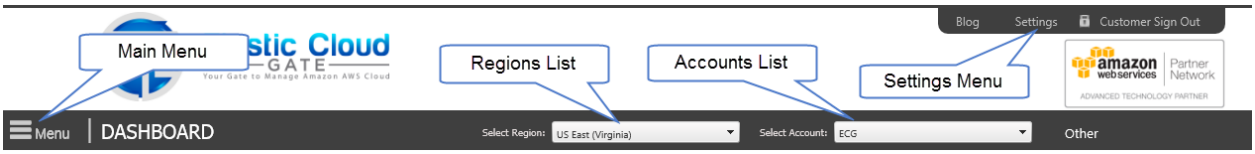
ELASTIC CLOUD GATE

User Manual

Table of Contents

Overview

Below is the list of common elements referred to in this user manual:



Main Menu
This menu is located on the left side of the top bar and is available on all pages. From the Main Menu, you can access all sections of ECG Portal.

Settings Menu
This menu is located on the right side of the top bar. Settings Menu provides access to frequently needed commands, including Manage Accounts, Manage Profile, and Change Password.

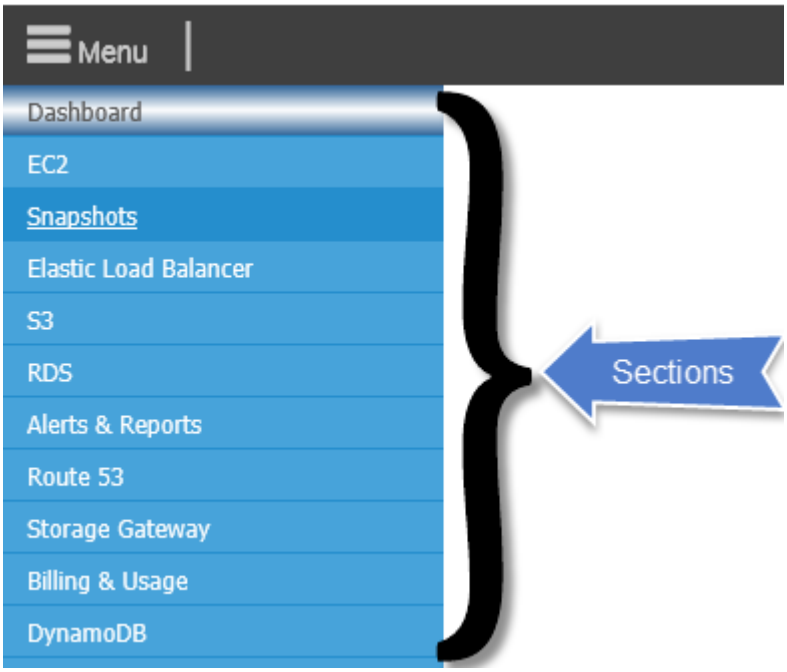
Accounts List
This list is located on the right side of the top bar. This is a drop down list containing all AWS Accounts currently setup under ECG Portal. When you select an account from this list, the data on the selected section will adjust according to the AWS Account.

Regions List
This list is located in the middle of the top bar. This is a drop down list of AWS Regions and is accessible only within the applicable section. When you select a different region from the one currently displayed, the data within that section will update accordingly.

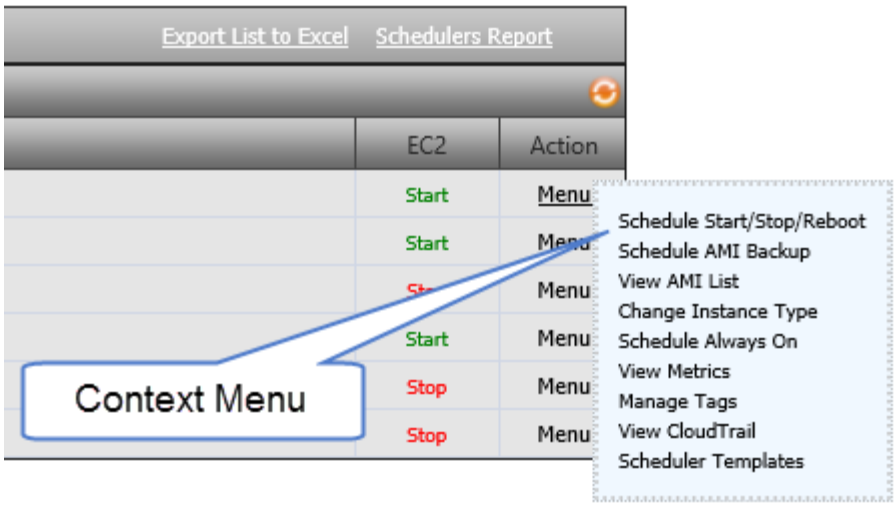
ECG provides you the option to set a default region that is automatically selected after login. To learn more about setting your default region, go to: How to update profile
How to update profile

Section
ECG Portal features are grouped together within related sections. For example, all features related to AWS EC2 Instances and EBS Volume are grouped together within the EC2 Section. Access the list of sections and switch between them by opening the Main Menu, as described above.

ECG allows you to set a default Section for login. To learn more about setting your default Section, go to: How to update profile
How to update profile

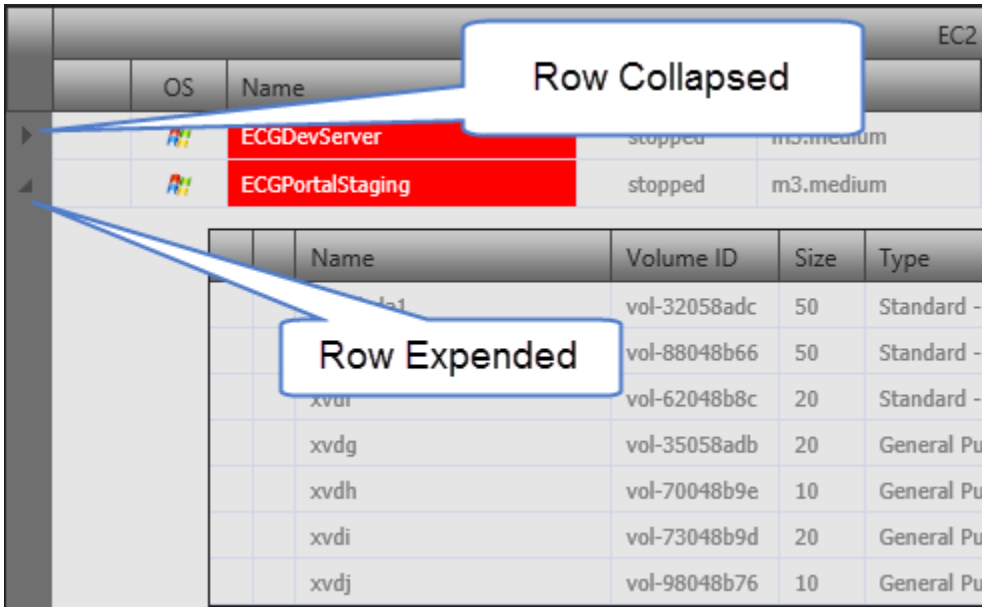


Context Menu
Context Menu is a menu that is available within certain data tables. Clicking a Context Menu shows the options available for the element shown in the table.



Expand Record/Black Arrow

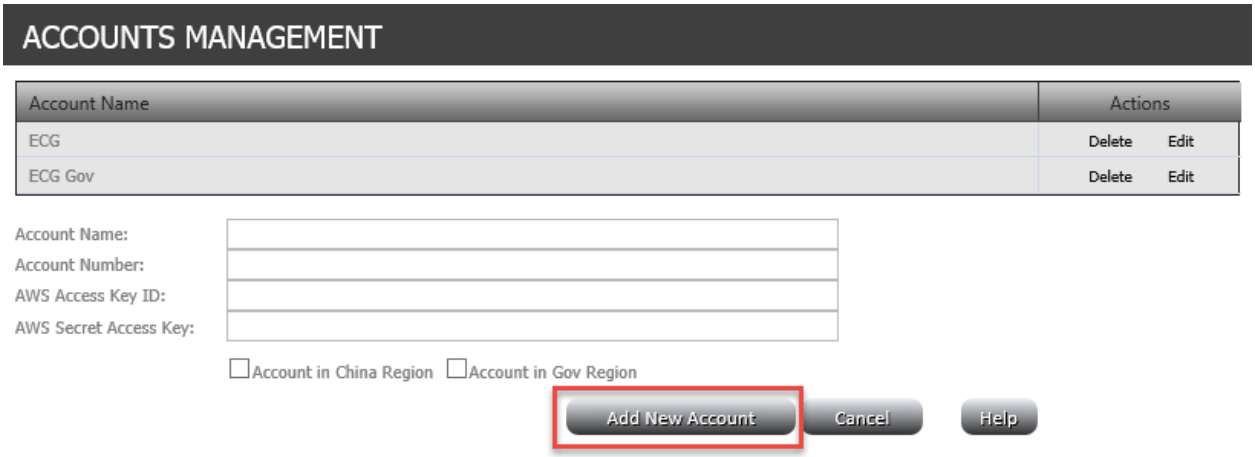
Some tables contain additional data viewable if the data record is expanded. To expand record, click the black arrow located in the first column. Anytime the black arrow is present in the first column, additional data for that record is available.



How to add or manage AWS Account

To add new AWS Account or manage an existing one, open the Settings Menu and select Manage Accounts.

To add a new account, enter the account name, account number (your AWS account number), the AWS Access Key, and the AWS Secret Key. Additionally, if the account is located in China or in CloudGov region, check the appropriate box.

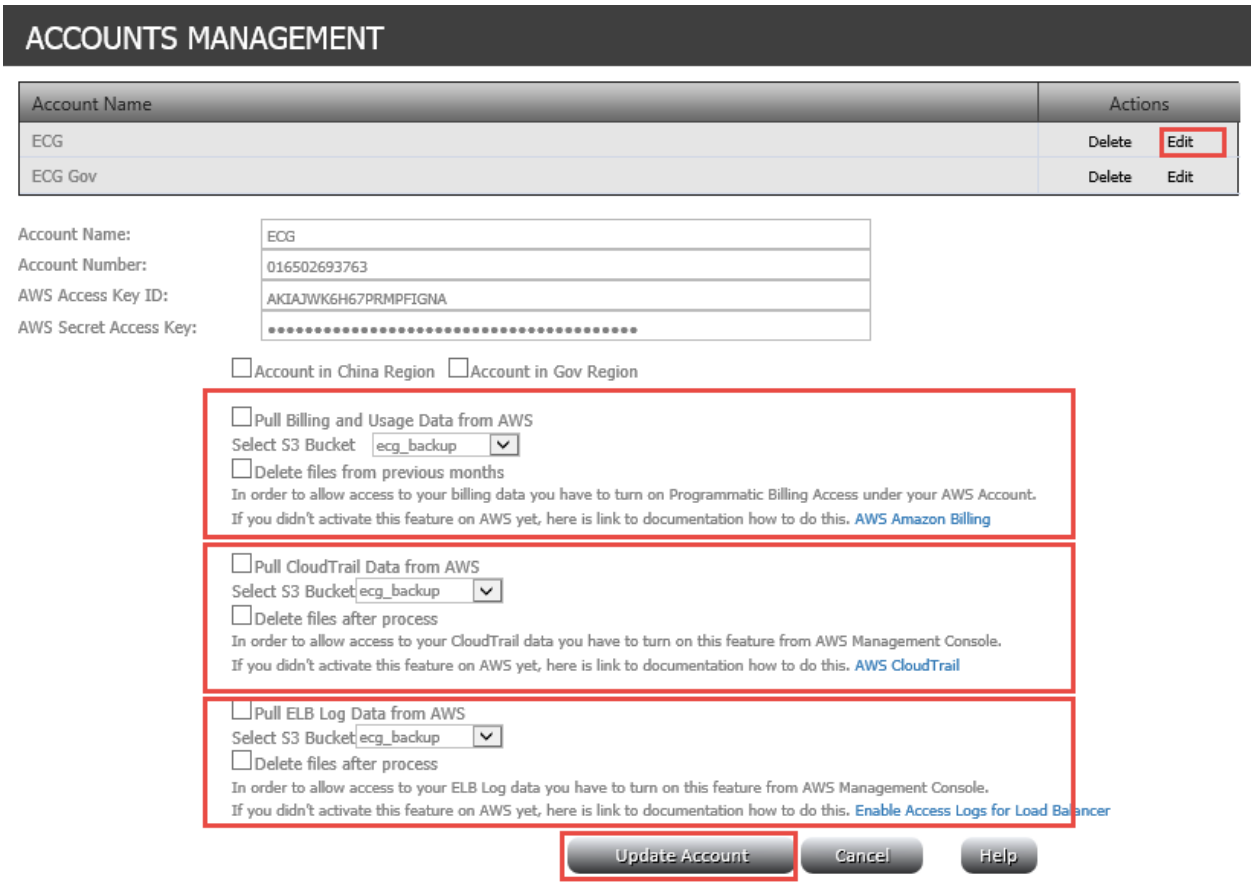


For more information about AWS Key, please read [“How to Start with Elastic Cloud Gate.”]

Click Add New Account to complete. Before the new account is added, the system will verify that entered information is correct. If you enter IAM keys, the minimum permission required to pass verification process is:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:DescribeAvailabilityZones"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

After adding a new account, you can make further configuration adjustments by clicking Edit in the table.



Several new options related to the given account are visible:

Pull Billing and Usage Data from AWS – When checked, the system downloads and processes your billing data from the selected S3 bucket.

Delete files from previous month – When checked, billing files from previous month are deleted from the S3 bucket.

Pull CloudTrial Data from AWS – When checked, the system downloads and processes your CloudTrail data from the selected S3 bucket.

Delete files after process – When checked, the system processes then deletes the CloudTrail file.

Pull ELB Log Data from AWS – When checked, the system downloads and processes your ELB Log data from the selected S3 bucket.

Delete files after process – When checked, the system processes then deletes the ELB Log file.

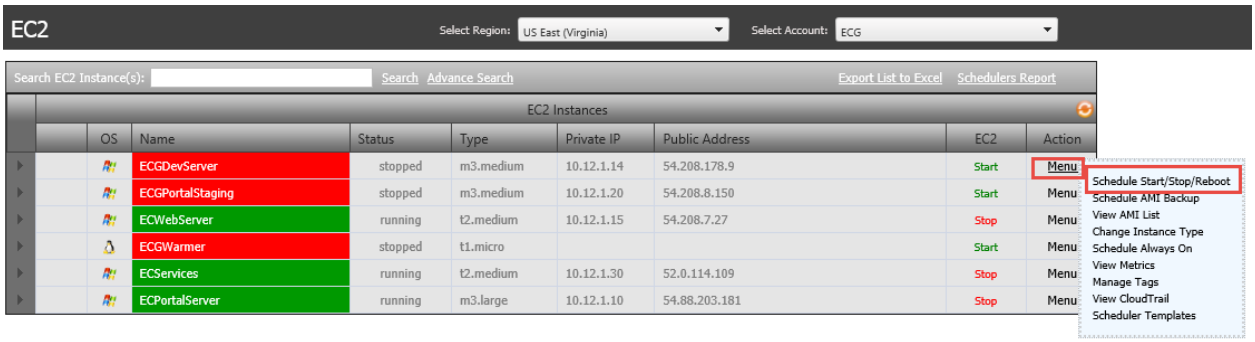
To finish configuration, click Update Account.
To delete account, click Delete from the table.

How to schedule Start/Stop/Reboot of EC2 Instance

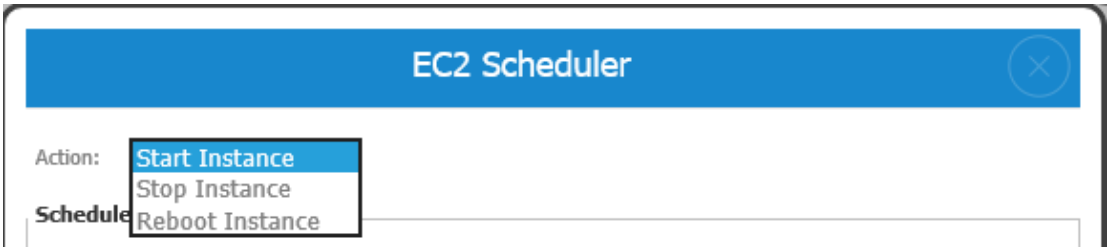
Follow these steps to schedule Start, Stop, or Reboot EC2 Instance:

Go to the EC2 section by selecting EC2 from Main Menu.

To open the scheduler wizard for a given EC2 instance, from the menu select Schedule Start/Stop/Reboot.

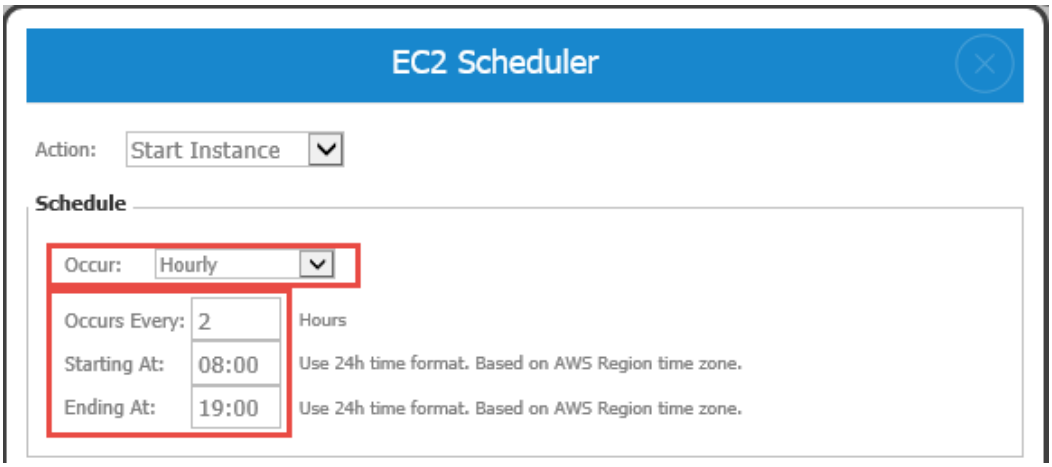


From the Action drop down list, select the schedule action (Start, Stop or Reboot).



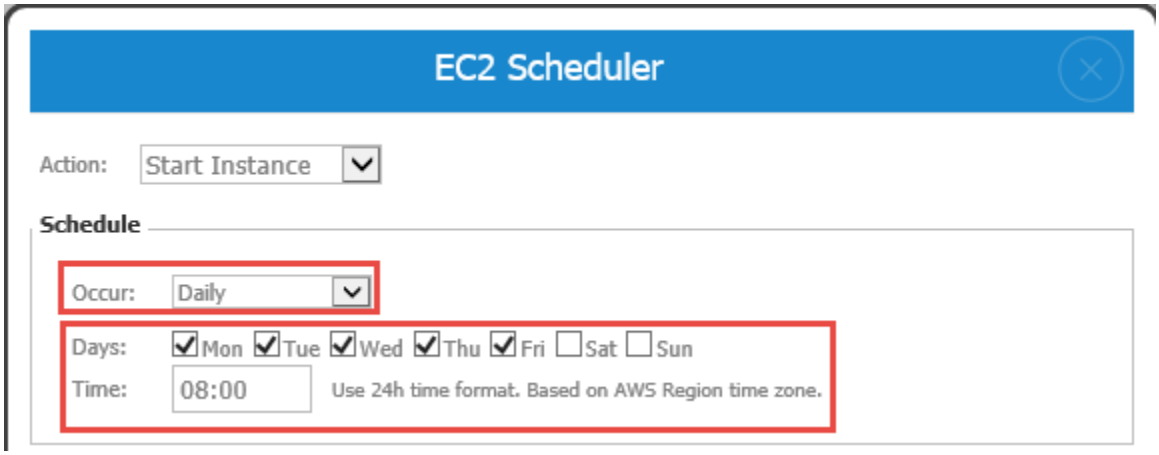
Next, set a schedule for the action to occur:

Hourly – The action is executed each set number of hours. Additionally, you can specify start and end time, e.g. to reboot Instance every 2 hours between 8AM and 7PM, here is how the setup looks:

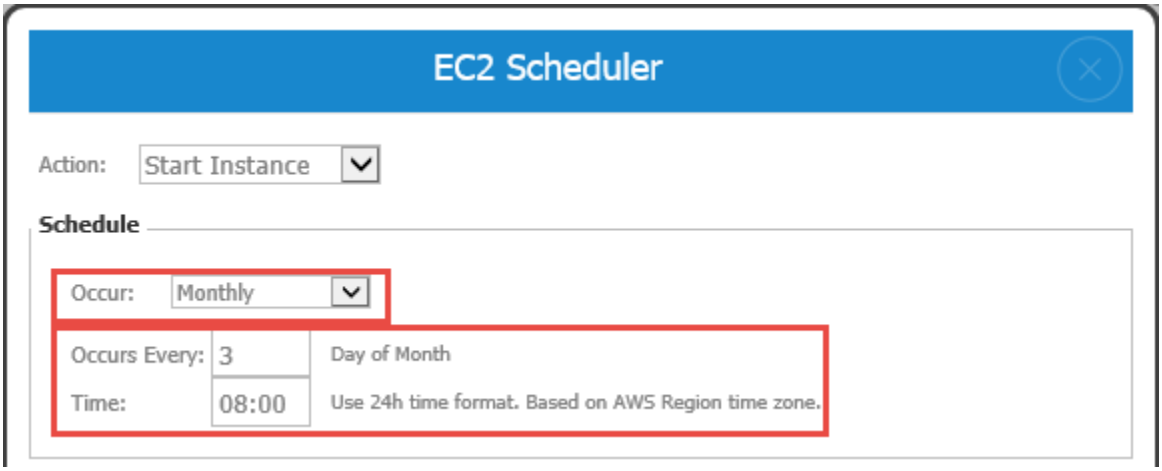


If you skip the start and end time, the instance reboots each set number of hours around the clock.

Daily – The action is executed each set day at the set time, e.g. to start Instance every weekday at 8AM, here is how the setup looks:

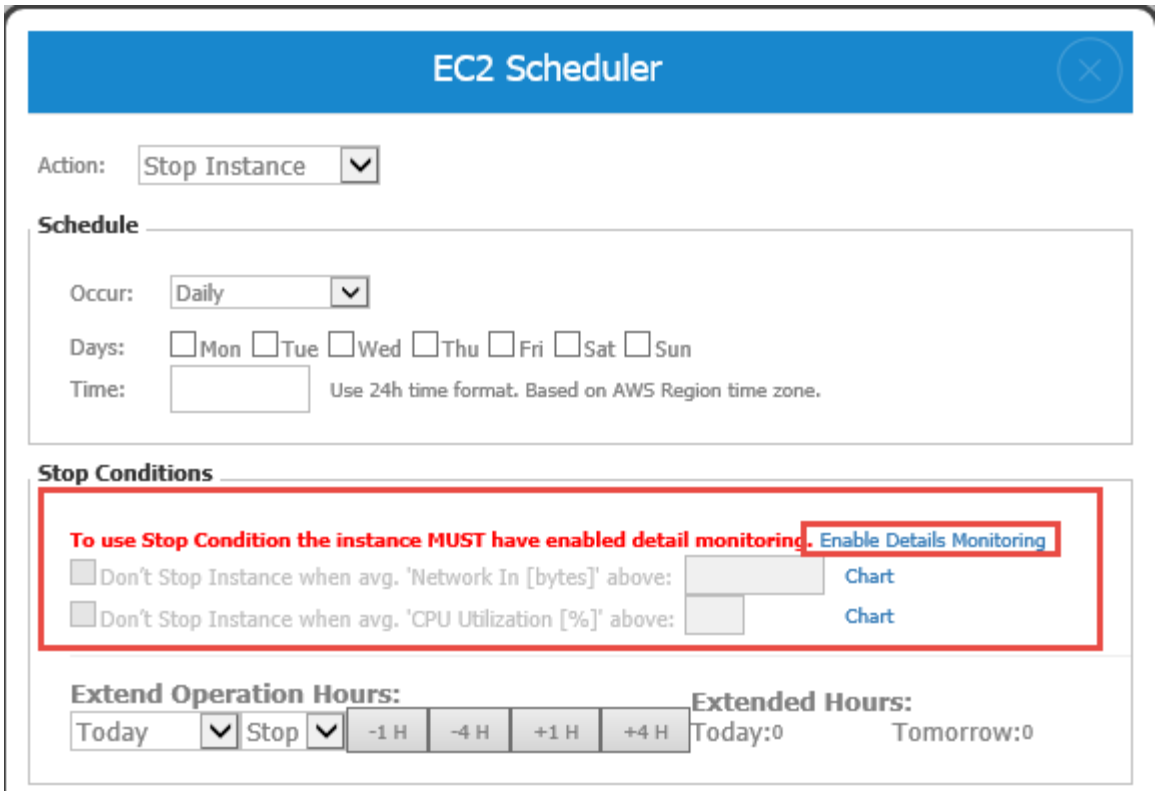


Monthly – The action is executed every set day of the month at the set time, e.g. to reboot Instance every 3rd day of the month at 8AM, here is how the setup looks:



Stop Condition

You may want to prevent Stop Instance when activity on the EC2 remains ongoing. To accomplish this, use the Stop Condition to specify when the stop action should not be executed. Specifications can be set based on the CPU or Network usage, e.g. specify prevent Stop Instance when the CPU usage is above a set threshold:



When the stop condition is specified, the system will check the given EC2 CloudWatch metric before Stop Instance occurs; if the value is greater than the threshold, the action will not execute.

To use the stop condition, EC2 must have Detail Monitoring turned on. If Detail Monitoring is not enabled, CloudWatch may return information that is delayed 15 minutes, and inaccurately report current usage condition.

Turn on Detail Monitoring directly from the AWS Management Console, or click the Enable Detail Monitoring link. If the link is not visible onscreen, Detail Monitoring is already turned on for the given EC2 instance.

Extend Operation Hours

You may need to temporarily change the schedule (e.g. stop the Instance two hours later). Instead of changing the entire schedule, the EC2 Instance operation can be extended by adding or subtracting hours.

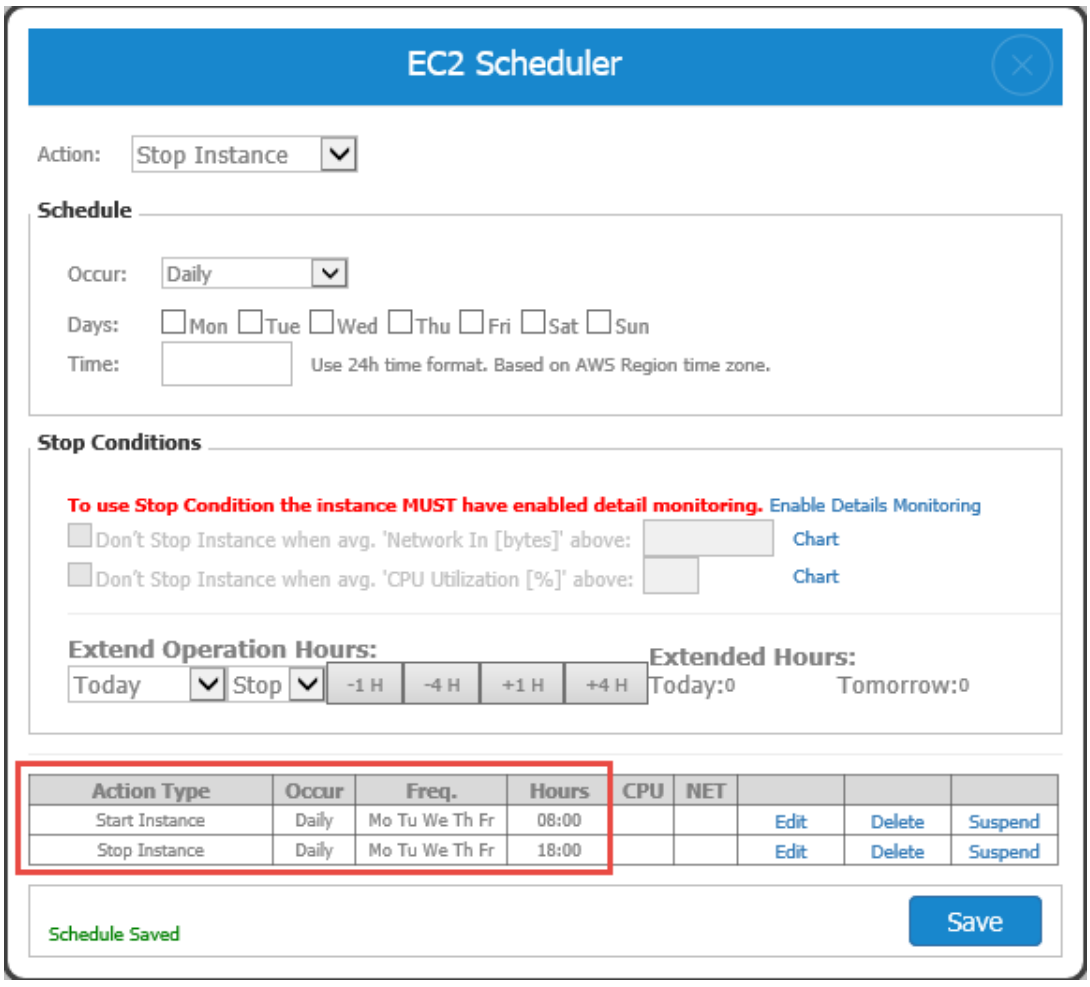
Select to apply new hours to today's or tomorrow's schedule and whether new hours should be applied to the Start or Stop action, e.g. to extend operation of the current day's EC2 Instance for an additional 2 hours, select Today and Stop and click the +1h button twice. You will see "Today: Stop +2" under Extended Hours.

Suspend/Resume Schedule

At any time, you can suspend or resume a previously suspended schedule: from the list of schedules, click Suspend or Resume. When Suspend is clicked, the scheduled action is suspended until you resume it. Please remember: if you suspend scheduled action for 6PM execution and you resume at 7PM the same day, it will not execute until next day at 6PM.

Action Type	Occur	Freq.	Hours	CPU	NET			
Start Instance	Daily	Mo Tu We Th Fr	08:00			Edit	Delete	Suspend
Stop Instance	Daily	Mo Tu We Th Fr	18:00			Edit	Delete	Suspend

By repeating the above steps, you can setup multiple schedulers for the same EC2 Instance using different actions. For example, to Start Instance every weekday at 8AM and stop it at 6PM, following is how the setup looks:

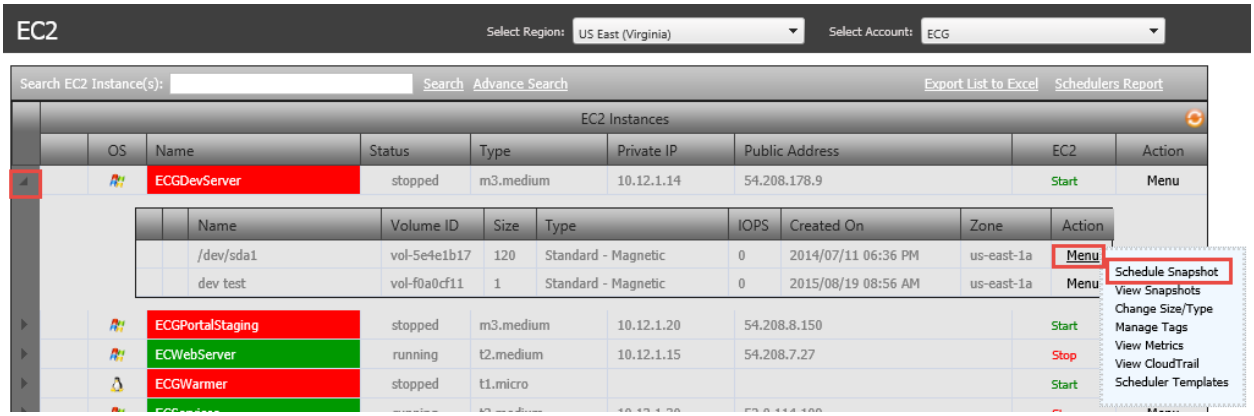


To schedule the same action for multiple EC2 Instances, please use Scheduler Templates. To learn more about templates please read: [Introduction to Scheduler Templates]

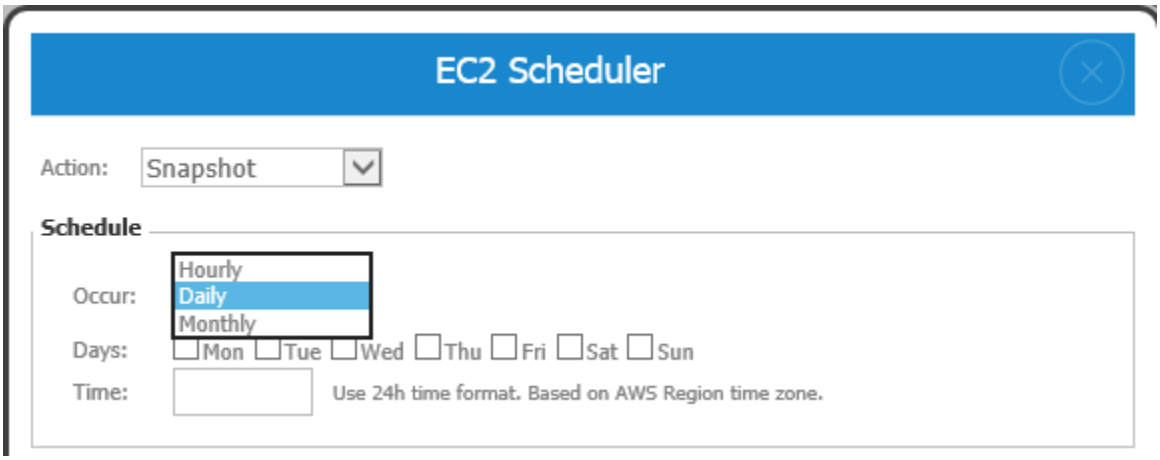
How to schedule backup of EBS volume (Snapshot)

To Schedule Snapshot of the EBS volume, follow these steps:

Select EC2 from the Main Menu to go to the EC2 section.
Select AWS Account and the Region for the EBS volume you want to schedule backup.
On the EC2 Instance list, click the black arrow on the left to expand EC2 of the attached EBS.
From the menu, select Schedule Snapshot.

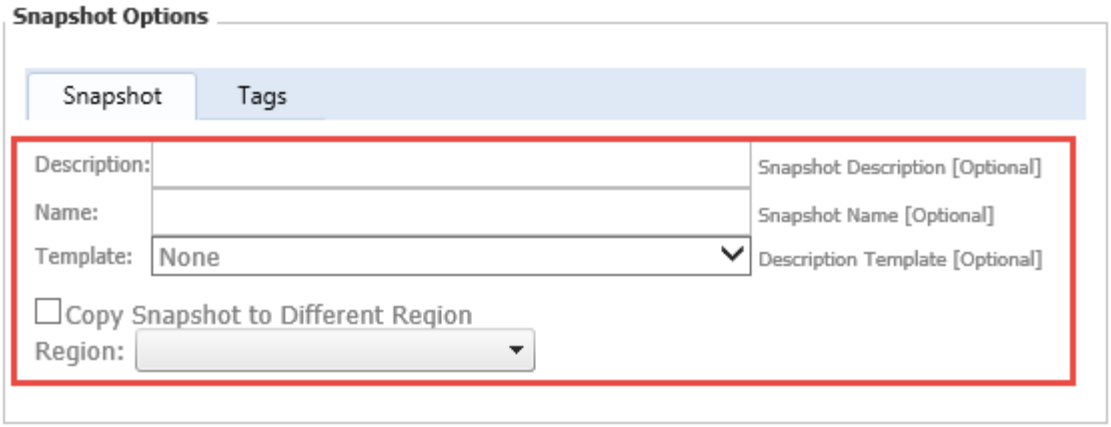


In the scheduler window, under the Schedule section, select snapshot frequency: options are Hourly, Daily or Monthly.

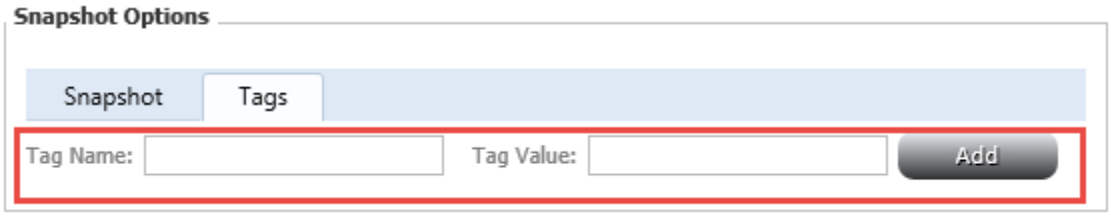


Optional settings for Snapshot:

Description – Applied to snapshot
Name – Applied to snapshot
Template – Name of pre-configured description template. Learn more about description templates in Introduction to Description Templates
Copy Snapshot to Different Region – Specify additional Region(s) where snapshots are copied after creation (cross-region snapshot)



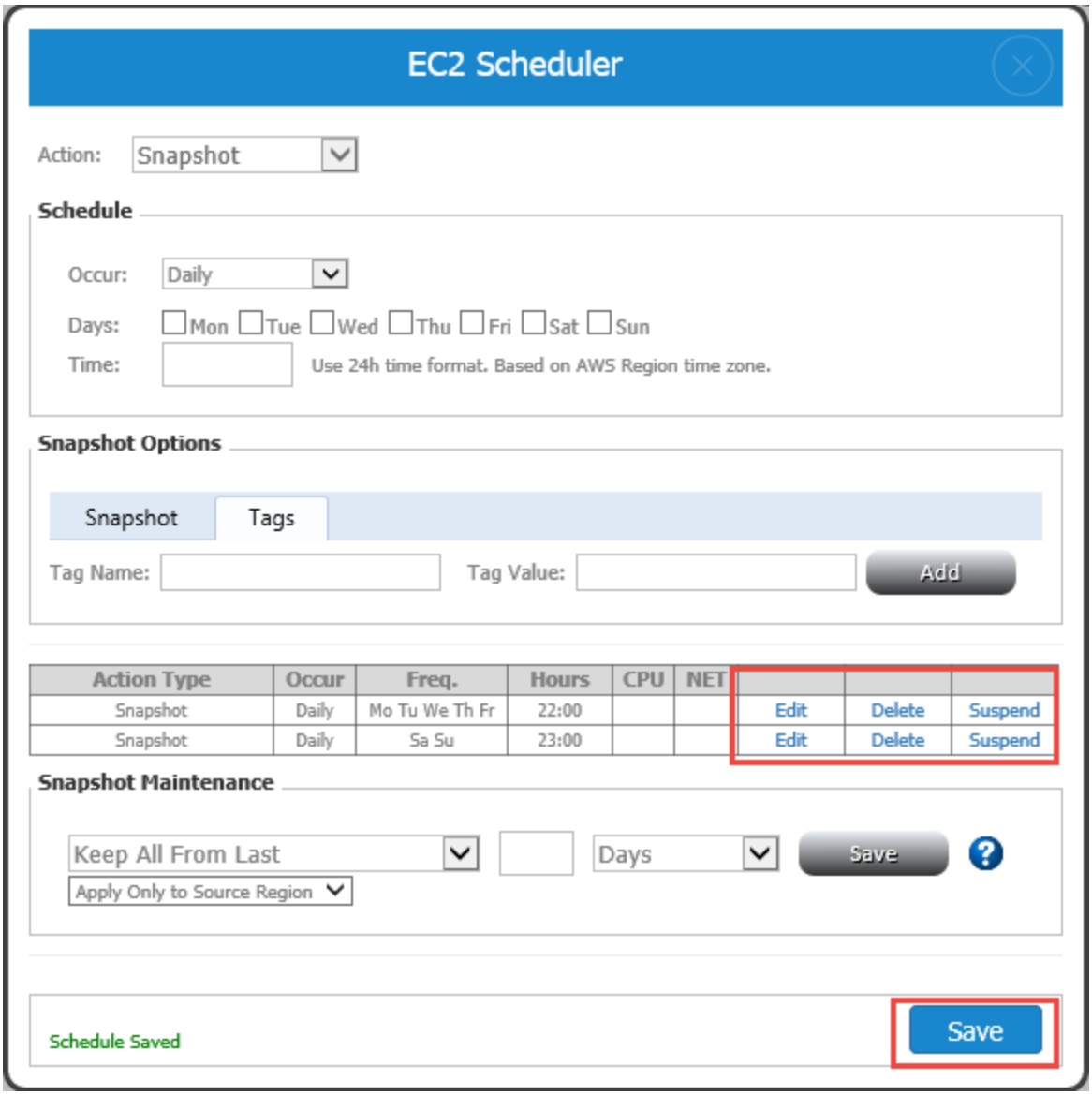
Tags – Create multiple tags to apply to the snapshot. To add tag(s), enter tag name, tag value and click Add.



Once you specify Description, Name, Template, and/or Tags, these settings will be applied to the cross-region snapshots as well.

To finish configuration, click Save.

A new row will appear in the table below the Snapshot Options section. This row has three options: Edit, Delete, and Suspend. Edit and Delete allow you to modify or delete the given scheduler; Suspend allows you to temporarily suspend execution of scheduler without deleting it. When Suspend is clicked, the option changes to Resume, which allows you to resume a suspended schedule in the future.



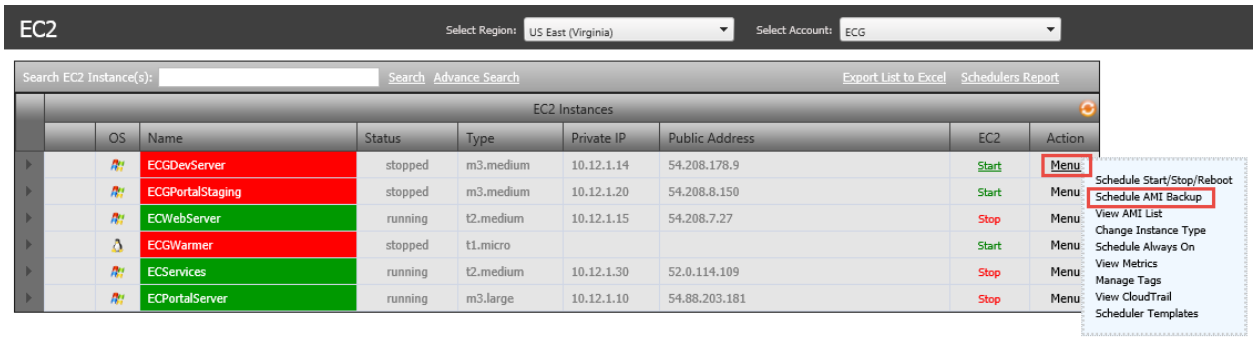
Multiple schedulers for the same EBS volume can be created based on different needs by repeating the above steps.

To learn more about applying the same scheduler configuration to multiple EBS volumes, please read: [Introduction to Scheduler Templates]

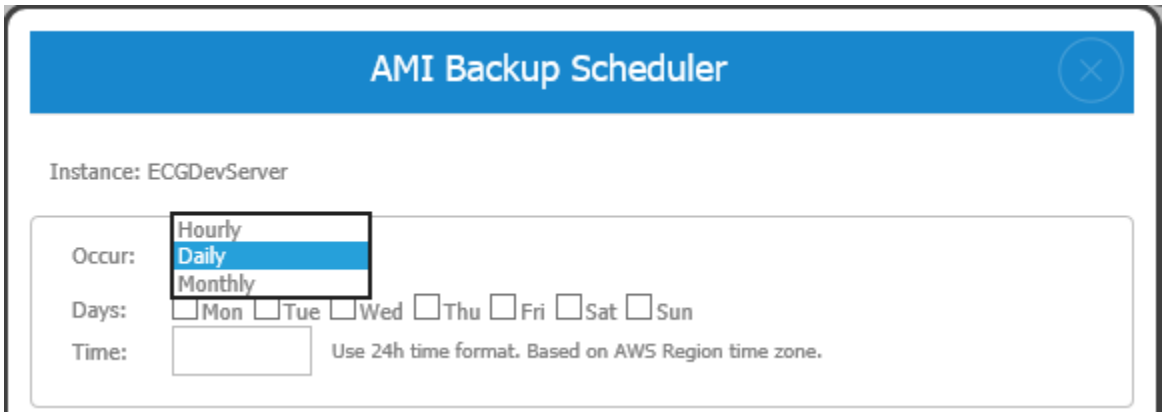
How to schedule backup of EC2 Instance (AMI)

To schedule EC2 AMI backup follow these steps:

Select EC2 from the Main Menu to go to EC2 Section.
Select AWS Account and Region for the EBS volume you want to schedule backup.
On the EC2 Instance list, from the menu select Schedule AMI Backup.

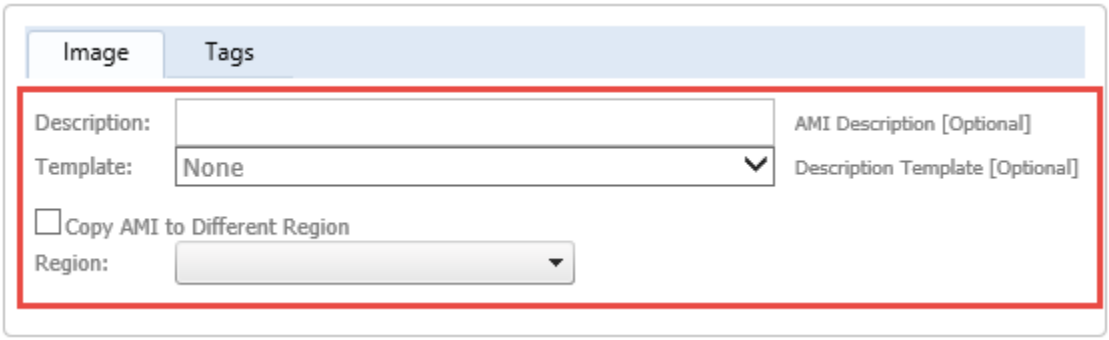


In the scheduler window under the Schedule section, select image (AMI) frequency: Hourly, Daily, or Monthly.

