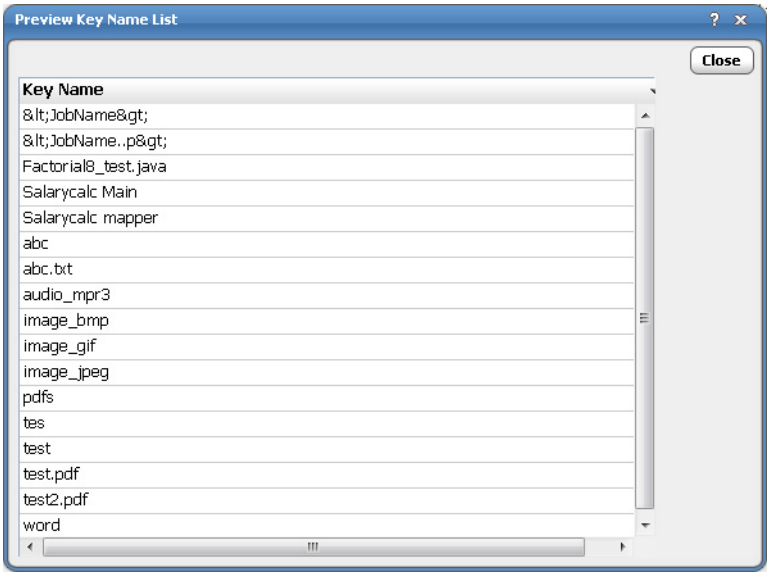
To define an Amazon S3 job that updates object(s):

1. From the **Amazon S3** tab, and select the **Update Object(s)** operation from the **Operation Type** list.



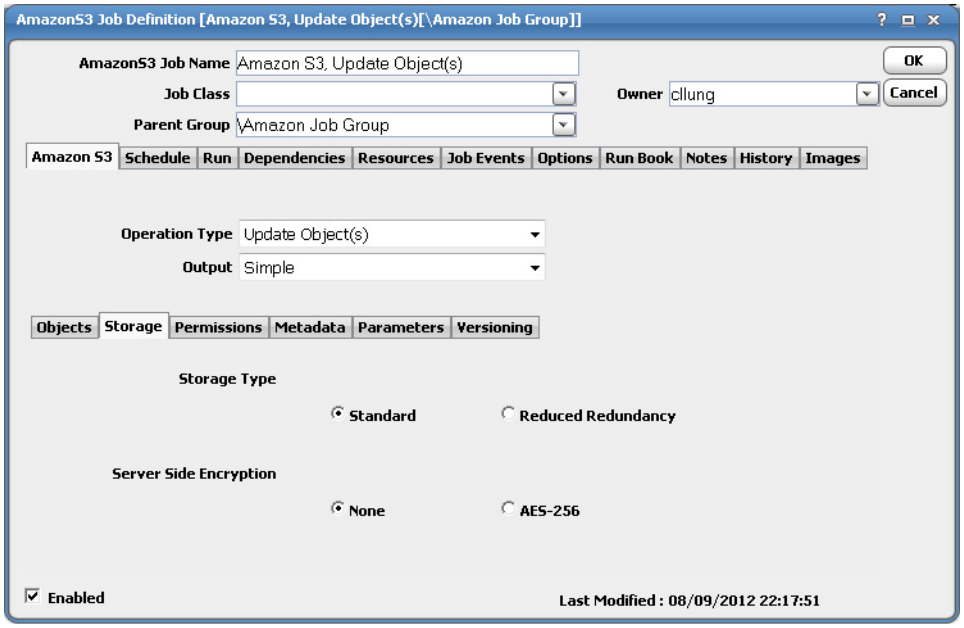
2. From the **Output** list, select one of the following output types:
   - **Simple** – will only return the updated object(s) name.
   - **Detail** – will return updated object(s) operation detail.
3. From the **Bucket Name** list, select the bucket you want to update the objects for.
4. In the **Key Name Prefix** field, enter a common prefix for the names of related keys.

   Optionally, you can click the **Preview** list button to display the **Preview Key Name List** dialog.



The dialog contains a list of existing key names that exist for the selected bucketed based on the Key Criteria entered.

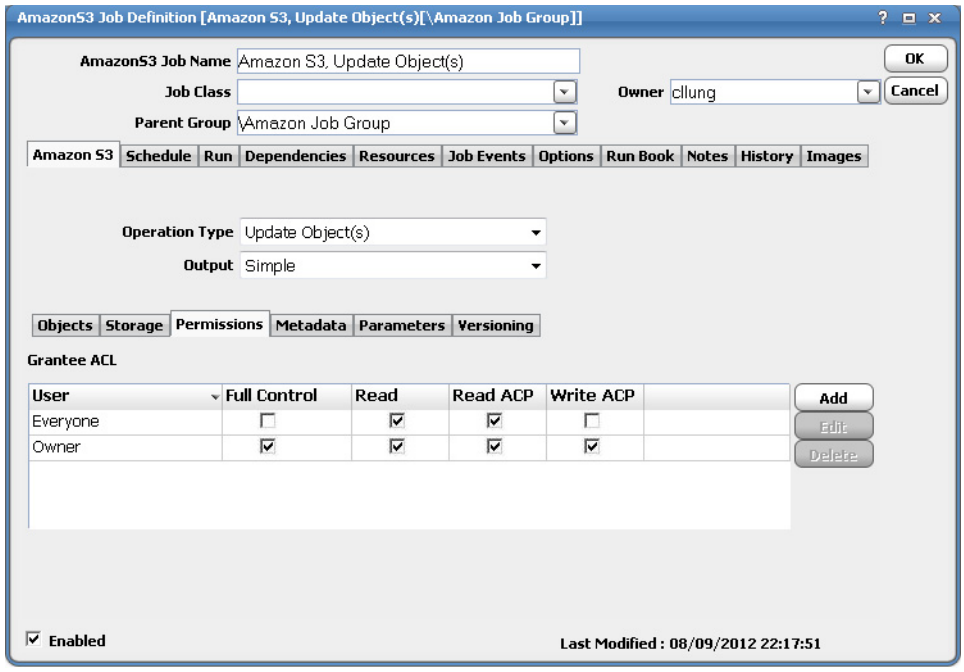
5. In the **Key Name Delimiter** field, enter a special character that will be used to mark the keys for delimiting hierarchy.
6. Click the **Storage** tab to set the storage type and server side encryption.