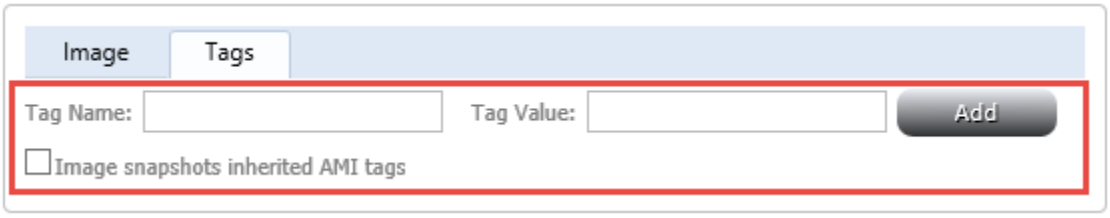


Optional settings for AMI:

Description – Applied to new image
Template – Name of pre-configured description template. You can read more about description templates in Introduction to Description Templates
Copy AMI to Different Region – Specify additional Region(s) where new images are copied after creation (cross-region image)



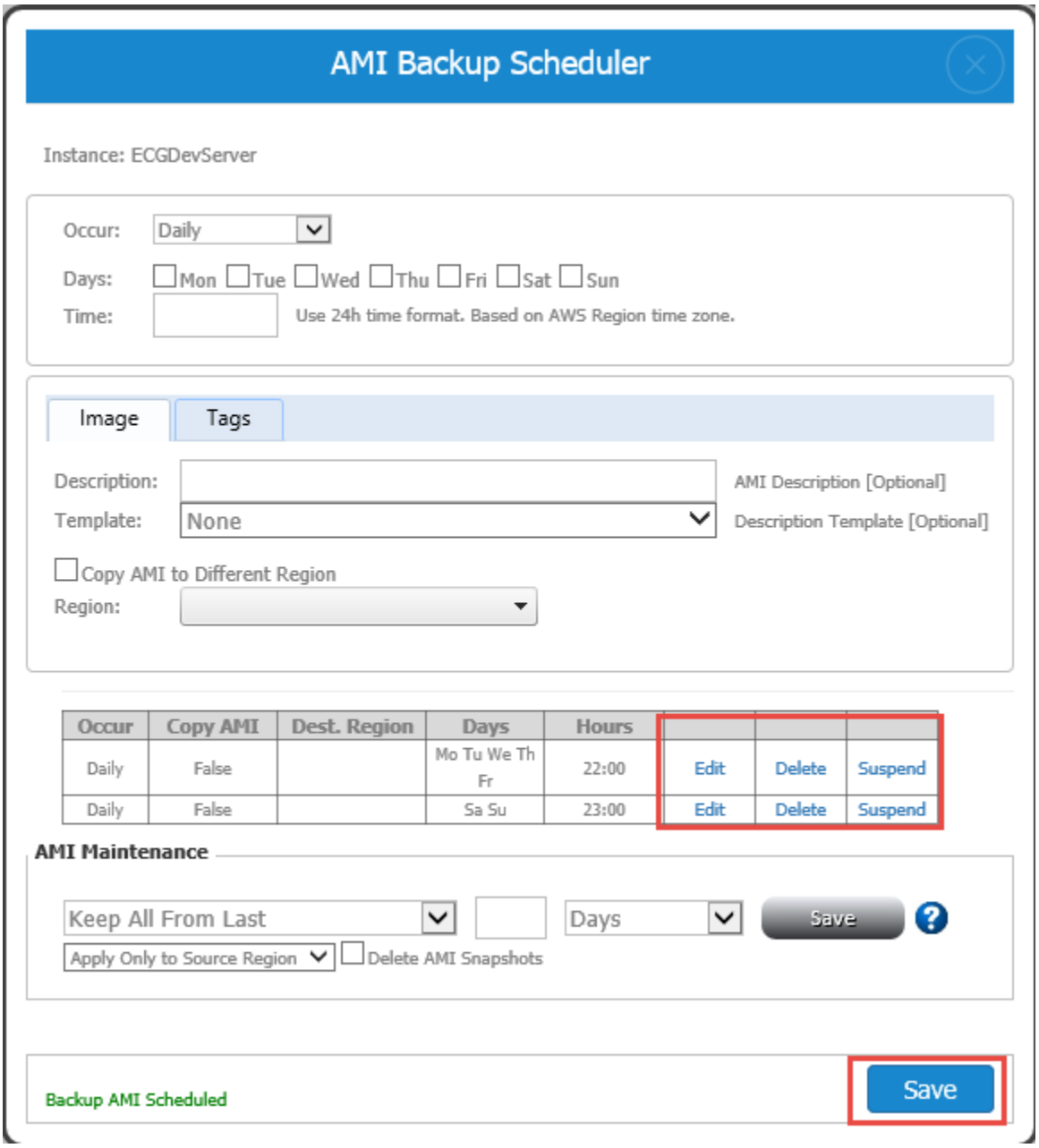
Tags – You can create multiple Tags to apply to new snapshots. To add a Tag, enter tag name, tag value, and click Add. To apply the same tags to an AMI-created snapshot, check the Image Snapshots Inherited AMI Tags option.



Once you specify Description, Template, or Tags, settings are also applied to the cross-region images.

When you complete configuration, click Save.

A new row appears in the table below AMI options.
In the same row are three options: Edit, Delete, and Suspend.
The first two allow you to modify or delete given scheduler; the Suspend option allows you to temporarily suspend execution of scheduler, without deleting it. When you click Suspend, the option will change to Resume, which allows the suspended schedule to be resumed in the future.



By repeating the above steps, you can create multiple schedulers for the same EC2 Instance according to different specifications.

To apply the same scheduler configuration to multiple EC2 Instances, please visit [Introduction to Scheduler Templates]

Introduction to Scheduler Templates

EC2 Scheduler Templates Manager is a tool for managing scheduler across multiple EC2 objects. Each template can have one or multiple actions assigned and one or multiple EC2 objects. Action types include:

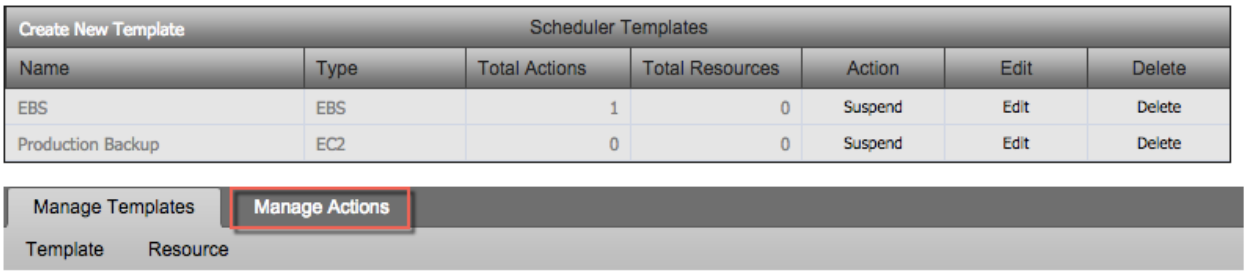
Start, Stop, or Reboot EC2 Instance
AMI Backup
EBS Volume Snapshot
Snapshots Maintenance
AMI Maintenance
Always On
Reboot WorkSpaces

How to manage templates

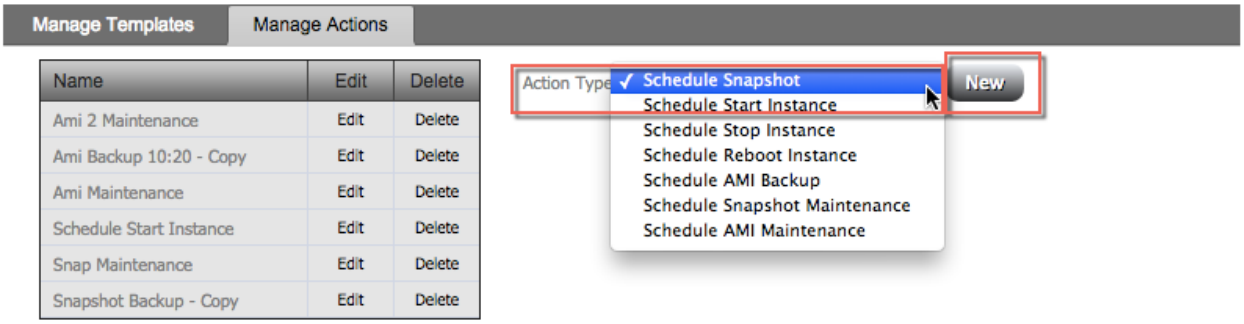
To open templates manager from the Main Menu, select Scheduler Templates.

Create or Manage Actions

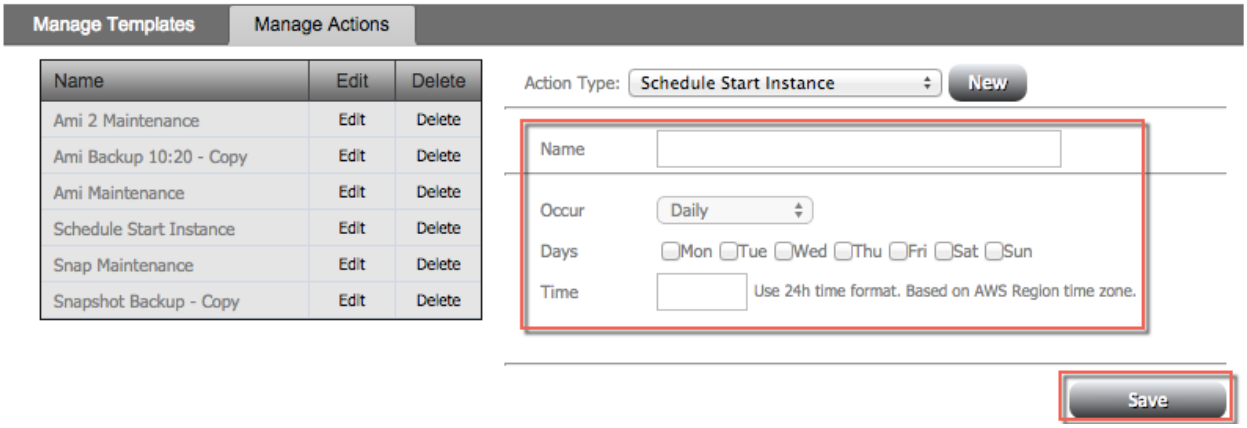
Switch to Manage Actions tab.



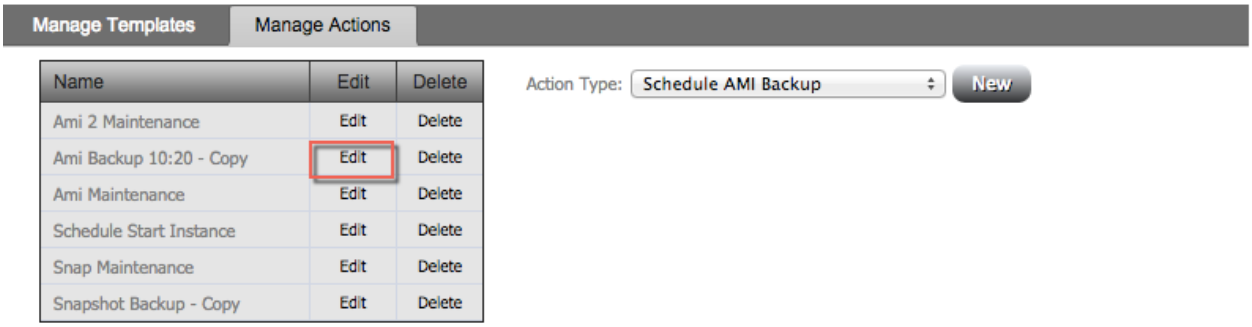
To Create a new action:
From the drop down list, select the action type and click New.



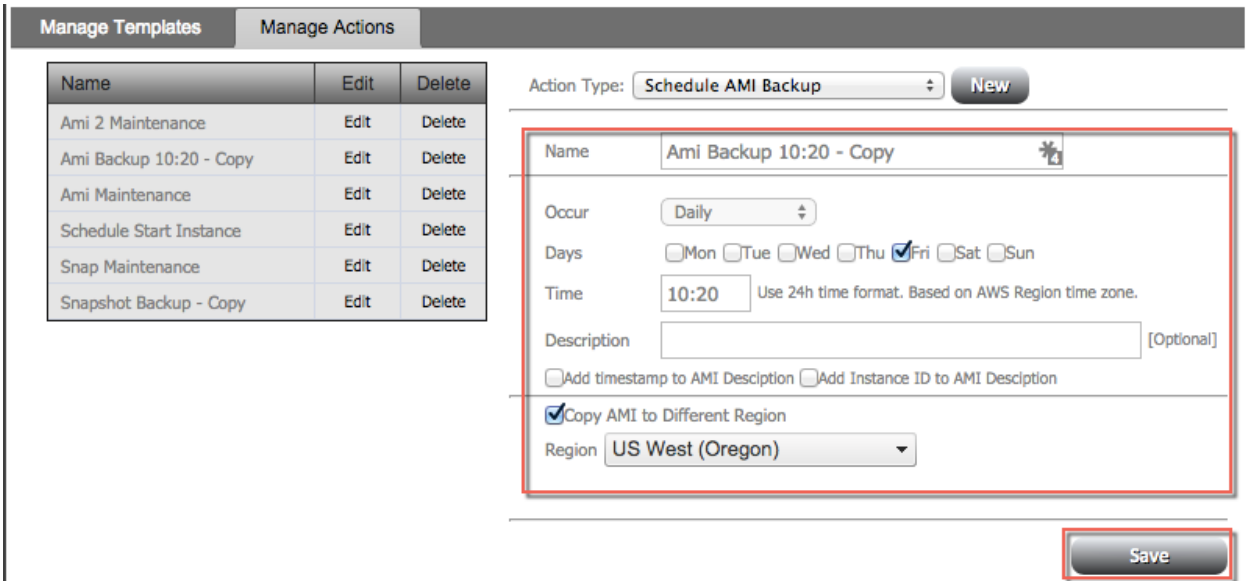
Enter all information required for a given action.
Click Save.



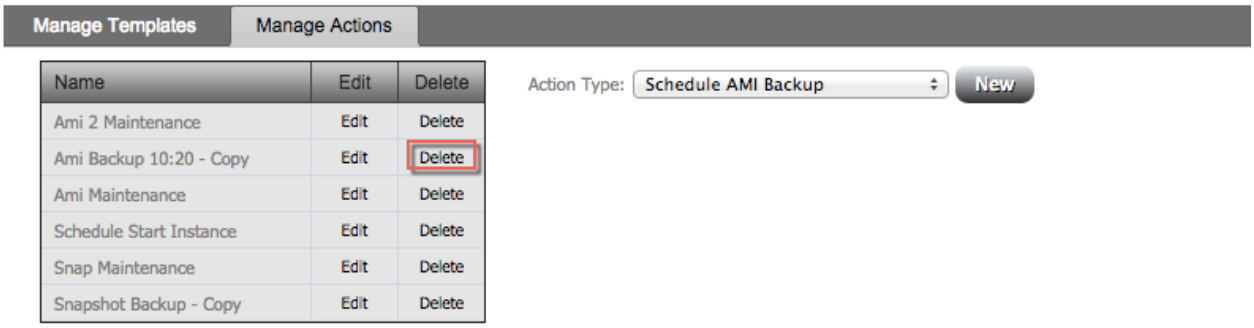
To Edit existing action:
From the table, click Edit.



All information is populated on the action template.
Make any change needed.
Click Save.



To Delete action:
From the table, click Delete.

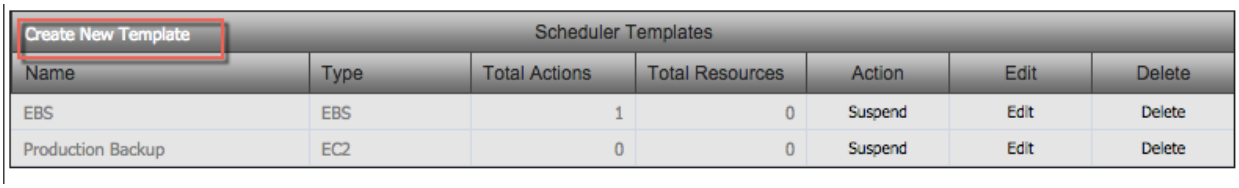


The deleted action is automatically removed from any assigned templates.

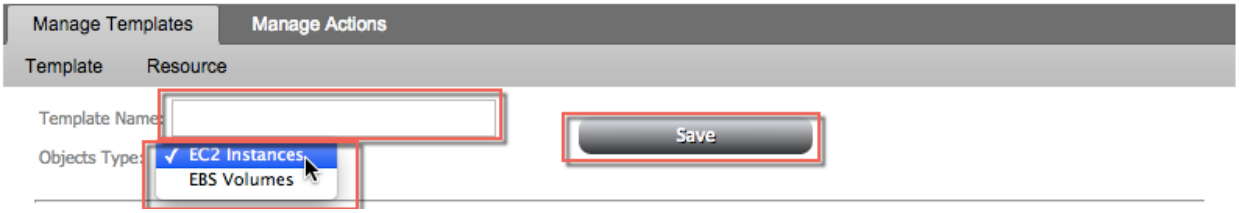
Create a new template

To Create a new template, follow these steps:

Click Create New Template.



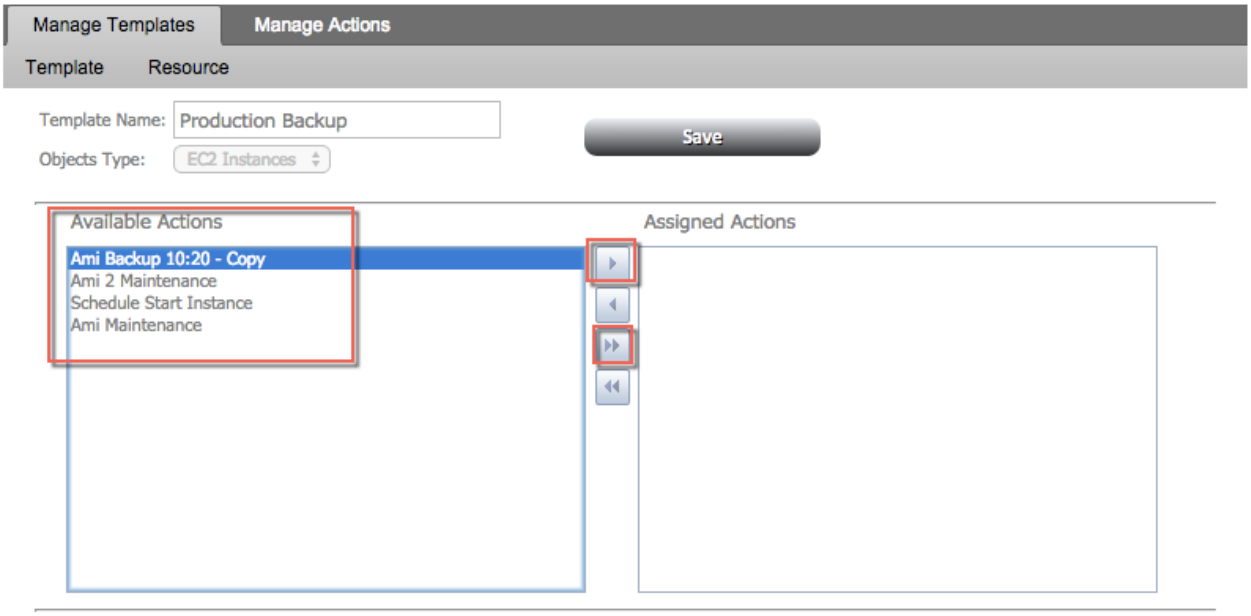
Enter template name
Select template type:
EC2 Instances – Within this type, available actions are relevant to EC2 Instances, e.g. Start, Stop, or Reboot EC2 Instance, AMI Backup, and Maintenance
EBS Volumes – Assign actions relevant to EBS volumes, including Schedule Snapshot or Maintenance of EBS volume
WorkSpaces – Assign actions relevant to WorkSpaces, including Schedule Reboot of WorkSpace.



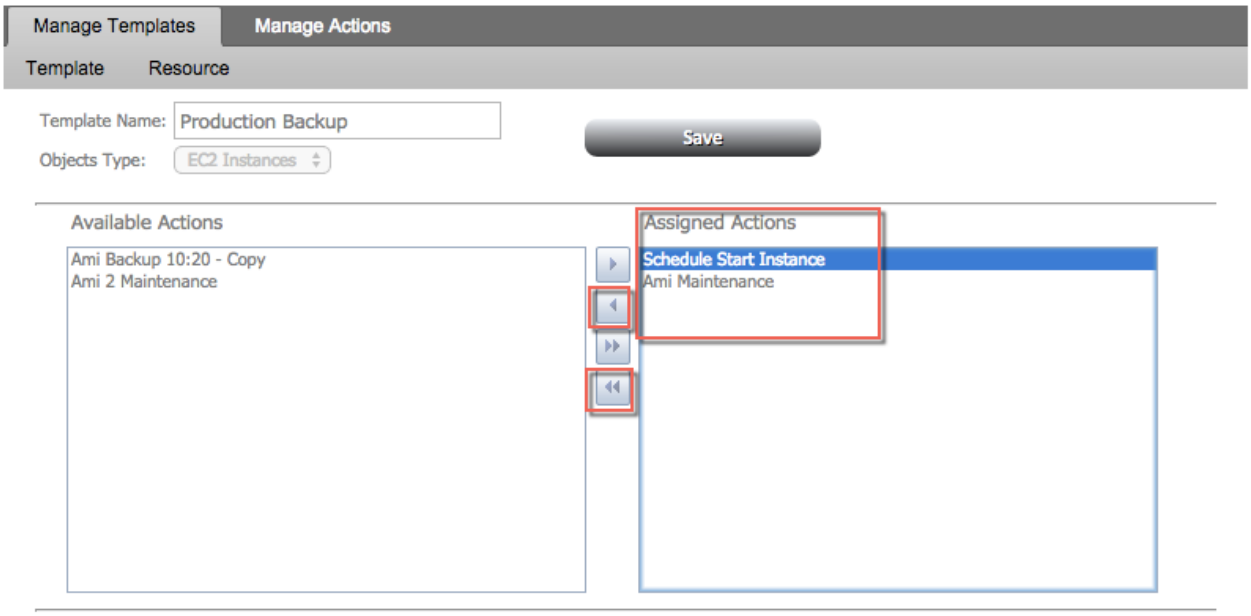
Click Save.
After a new template is created, you can add actions and resources within that template.

Assign Actions

To assign actions to the template, select an available action and click the -> button.
To assign all available actions, click the ->> button.



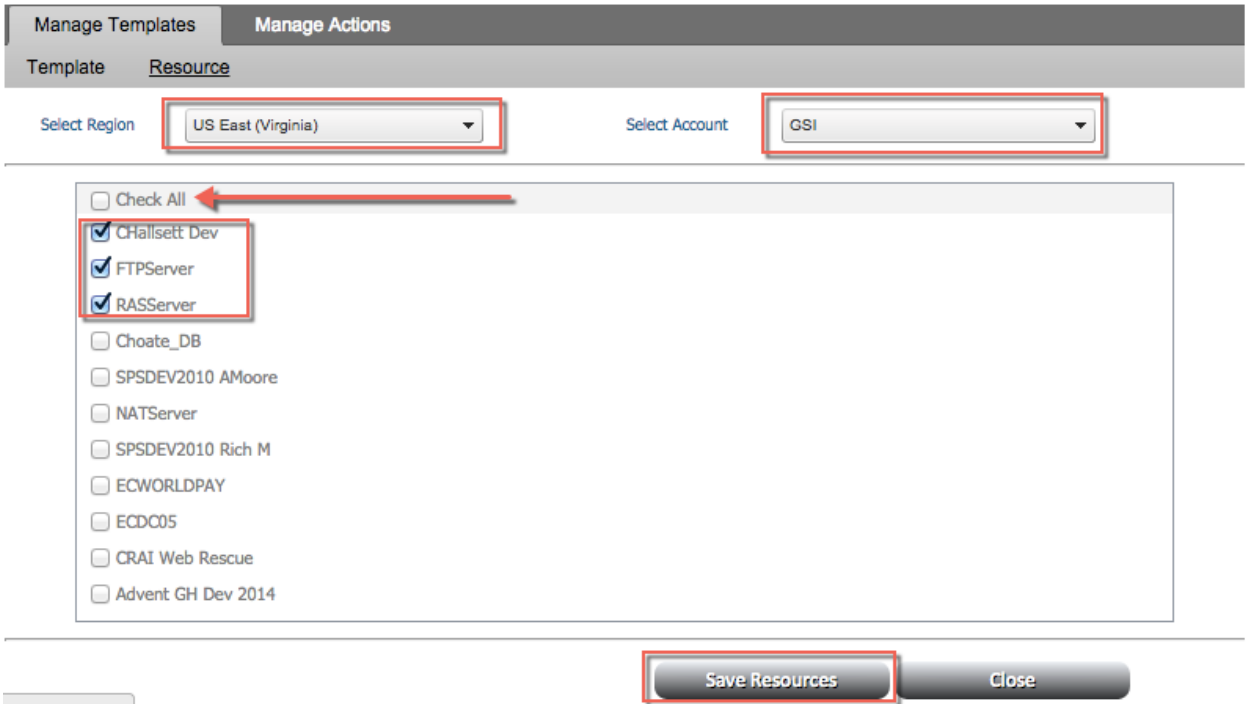
Once the action is assigned to the template, it disappears from Available Actions and reappears under Assigned Actions.
To remove action from the template, select assigned action and click the <- button.
To remove all actions from the template, click the <<- button.



Assign Resource

To assign resource, click Resource under the Manage Template tab.

On the list are the AWS Resources available under each selected AWS account and region. Check AWS objects (either EC2 Instance, EBS Volume or WorkSpace, depending on template type).
To assign all available resources under the given account and region, click Check All.
Click Save Resources.

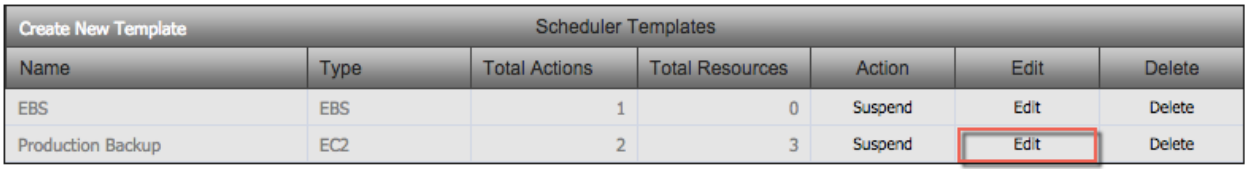


To remove resource(s) from the template, uncheck it from the list and click Save Resources. You can assign an AWS object from multiple accounts and regions: select a different AWS account or region and follow the same steps as above.

To temporarily suspend any AWS object from execution by template, check Suspend. To resume execution of a suspended AWS object, uncheck Suspend.

Manage existing template

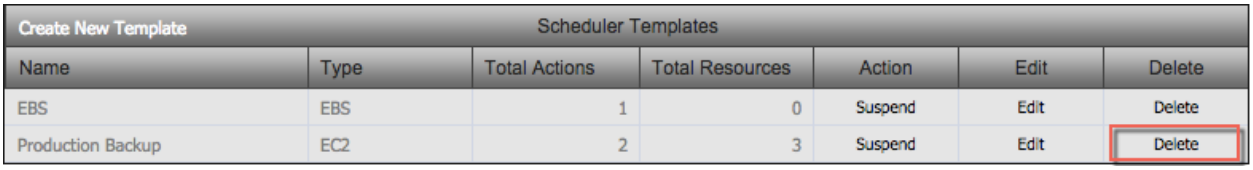
To edit existing template, click Edit in the Scheduler Templates table. The Manage Templates tab will populate allocated actions and resources.



Create New Template — Scheduler Templates

Name	Type	Total Actions	Total Resources	Action	Edit	Delete
EBS	EBS	1	0	Suspend	Edit	Delete
Production Backup	EC2	2	3	Suspend	Edit	Delete

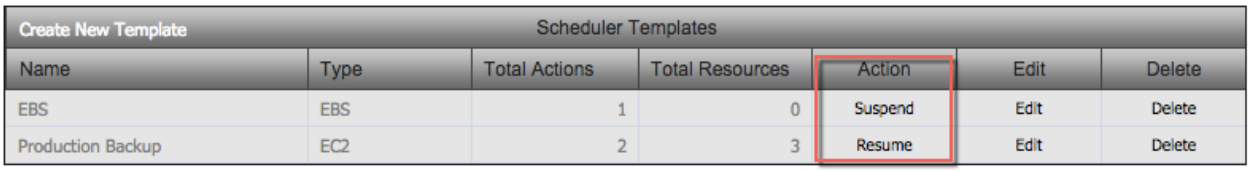
To delete existing template, click Delete in the Scheduler Templates table. This action will delete the template, including all assigned actions and resources.



Create New Template — Scheduler Templates

Name	Type	Total Actions	Total Resources	Action	Edit	Delete
EBS	EBS	1	0	Suspend	Edit	Delete
Production Backup	EC2	2	3	Suspend	Edit	Delete

At any time, you can suspend all actions assigned to a template by clicking Suspend in the Scheduler Templates table.
To resume suspended actions, click Resume.



Create New Template — Scheduler Templates

Name	Type	Total Actions	Total Resources	Action	Edit	Delete
EBS	EBS	1	0	Suspend	Edit	Delete
Production Backup	EC2	2	3	Resume	Edit	Delete

Please note: all actions assigned to the template will be either suspended or resumed.

To suspend execution of scheduled actions for a single AWS object (EC2, EBS, or WorkSpace) under a template, go to the resource tab, check the Suspend checkbox, and click Save Resource.

Manage Template Resources from EC2 Section

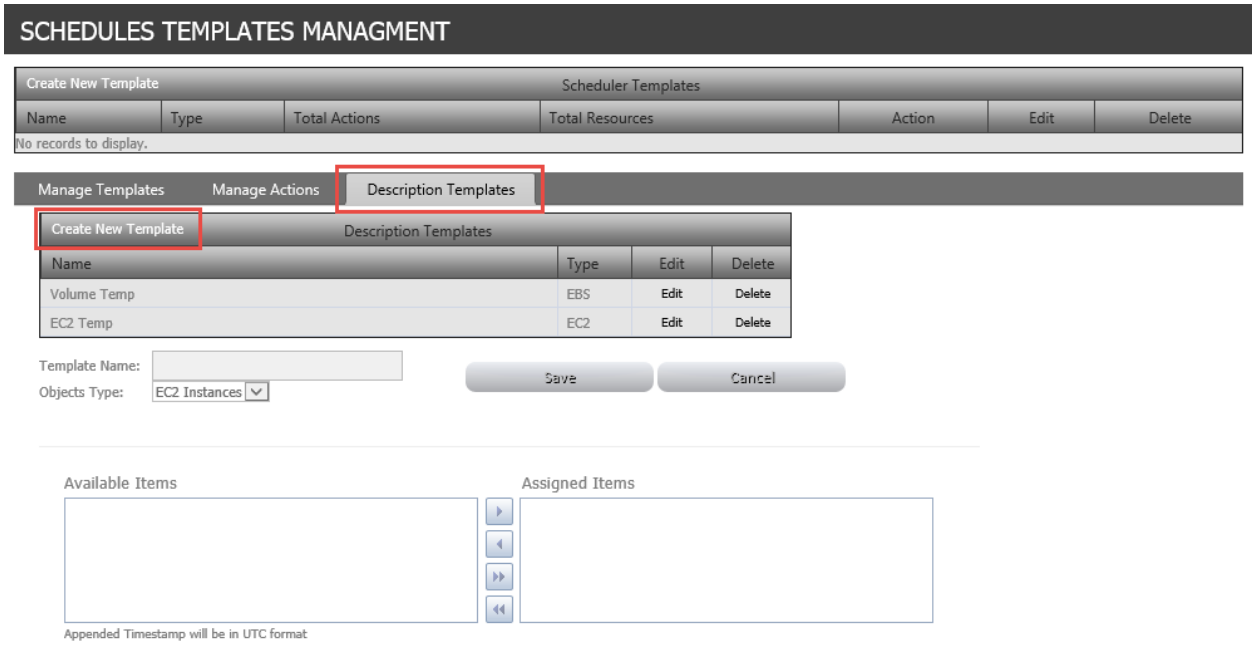
You can suspend, delete, or add EC2 Instance or EBS Volume to template(s) directly within the EC2 section by selecting Schedule Templates from EC2 or EBS Menu.
The new window opens and shows the list of templates you can add EC2 or EBS.
Below that is a list of templates with given EC2 or EBS already associated.
Use that list to delete association or suspend/resume execution of EC2/EBS.

Introduction to Description Templates

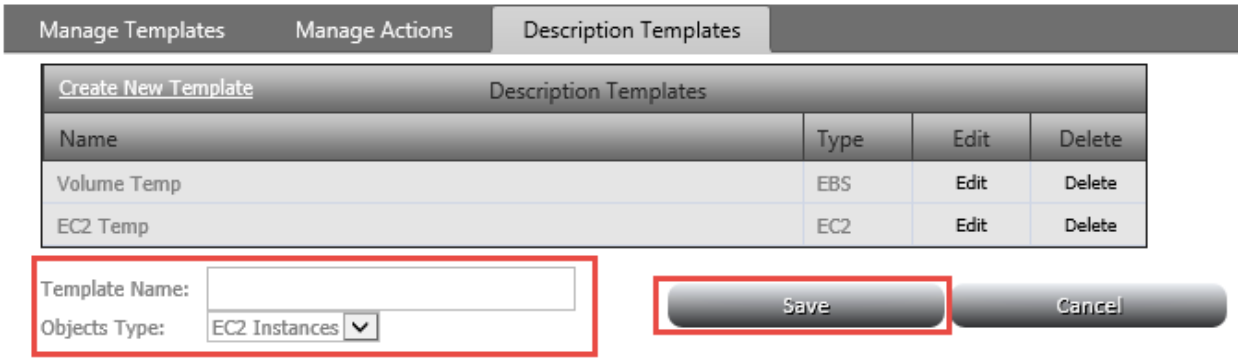
Description Template is the template containing certain information related to the given AWS object, including EC2 Instance ID or EBS Volume ID, which can be combined into one string and attached to the description of the snapshot or AMI.

Follow these steps to create Description Template:

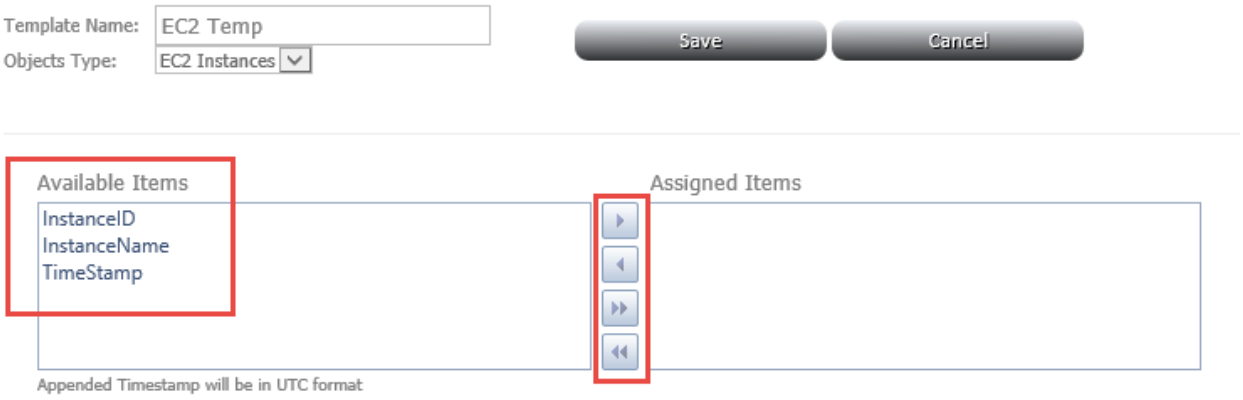
Go to the Scheduler Template section by selecting Scheduler Templates from Main Menu.
On the Scheduler Templates page, switch to the Description Templates tab.
Click Create New Template.



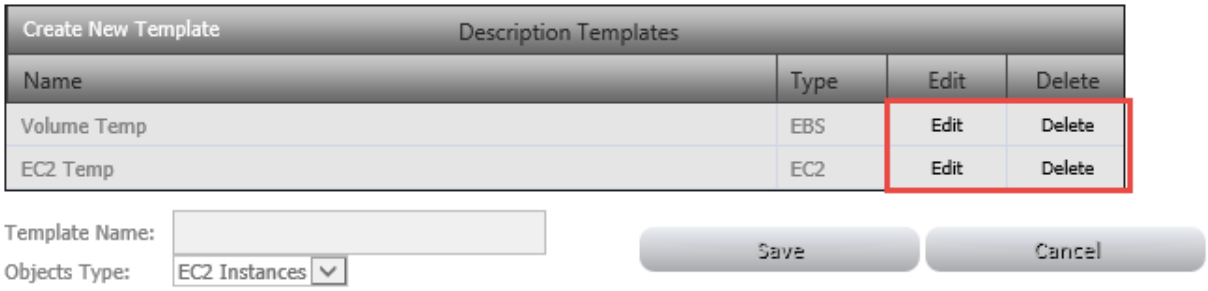
Enter Template Name: the name appears on the Description Template list, under AMI or Snapshot schedulers.
From the Object Type drop down list, select “EC2 Instance” to create a description template for AMI or EBS Volumes for Snapshot.
Click “Save”.



Within the Available Items list, you will see option (information) you can add to template. To assign or remove given option to/from template, select the item and click the appropriate arrow on the list.



To modify or delete template, select either Edit or Delete from the template names table.



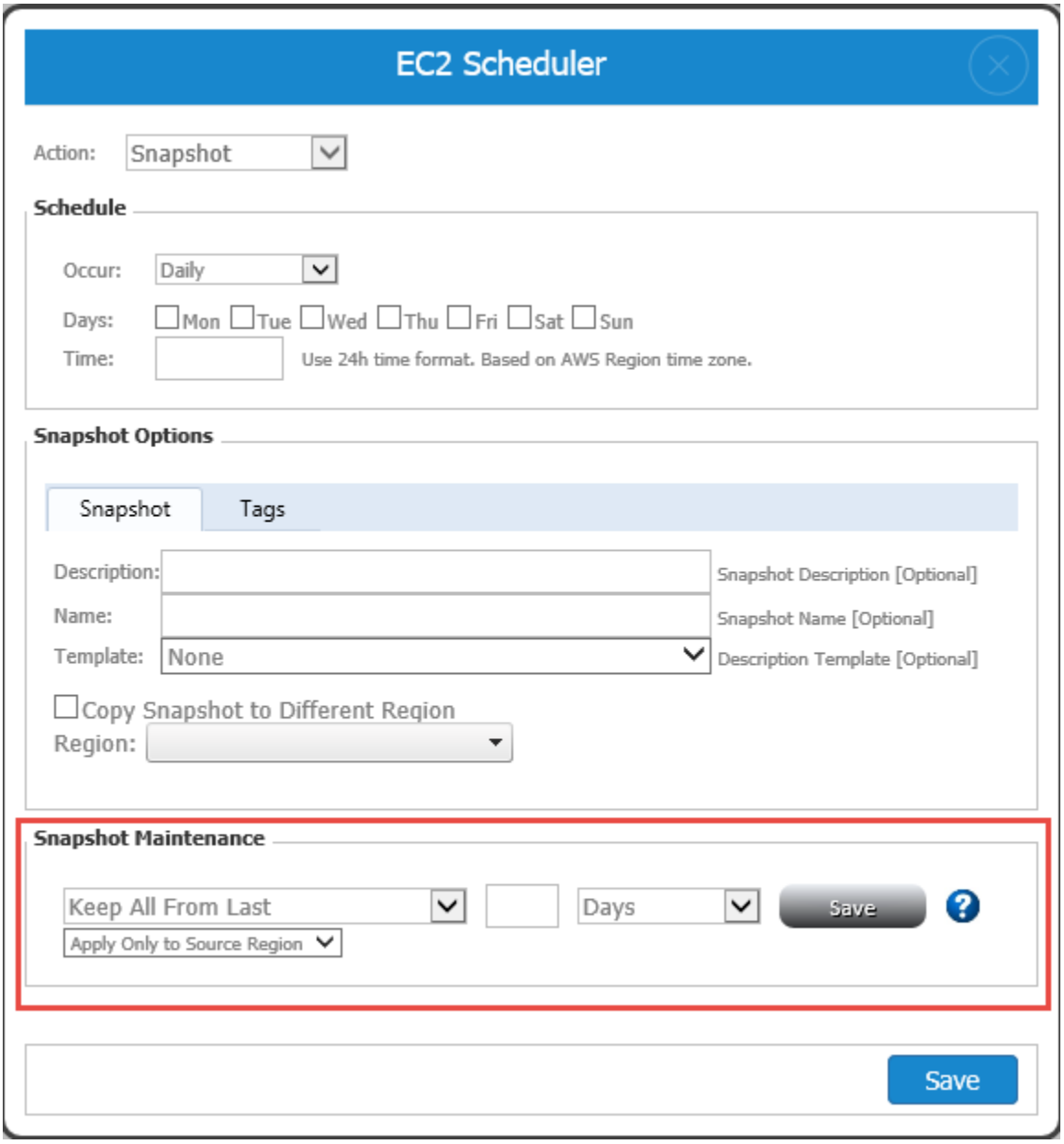
Note: the order you assign items to template does not guarantee the same order in the description of AMI or Snapshot.

How to schedule maintenance of Snapshots

Follow these steps to schedule Maintenance (retention period) of the old EBS Snapshots:

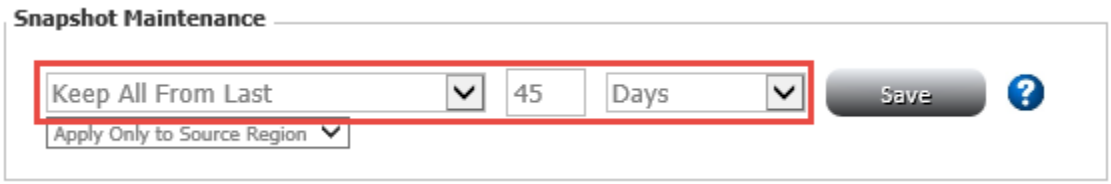
Go to EC2 section by selecting EC2 from the Main Menu.
Select AWS account and region of EBS volume to schedule backup.
On the EC2 Instance list, click the black arrow on the left to expand EC2 for the attached EBS.
From the menu, select Schedule Snapshot.

Under the Scheduler Window is the Snapshot Maintenance section, where the following configurations can be set:



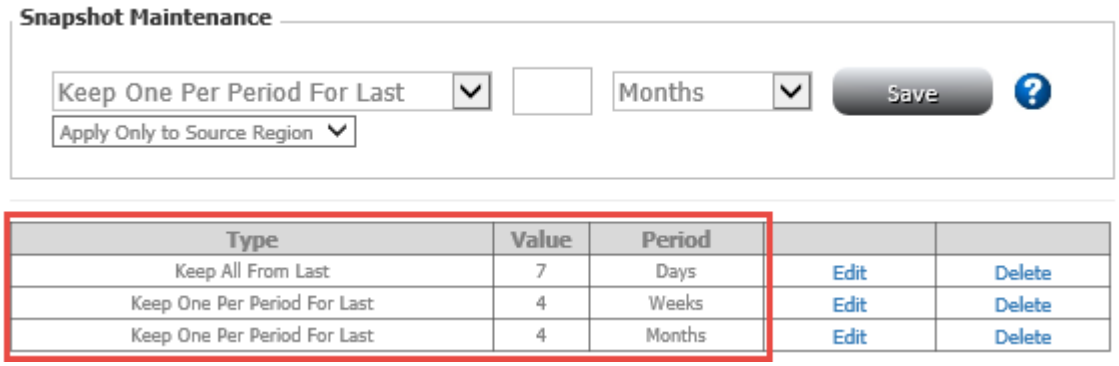
Two options define which Snapshots should not be deleted:

Keep All From Last – Keeps all Snapshots created within the last "x" periods (select as hours, days, weeks, months, or years), e.g. to keep all Snapshots created within the last 45 days, this is how your setup appears:



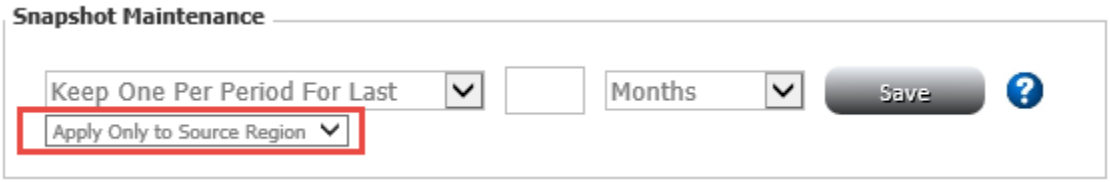
Keep One Per Period From Last – Only keeps the last Snapshots created in the given period (hours, days, weeks, months, or years), e.g. to keep one Snapshot per week from the last 8 weeks, this is how your setup appears:

To manage more complex needs, you can create multiple maintenances. For example, to setup maintenance to keep all Snapshots from the last 7 days, 1 Snapshot per week from the last 4 weeks, and 1 Snapshot per month from the last 4 months, this is how your setup appears:



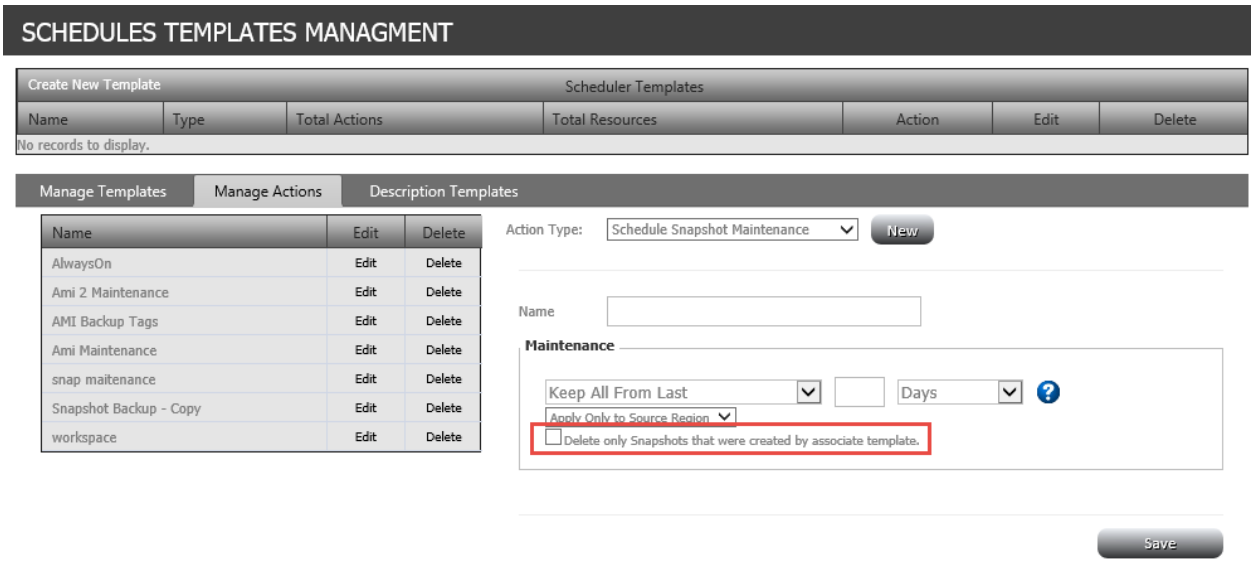
When you are using cross-region copy snapshot in your scheduler, you have another set of options that allow you to create more complex scenarios. Three options are available on the drop down list that allow you to schedule separate maintenance for source and destination region. These options are:

Apply Only to Source Region –Maintenance is applied only to snapshots in source region
Apply Only to Cross Region – Maintenance is applied only to snapshots in destination region
Apply to Both Regions – Maintenance is applied to both source and destination regions



When maintenance is running, Snapshots that do not match the scheduled criteria are deleted (except the most recent one) – for security reasons, the last snapshot is never deleted.

Additionally, maintenances scheduled under the EC2 section will delete all snapshots which do not meet the selected criteria, even snapshots created by our system.
To include only snapshots created by our system, use templates. Under the Schedule Snapshot Maintenance action is the checkbox Delete only Snapshots that were created by associate template. To use this feature, both Schedule Snapshot and Schedule Snapshot Maintenance must be associated with the same template.



Additionally, templates can be used to apply the same maintenance to multiple EBS volumes.

To learn more about templates, please read: [Introduction to Scheduler Templates]

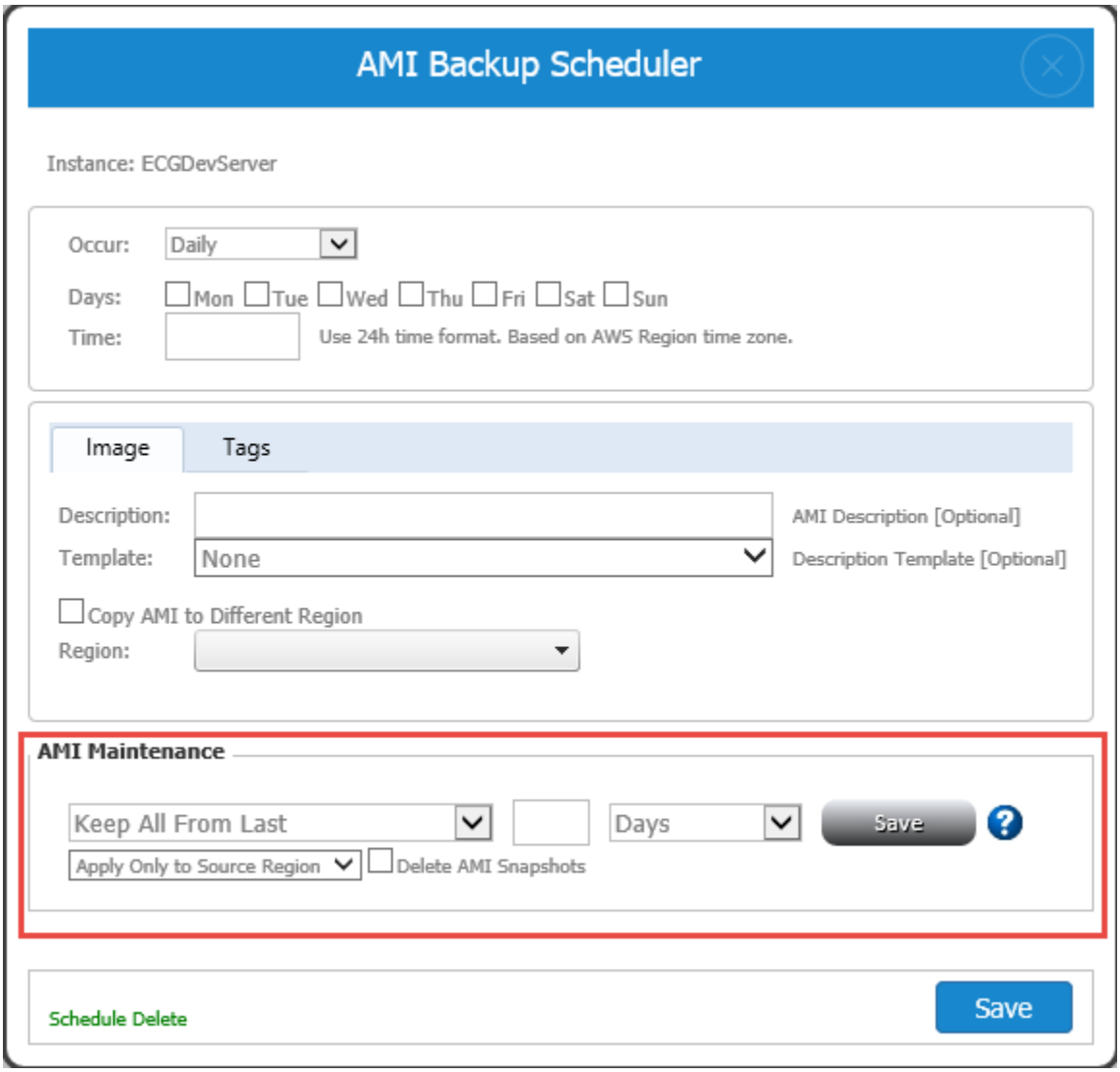
Note: the maintenance feature is only available under Deluxe or higher-rated plans.

How to schedule maintenance of AMIs

Follow these steps to schedule Maintenance (retention period) of the old AMIs (Images):

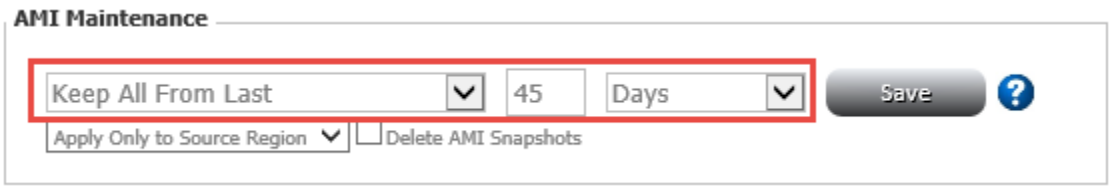
Go to the EC2 section by selecting EC2 from the Main Menu.
Select AWS account and region of EBS Volume to schedule backup.
From the menu's the EC2 Instance list, select Schedule AMI Backup.

Under Scheduler Window is the AMI Maintenance section, where the following configurations can be made:

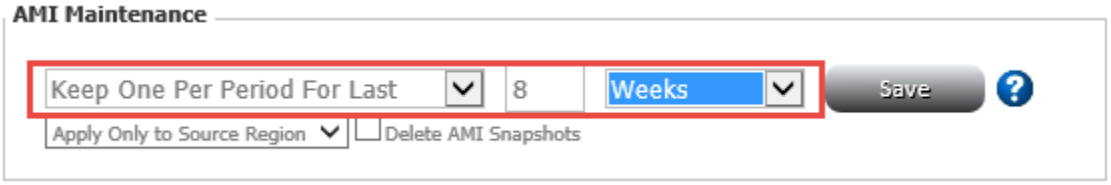


Two options define which AMI (Images) should not be deleted:

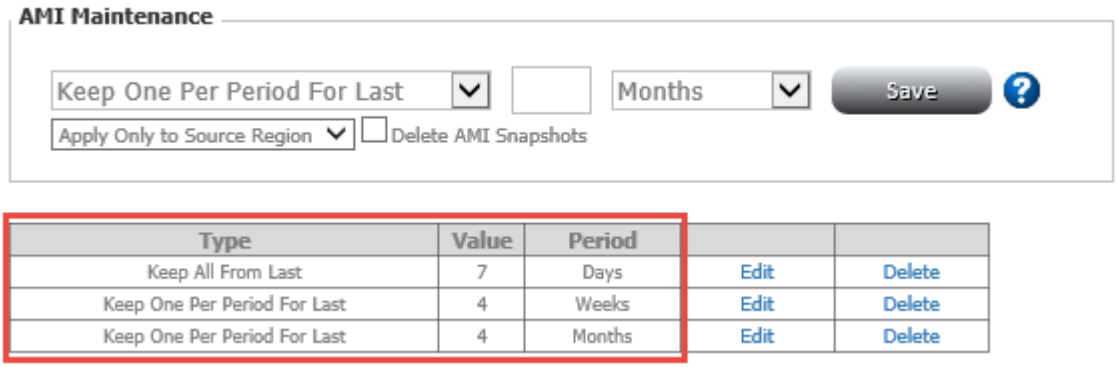
Keep All From Last – Keeps all AMIs created within the last "x" periods (select periods as hours, days, weeks, months, or years), e.g. to keep all AMIs created within the last 45 days, this is how your setup appears:



Keep One Per Period From Last – Keeps the last AMI created in the given period (hours, days, weeks, months, or years), e.g. to keep one AMI per week from the last 8 weeks, this is how your setup appears:



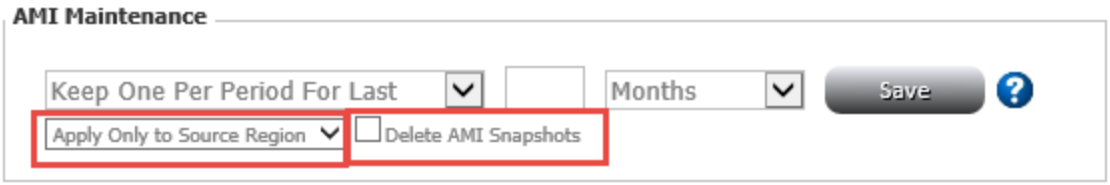
Create multiple maintenances to manage more complex needs, e.g. to setup maintenance that would keep all AMIs from the last 7 days, 1 AMI per week from the last 4 weeks, and 1 AMI per month from the last 4 months, this is how your setup appears:



When using cross-region copy Images in your scheduler, another set of options is available allowing creation of more complex scenarios. Three options that allow you to schedule separate maintenance for source and destination regions are available on the drop down list:

Apply Only to Source Region – Maintenance is applied only to AMIs in source region
Apply Only to Cross Region – Maintenance is applied only to AMIs in destination region
Apply to Both Regions – The same maintenance is applied to both source and destination regions

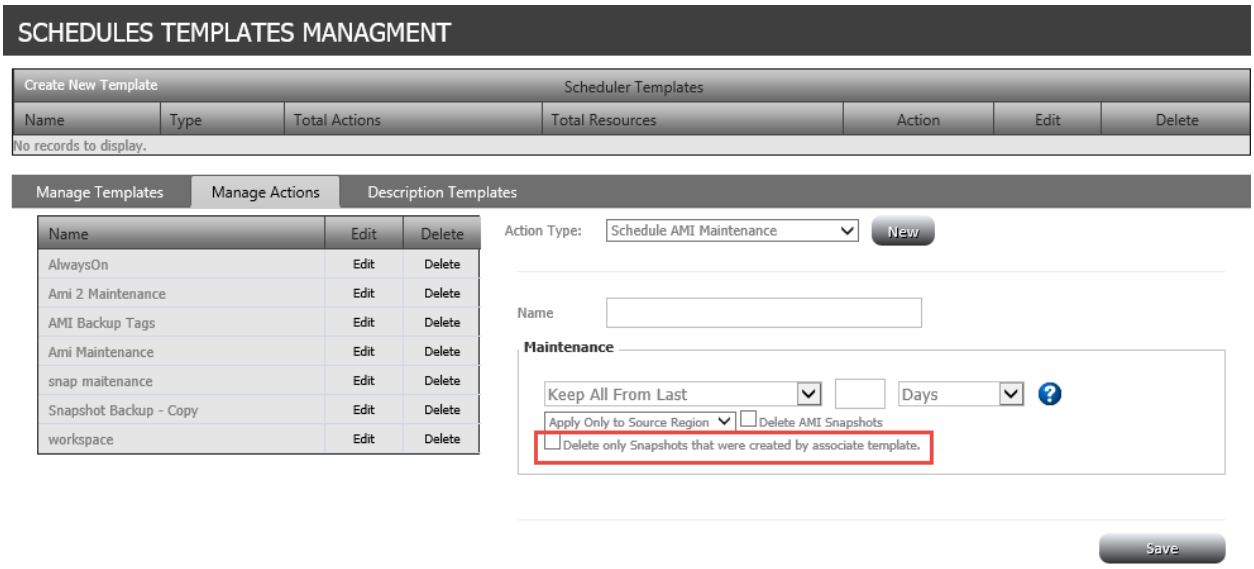
To delete all snapshots associated with AMI, check the Delete AMI Snapshots option.



When the maintenance is running, all AMIs that do not match scheduled criteria are deleted (except the most recent one) – for security reasons, the last AMI is never deleted.

Also, maintenances scheduled under the EC2 section delete all AMIs that do not meet your criteria, including AMIs created by our system.

Use templates to include only AMIs created by our system. Under the Schedule AMI Maintenance action is the checkbox Delete only Snapshots that were created by associate template. To use this feature, both Schedule AMI Backup and Schedule AMI Maintenance must be associated with the same template.



Additionally, templates can be used to apply identical maintenance to multiple EC2 Instances.

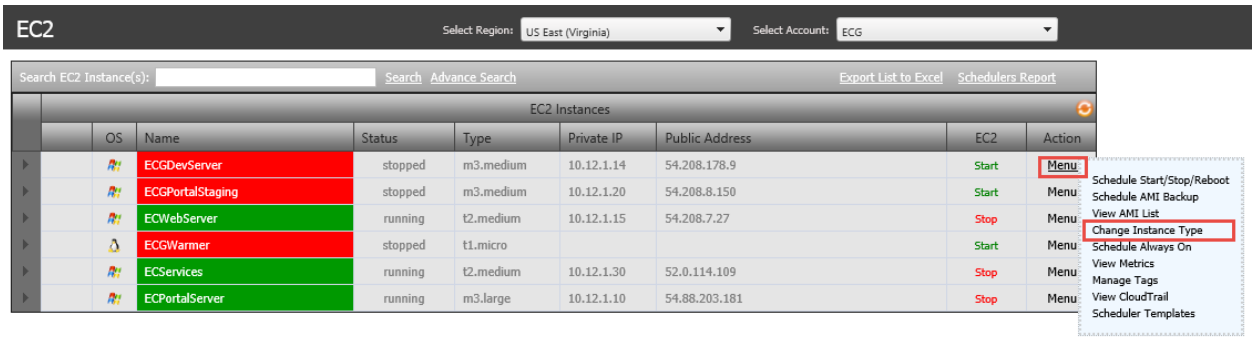
To learn more about templates, please read: [Introduction to Scheduler Templates]

Note: the maintenance feature is only available under Deluxe or higher-level plans.

How to change EC2 Instance type

Follow these steps to change instance type:

From the Main Menu, select EC2.
Under EC2 Instance list, find the instance to change.
From the menu, select Change Instance Type.

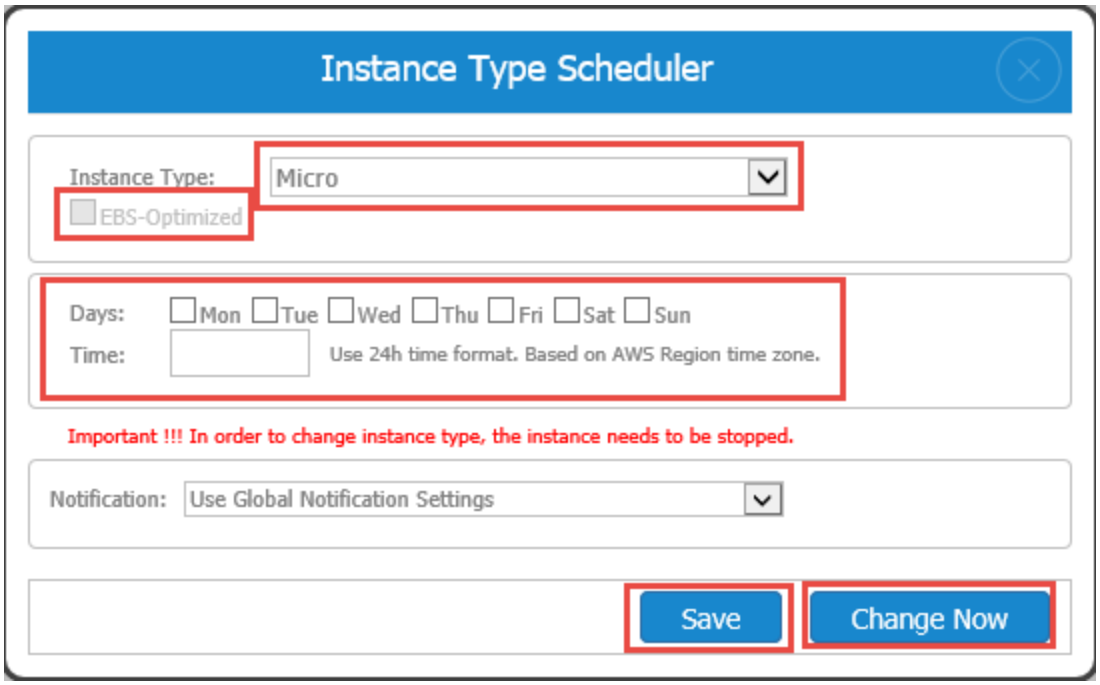


From the drop down list, select the new instance type.

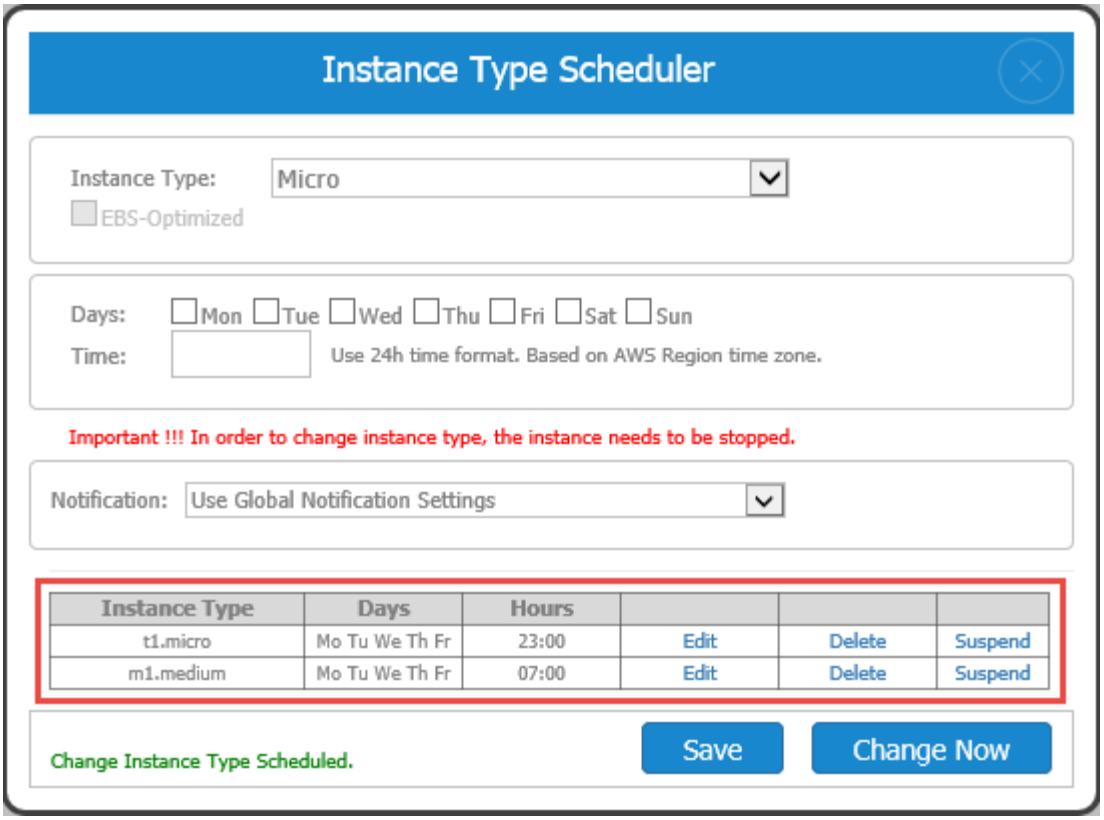
EBS-Optimized – turn on/off EBS optimization for the new instance. This option will be active based on the selected type of EC2 Instance – to read more about EBS-Optimized feature, please visit: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSOptimized.html

Notification – select how you want to be notified about execution of the scheduler. To read more about notification settings, go to: Email Notification Settings

To make this change immediately, click Change Now.
To make this change based on a schedule, select date and time to activate the change, then click “Save”.



You can create multiple schedulers, e.g. schedule the instance to run smaller overnight and larger during the day. Customized scheduling will save costs for underutilized instances.



Introduction to Always On – Monitoring status of EC2 Instance

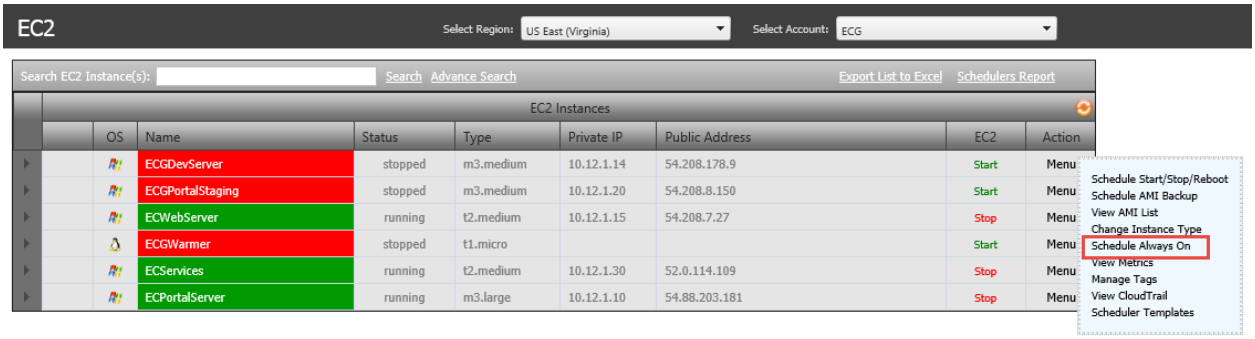
Elastic Cloud Gate Always On feature allows monitoring of the status of EC2 Instances.

Always On checks the status of the EC2 Instance each minute.
When the EC2 Instance monitoring status is not in Running mode, Always On attempts to start the instance.

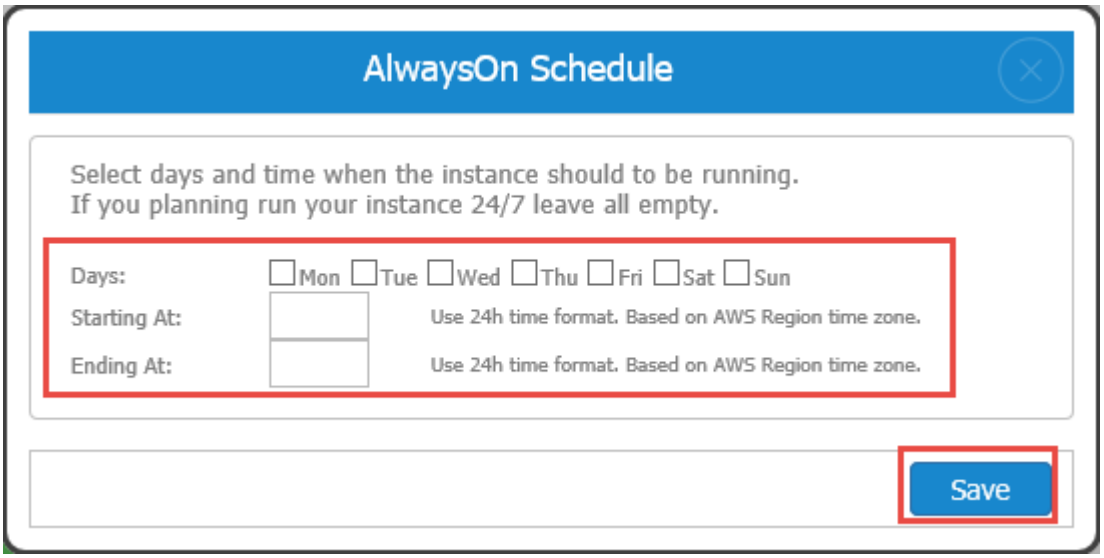
Always On can be setup to monitor given instance 24/7 or during certain weekdays or between given hours.

Always On Setup

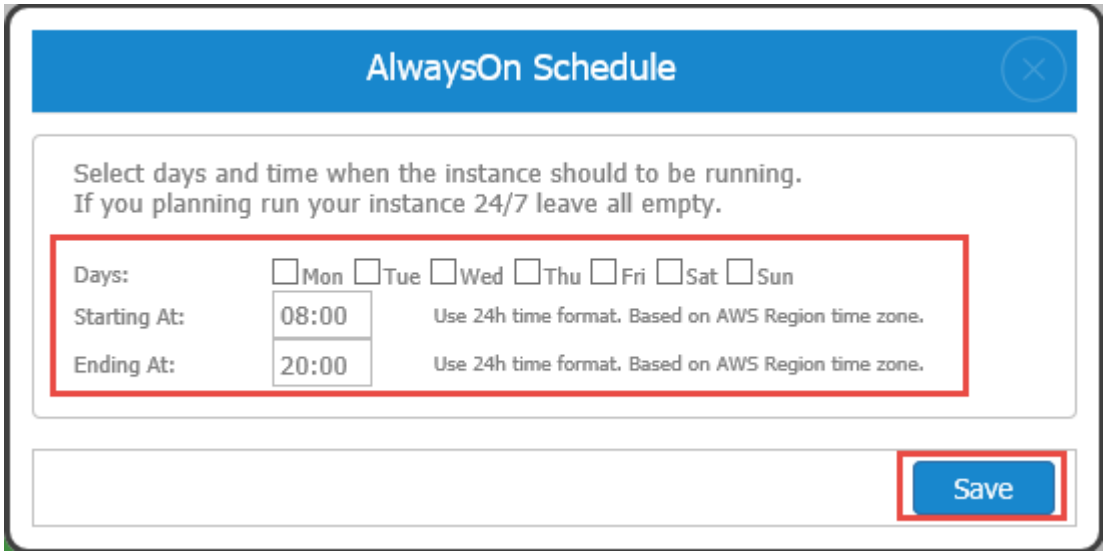
Follow these steps to setup Always On:
From the Main Menu, select EC2 from the EC2 section.
From EC2 Instance menu, select Schedule Always On.



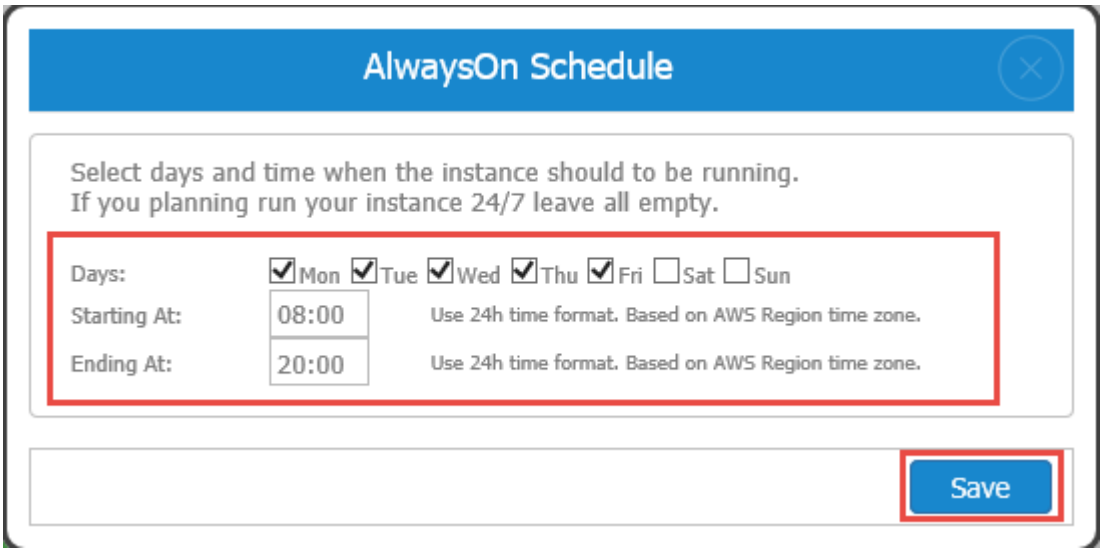
In the Always On schedule window, check days and enter start and end time for instance monitoring.
Examples:



- To monitor instance 24/7, leave all options blank.
- To monitor instance every day only between specified hours, leave days unchecked and enter Starting At and Ending At times.



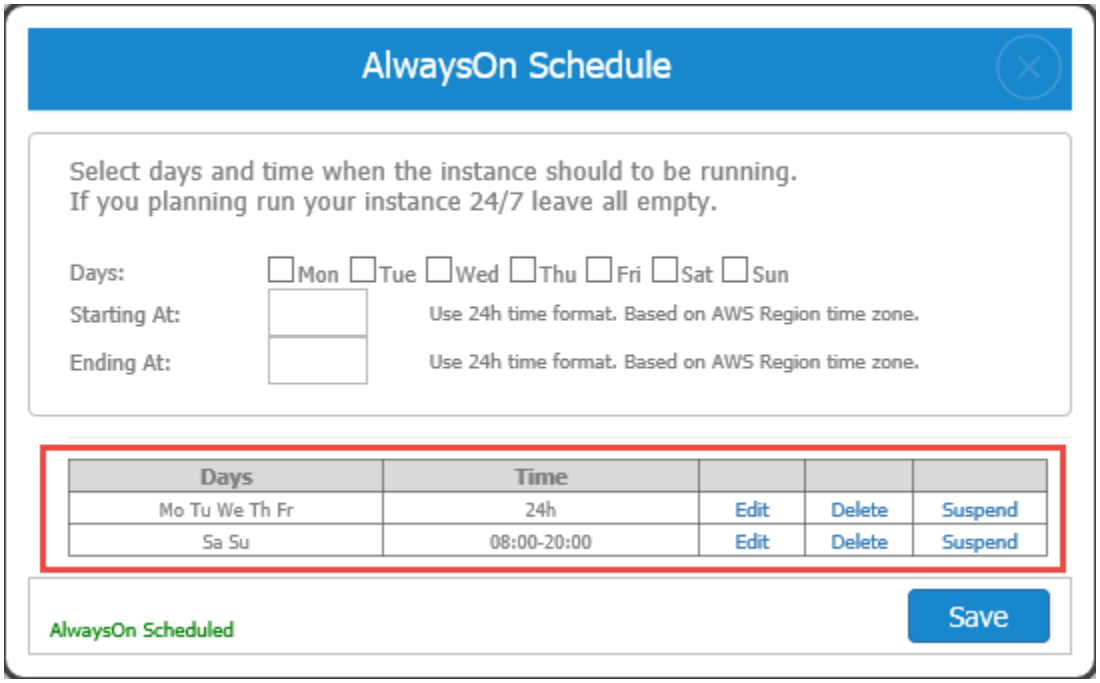
- To monitor instance 24 hours/day only during weekdays, leave Starting At and Ending At blank and check days you want instance monitoring.
- To monitor instance during given weekdays and between certain hours, check days and enter Starting At and Ending At times.



Click Save.

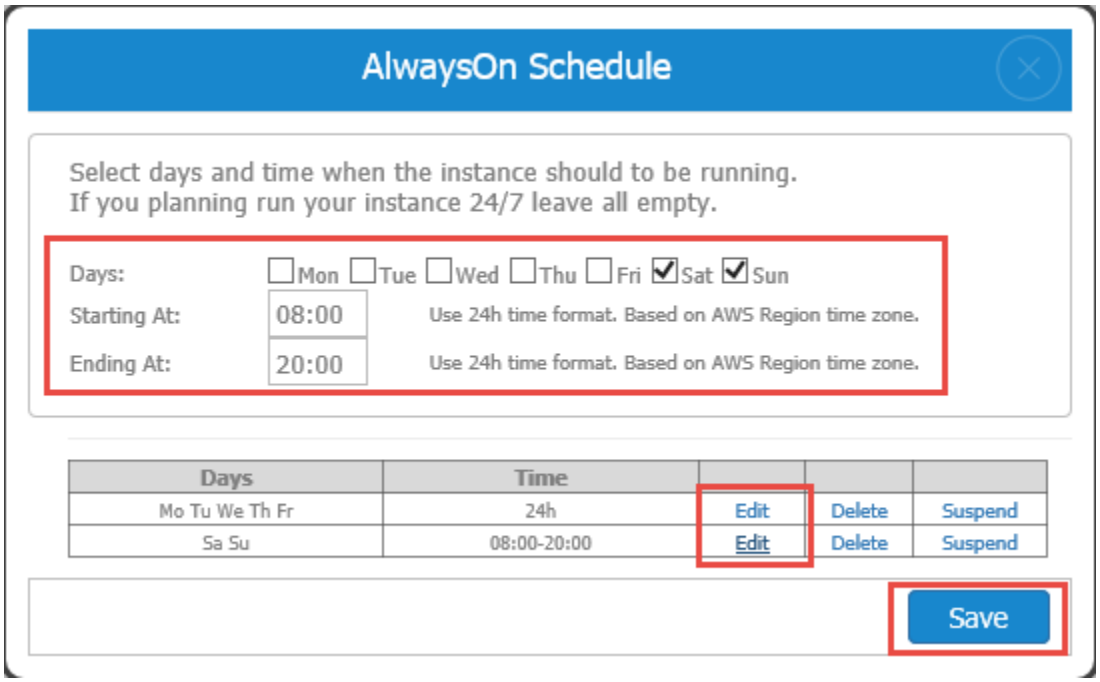
If an EC2 Instance requires more robust flexibility in monitoring (hours/days), you can schedule multiple Always On settings for the same EC2 Instance to meet your needs.

Example: you can create schedules to monitor EC2 instance:
1. Mon-Friday 24h
2. Sat-Sun from 8AM to 8PM

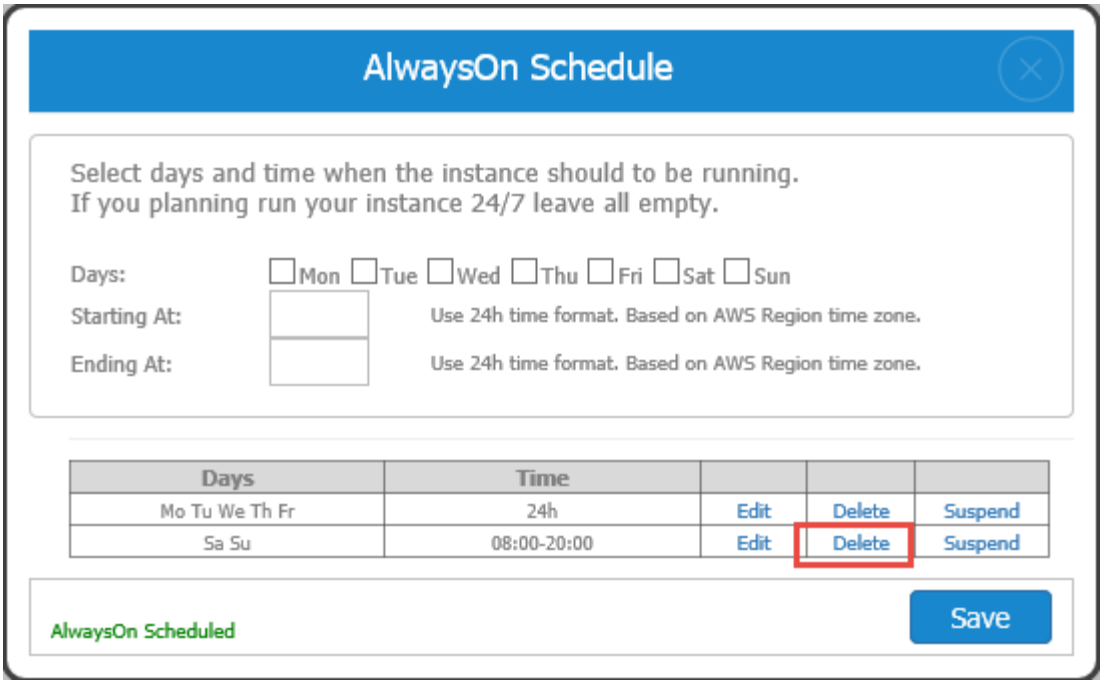


Always On Updating

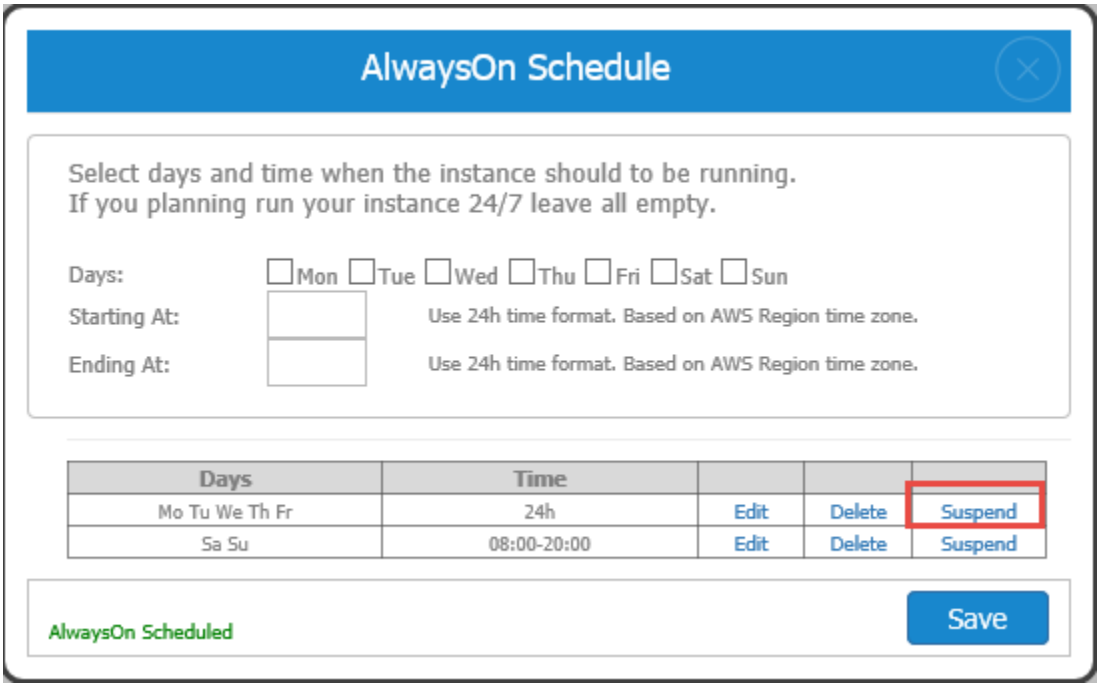
To update Always On: click Edit, make necessary changes, click Save.



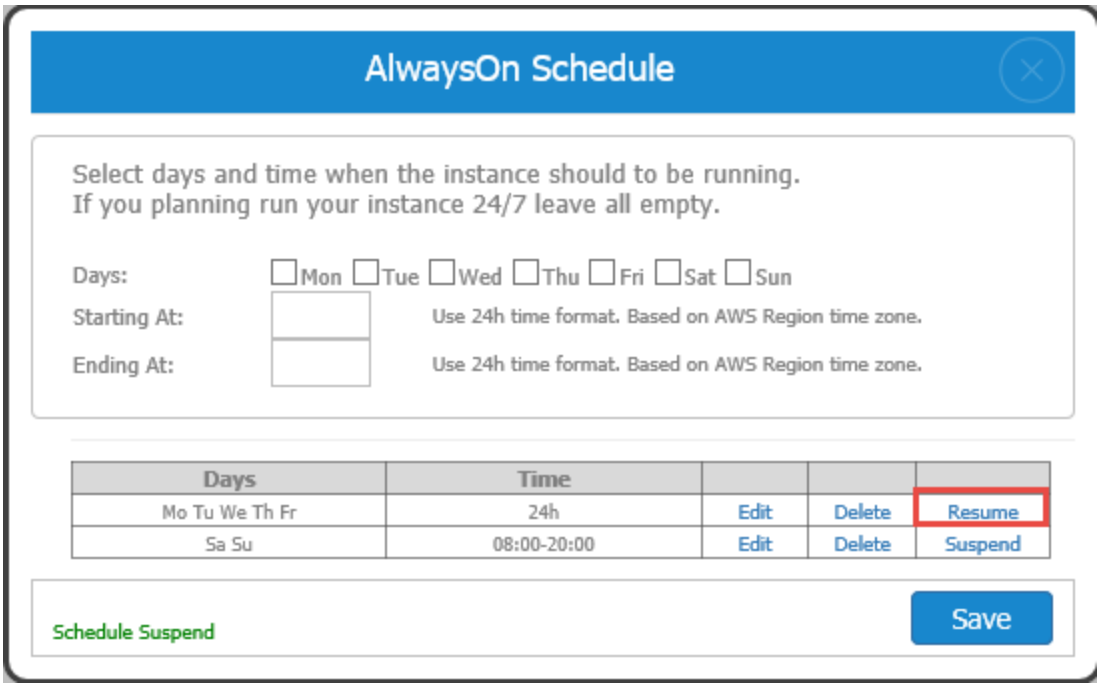
To delete Always On, click Delete.



If you need to stop an EC2 Instance that is monitored by Always On, you can suspend Always On by clicking Suspend.



To resume monitoring, click Resume.

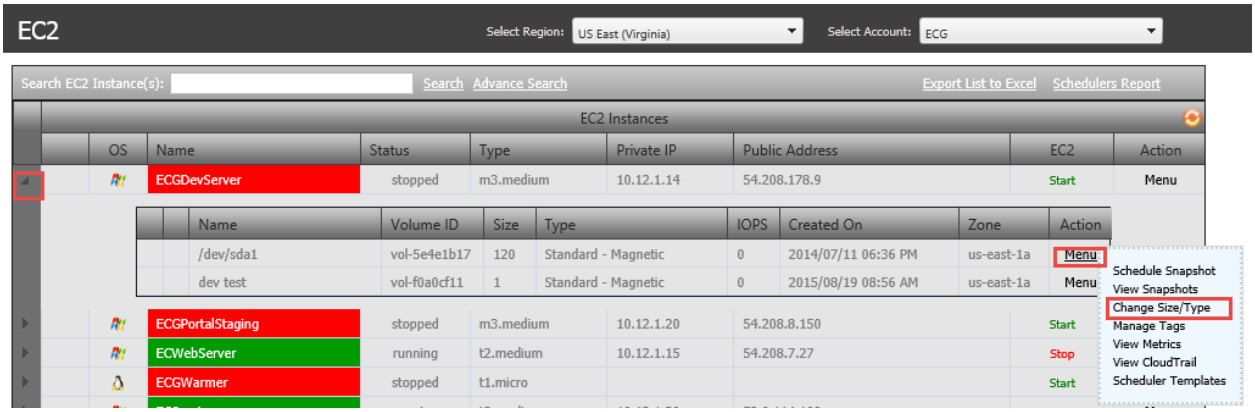


How to change size or type of EBS volume

If you are not an Elastic Cloud Gate member, go to this link to review the 8-step process to expand the EBS volume size:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-expand-volume.html

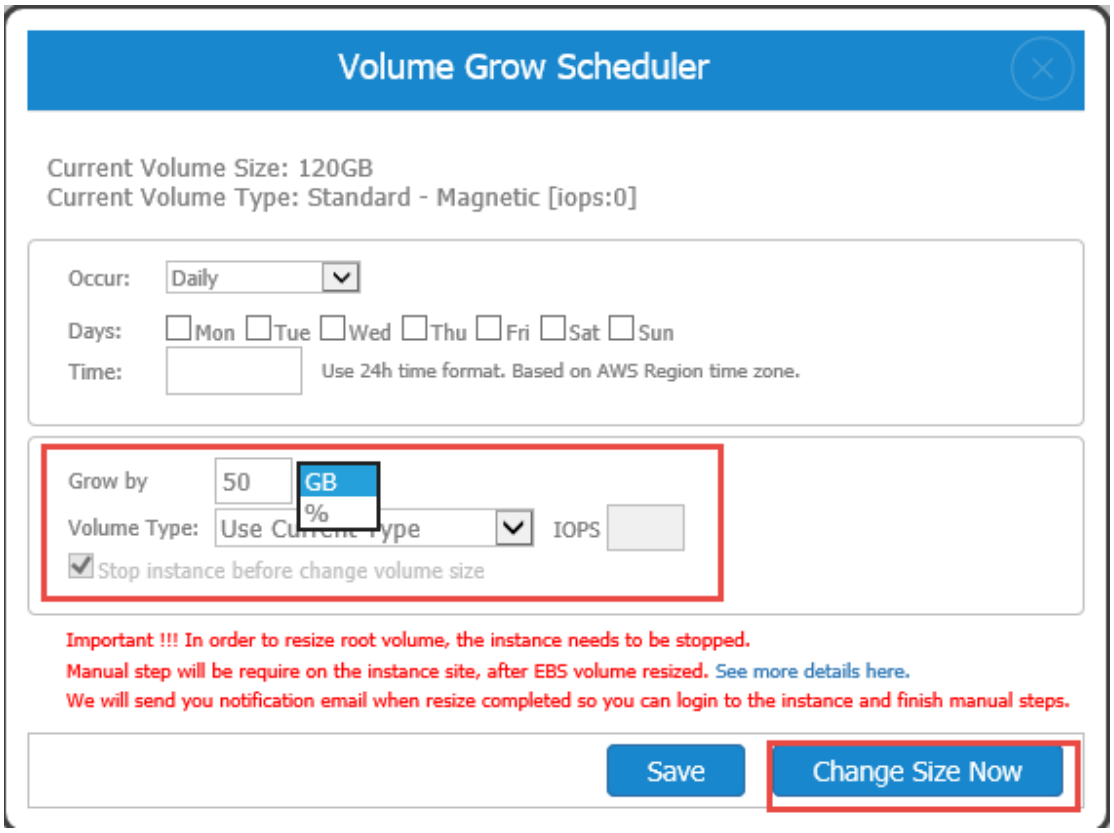
For Elastic Cloud Gate members, expanding the EBS volume size requires 2 steps:

From the Main Menu, select EC2.
Click the black arrow to the left of the EC2 instance to expand EBS volumes.
From the menu, select Change Size/Type.