This tab contains the following elements:

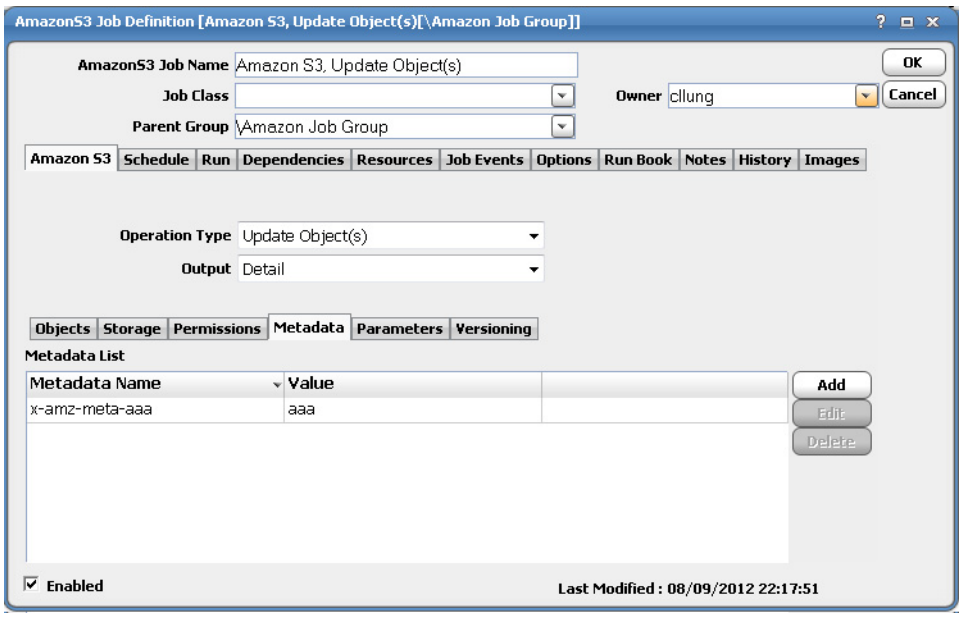
- **Storage Type** – Amazon S3 supports the following types of storage:
  - **Standard** – select for standard Amazon S3 storage. This is default.
  - **Reduced Redundancy** – Stores non-critical, reproducible data at lower levels of redundancy than the standard storage.
- **Server Side Encryption** – Amazon S3 will maintain encryption key and decrypted while downloading the objects.
  - **None** – No server side encryption. This is the default.
  - **AES-256** – 256-bit AES is used to encrypt your data.

7. Click the **Permissions** tab to add, edit, or delete Grantee ACL Users and assign them permissions.



To edit a grantee, select the grantee record, then click **Edit** to display the **Edit User** dialog.

8. Click the **Metadata** tab to add, edit or delete system and user-defined metadata. Metadata is a set of name-value pairs.

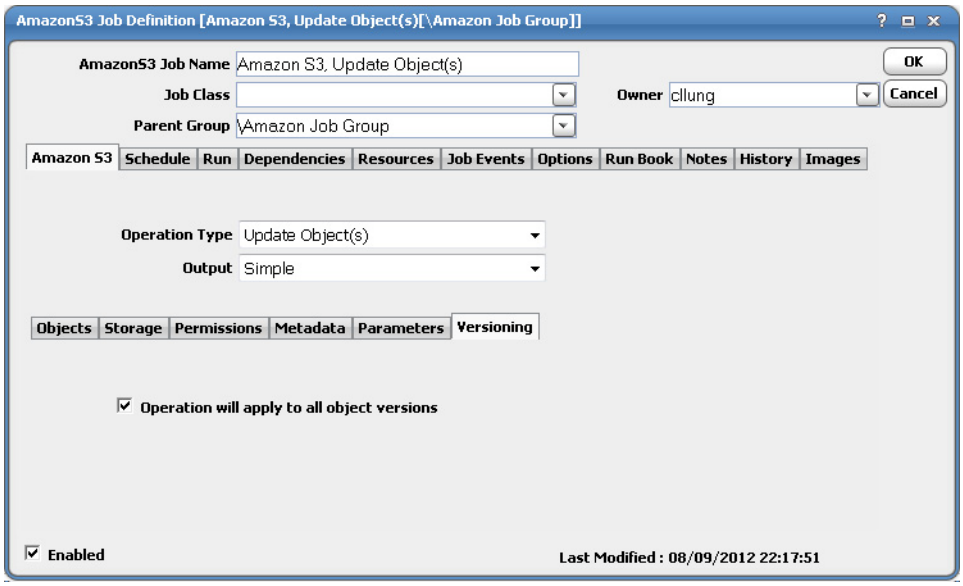


- To add metadata for an object, click **Add** to display the **Add Metadata** dialog.
- To edit an existing metadata record, select Edit to modify the metadata via the **Edit Metadata** dialog.

9. Click the **Parameters** tab to view or edit a list of parameters specified on the **Objects** tab. The parameter value is resolved during runtime.

To edit a parameter, select the parameter, then click **Edit** to display the **Parameter Definition** dialog.

10. Click the **Versioning** tab to set the versioning status and behavior.



Select the **Operation will apply to all object versions** option if you want the update operation to update all versions associated with the assigned object(s).

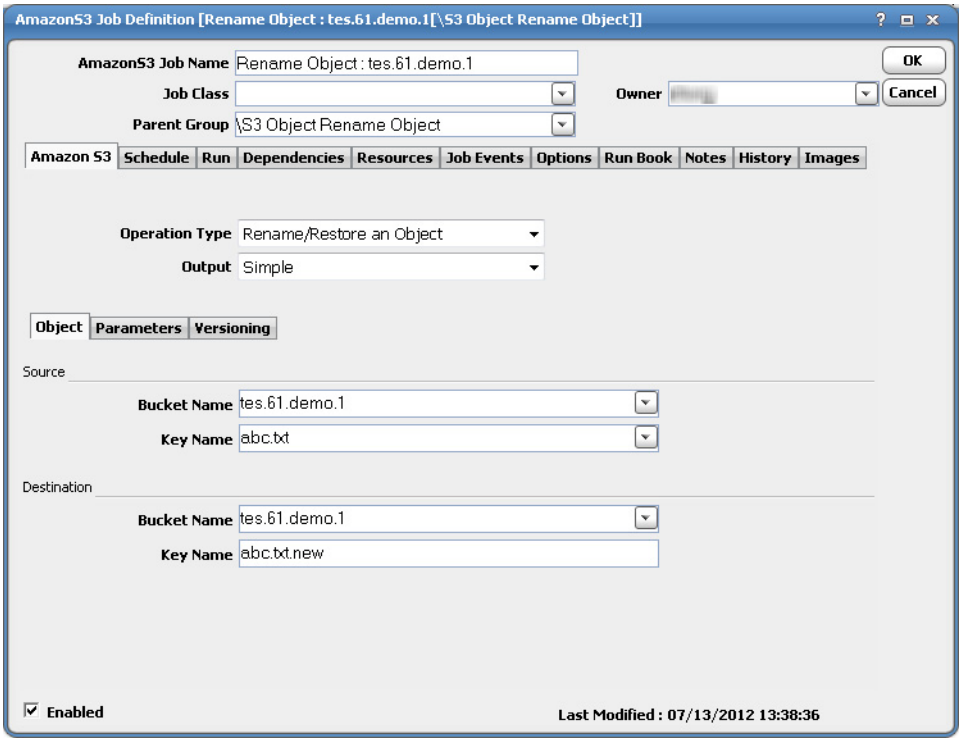
11. Click **OK** to save the job.

Rename/Restore Object Operation

This section describes the basic steps for defining an Amazon S3 job for renaming or restoring objects.

To define an Amazon S3 job that renames or restores objects:

1. From the **Amazon S3** tab, and select the **Rename/Restore Object** operation from the **Operation Type** list.



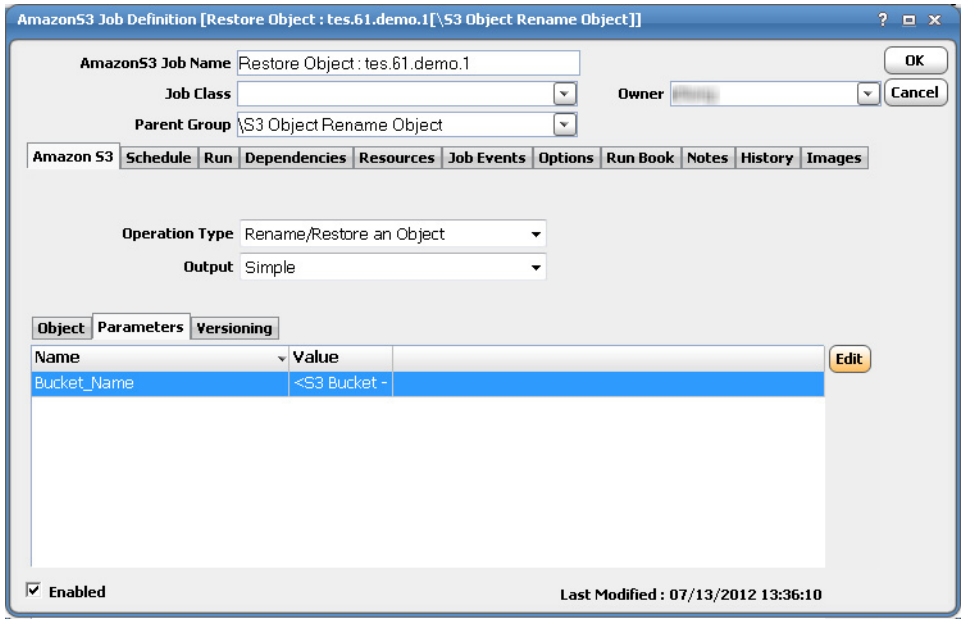
2. From the **Output** list, select one of the following output types:

   Simple – will only return the updated bucket name.

   Detail – will return update bucket operation detail.

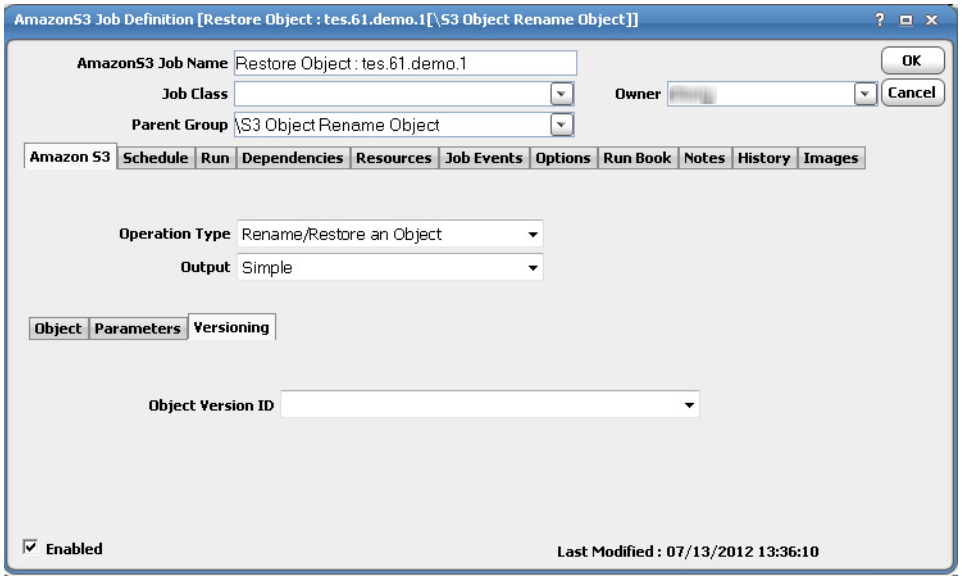
3. From the **Bucket Name** list, select the source bucket objects you want rename or restore.
4. In the **Key Name** field, enter the key name of the object.
5. From the **Bucket Name** list, select the destination bucket you want to put the renamed or restored bucket objects.
6. In the **Key Name** field, enter the key name of the object.