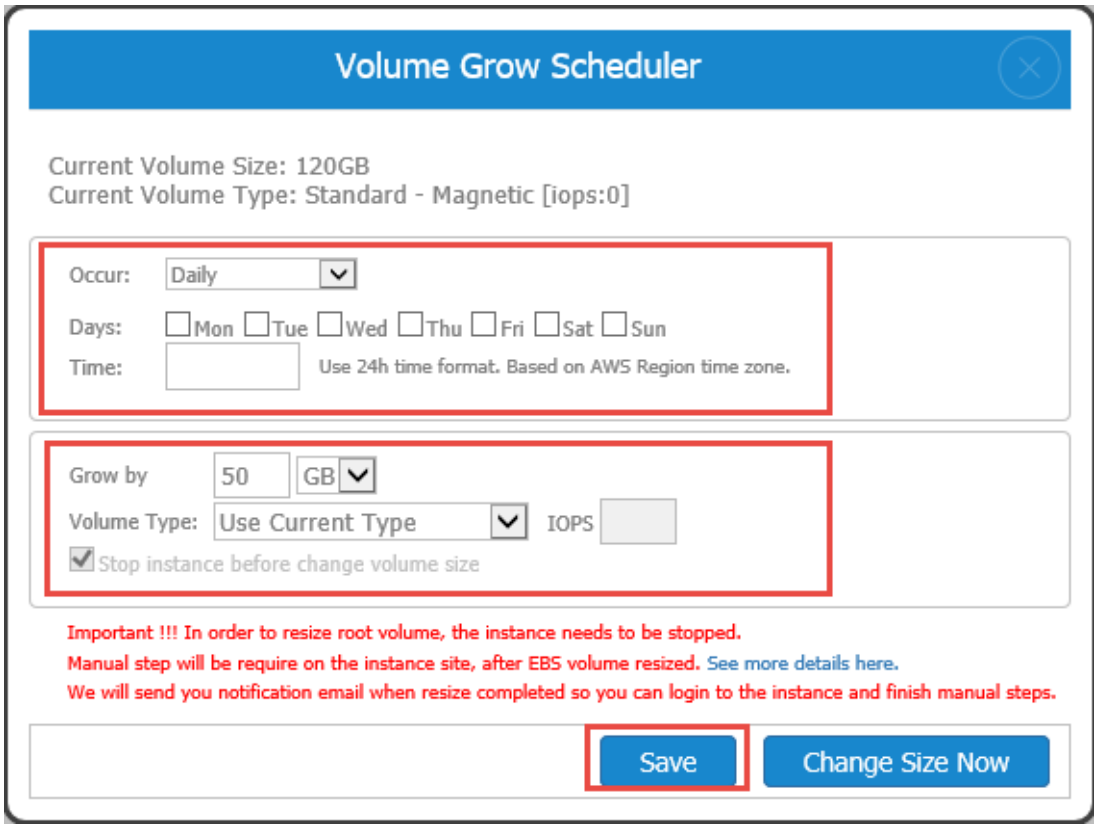


Under “Grow By”, enter the size or percentage to expand volume, e.g. if the current size of the volume is 100GB and you want to expand to 150GB, enter 50GB or 50%.
Type of the volume can be changed by selecting the new type from the drop down list, or leave Use Current Type to maintain the current type.

To apply changes, click Change Size Now.

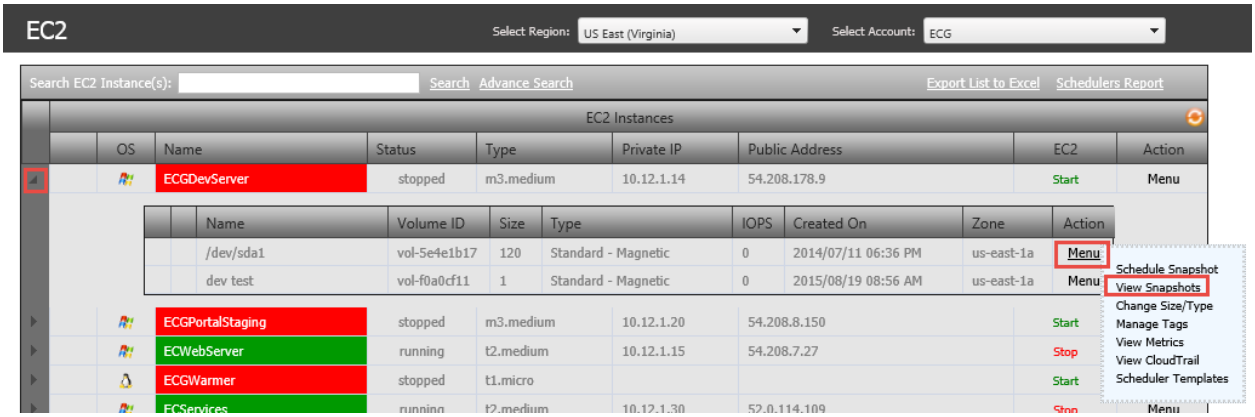


To execute changes on a regular basis, schedule changes by selecting Occurrence and Other Time Base options at the top of the windows, then click Save.

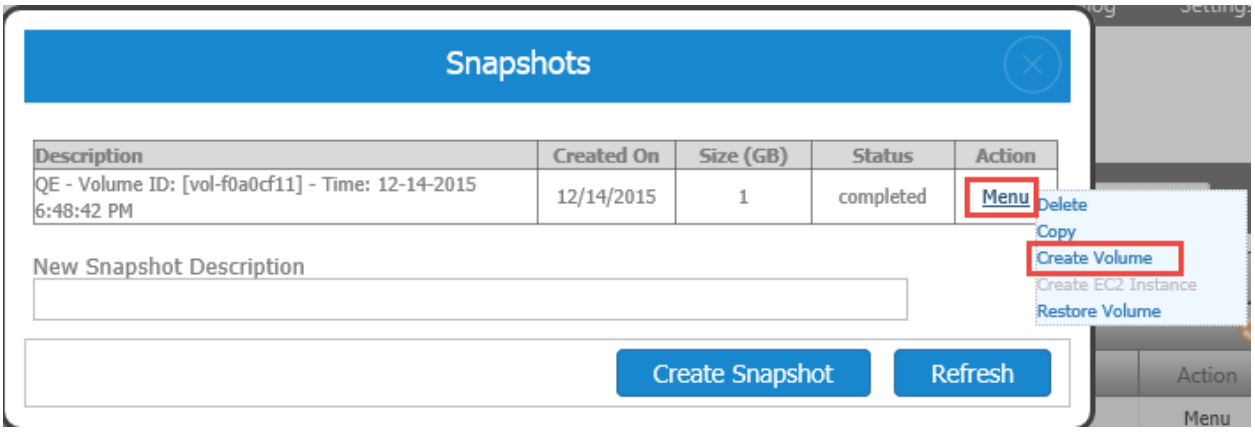


How to create a new EBS volume from snapshot

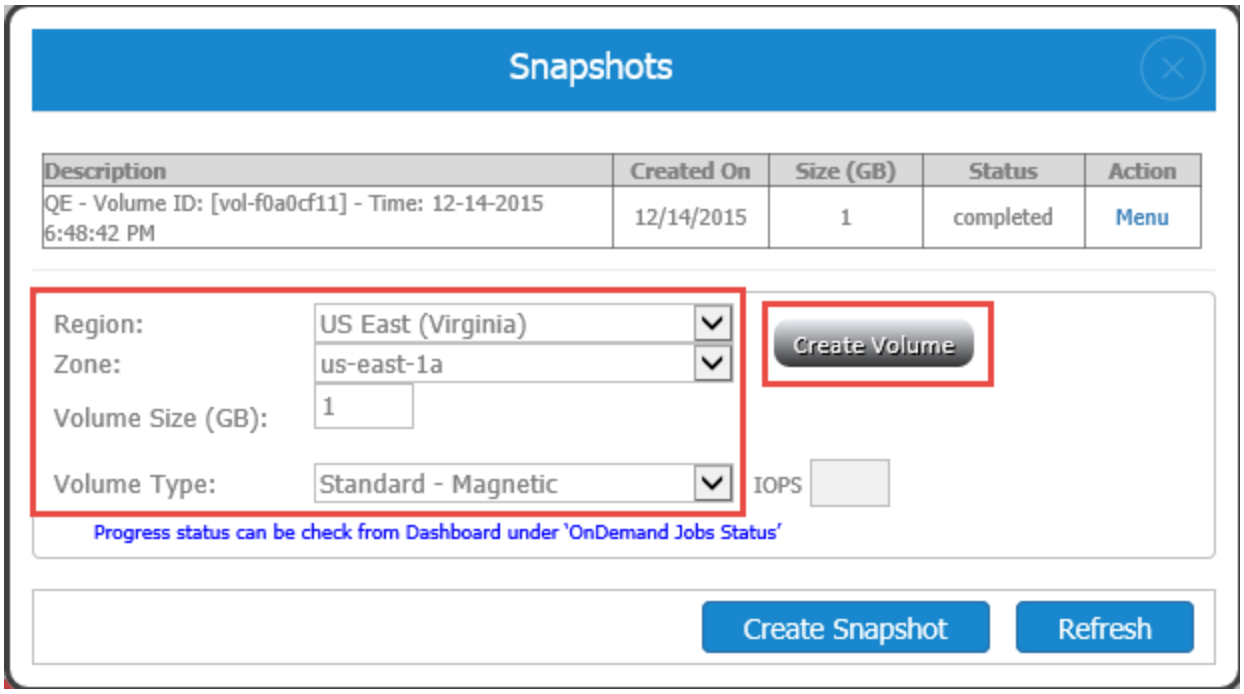
From the Main Menu, select EC2.
Click on the black arrow to the left of EC2 Instance to expand EBS volumes.
From the menu, select View Snapshots.



In the new window, find the snapshot to create volume and from the menu select Create Volume.



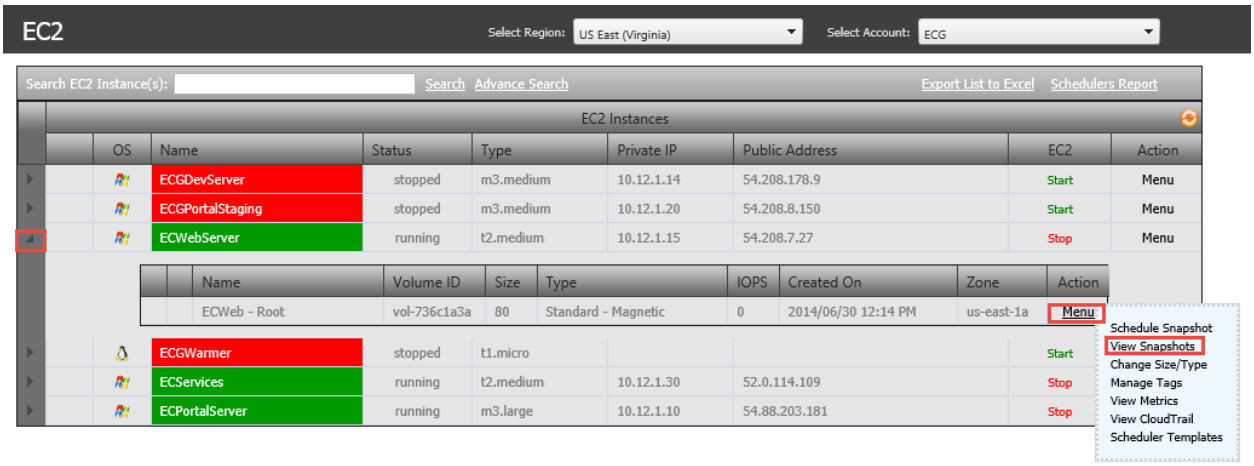
Select region and zone to create the new volume.
Select size and type of new volume, as well as IOPS (when applicable).
Click Create Volume.



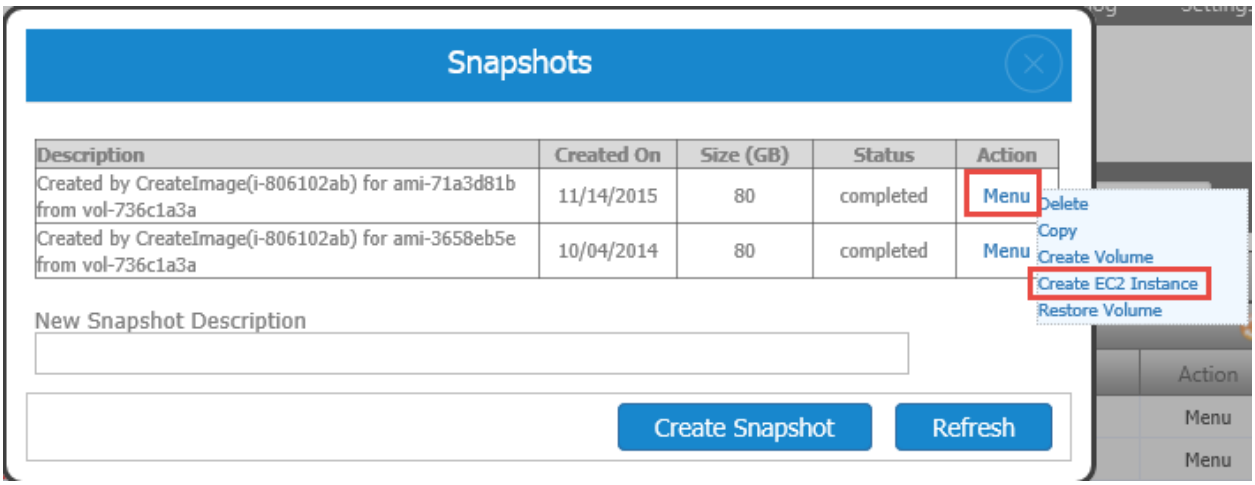
How to launch new EC2 Instance from snapshot

The same task can be accomplished more quickly using Elastic Cloud Gate console:

From the Main Menu, select EC2.
Click the black arrow on the left to expand EBS volume.
Identify root EBS volume and from the menu select View Snapshots.

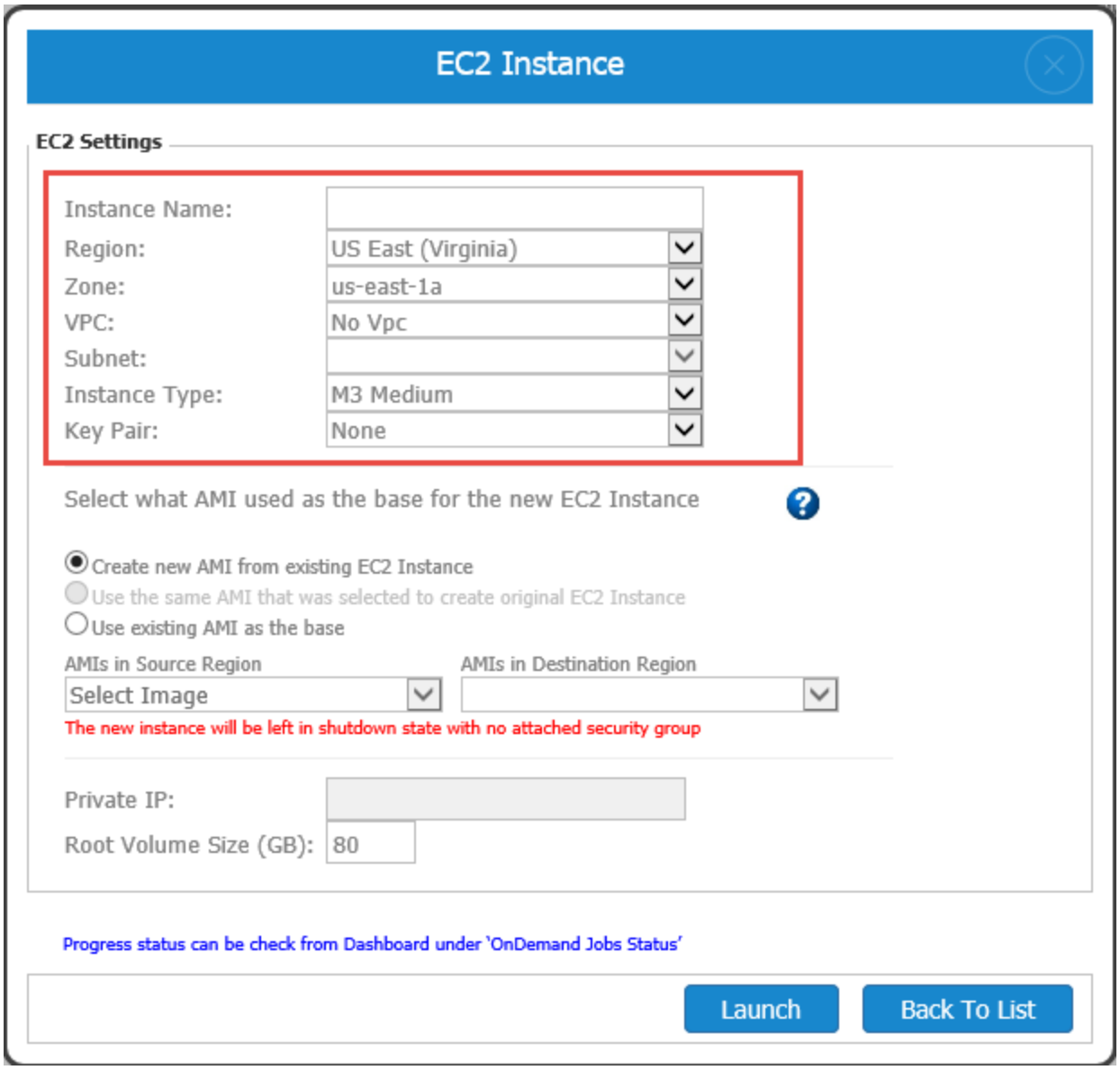


Under the Snapshot window, find the snapshot to create a new EC2 instance and from the menu select Create EC2 Instance.



Set EC2 configuration:

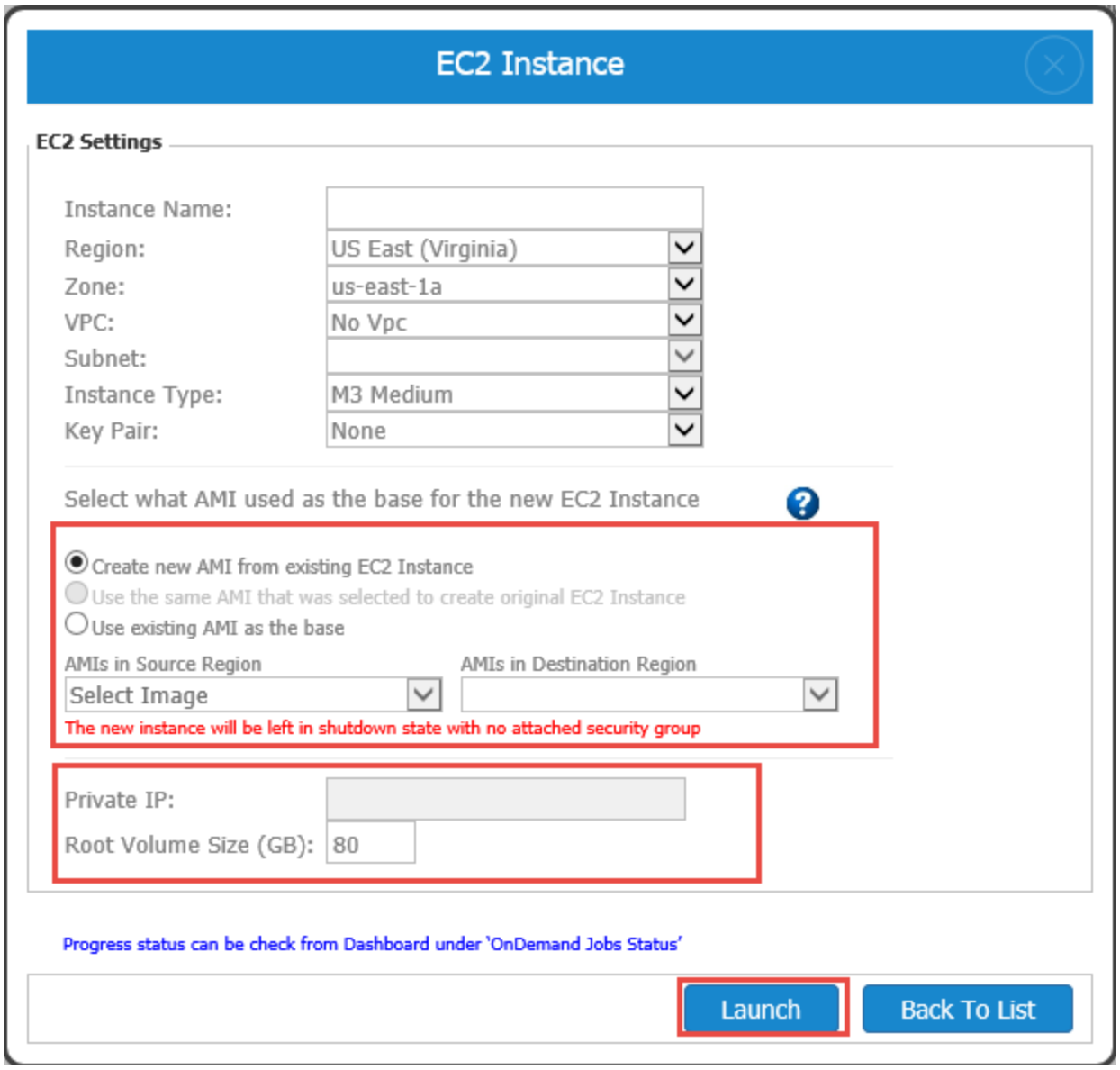
1. Enter name
2. Select region, zone, and VPC
3. Select instance type
4. Select key pair



Select AMI to use as the base, from the following options:

1. Create new AMI from the existing EC2 instance – Take a new AMI from the existing EC2 instance, which is used as the base for the new one.
2. Use the same AMI that was selected to create original EC2 instance – Use the same AMI that was chosen when you built the current instance.
3. Use existing AMI as the base – Choose existing AMI, either in source or destination region (if you are planning to launch new instance in different region), to use as the base

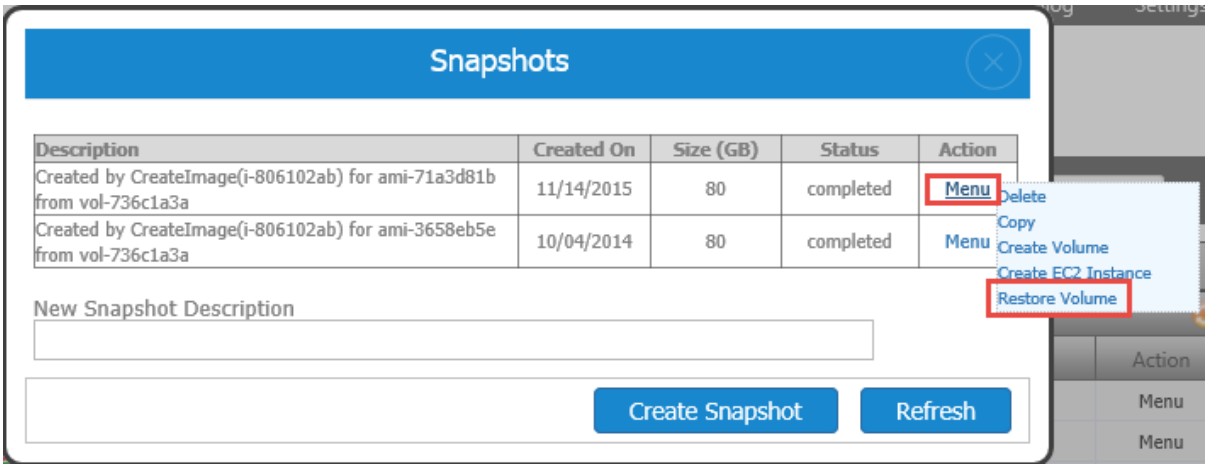
Additionally, you can specify private IP and/or new size of the root volume.
Click Launch.



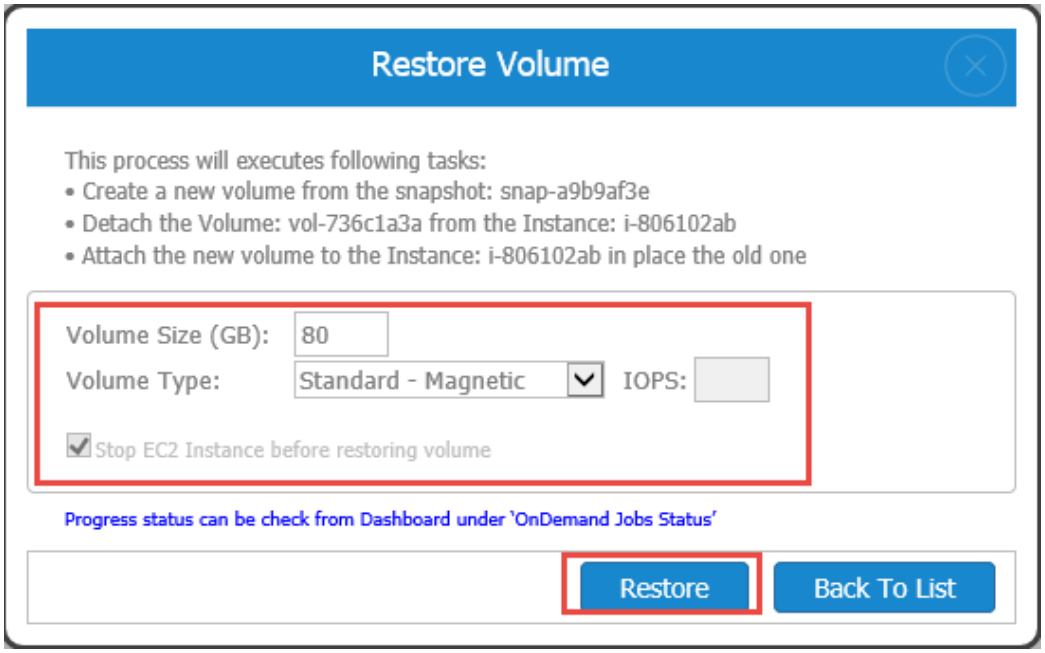
How to restore EBS volume from snapshot

Elastic Cloud Gate members have a quicker way to restore EBS volume:

From the Main Menu, select EC2 from the EC2 section.
Click on the black arrow to the left to expand EBS volume list.
From the menu, select View Snapshot.



In the new windows, find the snapshot to restore volume and from the menu select Restore Volume.
As an option, you can enter new size or type of the EBS volume.
Click Restore.

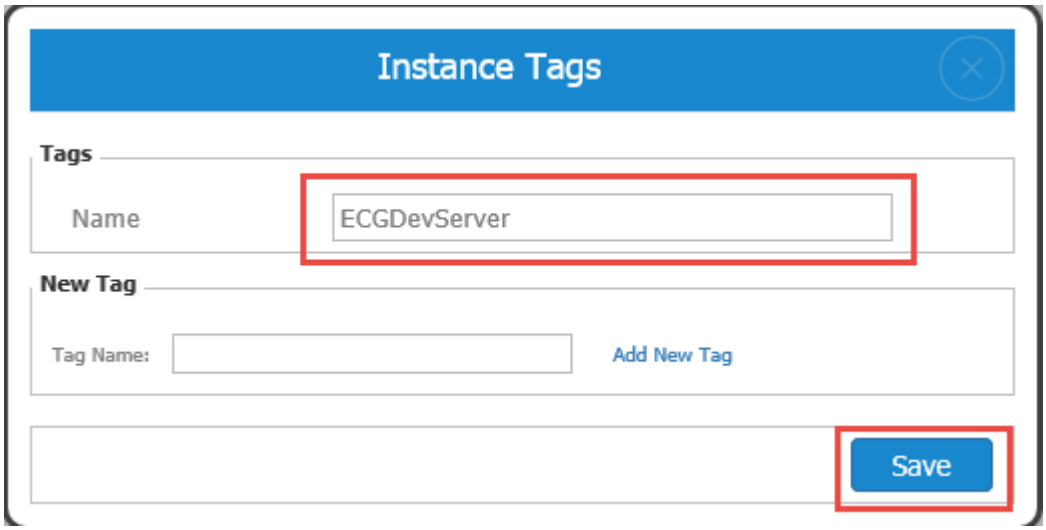


Note: if the restored EBS volume is the root volume, the underlining EC2 Instance will be stopped for the duration of time spent replacing the volume.

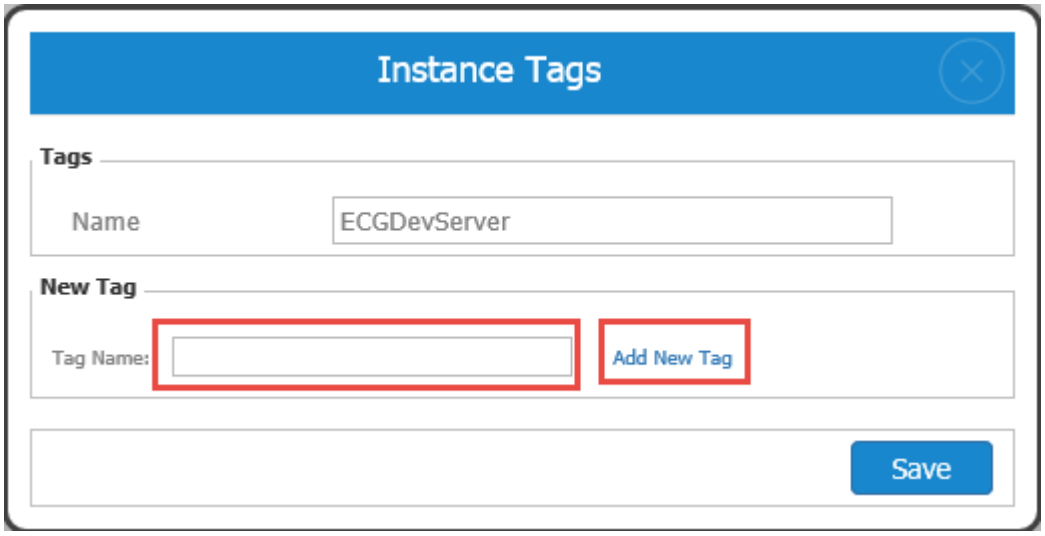
How to add/modify tags of EC2 Instance

Follow these steps to add or modify EC2 Instance tags:

From the Main Menu, select EC2.
Under the menu's EC2 Instance list, select Manage Tags.



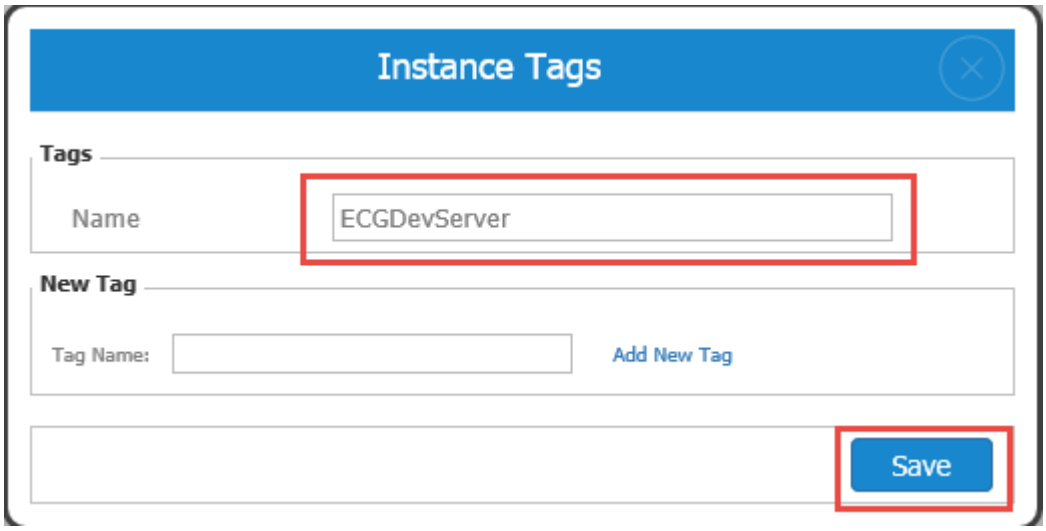
To modify the value of the existing tag, enter new value in the text box and click Save.
To add a new tag, enter tag name and click Add New Tag. The new tag appears on the list of tags, where you can then modify its value.



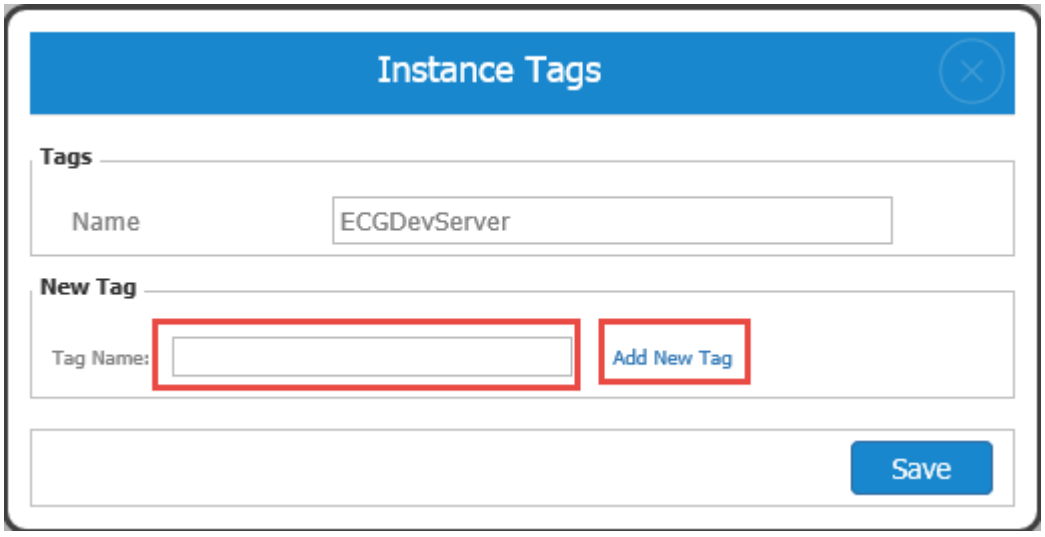
How to add/modify tags of EBS Volume

Follow these steps to add or modify EBS volume tags:

From the Main Menu, select EC2.
Click the black arrow on the left to expand the EC2 Instance's EBS volumes.
From the EBS menu, select Manage Tags.



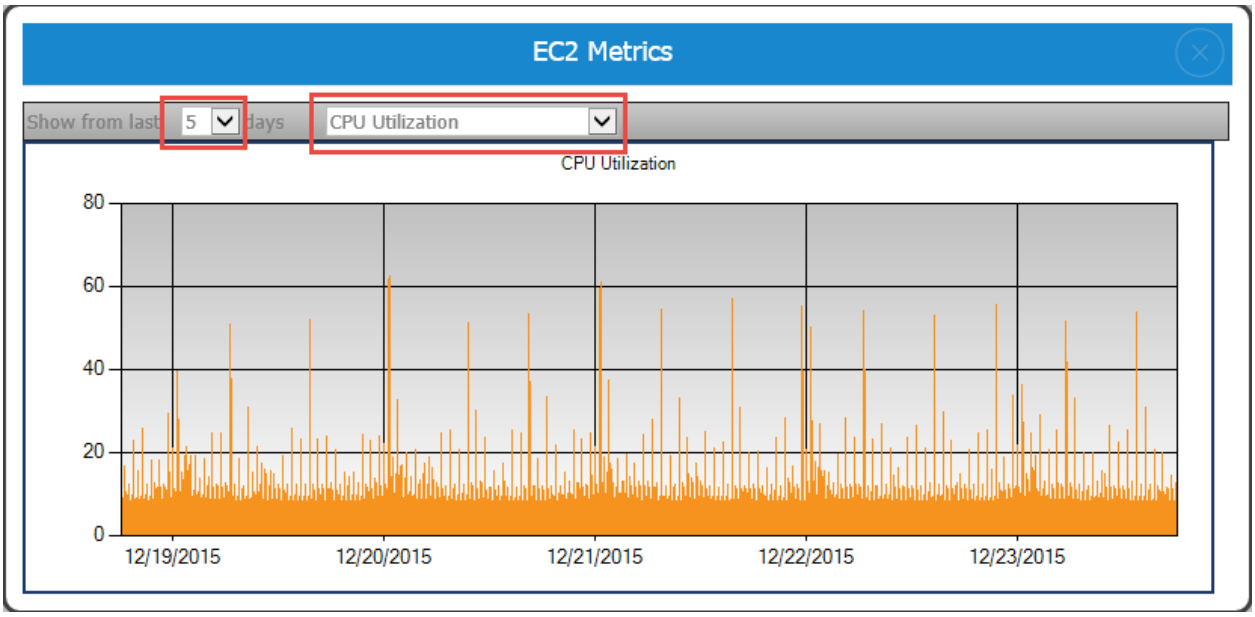
To modify the value of the existing tag, enter new value in the text box and click Save.
To add a new tag, enter tag name and click Add New Tag; the new tag appears on the list of tags, where you can then modify its value.



View metrics of EC2 Instance

Follow these steps to view EC2 Instance metrics:

From the Main Menu, select EC2.
Under EC2 Instance list from the menu, select View Metrics.



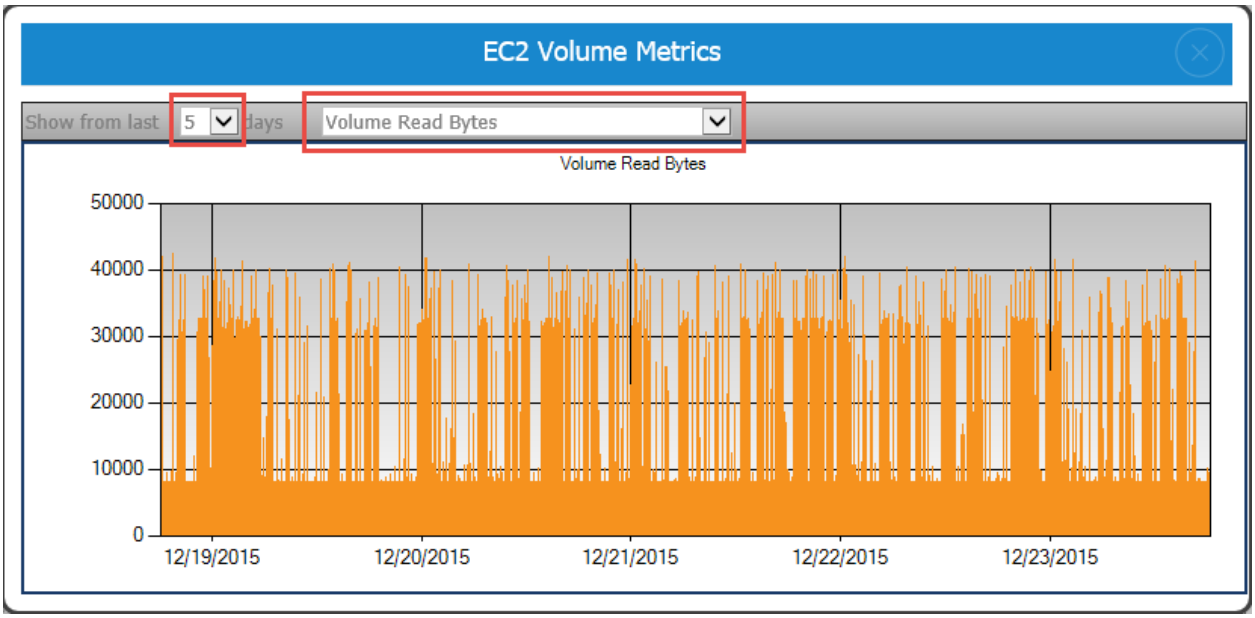
In the metric window are the following options:

- Show from last x days – Change the range of days to view selected metric
- List of metrics that are applied to EC2 instance – To view chart for a specific metric, select metric name from the drop down list

View metrics of EBS Volume

Follow these steps to view EBS volume metrics:

From the Main Menu, select EC2.
Click the black arrow on the left to expand the EC2 Instance's EBS volumes.
From the EBS menu, select View Metrics.



In the metric window are the following options:

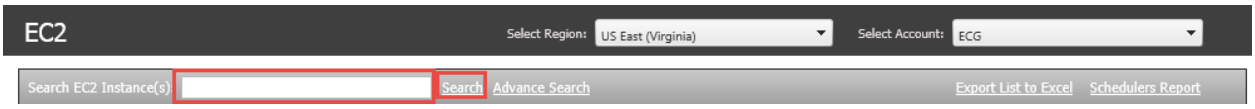
- Show from last x days – Change the range of days to view selected metric
- List of metrics that are applied to EBS volume – To view chart for a specific metric, select metric name from the drop down list

Search EC2 Instance

When many EC2 Instances are running, finding one to take specific action on can be difficult.

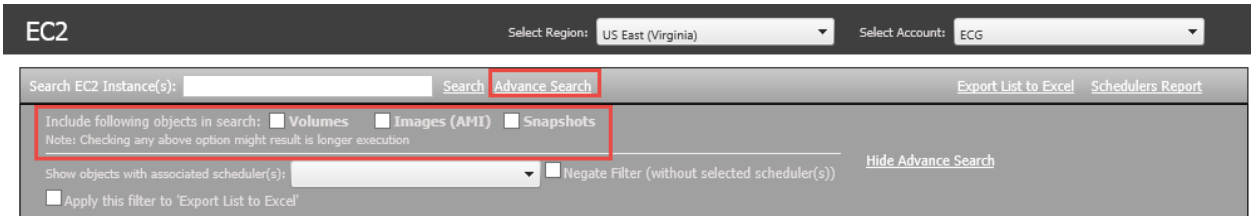
Under ECG portal is the option to search instances by numerous criteria.

To search for a particular instance, from the Main Menu select EC2.



At the top of all EC2 Instances is the box Search EC2 Instance(s). Use this box to search for Instances by:

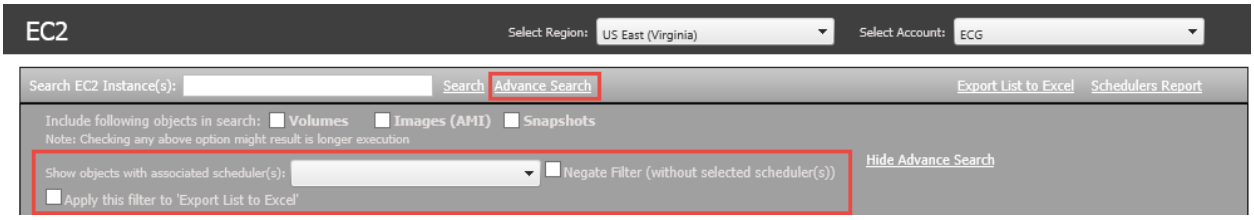
a. Name
b. Public IP (EIP)
c. Local IP
d. DNS Name
e. Instance ID



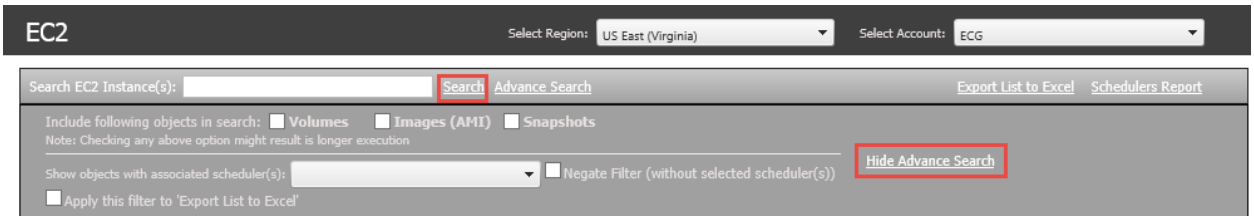
You can also search using advanced options: to do so, click Advance Search.
The expanded panel provides access to the following options:

1. Volumes – When checked, Instances are searched by:
   a. Attach EBS Volume name
   b. Attach EBS Volume ID
2. Images (AMI) – When checked, Instances are searched by:
   a. Image ID
   b. Image description
   c. Image name
   d. Snapshot ID from the root EBS of image
3. Snapshots – When checked (Volumes checked also), Instances are searched by:
   a. Snapshot ID
   b. Snapshot description
   c. Snapshot name

Additionally, instances and/or volumes can be filtered by scheduled action. Under Advance Search, expand the Show objects with associated scheduler(s) list and check actions. If you want to reverse the filter (meaning show objects that do not have scheduled action) check the Negate Filter checkbox.



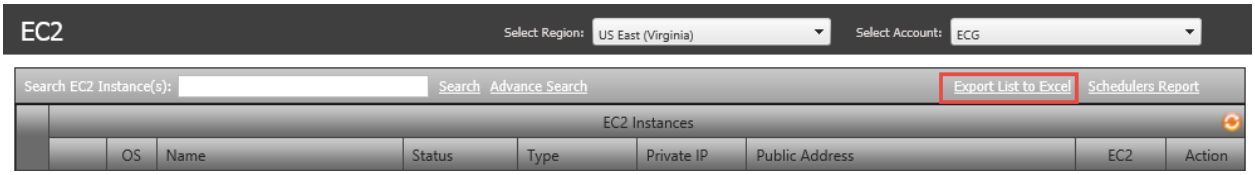
Enter your search criteria and click Search.



To hide the Advance Search panel, click Hide Advance Search.

How to Export list of EC2 Instances to Excel file

To export a list of all Instances with details, go to the EC2 section and at the top click Export List to Excel.

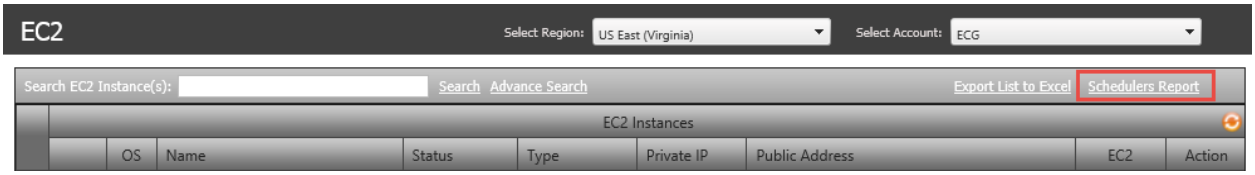


Detailed information about Instances is exported as a csv file. Information includes:

a. Instance name
b. Instance ID
c. Instance type
d. Instance Image ID
e. VPC information
f. IP addresses
g. Information about attached EBS volumes
h. Information regarding Instance and EBS volumes scheduled backup

How to export detail information about EC2 schedulers

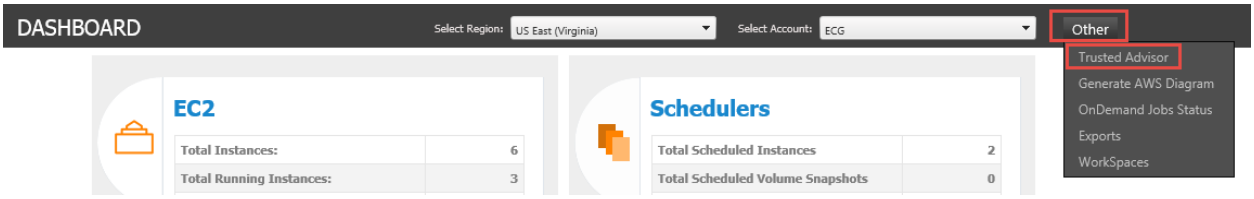
To export detail information about EC2 schedulers, from the Main Menu select EC2.
Under EC2 section, click Schedulers Report at the top of the EC2 list.