7. Click the **Parameters** tab to view or edit a list of parameters specified on the **Objects** tab. The parameter value is resolved during runtime.



To edit a parameter, select the parameter, then click **Edit** to display the **Parameter Definition** dialog.

8. Click the **Versioning** tab to set the versioning status and behavior.



If applicable, from the **Object Version ID** list, select the version of the object you want to restore or rename.

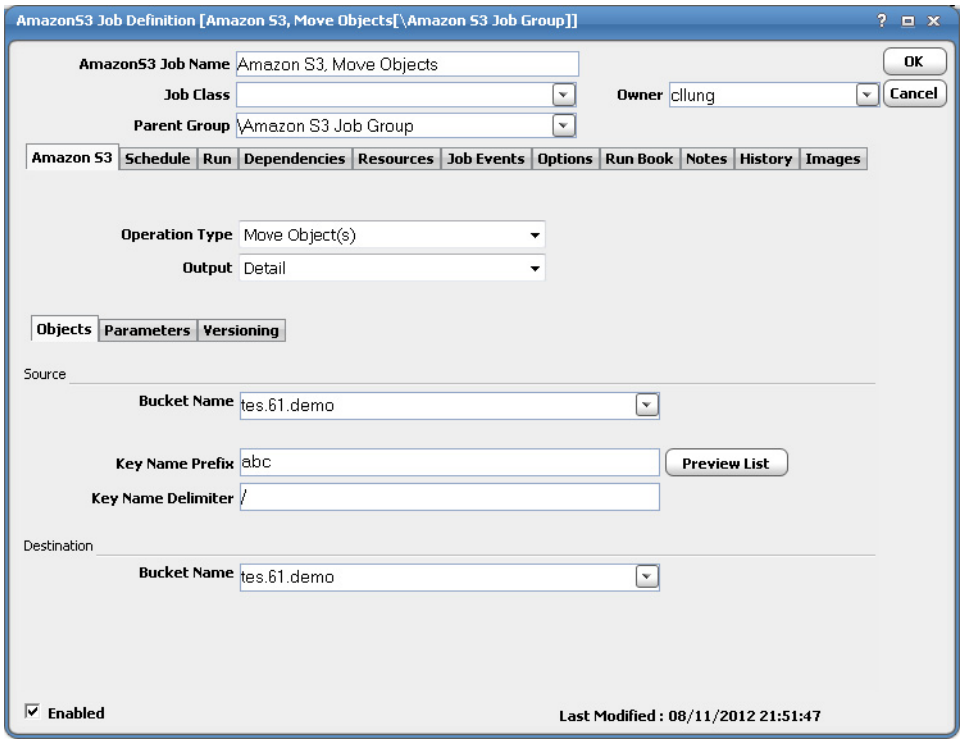
9. Click **OK** to save the job.

Move, Copy, and Delete Object(s) Operations

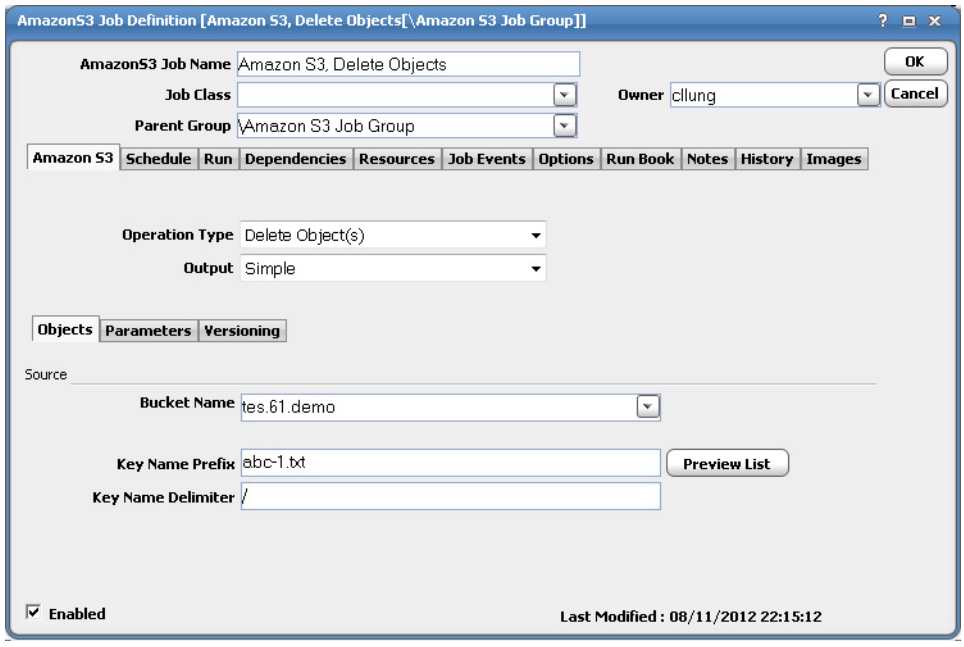
This section describes the basic steps for defining an Amazon S3 job for moving, copying, or deleting objects.

To define an Amazon S3 job that moves, copies, or deletes objects:

1. From the **Amazon S3** tab, and select the **Move Object(s)** or **Copy Object(s)** operation from the **Operation Type** list.



For the **Delete Object(s)** operation type, the **Objects** tab displays as follows:



2. From the **Output** list, select one of the following output types:

   – **Simple** – will only return the moved or copied object(s) name.

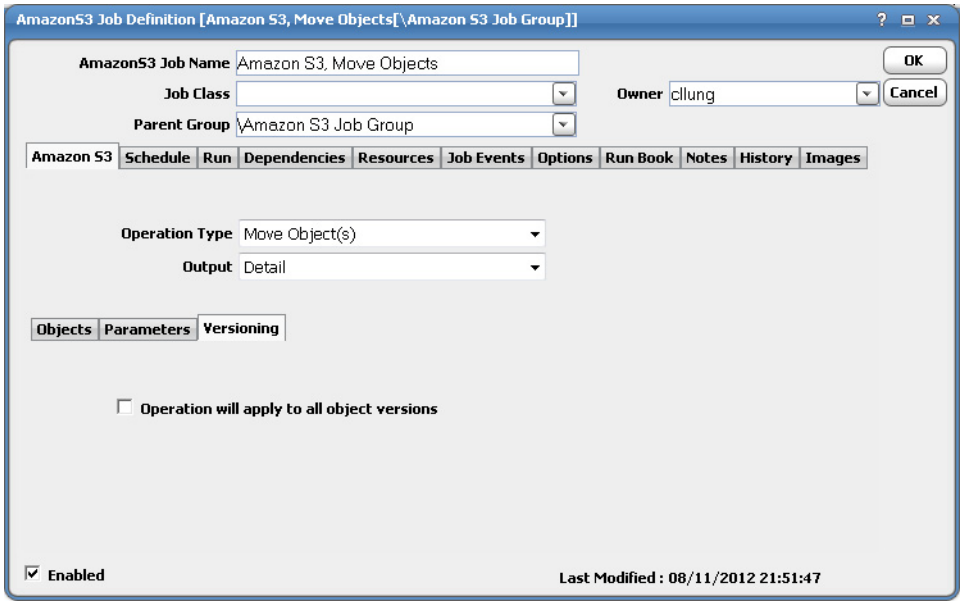
- **Detail** – will return the moved or copied object(s) operation detail.

3. From the **Bucket Name** list, select the source bucket you want to move, copy, or delete the objects from.
4. In the **Key Name Prefix** field, enter a common prefix for the names of related keys.

   Optionally, you can click the **Preview** list button to display the **Preview Key Name List** dialog.

   This dialog contains a list of existing key names that exist for selected bucket and entered Key Name Prefix.
5. In the **Key Name Delimiter** field, enter a special character that will be used to mark the keys for delimiting hierarchy.
6. For the **Move Object(s)** or **Copy Object(s)** operations, select the source bucket you want to move or copy the objects to from the **Bucket Name** list.
7. Click the **Parameters** tab to view or edit a list of parameters specified on the **Objects** tab. The parameter value is resolved during runtime.

   To edit a parameter, select the parameter, then click **Edit** to display the **Parameter Definition** dialog.
8. Click the **Versioning** tab to set the versioning status and behavior.



9. Select the **Operation will apply to all object versions** option if you want the **Move** or **Copy** operation to move or copy all versions associated with the assigned object(s).
10. Click **OK** to save the job.

Monitoring Amazon S3 Job Activity

As Amazon S3 operations run as pre-scheduled jobs, you can monitor the jobs as you would any other type of job in CWA using the **Job Details** dialog. You can also use Business Views to monitor job activity and view when the jobs are active (see your *Cisco Workload Automation User Guide* for instructions on using Business Views).

To monitor job activity:

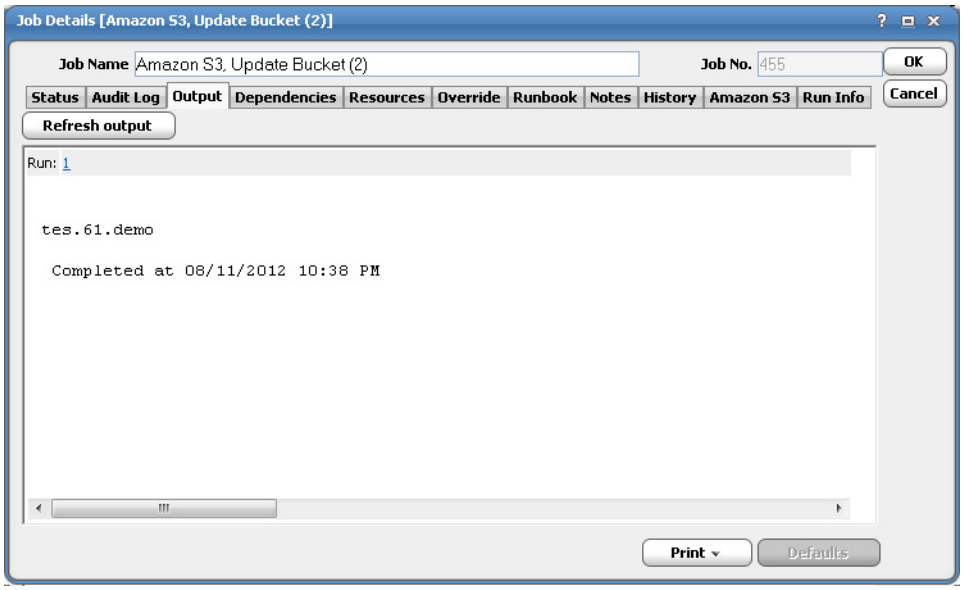
1. In the **Navigator** pane, select **Operations>Job Activity** to display the **Job Activity** pane.