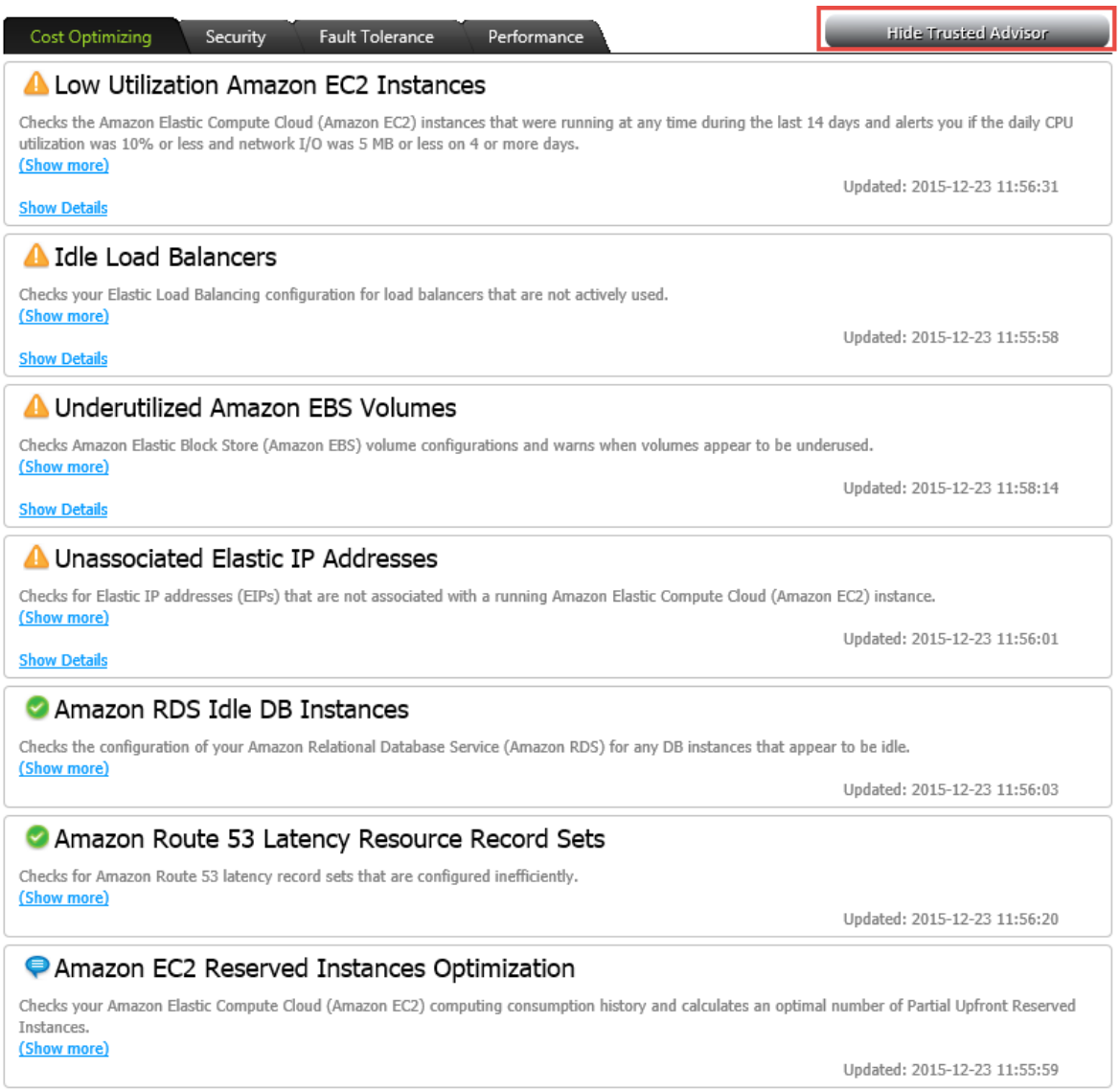
Exported excel file contains all EC2 Instances and attached EBS volumes, along with all actions scheduled for given EC2 or EBS.
When the action is scheduled using a template, the name of the template is also shown.

Review AWS Trusted Advisor

To review AWS Trusted Advisor, go to the ECG portal Dashboard.
From the Other menu located on the right side of the navigation panel, select Trusted Advisor.

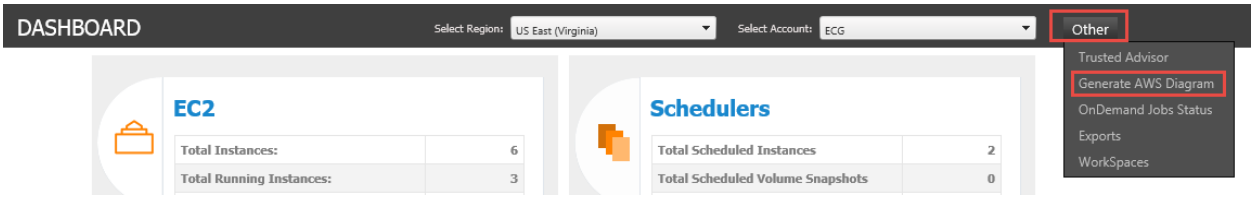


The Trusted Advisor panel opens above the Dashboard tails.
To close the Trusted Advisor panel, click Hide Trusted Advisor.



Generate AWS Diagram

Go to the ECG portal Dashboard.
From the Other menu located on the right side of the navigation panel, select Generate AWS Diagram.
A png file with the diagram of your AWS network will automatically download.



Searching and filtering Snapshots

Over time, the amount of snapshots generated under your AWS account will typically number in the hundreds.

ECG portal makes it easier to navigate these snapshots, using Filter and Search options.

To review all snapshots from the Main Menu, select Snapshots.

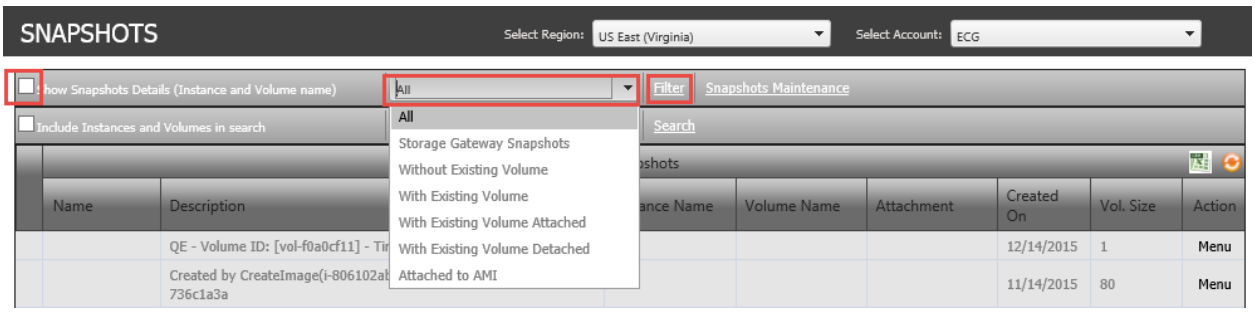
Filtering

To filter snapshots, from the navigation menu chose one of these options:

1. Storage Gateway Snapshot – Shows only snapshots created from the volume(s) attached to storage gateway
2. Without Existing Volume – Shows snapshots created from the volume that no longer exists
3. With Existing Volume – Shows snapshots created from still existing volume, regardless of attachment to any EC2 Instance
4. With Existing Volume Attached – Shows snapshots created from still existing volume and attached to an EC2 Instance
5. With Existing Volume Detached – Shows snapshots created from still existing volumes but not attached to any EC2 Instance
6. Attached to AMI – Shows only snapshots part of image (AMI)

Additionally, when the checkbox Show Snapshot Details (Instance and Volume name) is checked, information about EC2 Instances and EBS volumes is shown along with snapshot details.

To apply selected filter criteria, click Filter.



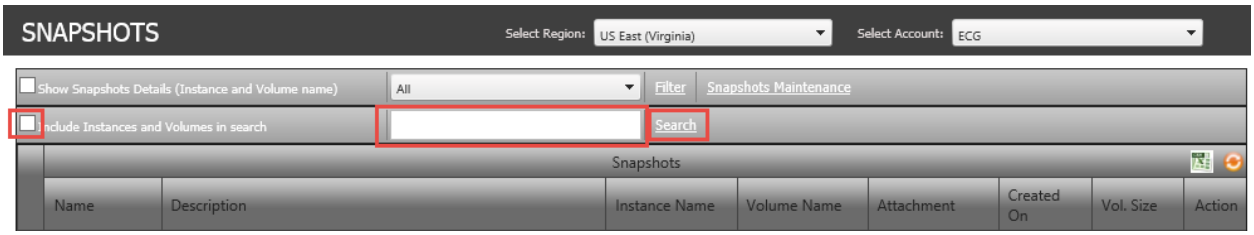
Searching

To search specific snapshot(s) in the search box, enter your criteria and click Search.
You can search snapshots by:

1. Description
2. Name
3. Snapshot ID
4. Volume ID

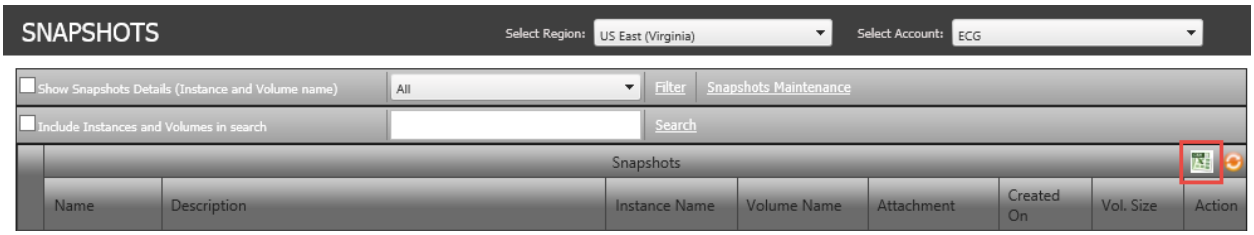
Additionally, when Include Instances and Volumes search is checked, you can also search by:

5. Attachment
6. Instance Name
7. Instance ID
8. Volume Name



Exporting

At any time, you can export all snapshots currently listed in the table to csv file: click the export icon located on the right hand site of the table header.

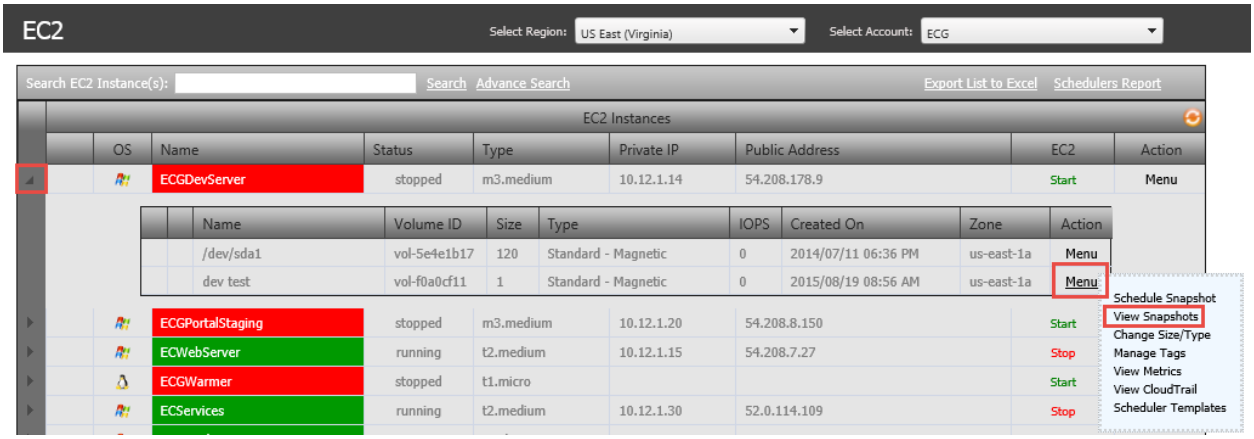


How to copy snapshots to different AWS Region

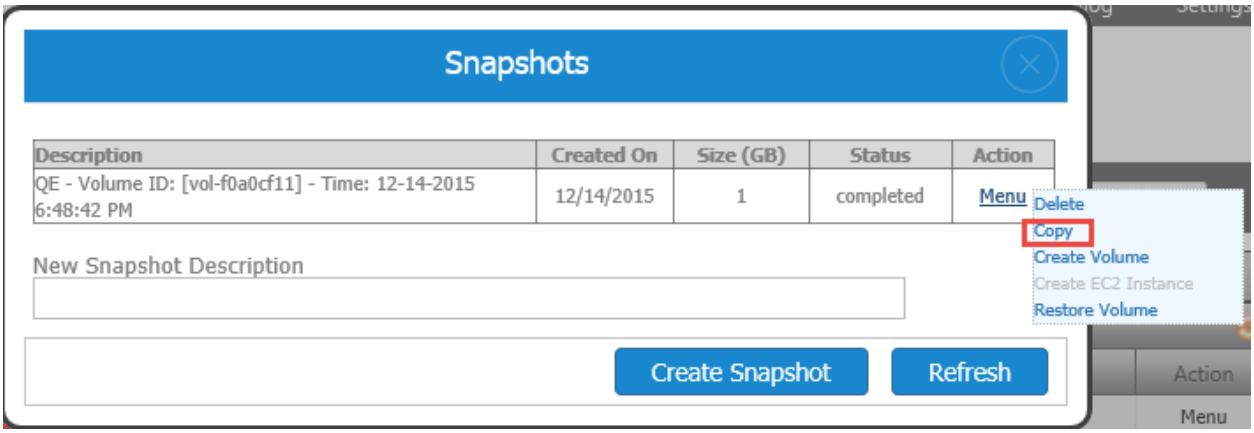
You can copy snapshot to a different region under EC2 or Snapshot section.

Follow these steps to copy Snapshot under EC2 section:

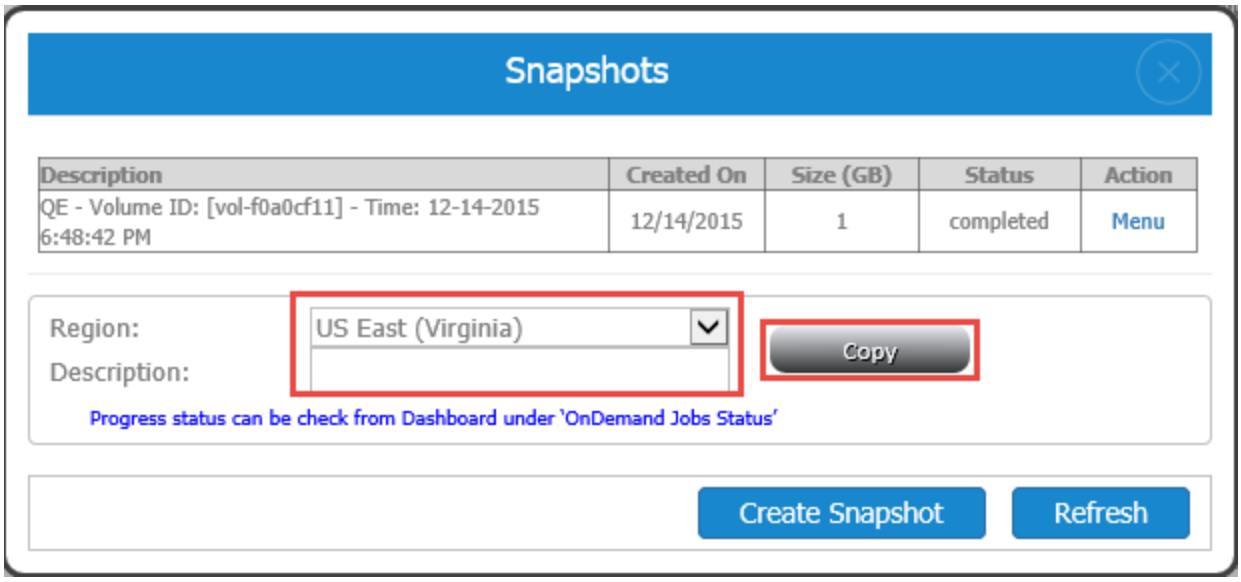
From the Main Menu, select EC2.
Click the black arrow on the left to expand volumes for a given EC2 Instance.
From the EBS volume menu, select View Snapshots.



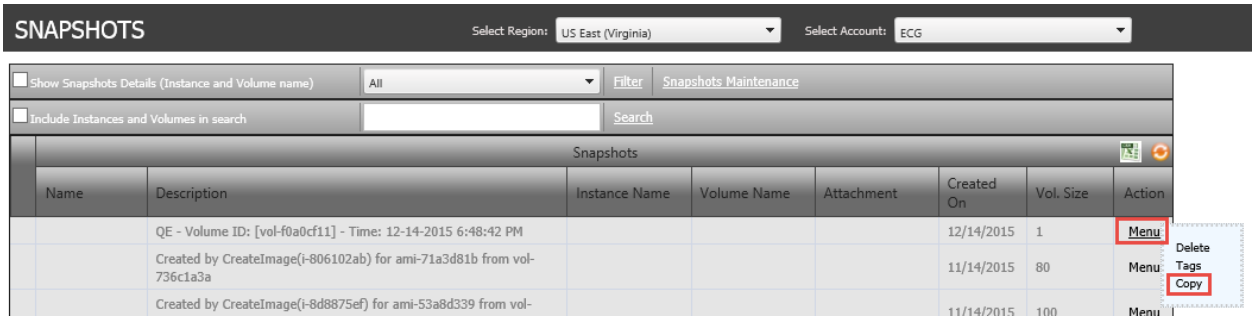
In the Snapshot window, identify the snapshot you want to copy and from the menu select Copy.



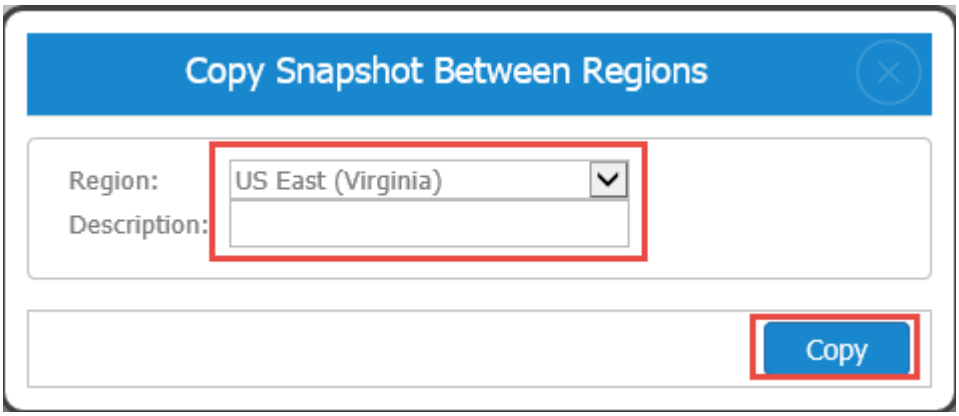
Select destination region.
Enter snapshot description.
Click Copy.



Follow these steps to copy snapshot under Snapshot section:
From the Main Menu, select Snapshots.
In the snapshot list, identify snapshot to copy from the menu, then select Copy.

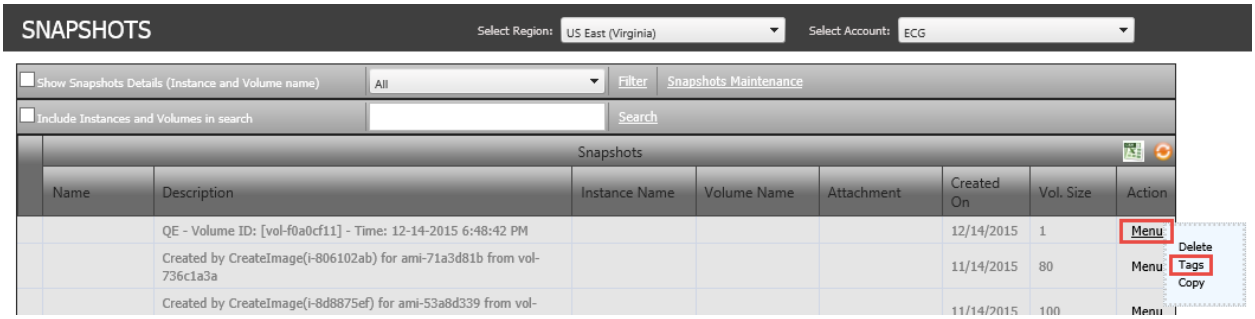


Select destination region.
Enter snapshot description.
Click Copy.

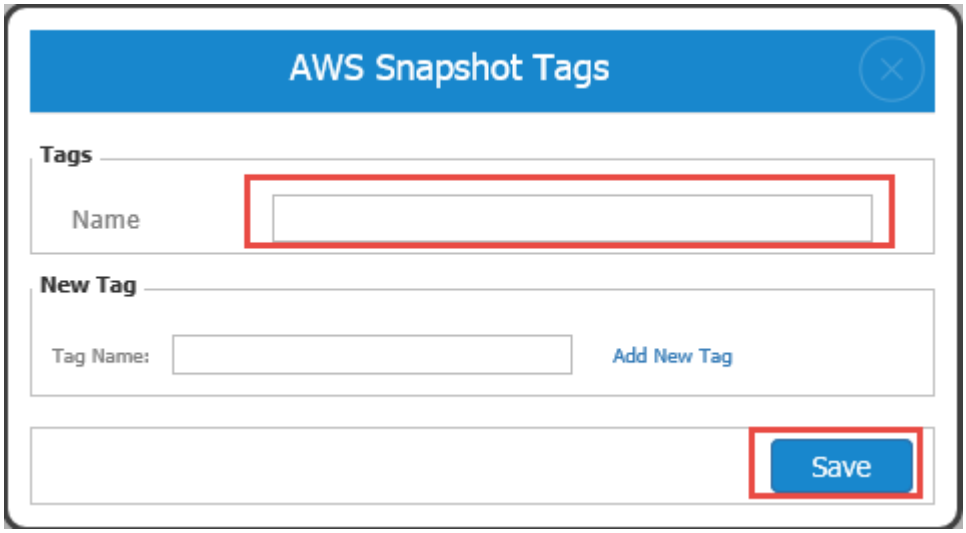


How to add/modify tags of snapshot

Follow these steps to modify snapshot tags:
From the Main Menu, select Snapshots.
In the snapshot list, identify snapshot to add/modify tags from the menu, then select Tags.

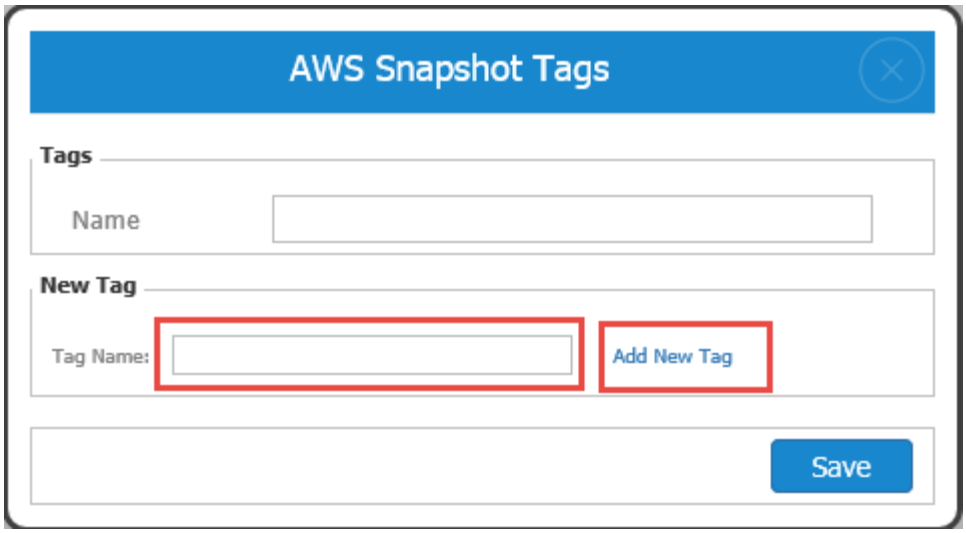


View current tags with value under the tag section. To modify value of the tag, enter new value and click Save.



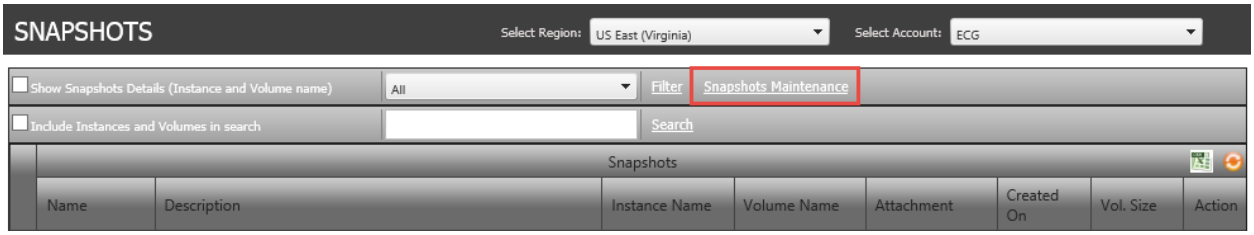
To add new tag, under the New Tag section enter new tag name and click Add New Tag.
The new tag appears under the tag section and the value can be entered.

After you enter new tag value, click Save.

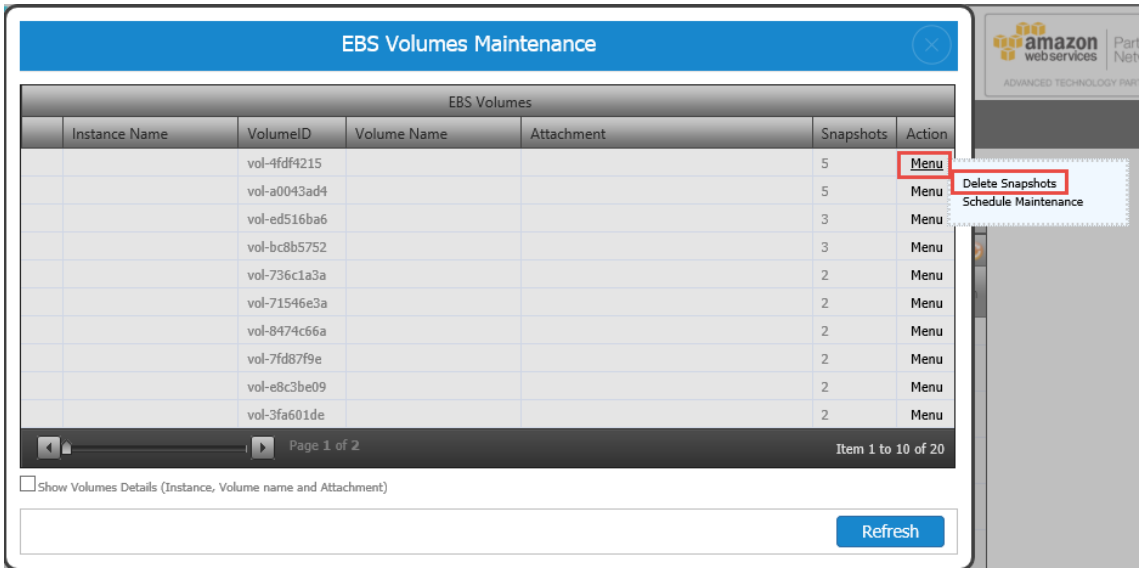


How to delete all snapshots from given EBS volume

To delete all snapshots at once from a single volume, from the Main Menu select Snapshots. Click the Snapshot Maintenance option, located above the snapshots list.



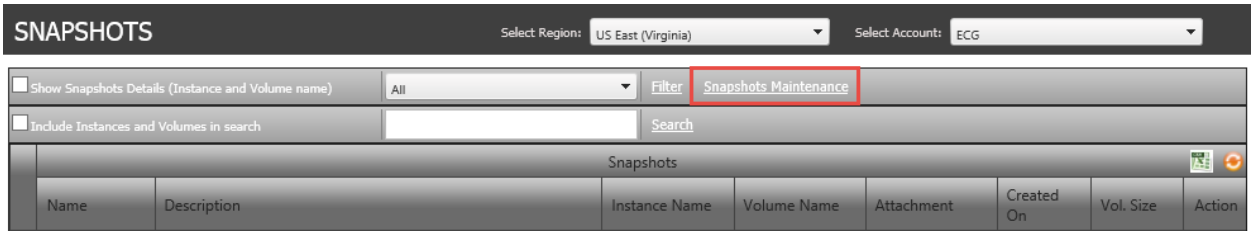
In the new window, identify the EBS volume to delete all snapshots from.
From the menu select Delete Snapshots.



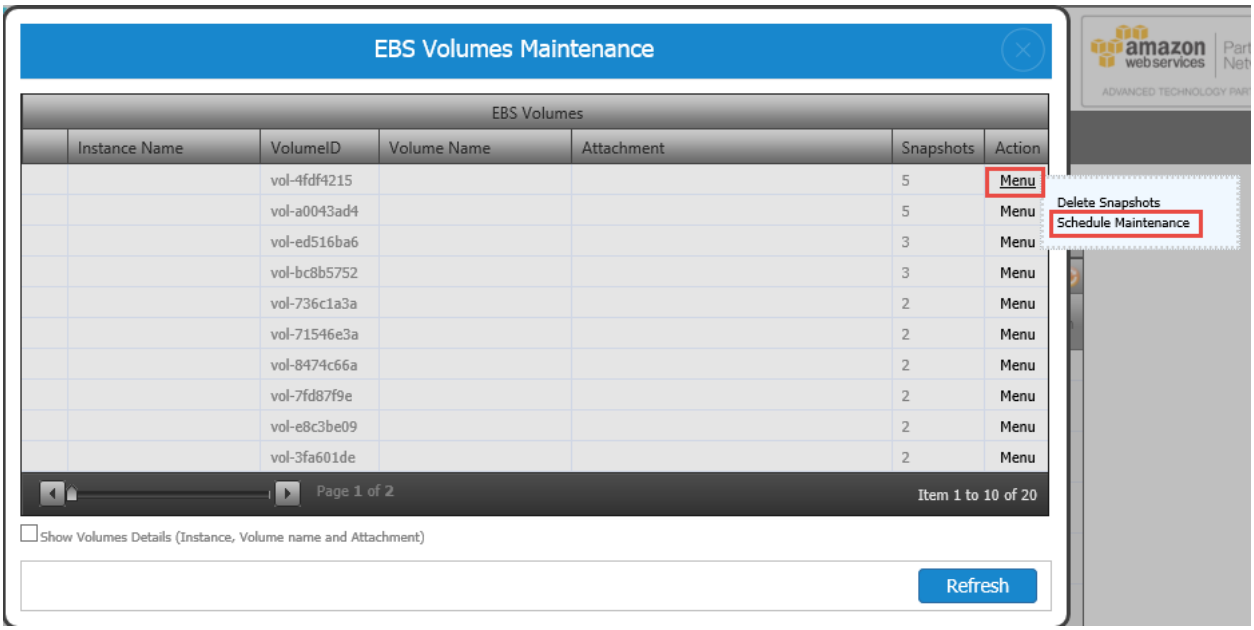
How to schedule maintenance of unknown snapshots

To schedule maintenance of snapshots that belong to a volume:

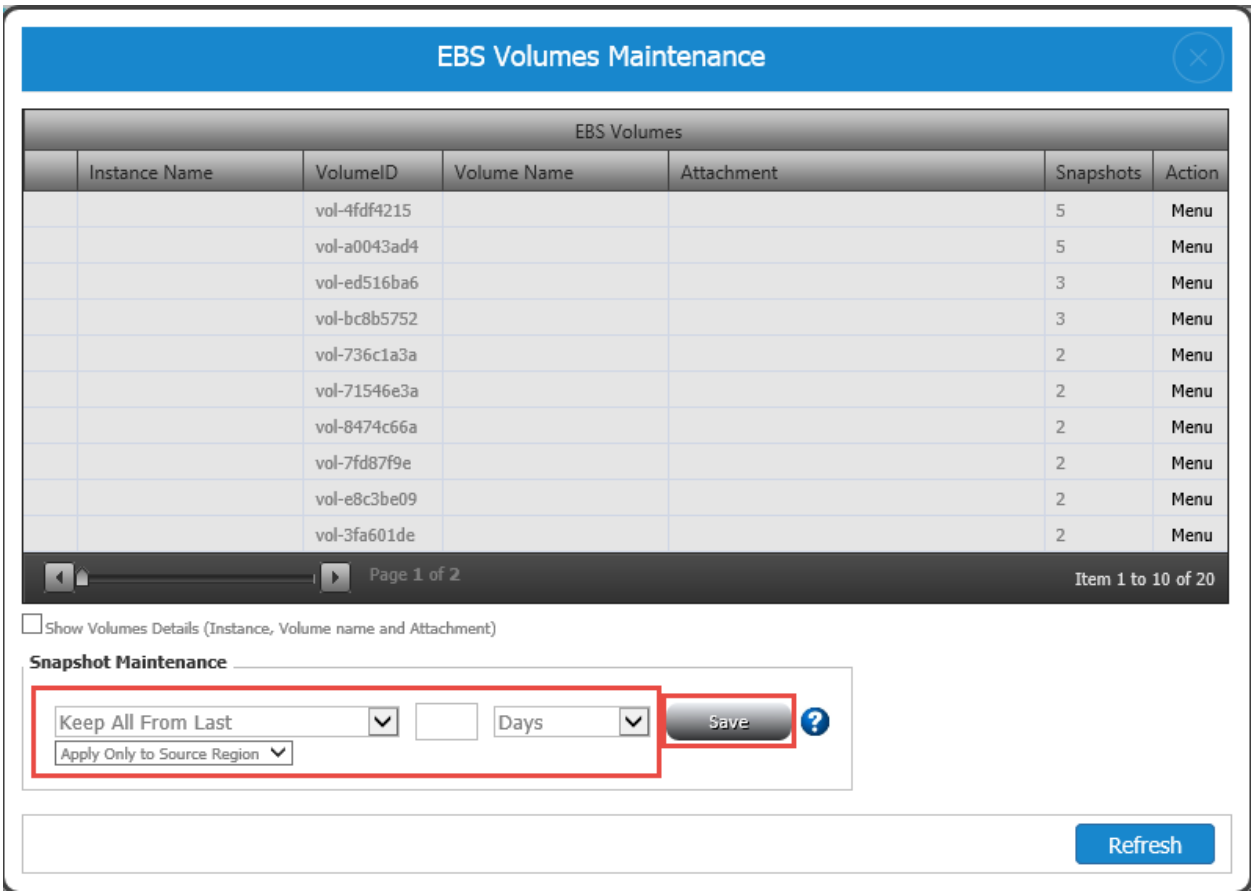
From the Main Menu, select Snapshots.
Click the Snapshot Maintenance option located above the snapshots list.



In the new window, identify the EBS volume to schedule maintenance for.
From the menu, select Schedule Maintenance.



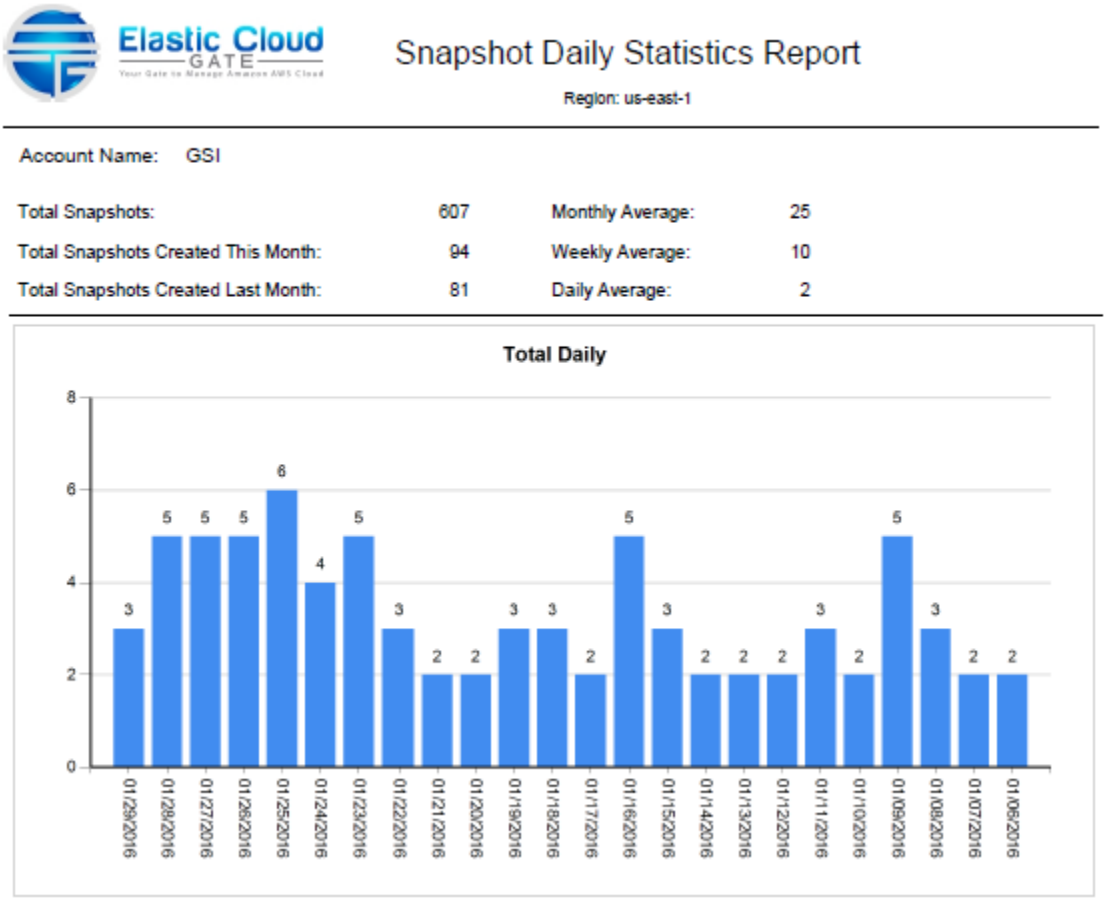
Select maintenance options and click Save.



To learn more about Snapshot Maintenance options, please go to:
[How to schedule maintenance of Snapshots]

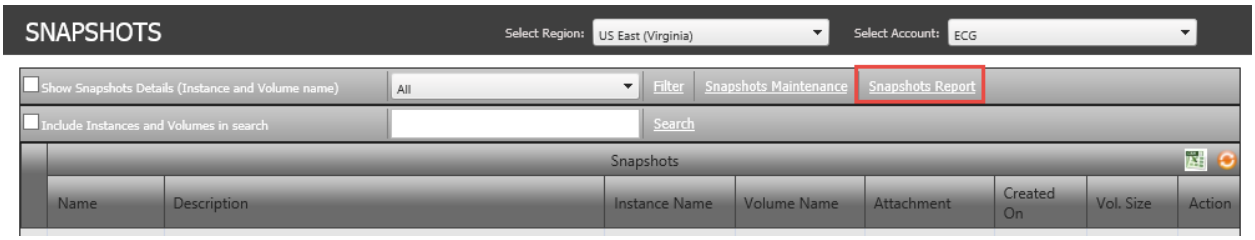
Snapshots Statistic Report

Snapshots Report is designed to provide overview of daily, weekly and monthly snapshots statistics.



Snapshots report can be schedule to be delivered as PDF over email

To schedule Snapshot report, go to Snapshot section and click “Snapshots Report”



Under Snapshot Report scheduler make following configuration:

Region:

All - report will be generate based on the snapshots from all AWS regions

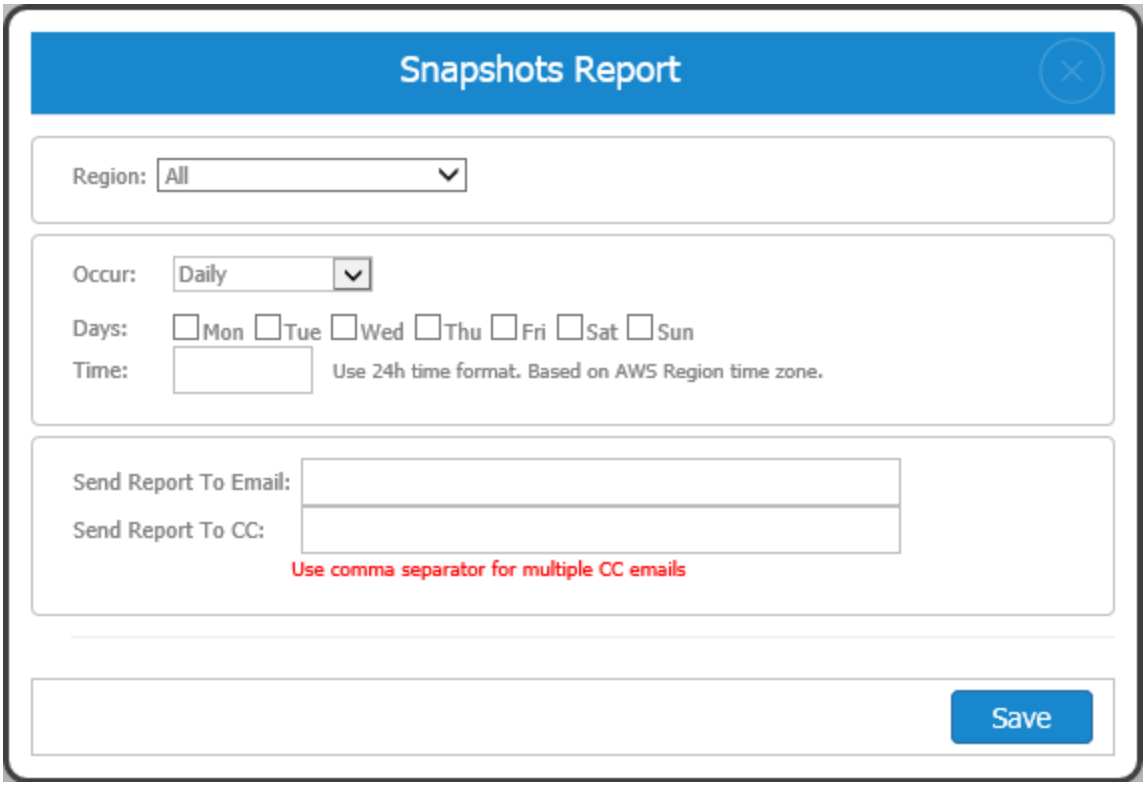
Select Region - report will be generated only based on the snapshots from selected AWS region

Occur:

Daily – daily statistics report will be send on selected days

Monthly – monthly statistics report will be send on the given day every month

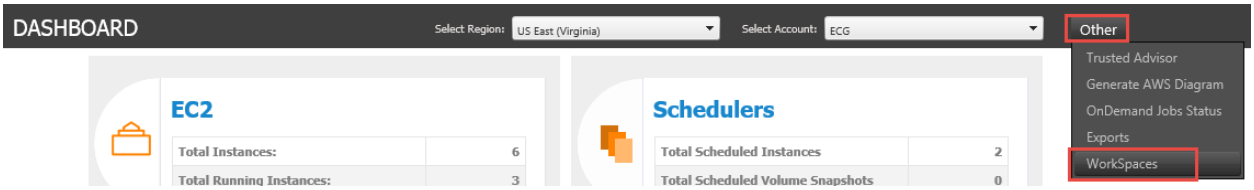
Report is sent to the user's email. Optionally, additional email(s) may also be specified. For multiple emails, use a comma separator



How to schedule reboot of WorkSpaces

Follow these steps to schedule reboot of WorkSpaces:

Go to ECG portal Dashboard.
From the menu Other (located on the right side of the navigation panel) select WorkSpaces.



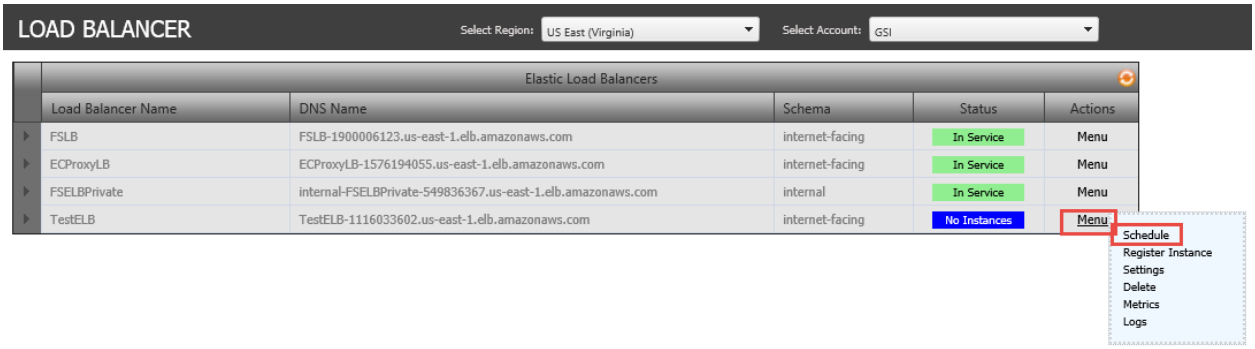
To reboot WorkSpace immediately from the menu, select Reboot.
To schedule WorkSpace reboot from the menu, select Schedule.
Configure when the reboot should occur and click Save.
To delete, edit, or suspend schedule, select appropriate action from the bottom table.

Use templates to schedule multiple WorkSpaces.
To learn more about templates go to: Introduction to Scheduler Templates

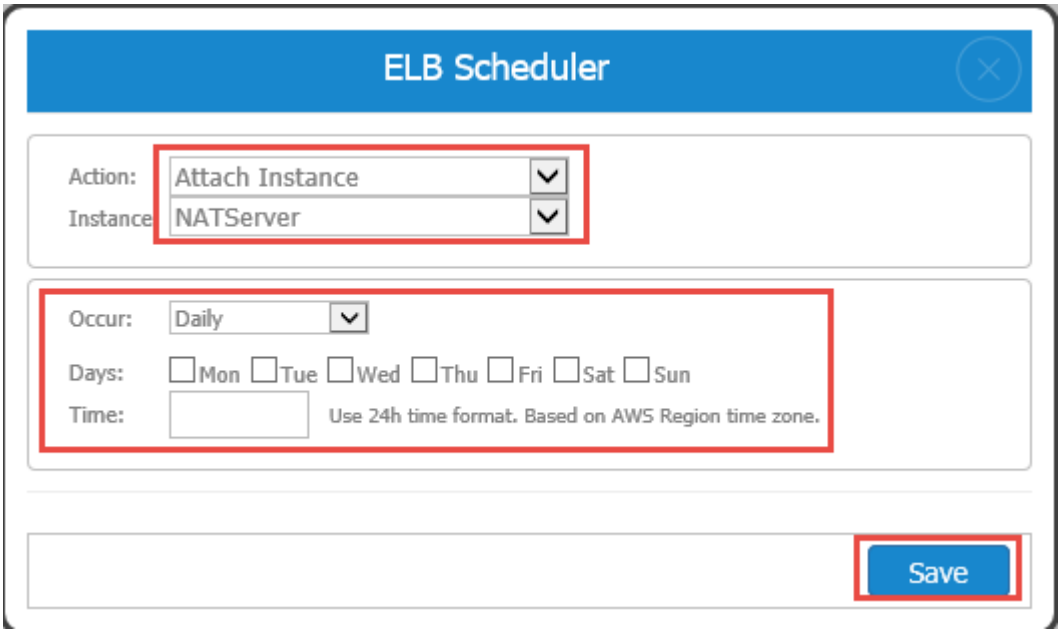
How to schedule attach/detach EC2 Instance to Elastic Load Balancer

Follow these steps to schedule Attach/Detach EC2 Instance to/from ELB:

From the Main Menu, select Elastic Load Balancer.
Under ELB table from the menu, select Schedule.