2. Right-click to select a job and choose **Details** from the context menu.

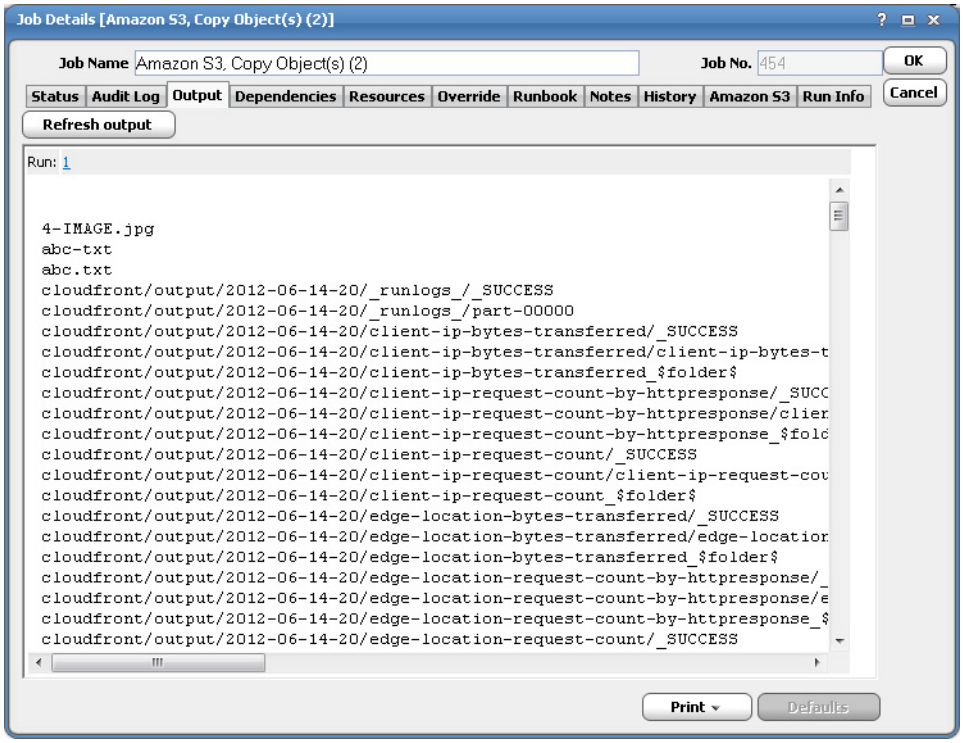
   The **Job Details** dialog displays. On the **Status** page, you can view the status of the job, the start and end time, how long it ran, and how it was scheduled. The external ID is the run ID associated with the specific execution of the job.

3. Click the **Output** tab to view the job output.

   If you selected **Simple** from the Job Definition's **Output** list, the **Output** tab displays as follows:

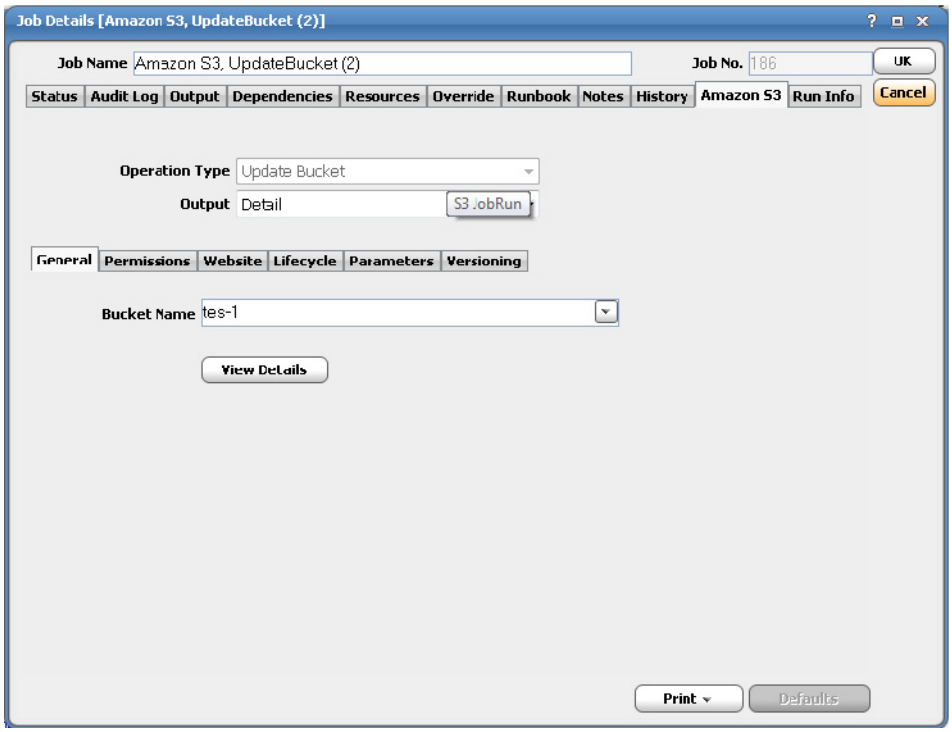


If you selected **Details** from the Job Definition's **Output** list, the **Output** tab displays as follows:



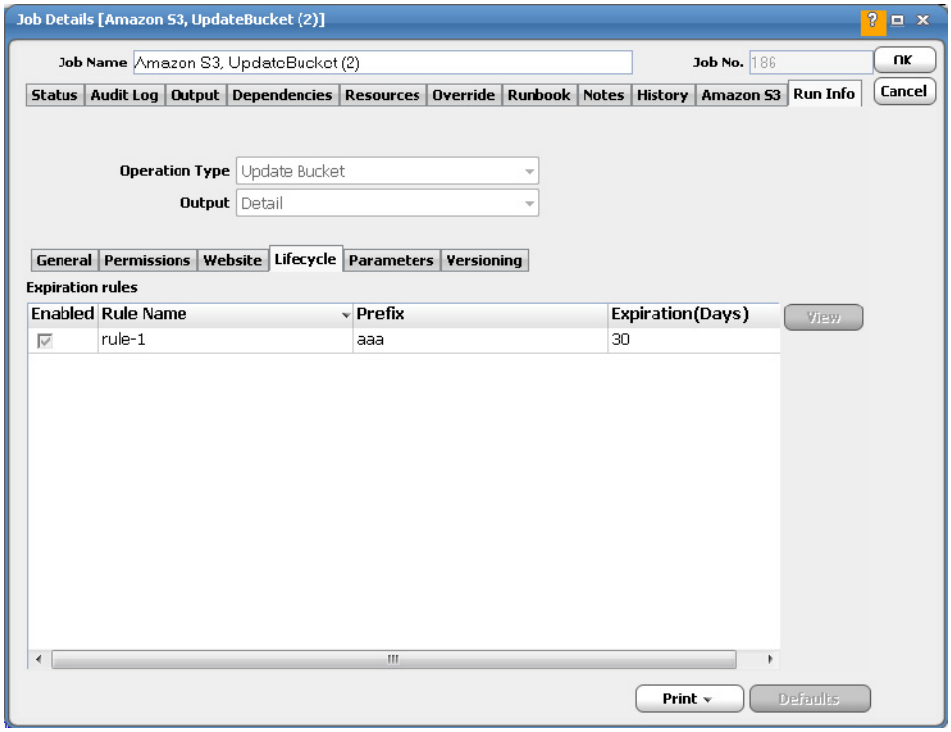
CWA can be configured to save or discard job output by default from the **Defaults** tab of the **System Configuration** dialog. Regardless of the system default, any individual job instance can be configured from its job definition to override the system default. Each time a job is rerun, that run's output is separated by a block of number signs.

4. Click the **Amazon S3** tab to view the original request along with variables used when this job was submitted. This tab allows you to override the output format and parameter values prior to run or rerun. Overrides are not permitted when the job is running.



While the job is running, the fields are disabled; however, prior to running or rerunning the job, you can override any value on this screen. Your changes here only apply to this instance of the job (the original job definition is not affected).

5. Click the **Run Info** tab to view the run status, start, and end time for each step in the Amazon S3 job. This tab is read-only.



6. When you have finished viewing the job activity details, click **OK** to close the dialog.

Controlling Adapter and Agent Jobs

Scheduler provides the following job control capabilities for either the process currently running or the job as a whole:

- Holding a Job–Hold a job waiting to run.
- Aborting a Job–Abort an active job.
- Rerunning a Job–Rerun a job that completed.
- Making One Time Changes to an Adapter or Agent Job Instance–Make last minute changes to a job.
- Deleting a Job Instance before It Has Run–Delete a job instance before it has run.

Holding a Job

Adapter/agent jobs are held in the same way as any other Scheduler jobs.

Adapter/agent jobs can only be held before they are launched. Once a job reaches the Adapter/Agent system, it cannot be held or suspended.

To hold a job:

1. From the **Job Activity** pane, right-click on the job.
2. Select **Job Control>Hold/Stop**.

Aborting a Job

Adapter/agent jobs are aborted in the same way as any other Scheduler jobs.

To abort a job:

1. From the **Job Activity** pane, right-click on the job.
2. Select **Job Control>Cancel/Abort**.

Rerunning a Job

On occasion, you may need to rerun an Adapter/Agent job. You can override parameter values first, if necessary, from the Adapter/Agent tab.

To rerun a job:

1. From the **Job Activity** pane, right-click the Adapter/Agent job you need to rerun.
2. Select **Job Control>Rerun** option from the context menu.

Making One Time Changes to an Adapter or Agent Job Instance

Prior to a run or rerun, you can edit data on the specific **Adapter/Agent** tab. To ensure that there is an opportunity to edit the job prior to its run, you can set the **Require operator release** option on the **Options** tab in the Adapter **Job Definition** dialog. Use this function to make changes to an Adapter job after it enters Waiting on Operator status as described in the following procedure.

To make last minute changes:

1. From the **Job Activity** pane, double-click the Adapter/Agent job to display the **Job Details** dialog.
2. Click the Adapter tab.
3. Make the desired changes to the job and click **OK** to close the **Job Details** dialog.
4. If this job is Waiting on Operator, perform one of the following tasks:

- To release the job, select **Job Control->Release**.
- To rerun the job with changes, select **Job Control->Rerun**.

Deleting a Job Instance before It Has Run

Adapter/Agent job instances are deleted in the same way as any other Scheduler job.

Deleting a job from the **Job Activity** pane removes the job from the Scheduler job activity only. The original definition is left in tact.

To delete a job instance:

1. From the **Job Activity** pane, right-click the Adapter/Agent job to be deleted.
2. Select **Remove Job(s) From Schedule**.

5

Configuring service.props

About Configuring service.props

The **service.props** file is used to configure adapter behavior. **service.props** is located in the \config directory located under the Adapter's GUID directory, You can create both the directory and file if it does not yet exist. Properties that can be specified in service.props control things like logging and connection configuration. Many of the properties are specific to certain adapters; others are common across all adapters.

service.props Properties

The table below lists many of the parameters that can be specified in service.props. Some properties apply to all adapters (shaded in the table) and some properties are adapter-specific as indicated by the **Applicable Adapter(s)** column. The properties are listed in alphabetical order.