Select either Attach or Detach Instance.
From the Instance list, select EC2 instance you want to attach or detach.
Configure when the action should be executed.
Click Save.

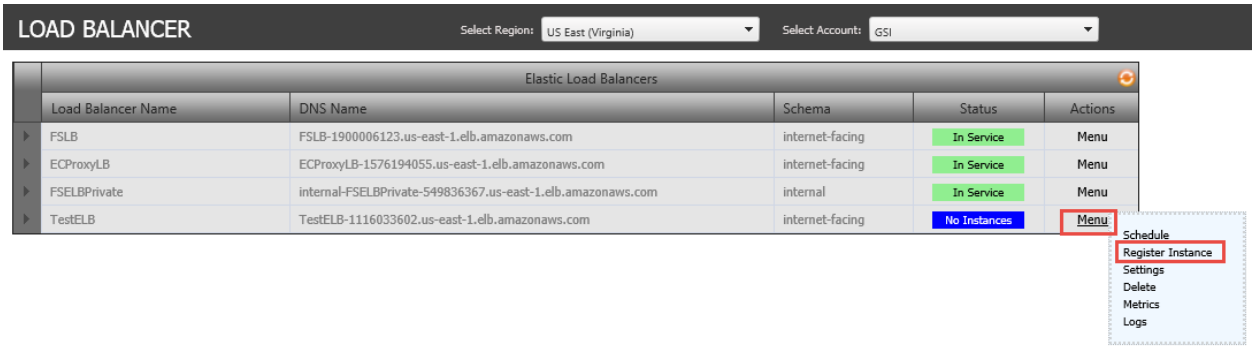


To delete, edit, or suspend schedule, select the appropriate action from the bottom table.

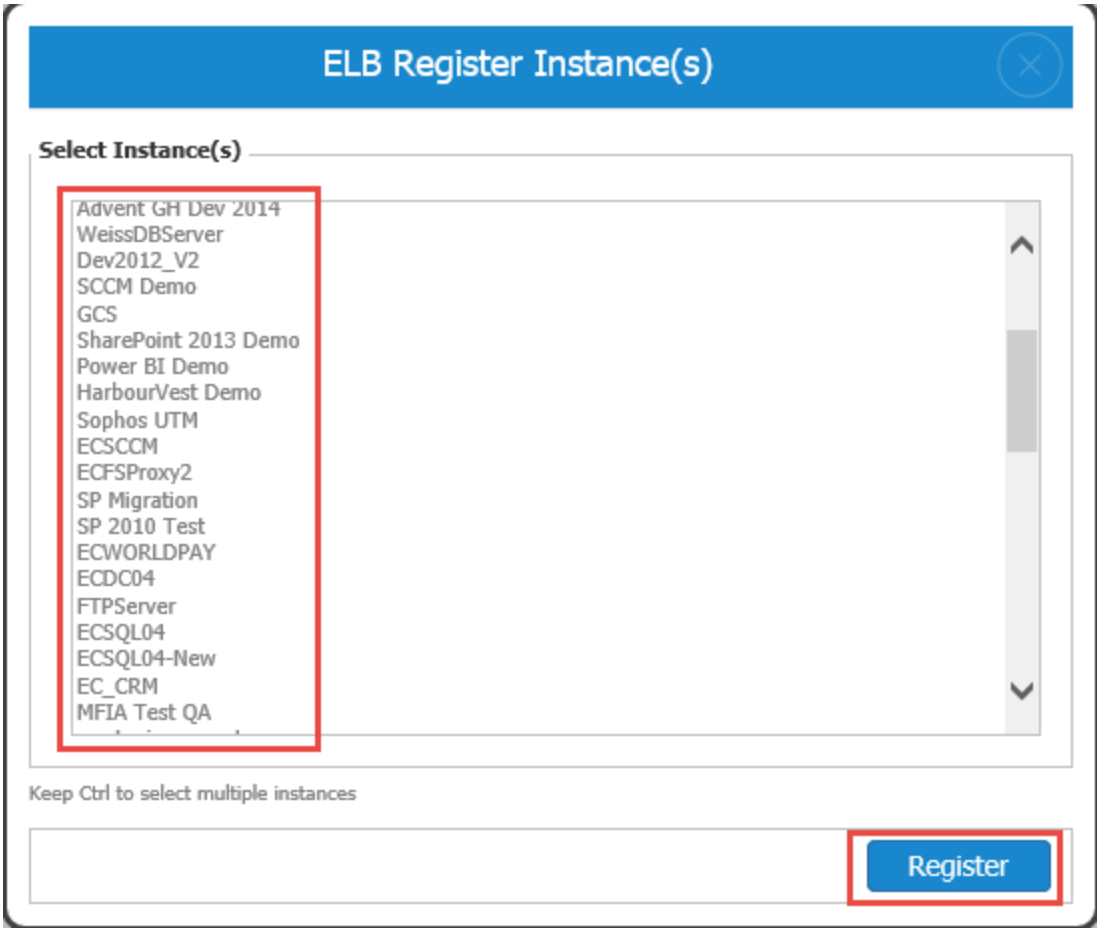
How to register new EC2 Instance under Elastic Load Balancer

Follow these steps to register EC2 Instance under ELB:

From the Main Menu, select Elastic Load Balancer.
Under the ELB table from the menu, select Register Instance.

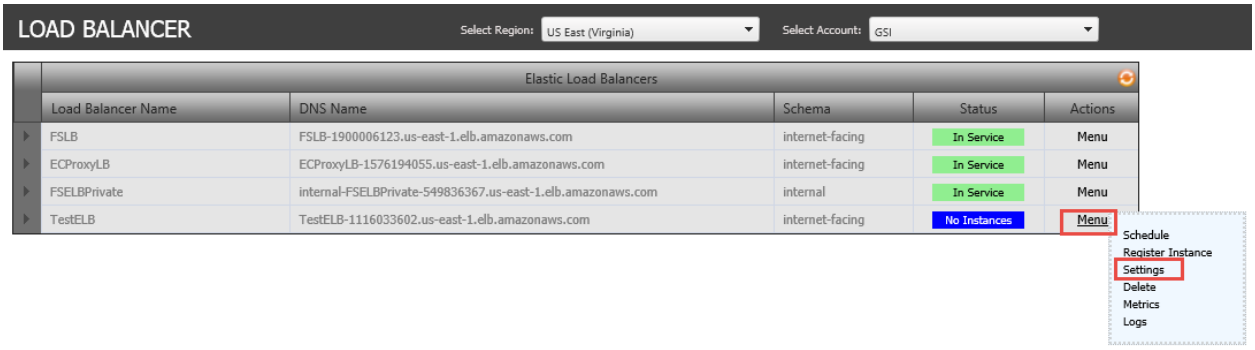


In the new window, select the Instance or multiple Instances you want to attach to the given ELB. To select multiple Instances, press and hold *Ctrl* key.
Click Register.



How to modify Elastic Load Balancer settings

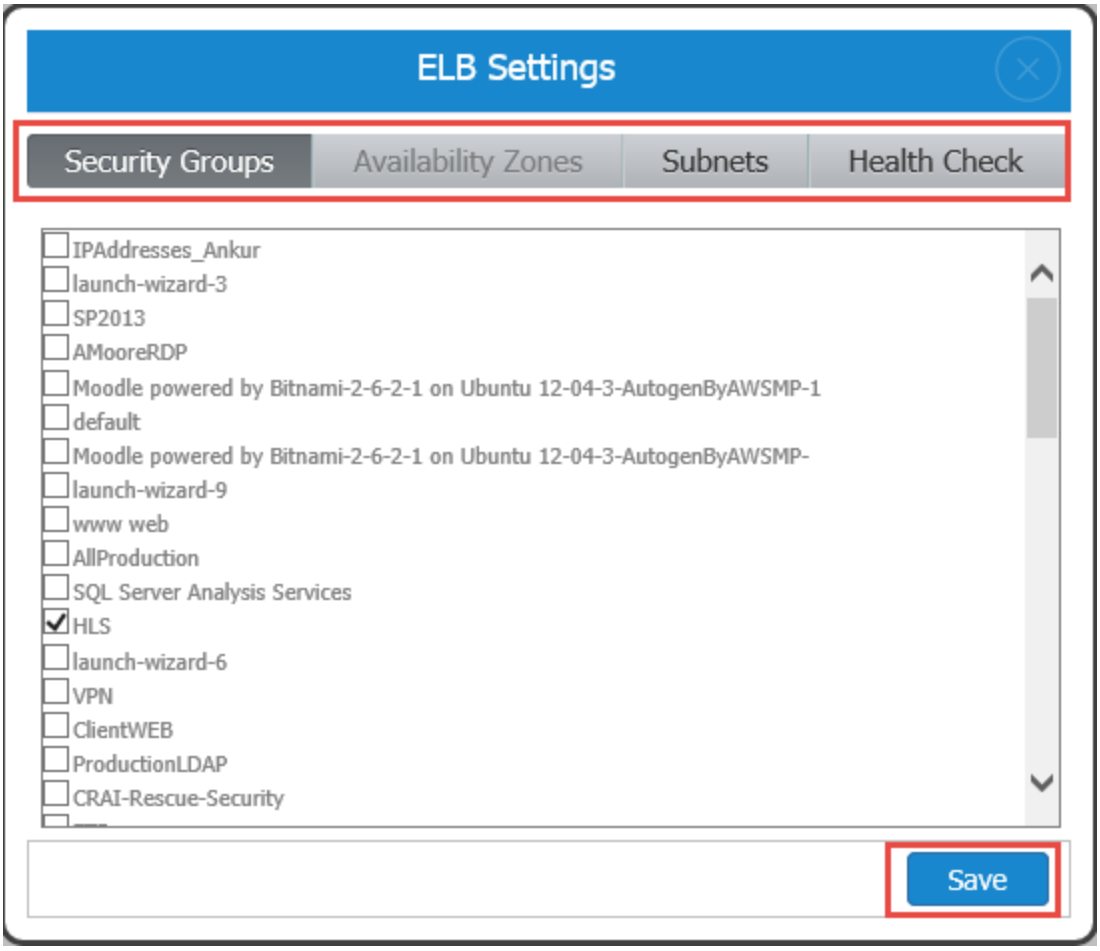
To modify setting of the existing ELB: from the Main Menu, select Elastic Load Balancer. Under the ELB table from the menu, select Settings.



The new window offers 4 tabs where you can change settings:

a. Security Groups
b. Availability Zones
c. Subnets
d. Health Check

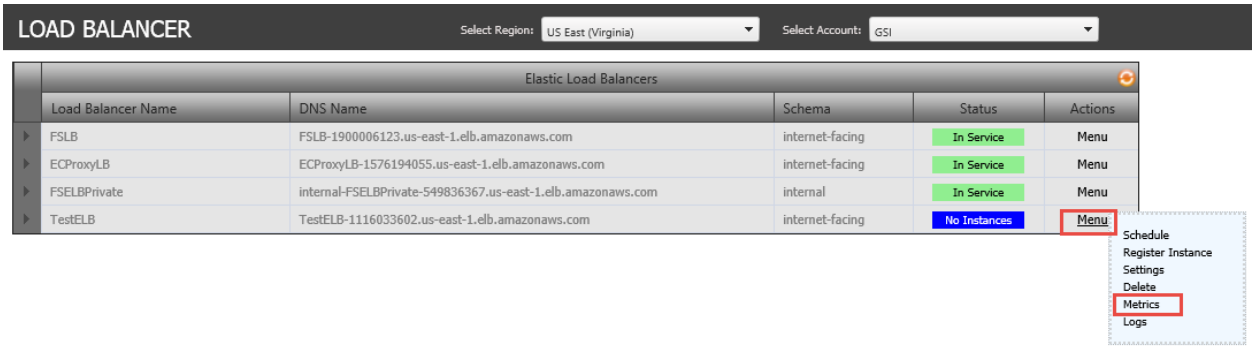
After you make all changes, click Save.



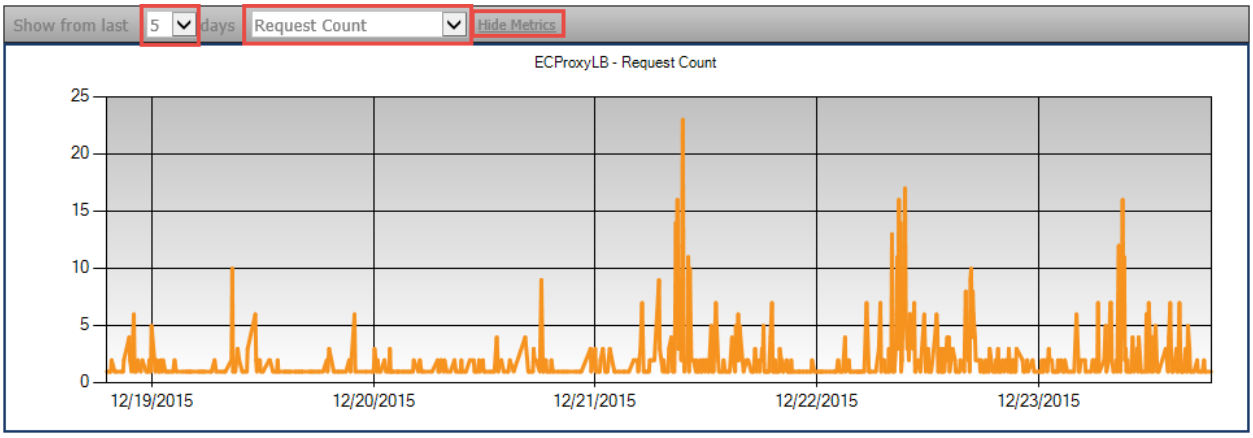
Review metrics of Elastic Load Balancer

Follow these steps to review metric or logs of ELB:

From the Main Menu, select Elastic Load Balancer.
Under the ELB table from the menu, select Metrics.



The metric chart appears under ELB table.
Under metric chart, options are available to change time range and counters
To hide the chart, click Hide Metrics.



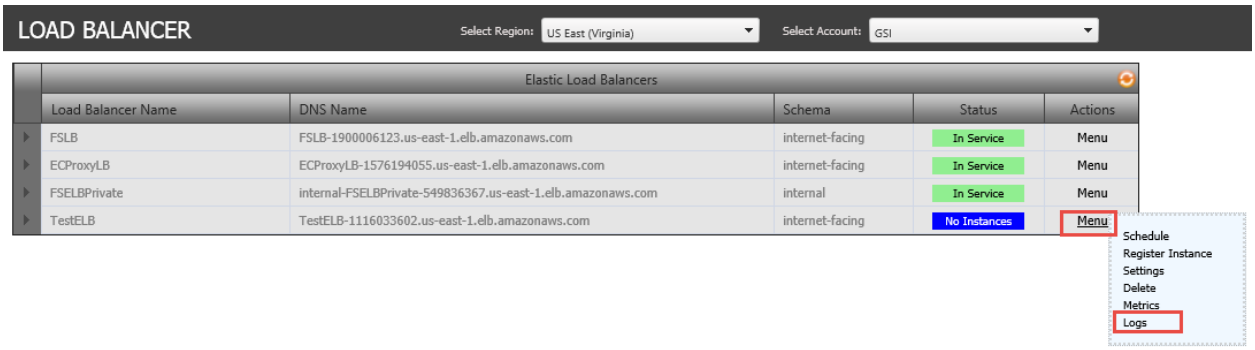
Review logs of Elastic Load Balancer

Before ELB logs can be reviewed, this feature must be turned on under Account Settings. To learn more about Account Settings go to:

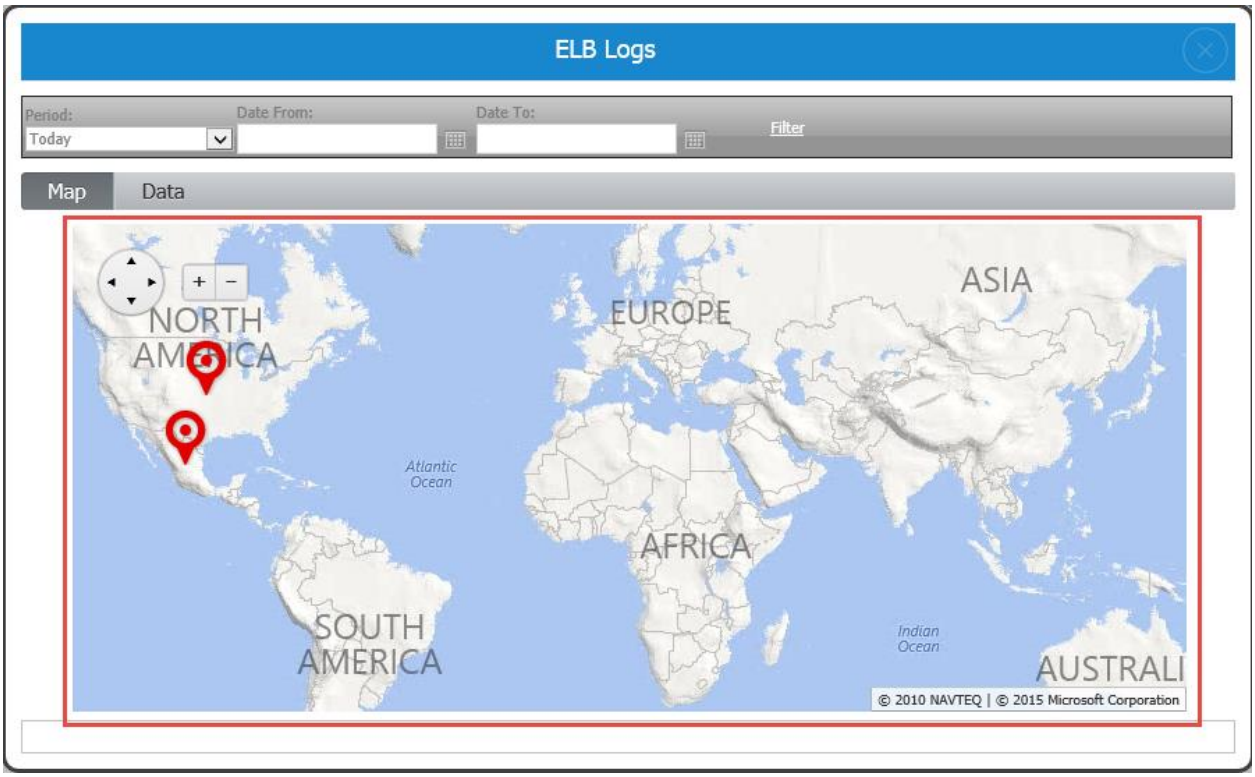
How to add or manage AWS Account

When ELB login is turned on, follow these steps to review logs:

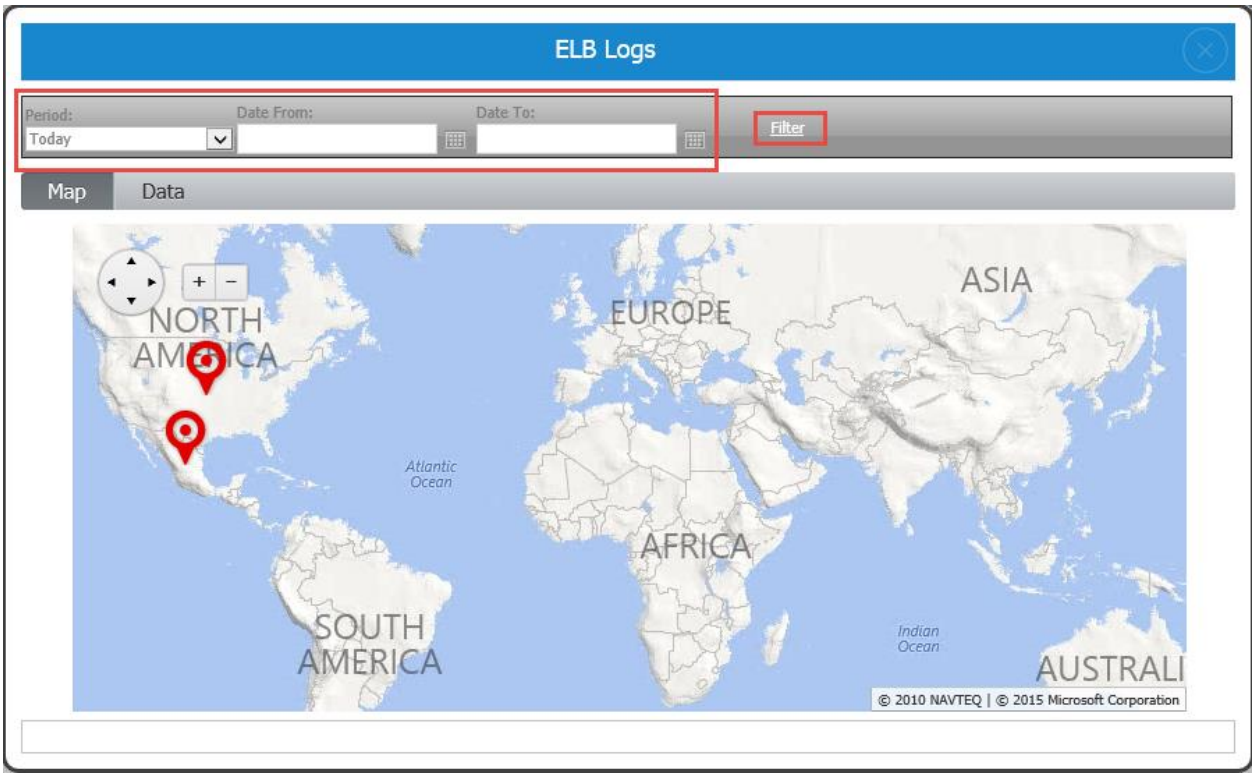
From the Main Menu, select Elastic Load Balancer.
Under the ELB table from the menu, select Logs.



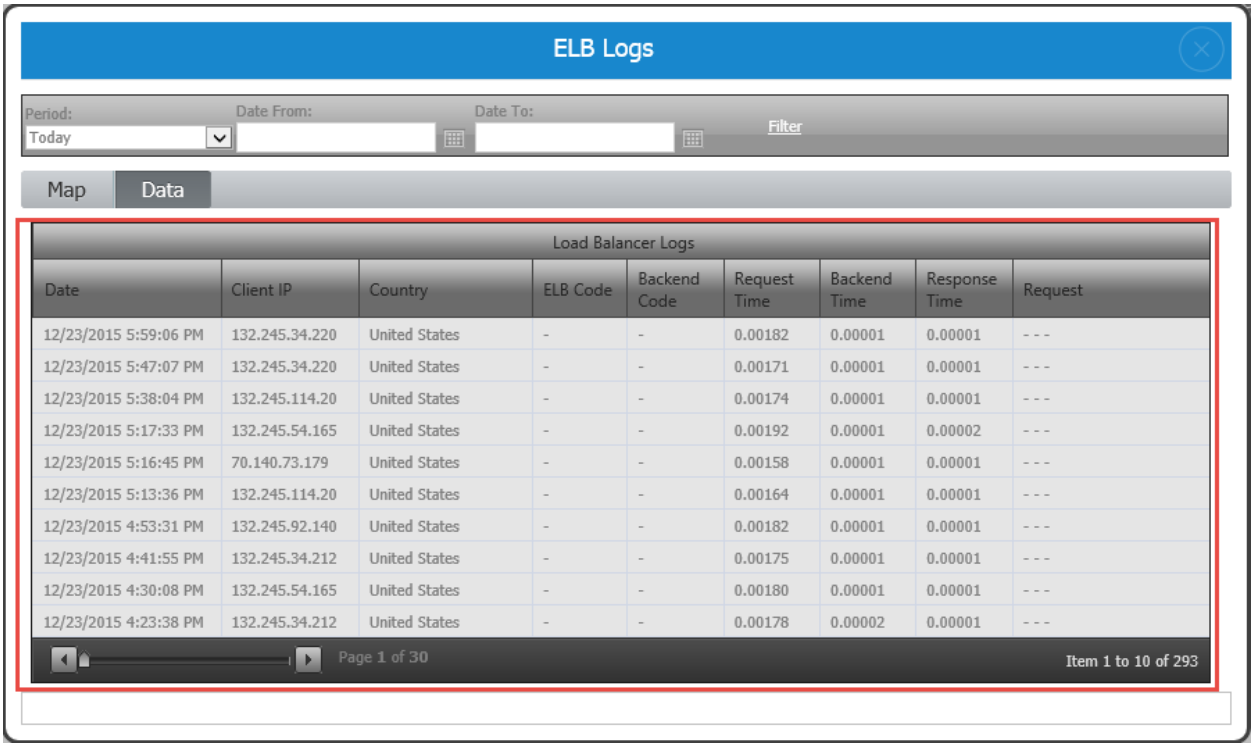
A new window shows a map with all locations that have sent traffic through ELB in the current day.



The range of days to view data can be changed using the filter located in the top panel. After setting days range, click Filter to apply changes.



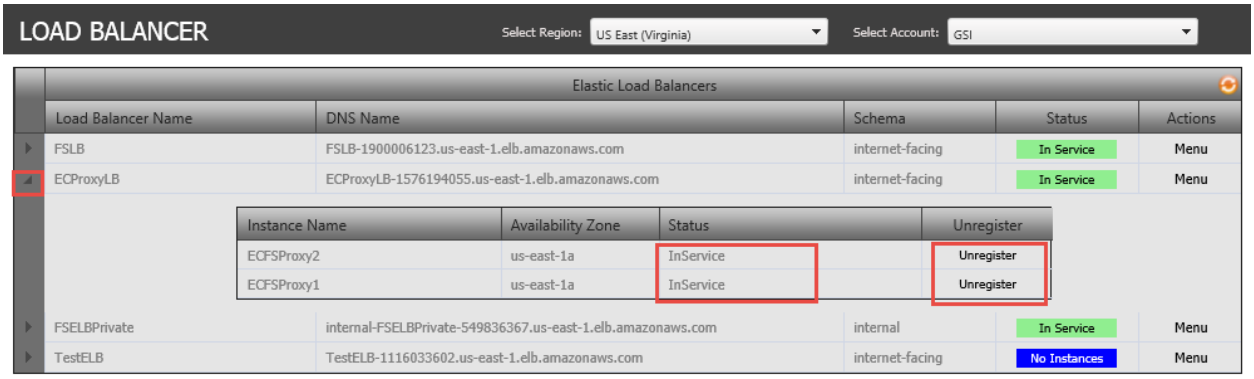
To review detailed data about requests, switch to the Data tab.



How to verify status or unregister EC2 Instance from Elastic Load Balancer

Follow these steps to verify status of registered EC2 Instances:

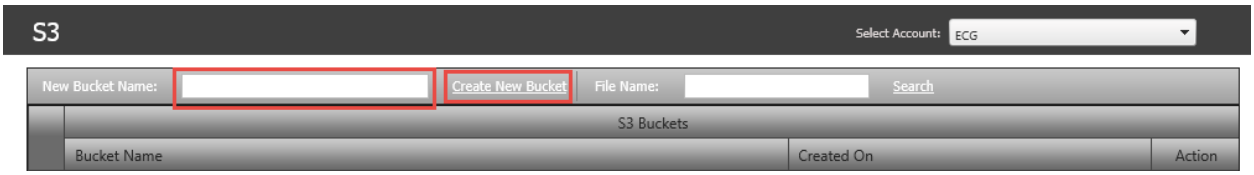
From the Main Menu, select Elastic Load Balancer.
Click the black arrow on the left to expand EC2 Instances.
A list of all Instances registered under the given ELB is shown. The status of each Instance is displayed in the Status column.
To unregister an Instance from ELB, click Unregister.



How to create new S3 Buckets

Follow these steps to create a new S3 bucket:

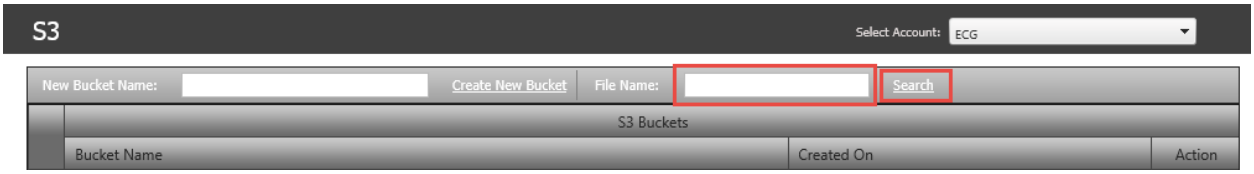
From the Main Menu, select S3.
Under the S3 section, in the top panel enter new bucket name.
Click Create New Bucket.



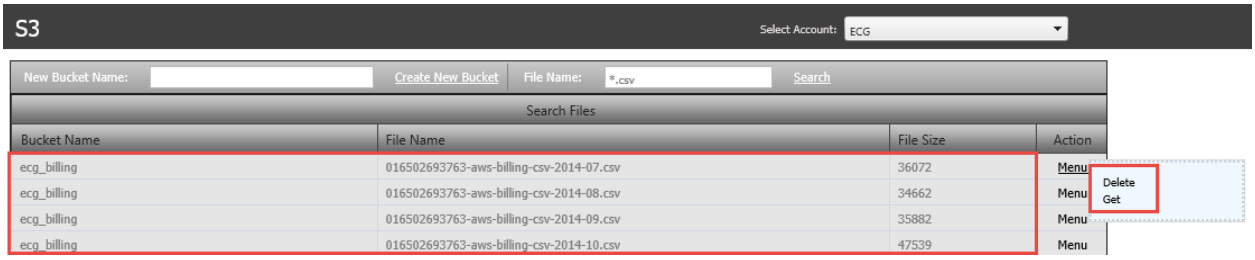
How to search files across all your S3 Buckets

Follow these steps to search file(s) across all S3 buckets:

From the Main Menu, select S3.
Under the S3 section, in the File Name box in the top panel, enter file you are looking for. You can enter the full name of the file or you can use * to enter pattern, e.g. *.csv will search all files with extension csv.
Click Search.

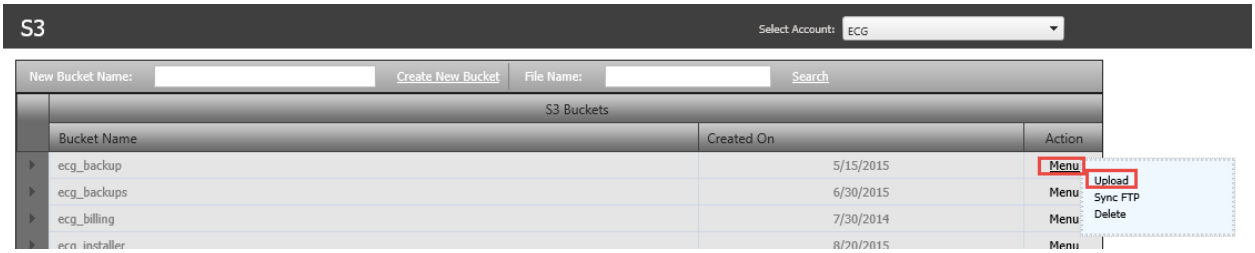


The new panel shows up within the search result.
Files can be downloaded or deleted from the menu.

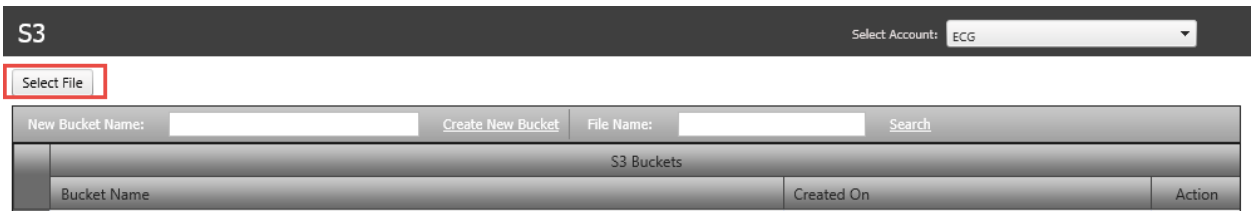


Upload and download file from S3 Bucket

To upload file to S3 bucket, go to the S3 section by clicking S3 from the Main Menu.
From the S3 bucket menu, select which file you want to upload, then click Upload.

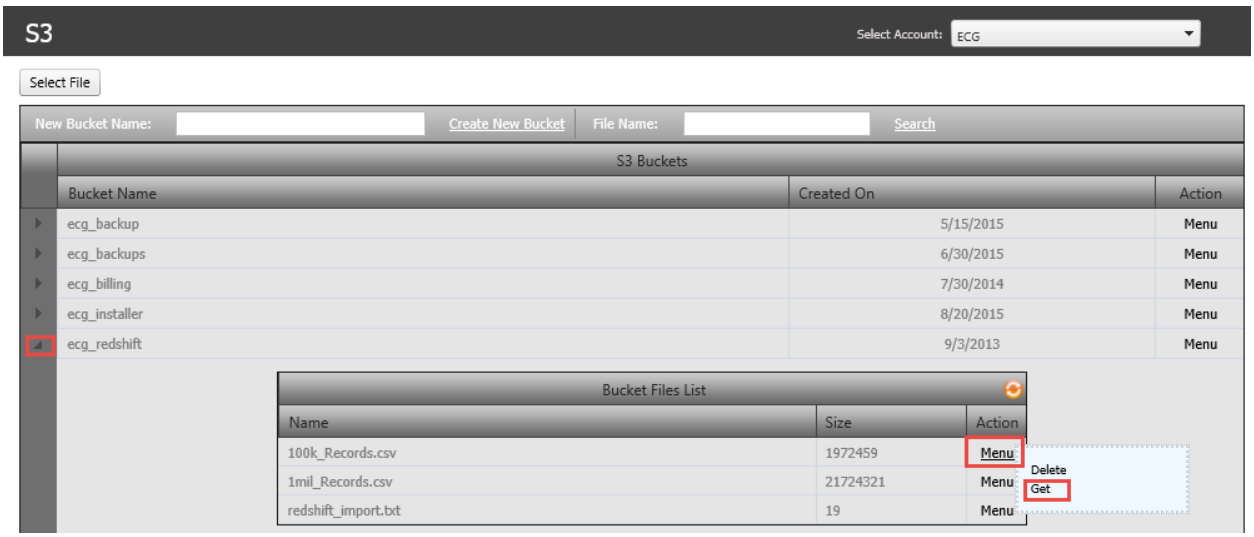


A new Select File button appears at the top of the page.
Click Select File and select the file you want to upload.
The selected file uploads to the S3 bucket



Follow these steps to download file from S3 bucket:

Click the black arrow on the left to expand files under S3 bucket.
Locate the file you want to download.
From the menu, select Get.

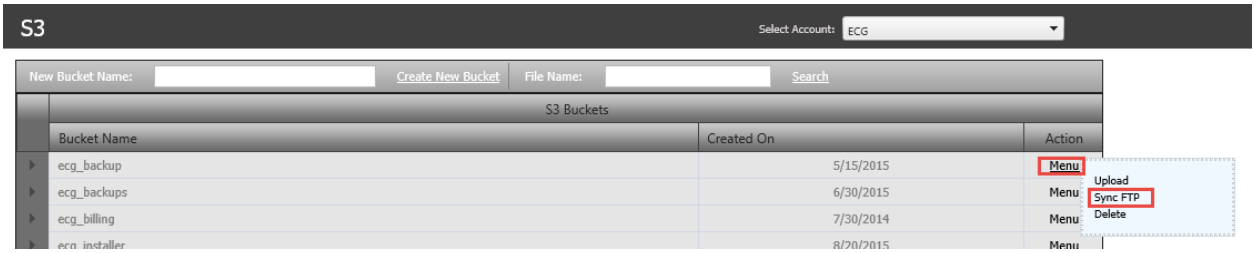


Under the same menu, you will see the option Delete, which allows a given file to be deleted from S3 bucket.

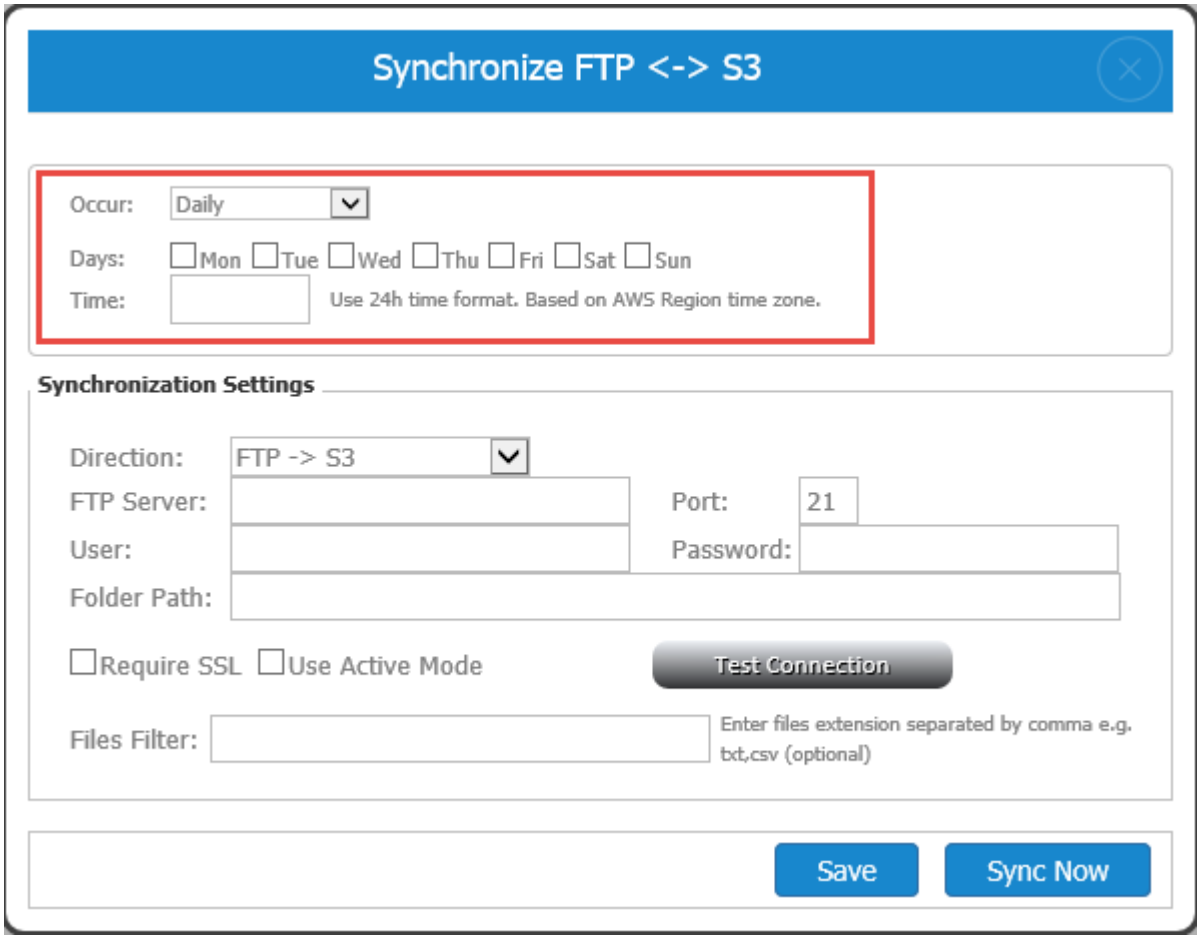
How to synchronize files between S3 Bucket and FTP Server

Follow these steps to synchronize files between S3 bucket and FTP server:

From the Main Menu, select S3.
Under S3 bucket, choose Sync FTP from the menu.

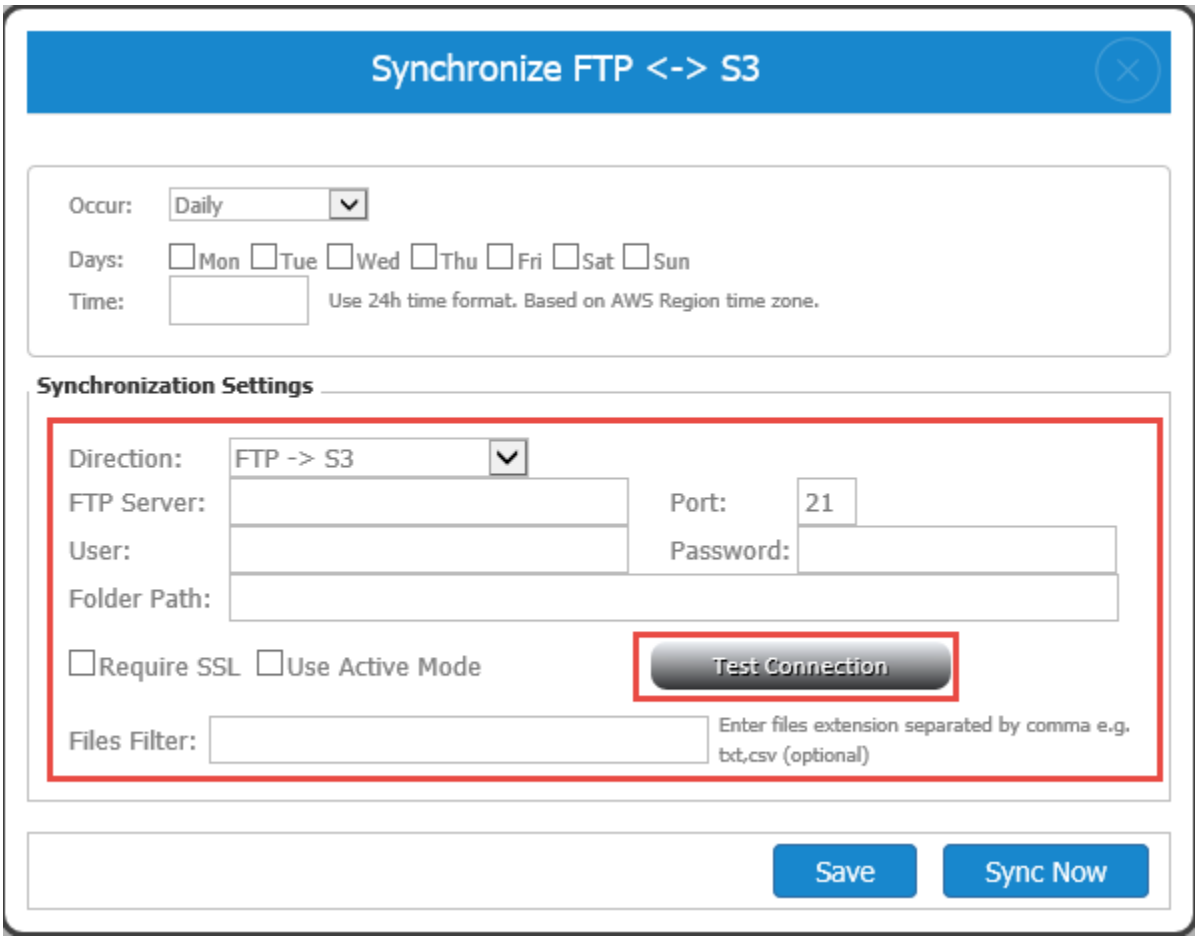


In the top part of the new window, select when synchronization should occur. You can skip this step to start synchronization immediately.

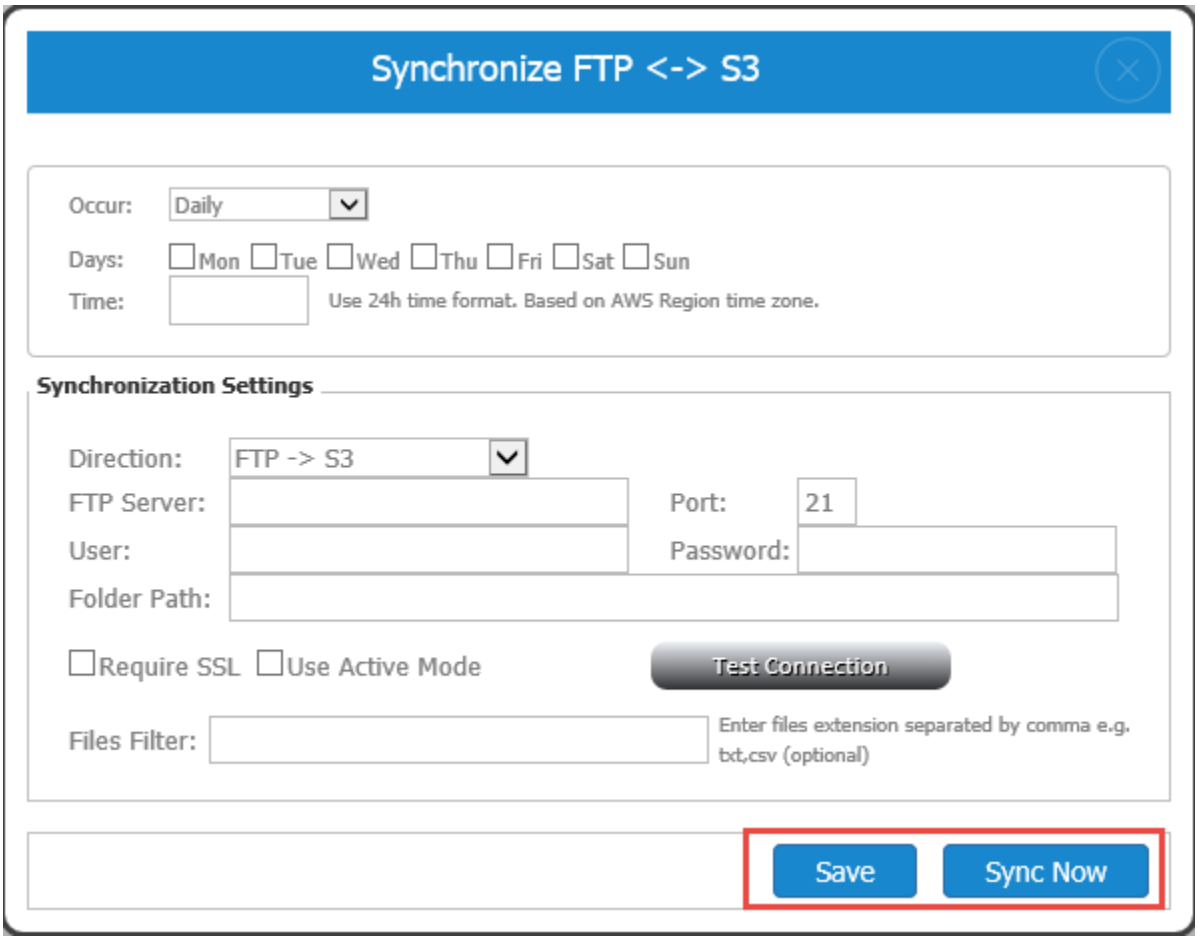


In the bottom part of the new window, configure synchronization:

a. Direction – Choose to sync FTP with S3, or S3 with FTP
b. Enter FTP server connection information
c. To test connection to FTP, click Test Connection
d. Files Filter – Specify extension of the files you want to synchronize



Click Save to save scheduler, or click Sync Now to start synchronization without scheduling.

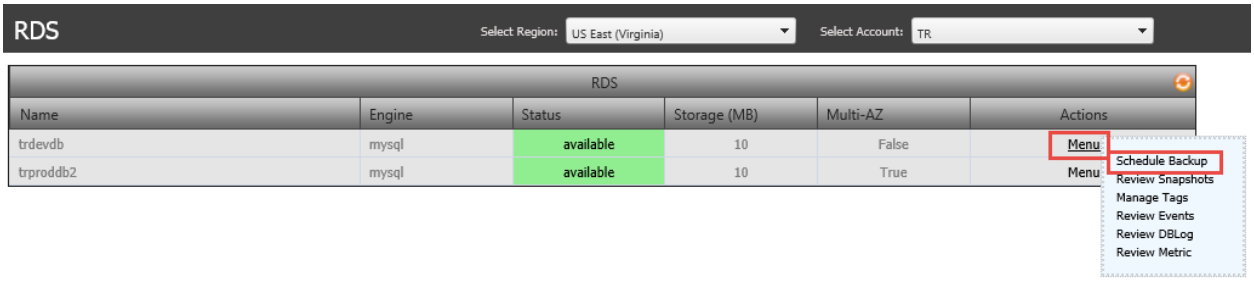


Note: maximum size of a single file cannot exceed 50MB. All files larger than 50MB are skipped in the synchronization process.

How to schedule and maintain RDS backups

Follow these steps to schedule RDS backup:

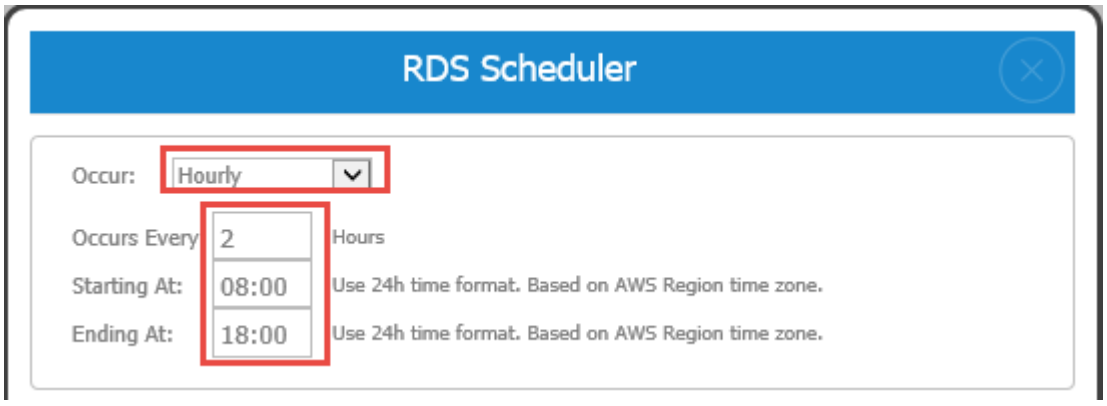
To go to RDS section, select RDS from the Main Menu.
Under RDS table menu, select Schedule Backup.



In the upper section of the RDS Scheduler, choose how frequently you want to create DB Snapshot.

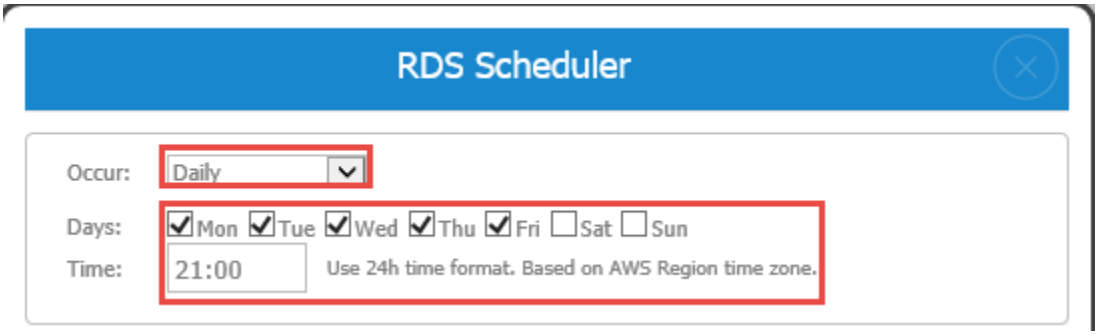
Occurrence:

Hourly – The snapshot is taken every given number of hours. Additionally, you can specify start and end time, e.g. to take a snapshot every 2 hours between 8AM and 7PM, this is how your setup looks:

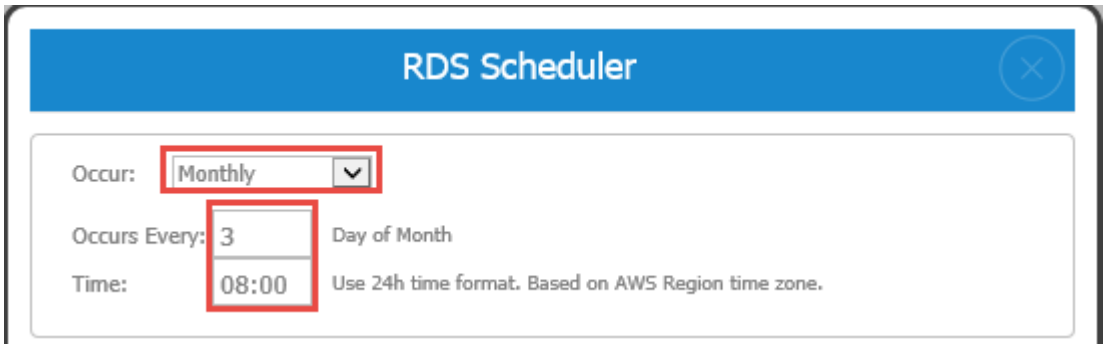


If start and end time are skipped, the snapshot will be taken every given number of hours around the clock.

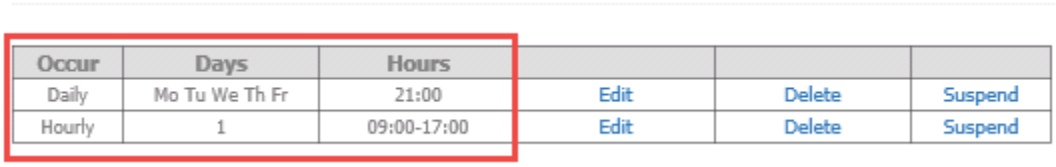
Daily – DB Snapshot is taken every selected day and time, e.g to take a snapshot every Monday, Wednesday, and Friday at 9PM, this is how your setup looks:



Monthly – DB Snapshot is taken every given day of the month at a given time, e.g. to take a snapshot every 3rd day of the month at 8AM, this is how your setup looks:



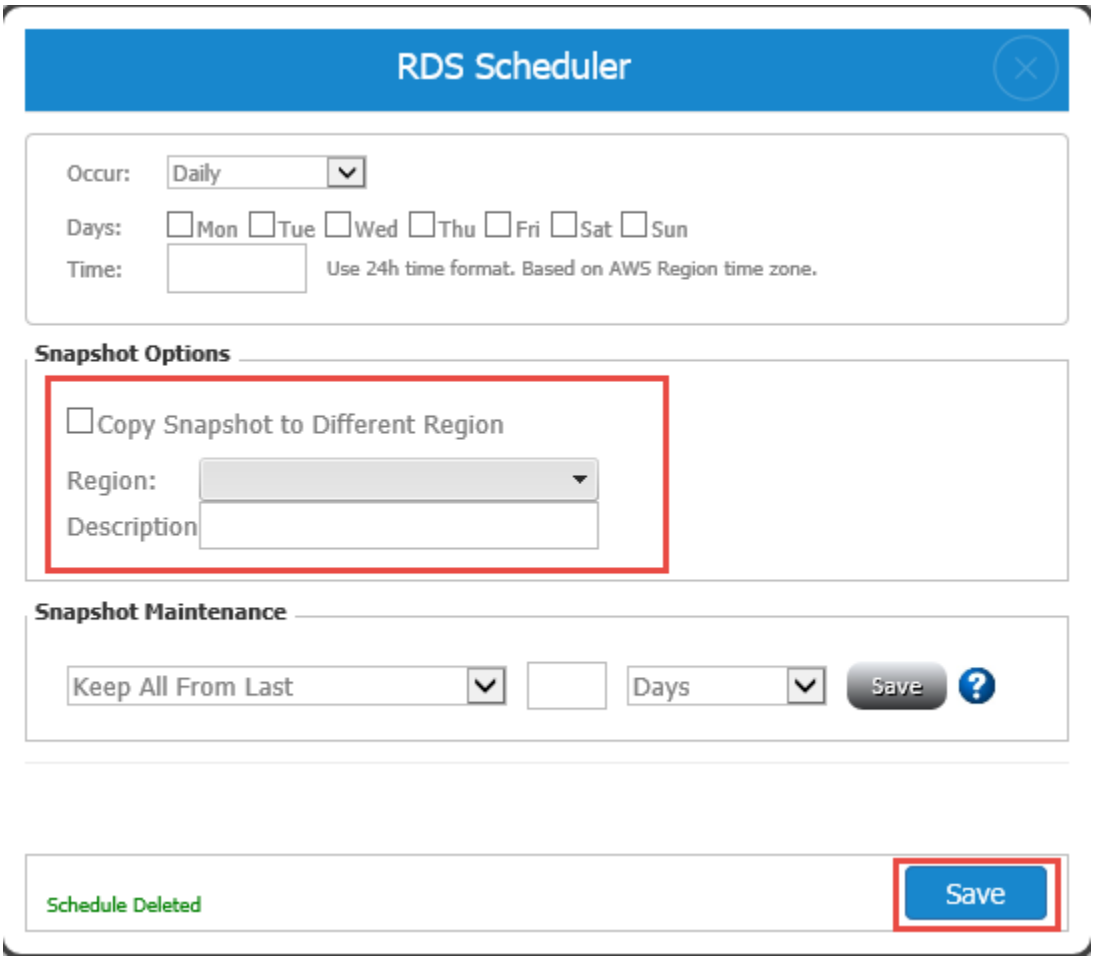
You can setup multiple schedulers for the same RDS Instance and mix different frequencies if necessary. For example, to take a snapshot every hour from 9AM to 5PM and another one daily at 11PM, this is how your setup looks:



Occur	Days	Hours			
Daily	Mo Tu We Th Fr	21:00	Edit	Delete	Suspend
Hourly	1	09:00-17:00	Edit	Delete	Suspend

In the next section, optional settings can be configured:
Description – DB snapshot description
Copy Snapshot to Different Region – when checked, this option copies the new DB Snapshot to the selected AWS region. You can select multiple destination regions. DB Snapshot is copied to all AWS regions simultaneously.

Click Save.



You can edit, delete, or suspend scheduler by clicking appropriate action in the scheduler table.

Occur	Days	Hours			
Daily	Mo Tu We Th Fr	23:00	Edit	Delete	Suspend
Hourly	1	09:00-17:00	Edit	Delete	Suspend

Schedule Maintenance (retention period) of the old DB Snapshots:

Amazon AWS allows only 50 manual snapshots to be kept: the error “cannot create more than 50 manual snapshots,” may appear following extended scheduler use. Schedule retention of old DB Snapshots to prevent this:

Two options define which DB Snapshots are not deleted:
Keep All From Last – Keeps all DB Snapshots created within the last x periods (select period as hours, days, weeks, months, or years), e.g. to keep all DN Snapshots created within the last 45 days, this is how your setup looks:

Keep One Per Period From Last – Keeps the DB Snapshots created last in the given period (hours, days, weeks, months, or years), e.g. to keep one DB Snapshot per week from the last 8 weeks, this is how your setup looks:

After configuring maintenance criteria, click Save.

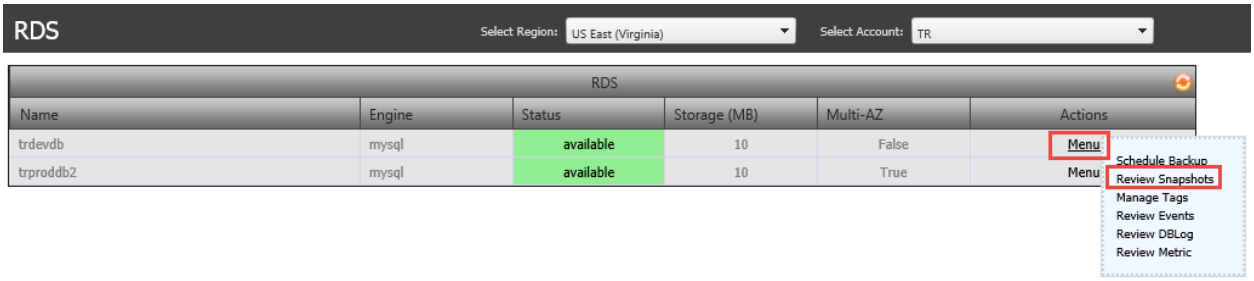
The maintenance process runs once per day.
All DB Snapshots that do not match the scheduler are deleted.

Create multiple schedules to setup an advanced maintenance plan for RDS. For example, to setup maintenance to keep all DB Snapshots from the last 7 days, 1 DB Snapshot per week from the last 4 weeks, and 1 DB Snapshot per month from the last 4 months, this is how your setup looks:

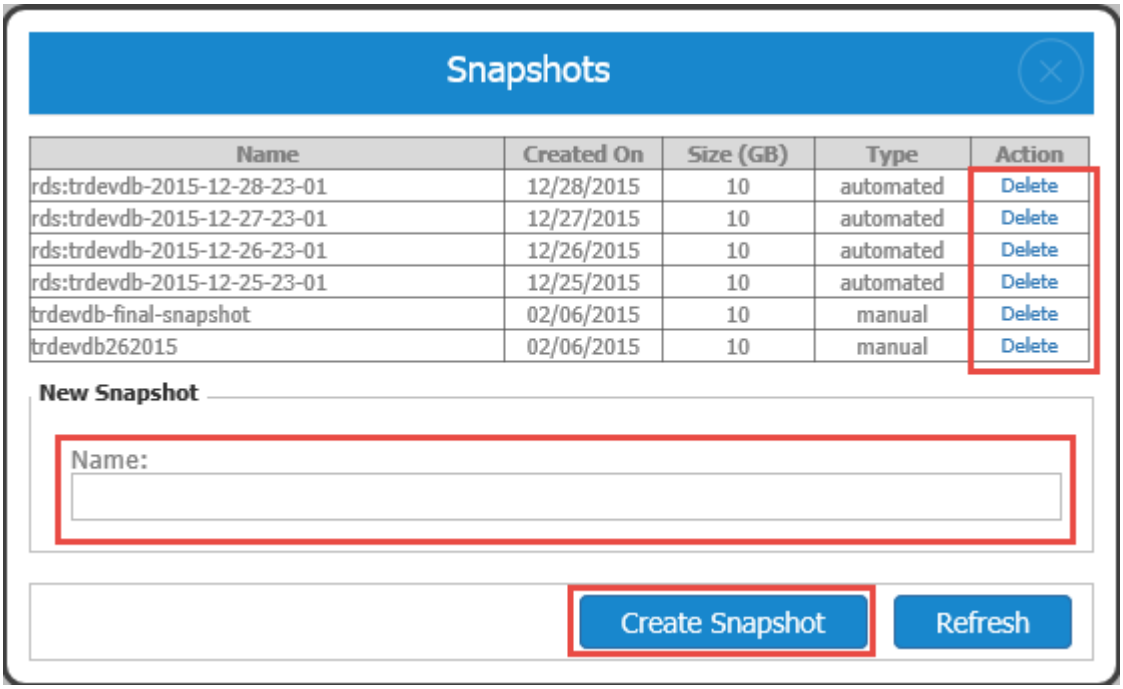
Type	Value	Period		
Keep All From Last	7	Days	Edit	Delete
Keep One Per Period For Last	4	Weeks	Edit	Delete
Keep One Per Period For Last	4	Months	Edit	Delete

How to review, create or delete RDS snapshots

From the Main Menu, select RDS.
On the list, locate RDS to review and from the menu select Review Snapshots.



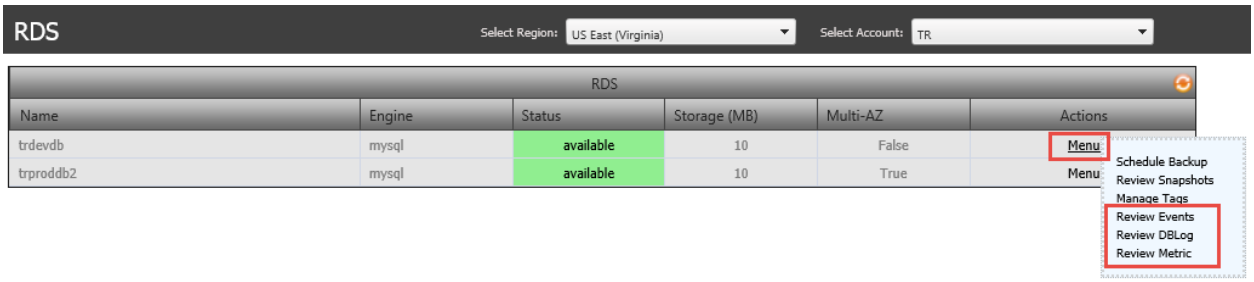
The list of all snapshots created from the given RDS is visible in the new window.
To delete snapshot, click Delete in Action colum.
To create a new snapshot, enter snapshot name and click Create Snapshot.



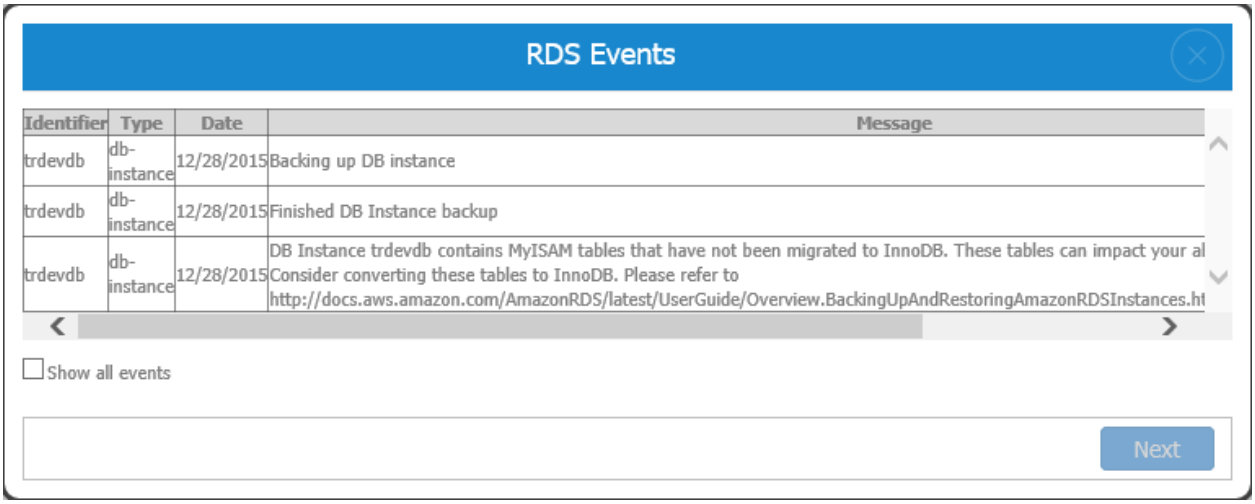
Review events, logs, and metrics of RDS

To review events, logs, or metrics of RDS, go to the RDS section and from the menu select (respectively):

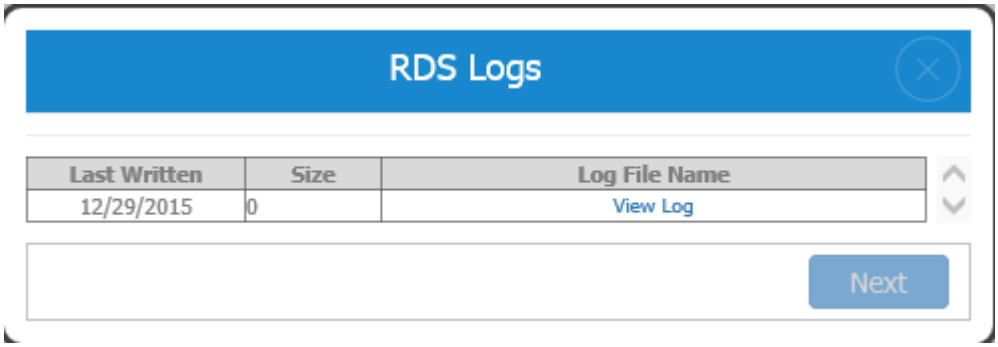
- Review Events
- Review DBLog
- Review Metric



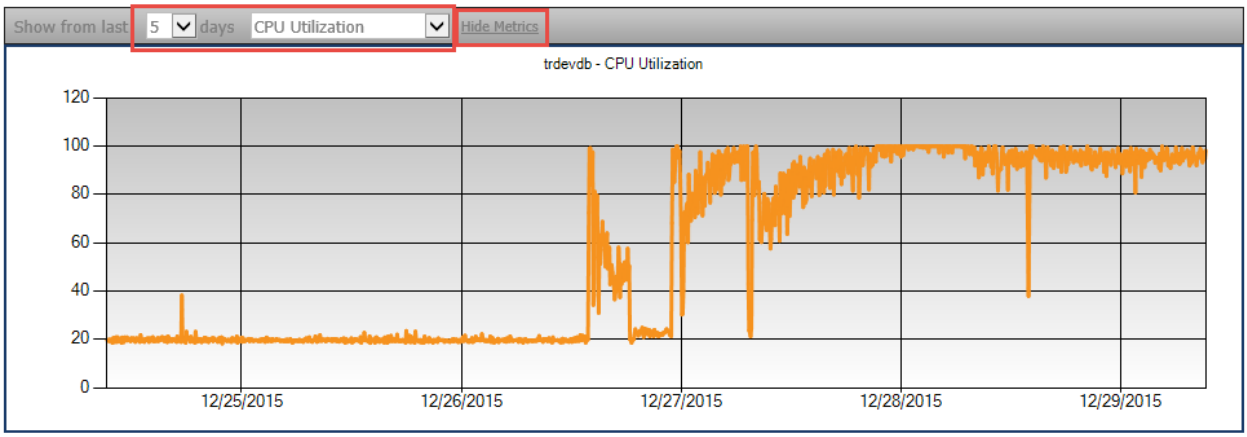
RDS Events



RDS Logs

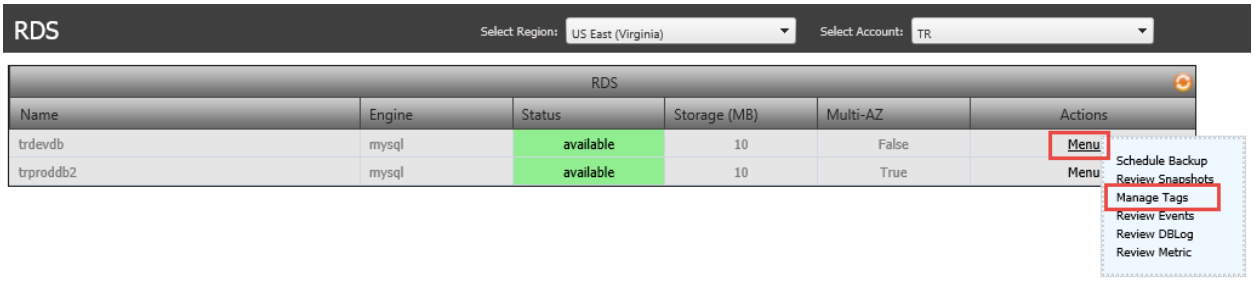


RDS Metrics

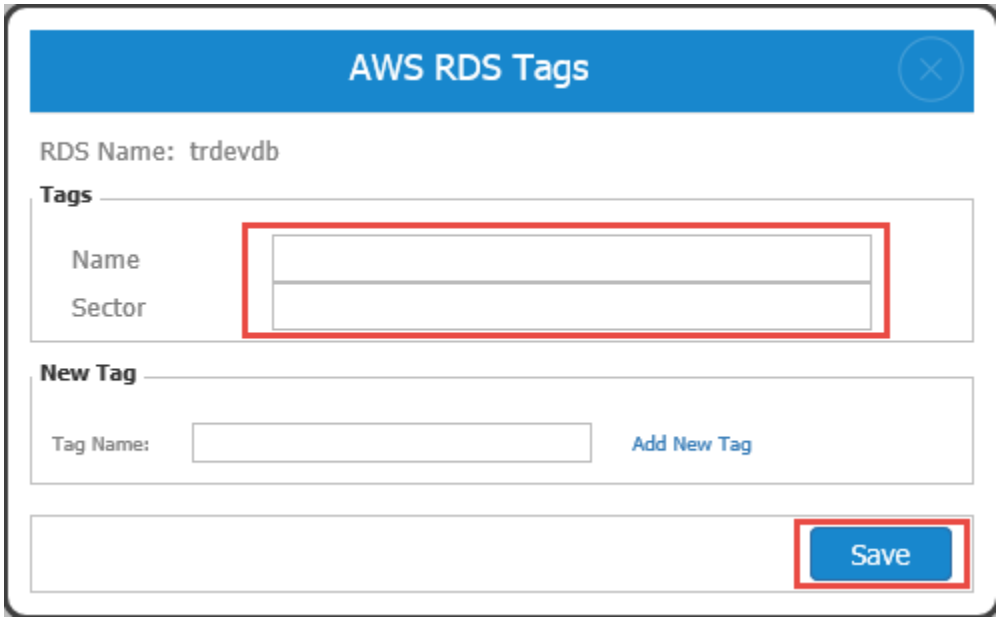


How to add or modify RDS tags

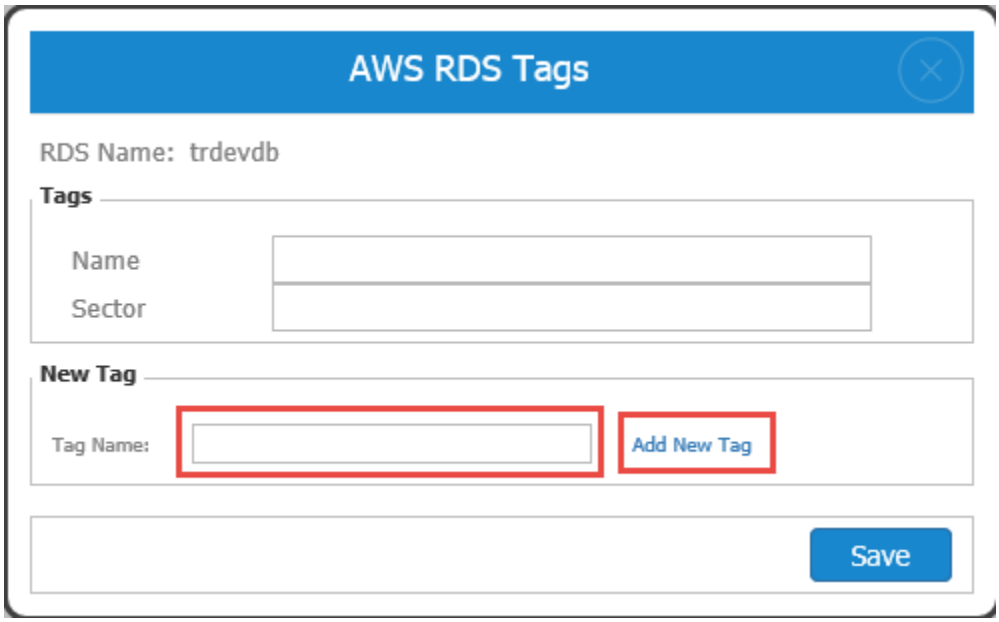
To manage RDS tags, go to the RDS section and from the menu select Manage Tags.



To change value of existing tag, enter new value in the text box after tag name and click Save.



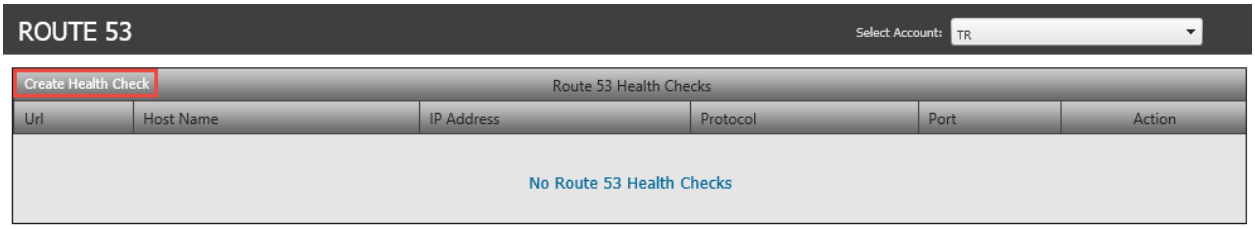
To add new tag, enter tag name and click Add New Tag.
The new tag will show up in the tags list where you can enter the new value.



How to create Route 53 Health Check

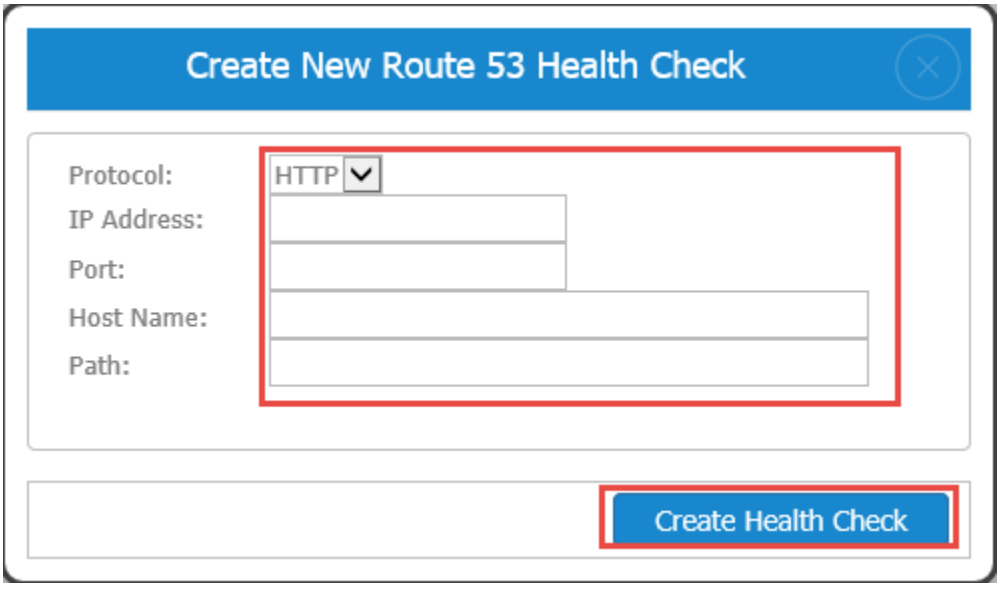
Follow these steps to create Route 53 Health Check:

From the Main Menu, select Route 53
On the top panel, click Create Health Check

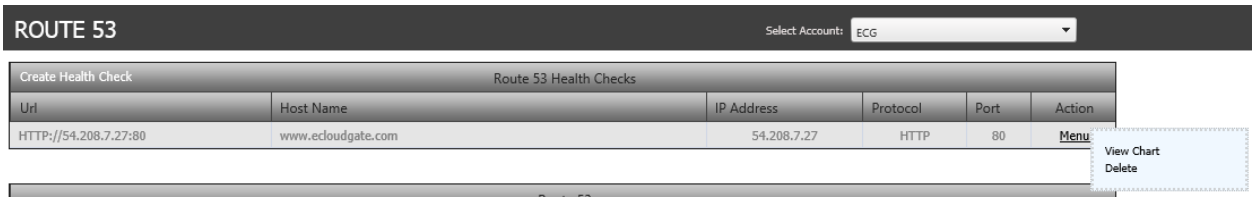


Configure Health Check:

a. Protocol – The internet protocol used to communicate with your server. You can select either HTTP or TCP
b. IP Address – IP address of the server to check
c. Port – The port the health check tries to communicate with server
d. Path – Optional value represents the part of URL after IP e.g. /Server/index.html



Click Create Health Check.

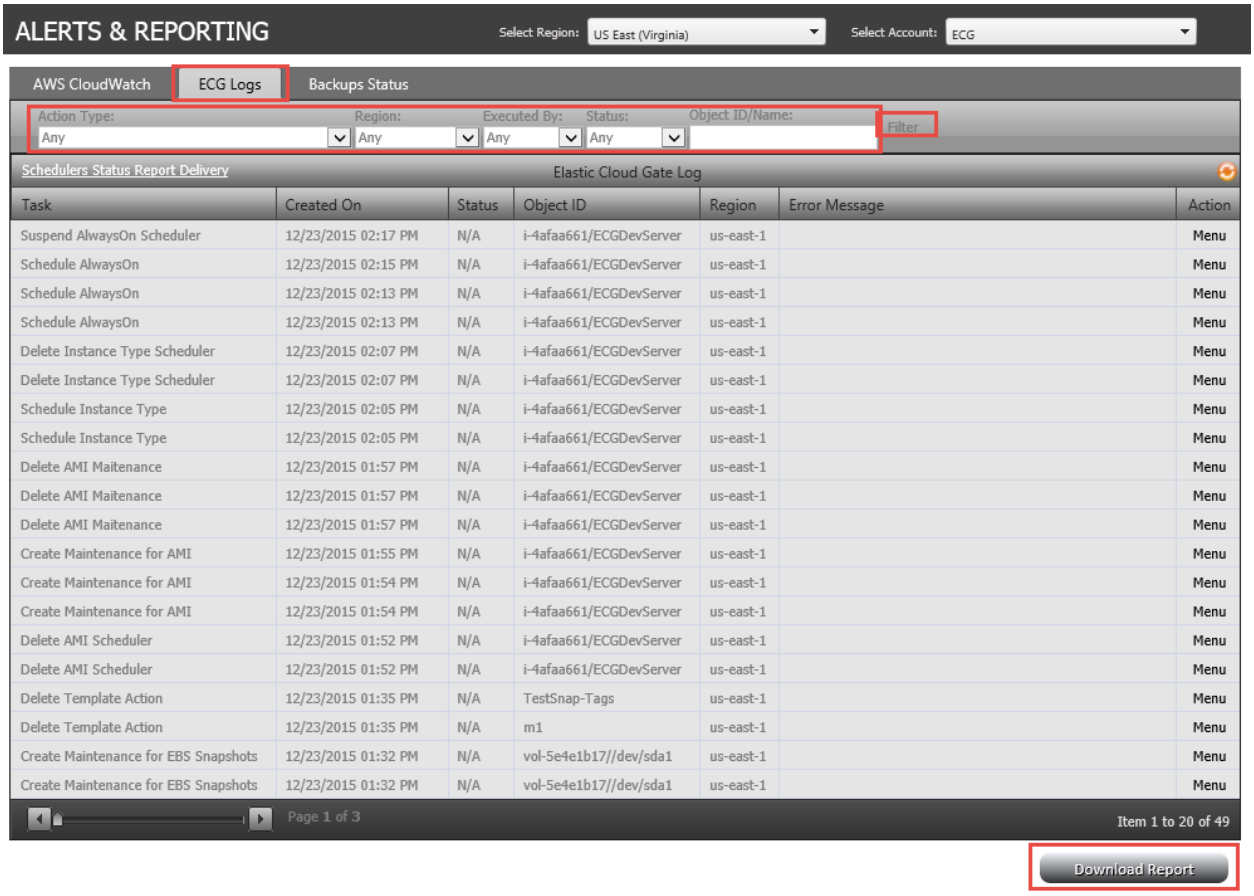


ECG Logs – review and schedule report delivery via email

ECG Logs give an overview of all actions taken on ECG portal (e.g. create or delete schedule, review the log of executions of schedulers, etc.).

To review ECG Logs from the Main Menu, select Alerts & Reports.
Under Alert & Report section, switch to the ECG Logs tab.

To filter log, select filter options and click Filter.

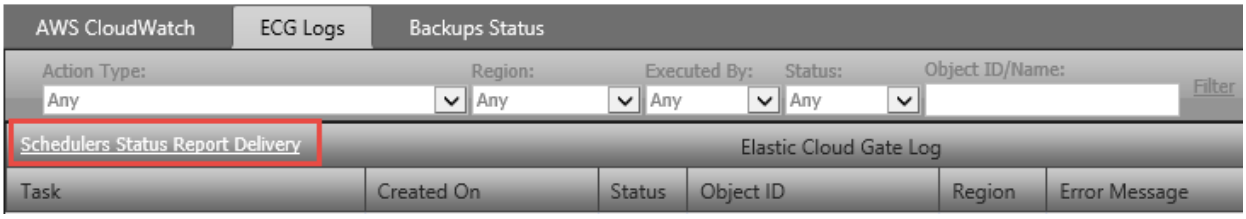


To download Log report, click Download Report.

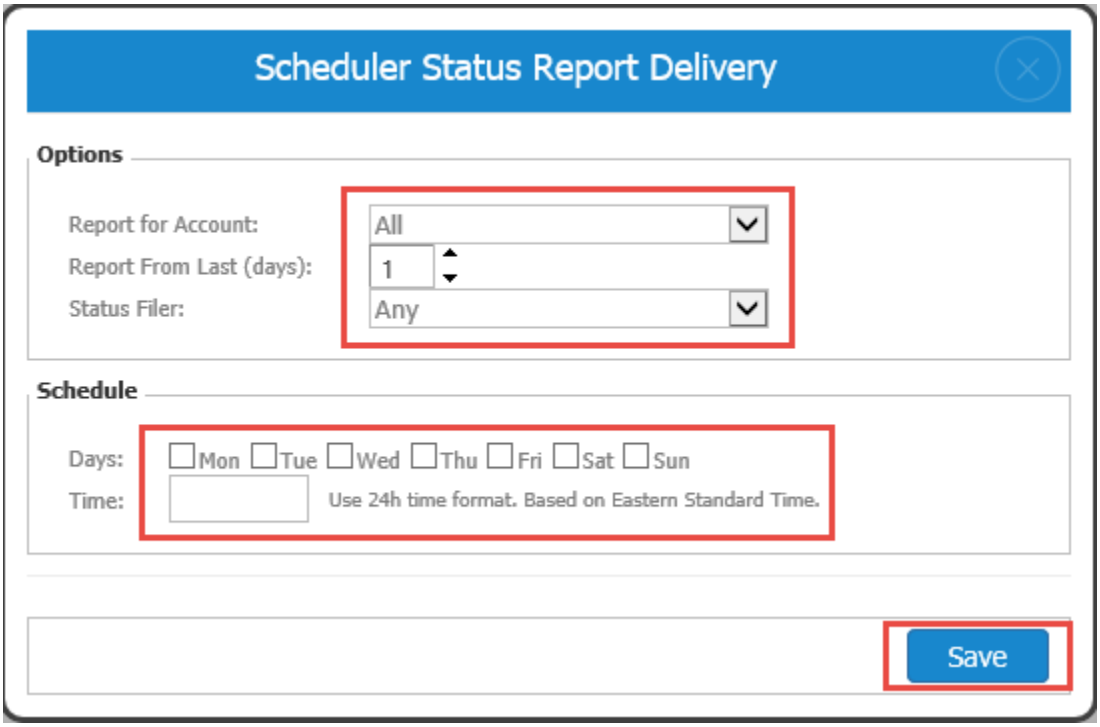
Additionally, you can schedule the Schedulers' status report for delivery via email on a regular basis.

To schedule delivery report from the top panel:

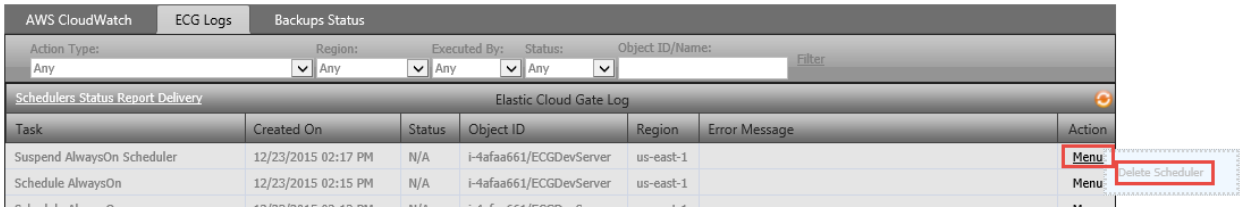
Click Schedulers Status Report Delivery.



Under Report for Account, select account or leave All to get report for all accounts.
Select how many last days should be included in report.
You can filter execution on report by status by selecting Success or Failed from the status filter list, or leave Any to include all executions.
Enter day(s) and time you want the report sent.
Click Save.

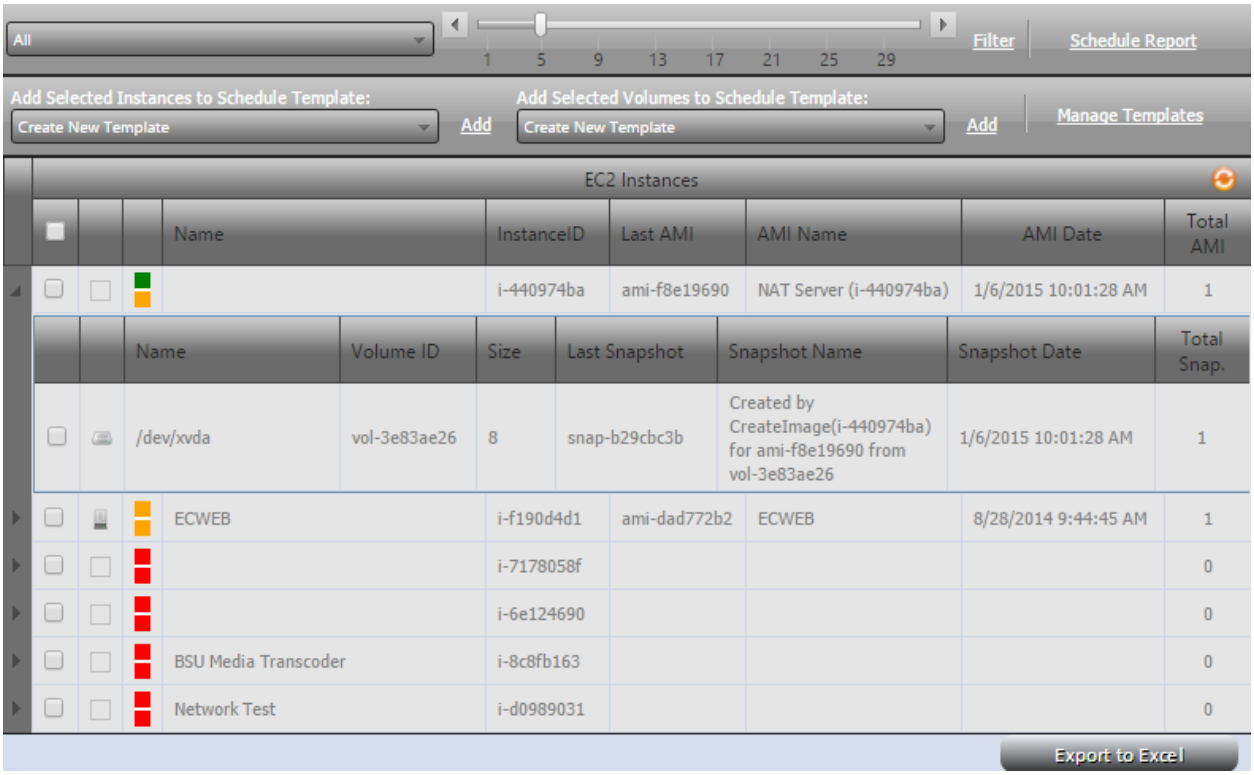


To delete scheduler for an object that does not exist anymore, find the execution information on the list and from the menu select Delete Scheduler.



Review backup status

Backup Status report is designed to provide detailed overview of the status EC2 (AMI) and EBS (Snapshots) backups. To open Backup Status report from the Main Menu, select Alerts & Report; when the page opens, switch to Backup Status tab.



Information available in the report:

EC2 Instance:

- Instance ID
- Instance Name
- Last AMI ID
- Last AMI Name
- Last AMI Date
- Total AMIs

EBS Volume:

- Volume ID
- Volume Name or device mapping
- Last Snapshot ID
- Last Snapshot Name
- Last Snapshot Date
- Total Snapshots

Additionally, two more columns show the schedule and backup status.
Whenever the icon in the second column is visible, the EC2 or EBS has scheduled a backup.
The third column contains two boxes with the following meaning:

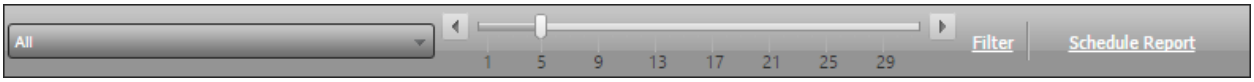
The top box represents status of the AMI backup, where:

- Green – There is AMI backup no older than 30 days
- Orange – There is AMI backup older than 30 days
- Red – Given EC2 does not have AMI backup

The bottom box represents status of the EBS volumes, where:

- Green – All volumes attached to EC2 have backup no older than 7 days
- Orange – Some volumes attached to EC2 do not have backups, or backups are older than 7 days
- Red – More than 50% of volumes attached to given EC2 do not have backups

Filters



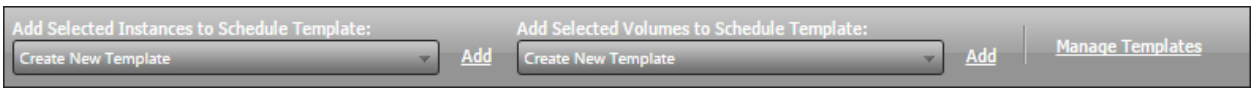
You can filter reports by selecting from five available options on the drop down list:

- All – Report shows status for all EC2 instances
- Show Instance without AMI – Report shows only EC2 without AMI
- Show Instance with AMI older than – Report shows EC2 with AMI that are older than selected amount of days; select amount of days on the slide bar
- Show Instances without volume snapshot – Report shows EC2 where at least one volume does not have snapshot
- Show Instances with volume snapshot older than – Report shows EC2 where at least one volume has snapshot older than selected amount of days; select amount of days on the slide bar

After selecting filter option, click Filter to see EC2 Instances that meet selected criteria.