Property	Applicable Adapter(s)	Default	What It Controls
BYPASS_SEC_VALIDATION	Oracle Apps	N	If set to Y, the secondary user validation is bypassed. If not, secondary user validation is performed.
CLASSPATH	All	<none>	(Optional) – The path to the JDBC driver. If the default CLASSPATH used when the Adapter process is started does not include an appropriate JDBC driver jar required to connect to the PowerCenter Repository Database, you will need to specify this *service.props* configuration
CONN_SYNC	Informatica, Oracle Apps, SAP	N	Setting this flag to Y allows synchronous connections without overloading the RDOnly Thread. If set to N, the adapter might stop trying to reconnect after an outage or downtime.
DISCONN_ON_LOSTCONN	Informatica	N	Setting this flag to Y avoids an unnecessary logout call to the Informatica server when the connection is lost. This logout call usually hangs.
EnableDynamicPollingInterval	All	N	Use to avoid frequent polling on long-running jobs. When set to Y in service.props of a particular adapter, these properties are enabled: MinDynamicPollInterval–Minimum value should be 5 seconds. MaxDynamicPollIntervalInMin–Maximum value should be 5 minutes. PercentOfEstDuration–Default value is 5.

Property	Applicable Adapter(s)	Default	What It Controls
HADOOP_JAVA_HOME	Sqoop	<none>	If the Java version used in the Hadoop environment is lower than Java 8, then install the same lower JDK version in the in the Master and include the path of the JDK in this property.
IGNORE_CODES	Informatica	<none>	This parameter can be set in service.props, job configuration and connection configuration parameters. The order of precedence is service.props (applicable for all jobs running in all connections), job level (only for that particular job), and connection (applicable for all jobs in the connection). This parameter is used to specify Informatica-specific error codes, separated by commas (,), that you want to ignore while running a job.
IGNORESUBREQ	Oracle Apps	N	Y or N. Setting this flag to Y stops huge job xml file transfers back and forth between the adapter and the AdapterHost during polls when a single request set has multiple sub-requests of more than 100. The default value is N or empty.
kerbkdc	MapReduce	<none>	If the Hadoop cluster is Kerberos secured, use this value to specify the KDC Server. For example, **`kerbkdc=172.25.6.112`**
kerbrealm	MapReduce	<none>	If the Hadoop cluster is Kerberos secured, use this value to specify the Kerberos Realm. For example, **`kerbrealm=TIDALSOFT.LOCAL`**
Keystore	BusinessObjects, BusinessObjects BI, BusinessObjects DS, Cognos, JD Edwards, Oracle Applications, UCS Manager, VMware, Web Service	<none>	Specify Keystore=c:\\<adapter_certificate_directory>\\<your_trusted_keystore>.keystore when importing certificates into a Java keystore.
LAUNCH_DELAY (in milliseconds)	Informatica	<none>	This parameter can be set in service.props, job configuration and connection configuration parameters. The order of precedence is service.props (applicable for all jobs running in all connections), job level (only for that particular job), and connection (applicable for all jobs in the connection). If a non-zero value is set for this parameter, then the jobs are delayed for the specified number of milliseconds before being submitted to Informatica.

Property	Applicable Adapter(s)	Default	What It Controls
LoginConfig	BusinessObjects BI Platform, BusinessObjects Data Services	<none>	Specifies the location of the login configuration if using WinAD or LDAP authentication. For example: LoginConfig=c:\\windows\\bscLogin.conf where "`c:\\windows\\bscLogin.conf`" is the location of the login configuration information. Note the use of \\ if this is a Windows location.
MaxLogFiles	Informatica, JDBC, PeopleSoft	50	(Optional) – Number of logs to retain.
OUTPUT_ASYNC_LOGOUT	Informatica	N	Setting this flag to Y avoids jobs getting stuck in Gathering Output status.
OUTPUT_SYNC	All	Y	Enables concurrent output gathering on a connection. To enable this feature, set the value to N.
POLL_SYNC	All	Y	Enables concurrent polling on connections of the same type. This is helpful when there is a heavily load on one connection of an adapter. The heavily loaded connection will not affect the other adapter connection. To enable this feature, set the value to N.
QUERY_TIMEOUT	Oracle Apps	N	Y or N. If set to Y, the timeout value defined using the parameter QUERY_TIMEOUT_VALUE is applied to the SQL queries. Default value is N or empty.
QUERY_TIMEOUT_VALUE	Oracle Apps	unset	The time period in seconds that SQL queries wait before timeout. If 0 or not set, there is no timeout.
READPCHAINLOG	SAP	Y	Used to control the log gathering in SAP Process Chain jobs. This property depends on the Summary Only check box of the job definition Options tab.
SCANFOR_SESSIONSTATS	Informatica	Y	Y or N – Set this parameter to N to turn off the default behavior of Informatica jobs collecting the session statistics during the job run.
SCANFOR_SESSIONSTATS_AFTER_WF_ENDS	Informatica	N	Y or N – Set this parameter to Y to turn off the gathering of session statistics during each poll for the status of Informatica jobs.
TDLINFA_LOCALE	Informatica	<none>	Points to the Load Manager Library locale directory. See "Configuring the Informatica Adapter" in the *Informatica Adapter Guide* for how to set this for Windows and Unix environments.
TDLINFA_REQUESTTIMEOUT	Informatica	<none>	(Optional) – The number of seconds before an API request times out. The default is 120 seconds, if not specified.
TDLJDBC_LIBPATH	JDBC	<none>	(Windows only, optional) An alternate path to the JDBC library files. The library file path should have been configured given system environment variables. This option is available in case you wish to use an alternate set of libraries and may be helpful for trouble-shooting purposes.

Property	Applicable Adapter(s)	Default	What It Controls
TDLJDBC_LOCALE	JDBC	<none>	The path to the JDBC locale files.
TRANSACTION_LOG_BATCH_SIZE	MS SQL	5000	Set this parameter if more than 5000 lines need to be read from the transaction table.
version_pre898	JD Edwards	N	If running on a JD Edwards server version that is less than 8.9.8, set version_pre898=Y.