Managing Scheduler Templates

You have an option to add selected EC2 Instances or EBS Volumes to existing or new Scheduler Template.



To learn more about Scheduler Templates, please read: Introduction to Scheduler Templates

To apply EC2 to template:

- Check EC2 instance you want to apply to template; check them individually or all by clicking the checkbox in header
- Select template name from the left drop down list; to create new template, select Create New Template from the list
- Click Add
- If you selected new template, the popup windows will ask you for the name of the template
- All selected EC2 Instances are assigned to the selected or new template; if you are adding EC2 Instance to the existing template and selected Instance is already assigned to that template, it is not duplicated

To apply EBS to template:

- Check EBS volumes you want to apply to template; check them individually or all by clicking the checkbox in header
- Select template name from the right drop down list; to create new template, select Create New Template from the list
- Click Add
- If you selected new template, the popup windows ask you for the name of the new template
- All selected EBS volumes are assigned to the selected or new template; if you are adding EBS volume to the existing template and selected volume is already assigned to that template, it is not duplicated

Note: the report schedule status only shows if the given template has assigned backup action. In other words, when you create a new template or add EC2/EBS to existing templates that do not have assigned AMI/Snapshot action, the schedule icon does not appear on the report.

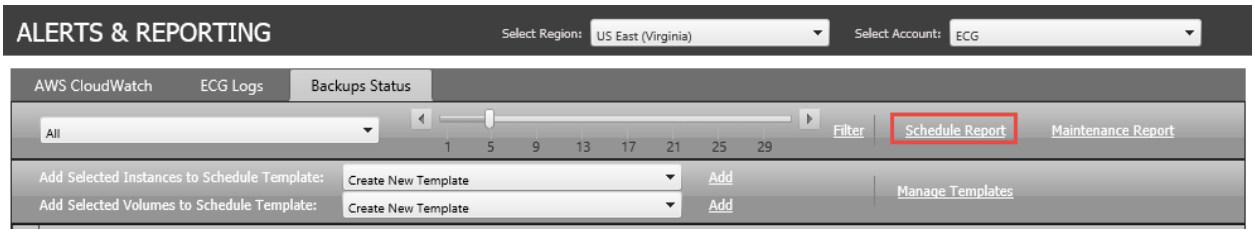
Exporting Report

You can export report to Excel by clicking Export to Excel.

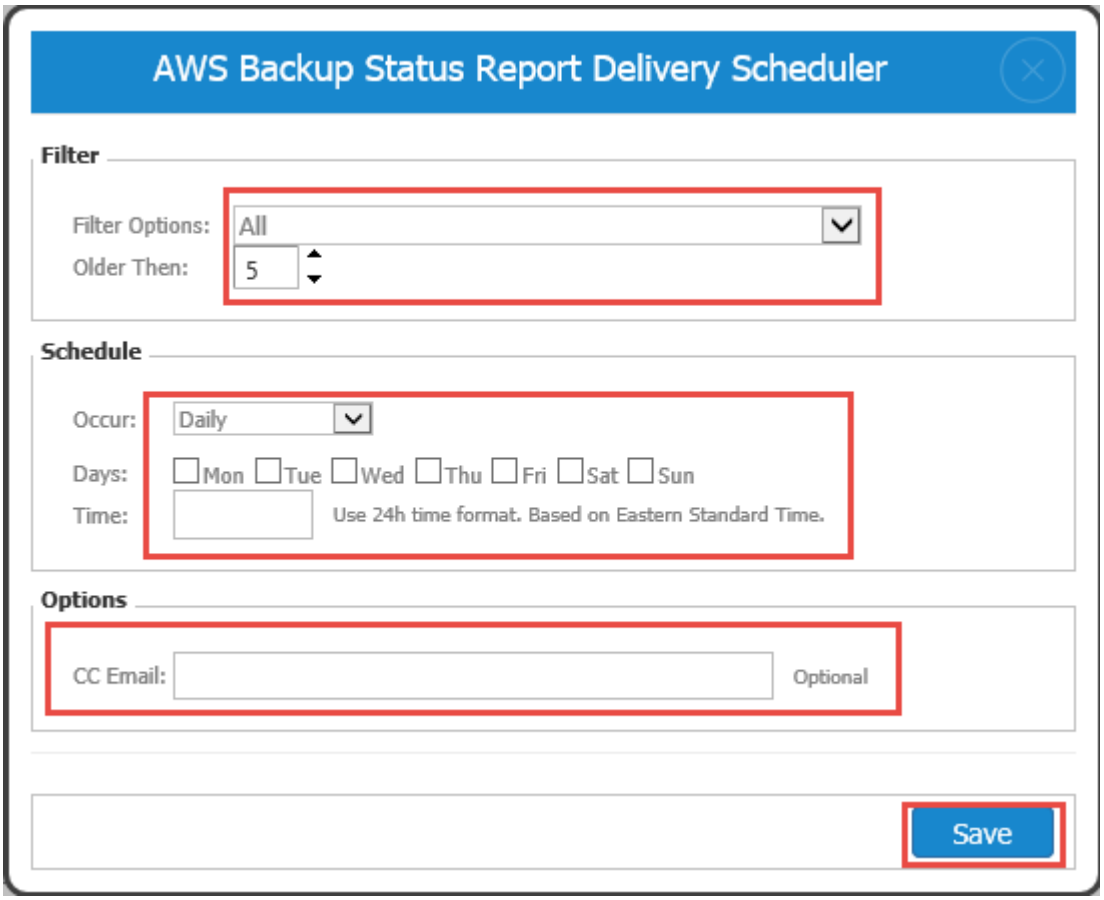
How to schedule status backup delivery via email

To schedule a Backup Status report for regular delivery to email:

Go to Alerts & Reporting section.
Switch to the Backup Status tab.
On the top panel, click Schedule Report.



From the new popup window, select filter options and schedule report delivery.
As an option, you can enter additional email(s) where the report is sent; emails must be separated by commas.
Click Save.

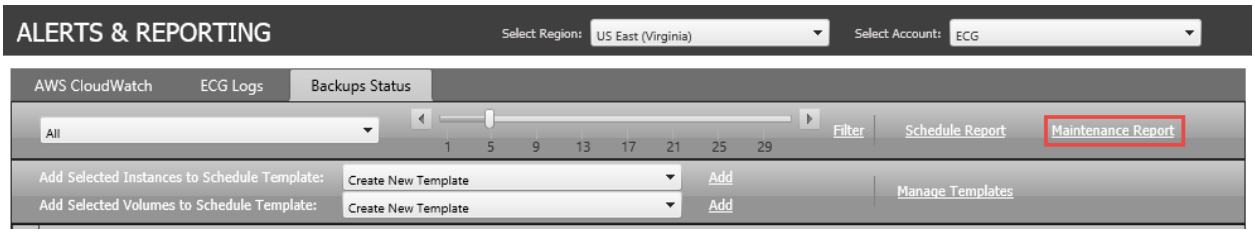


Maintenance schedulers report

Maintenance scheduler report is designed to provide information about all EC2 Instances and EBS volumes that have scheduled maintenance across all accounts.

Follow these steps to open maintenance report:

Go to Alerts & Reporting section.
Switch to the Backup Status tab.
On the top panel, click Maintenance Report.

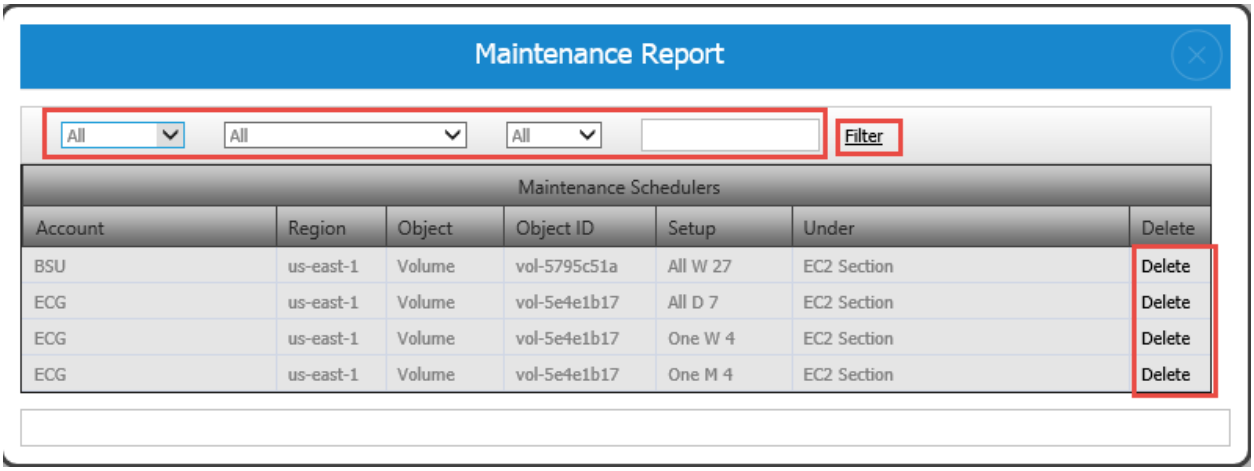


New windows with maintenance schedulers open.

You can filter report by:

- Account
- Region
- Object Type – Volume or AMI

Additionally, you can search given object by entering ID of the object.
After specifying filter criteria, click Filter to apply.



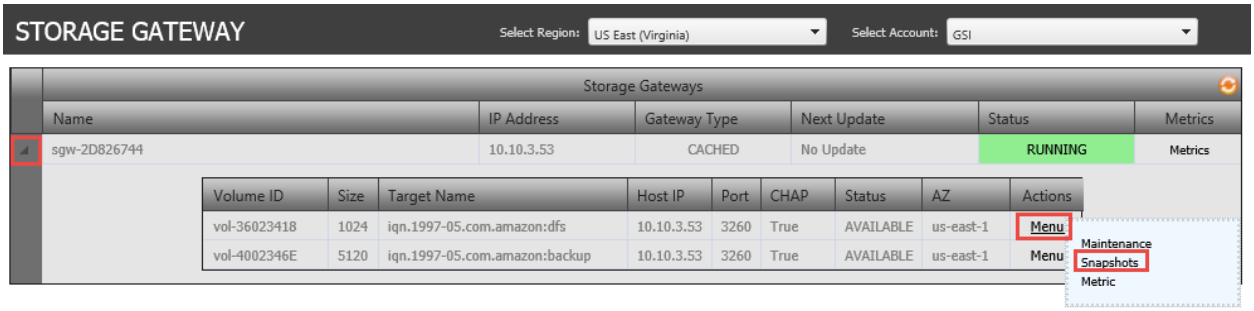
Delete maintenance for a given object by clicking Delete in the last column.

How to schedule maintenance of Storage Gateway backups

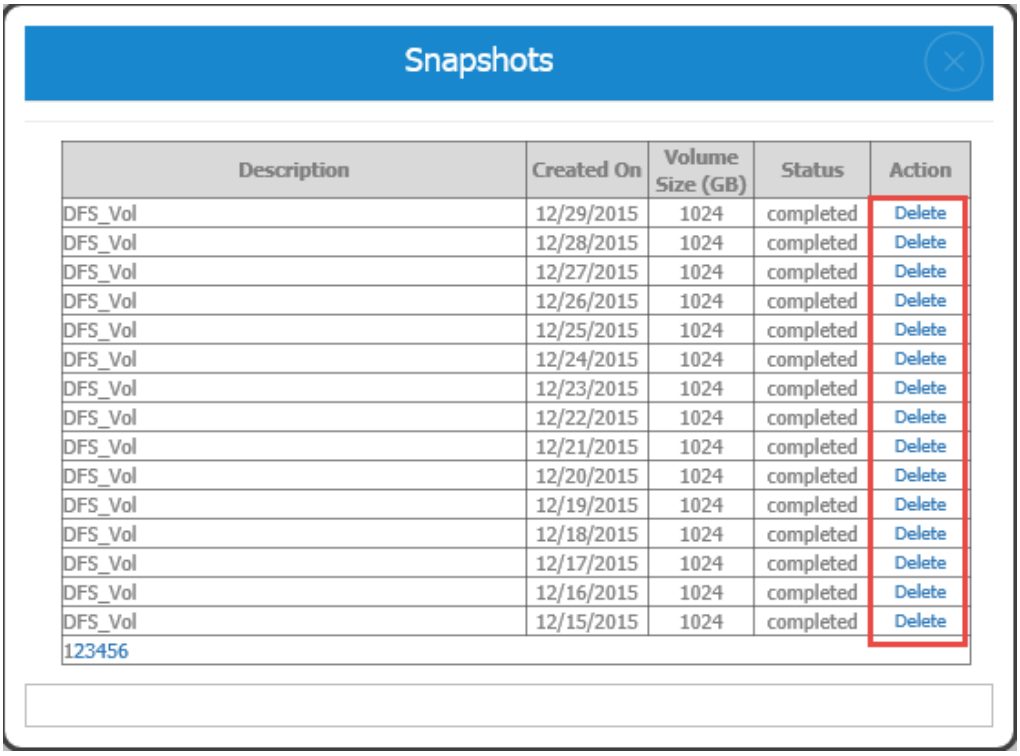
The amount of snapshots created from Storage Gateway over time is significant.
ECG allows schedule maintenance of the Storage Gateway snapshot in the same manner as regular EBS volumes.

To manage Storage Gateway snapshot from the Main Menu, select Storage Gateway.
On the new page, click the black arrow on the left to expand the volumes list for the given storage gateway.
There are two options to manage snapshots:

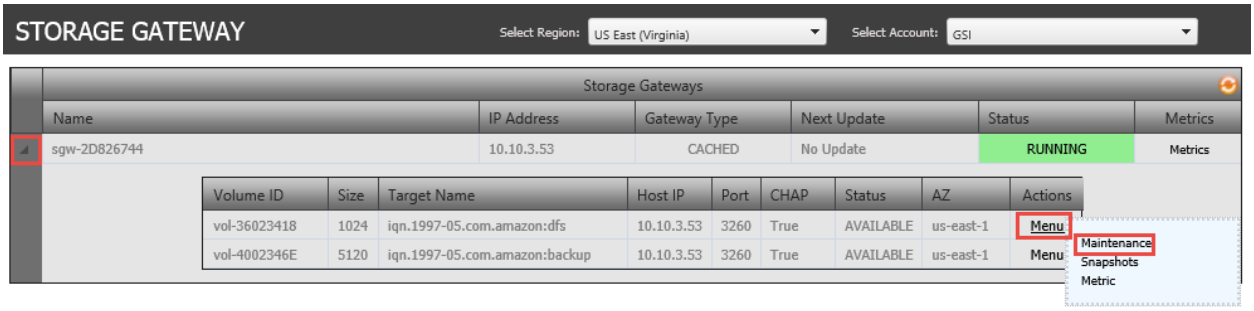
1. From the storage gateway volume menu, select Snapshots:



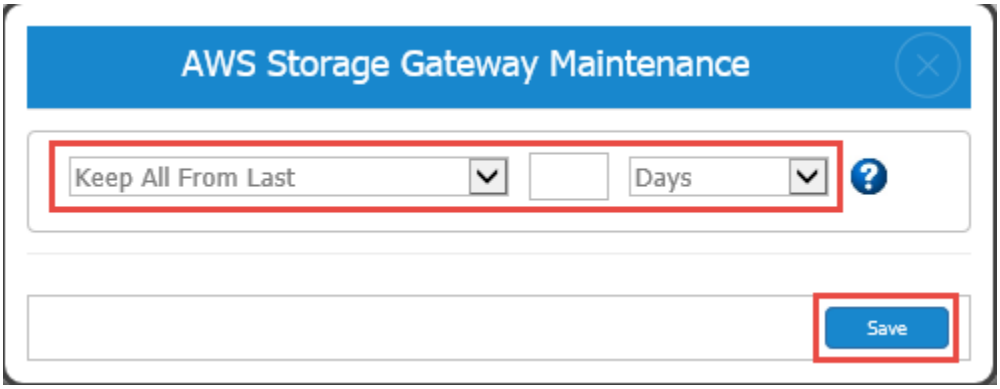
This opens new windows with the list of all snapshots taken from the selected volume.
You can delete any snapshot by clicking Delete under the action column.



2. To automate this process from the menu, select Maintenance.



This opens a window where maintenance of the snapshot can be scheduled for the selected volume based on your own criteria. You can read more about criteria options here: How to schedule maintenance of Snapshots



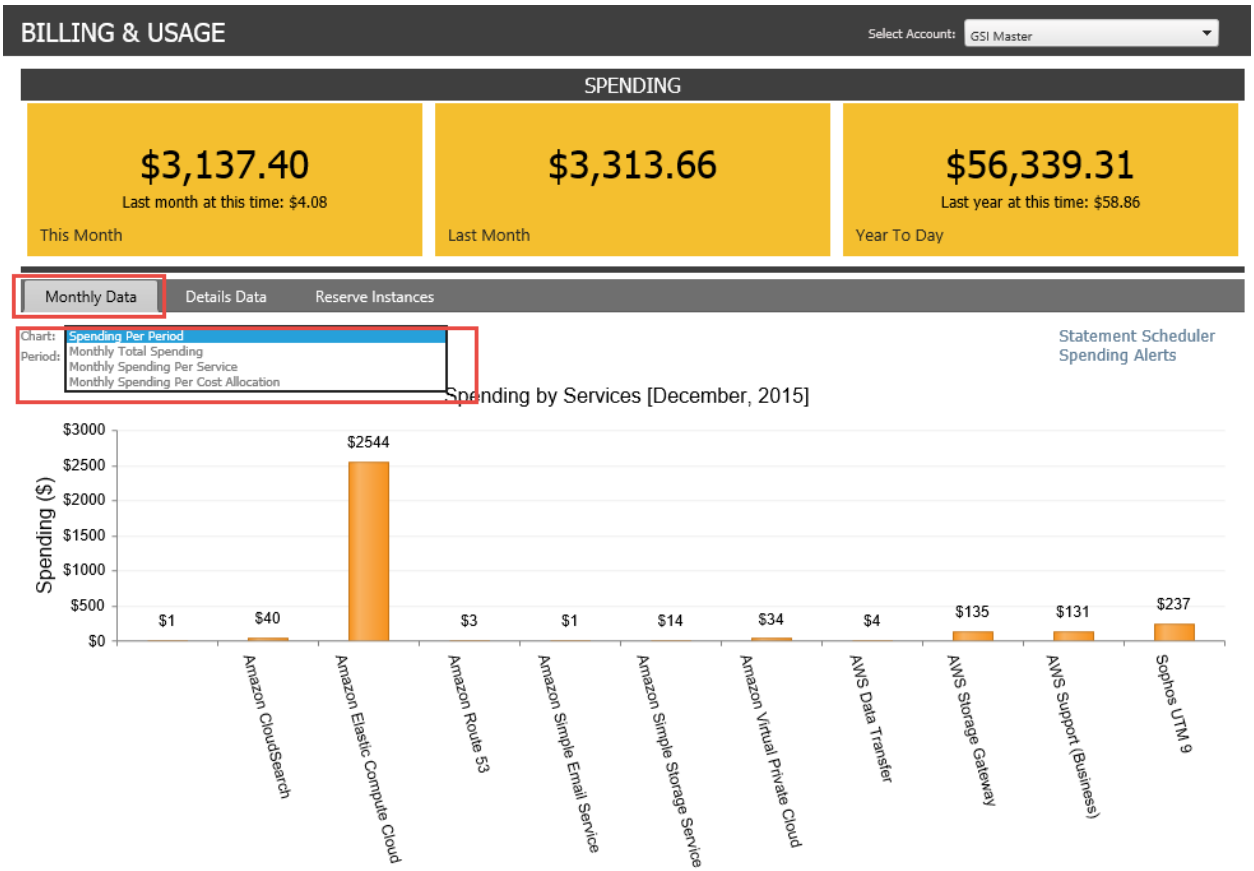
Billing and Usage review

The Billing & Usage section provides an overview and in-depth analysis of AWS Spending. Before you begin exploring your AWS spending, configure from Manage Accounts to allow our system to pull the spending data from AWS. To learn more about how to turn on this option, go to

How to add or manage AWS Account

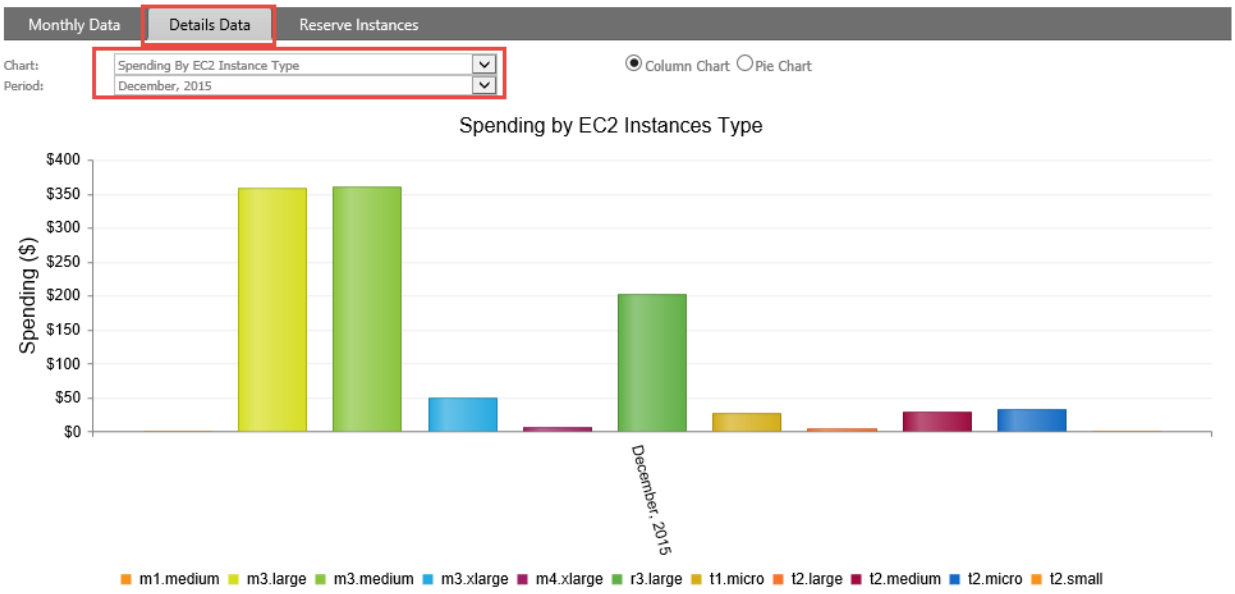
On the Billing & Usage page, you can review spending according to the following options:

1. Billing period
2. Spending by services
3. Spending by cost allocation

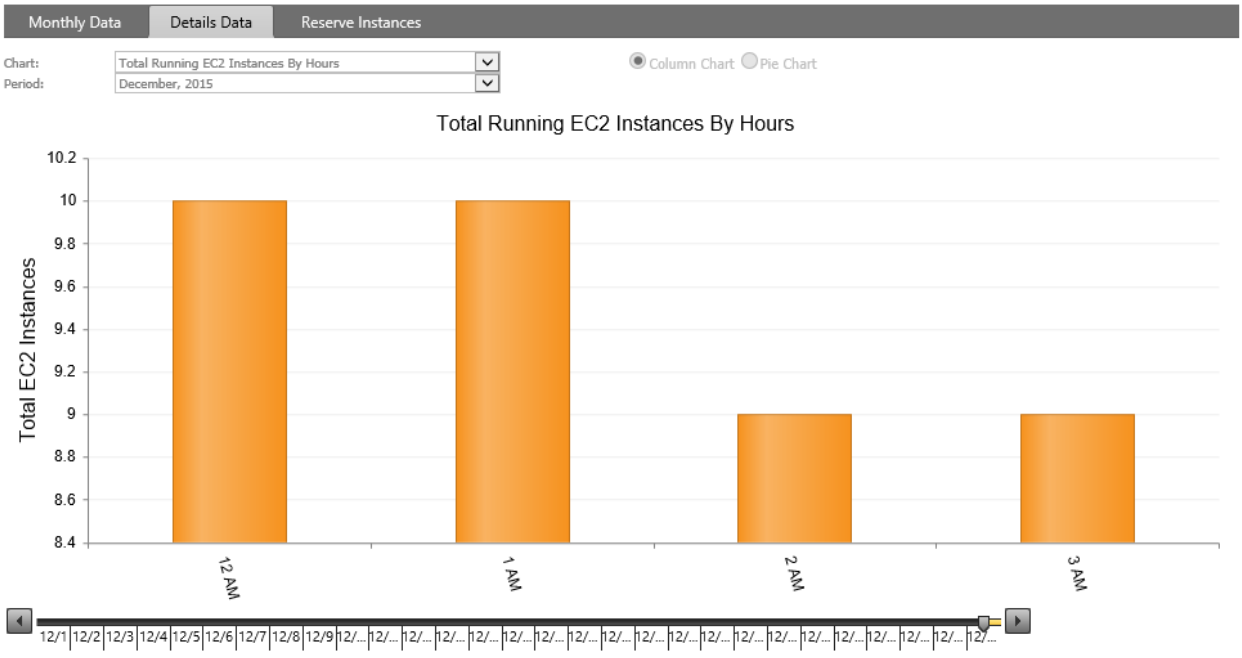


The Details Data tab allows more in-depth analysis. You have an option to see your spending by:

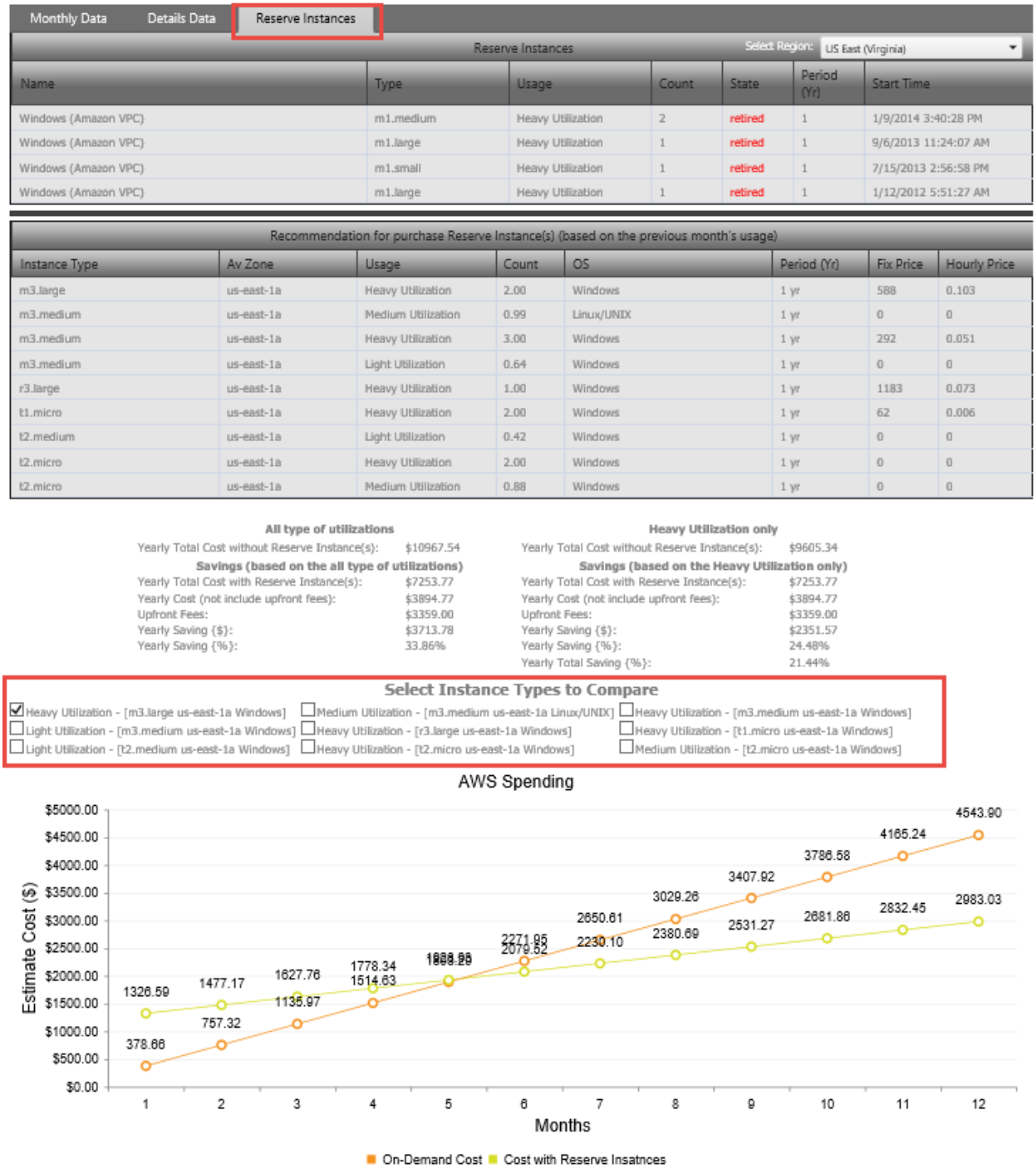
1. Availability Zones
2. Regions
3. EC2 Instance Type
4. RDS Instance Type



Additionally, you can display total running EC2 Instances per hour.
Note: to see detailed data, turn on details billing on AWS.



The Reserve Instances tab provides an overview of your reserve Instances, as well as analytic tools to estimate cost reductions by buying more reserve Instances.

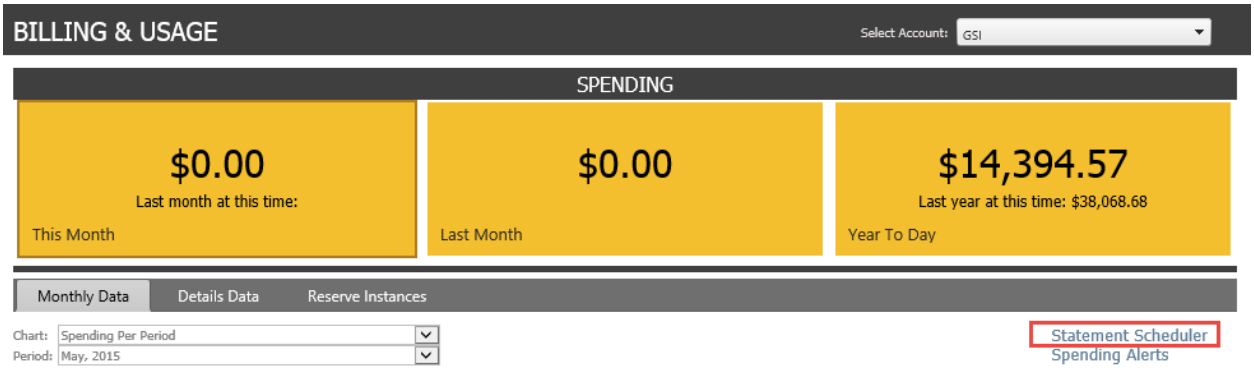


At the of the bottom page, you have the option to download a billing statement for the selected period.

How to schedule AWS billing statement delivery via email

You can schedule delivery of AWS billing statements via email on a regular basis.

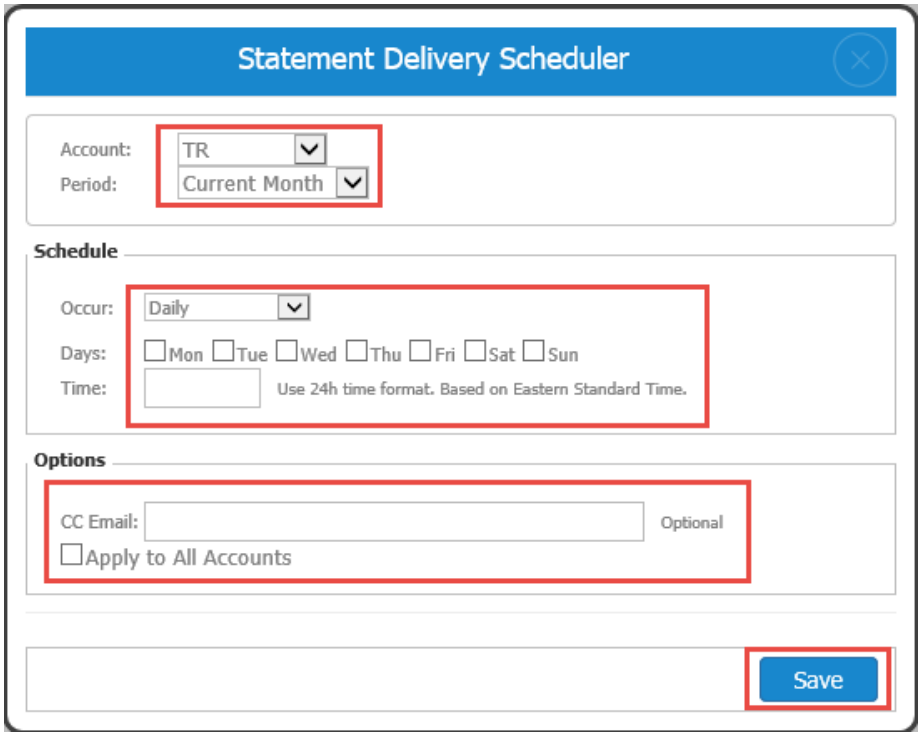
To schedule billing statements, go to the Billing & Usage section.
On the Monthly Data tab, click Statement Scheduler.



From the scheduler window, the following configurations can be set:

a. Account – The AWS account to receive statement data from
b. Period – Select either current or previous month
c. Under Scheduler section, select how frequently reports are sent
d. Report are sent to the user's email. Optionally, additional email(s) may also be specified. For multiple emails, use a comma separator

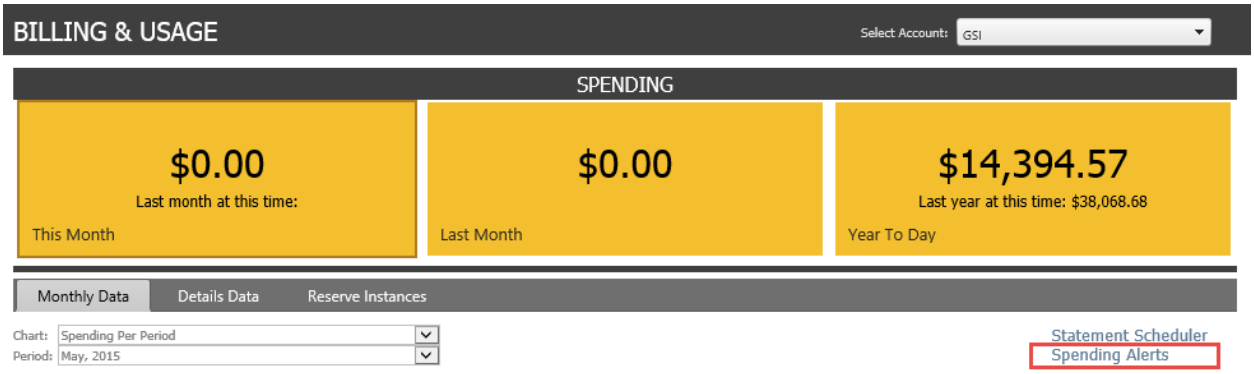
Click Save.



How to setup spending alerts

Setup alerts to notify you when total spending or spending for a given AWS service goes over your limit.

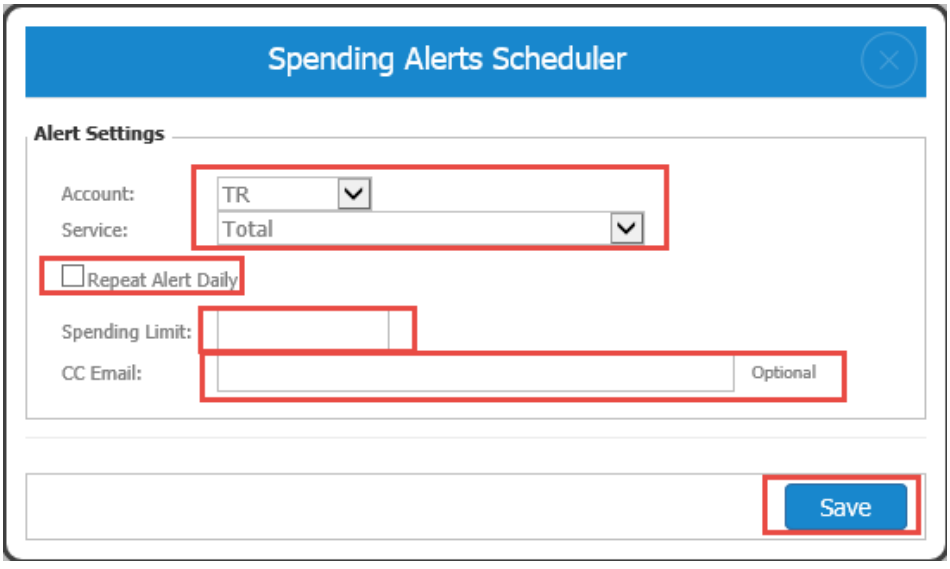
To setup spending alerts, go to the Billing & Usage section; on the Monthly Data tab, click Spending Alerts.



In the scheduler windows, select the AWS account and service you want to monitor. Leave Total selected under service to setup alerts for total spending.

Under Spending Limit enter the amount that is the threshold for an alert. When your spending goes over that limit, the alert is sent to the user's email.
Optionally, you can enter more emails for alert notification; use a comma separator for multiple emails.
When your spending exceeds the specified limit, an alert is sent once per billing period.
To receive alerts every day, check Repeat Alert Daily.

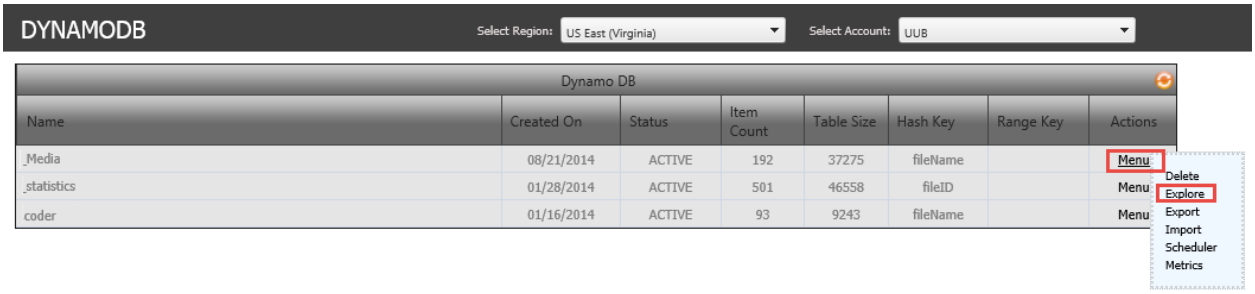
To save your alert configuration, click Save.



Explore Dynamo DB

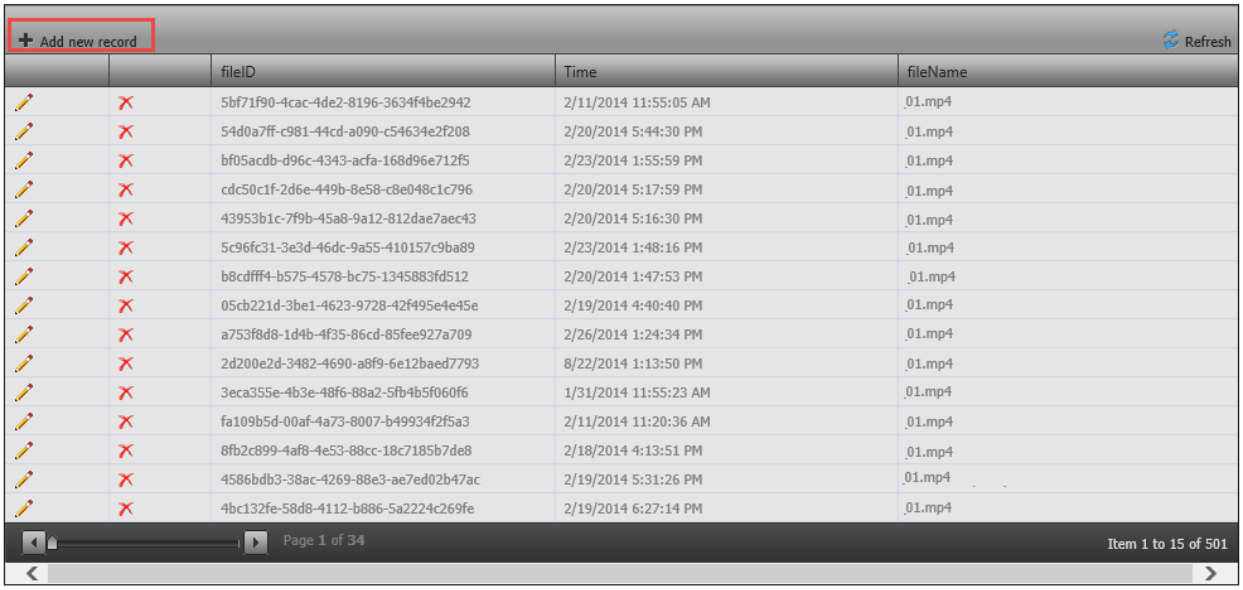
To explore DynamoDB data from the Main Menu, select DynamoDB.

Under the DynamoDB page from the context menu, select Explore.

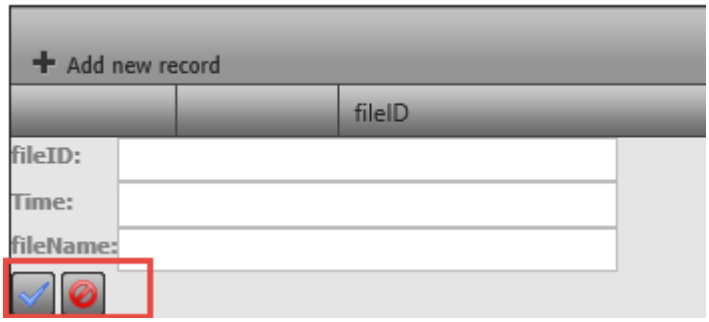


All data records are visible in the table.

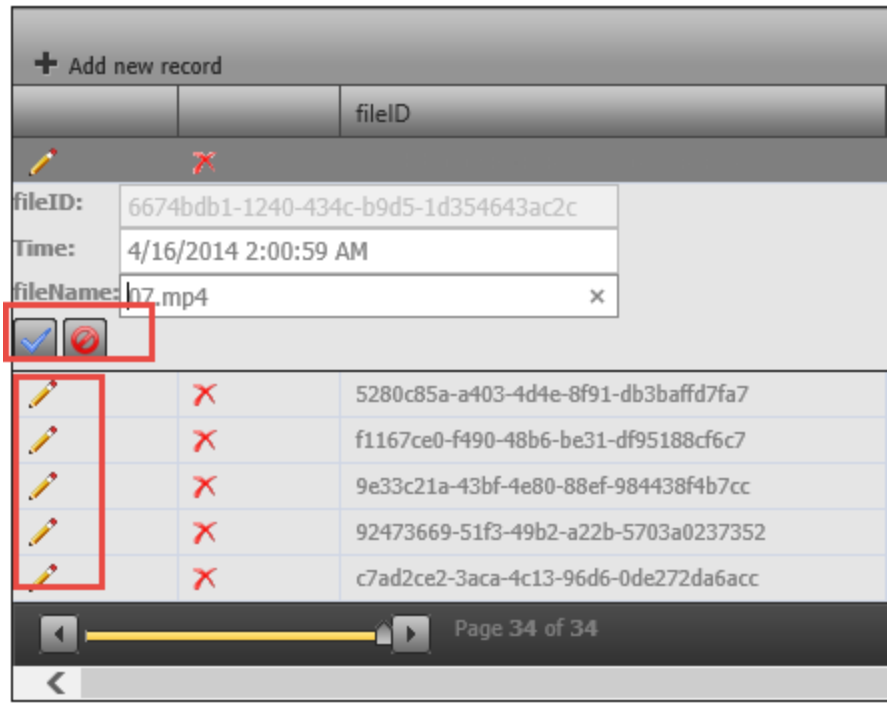
Add Data – To add a new record, click Add new record.



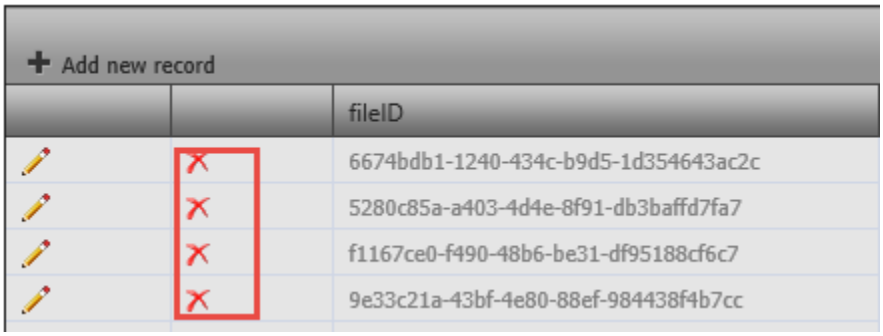
Fill out the data form and click Insert. To discard this action, click Cancel.



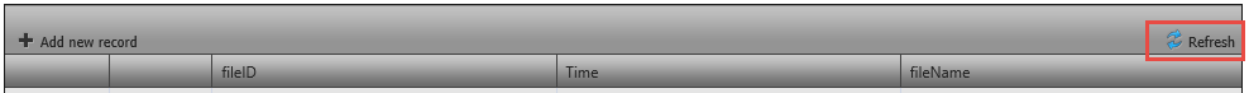
Update Data – To update existing data, click Edit from the first column. Make changes in the data form and click Update. To discard this action, click Cancel.



Delete Data – To delete existing records, click Delete from the second column.



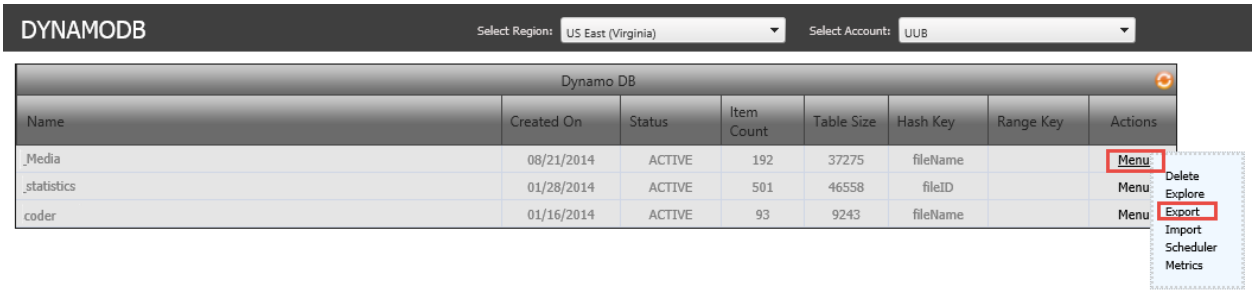
Data can be refreshed at any time by clicking Refresh from the top panel.



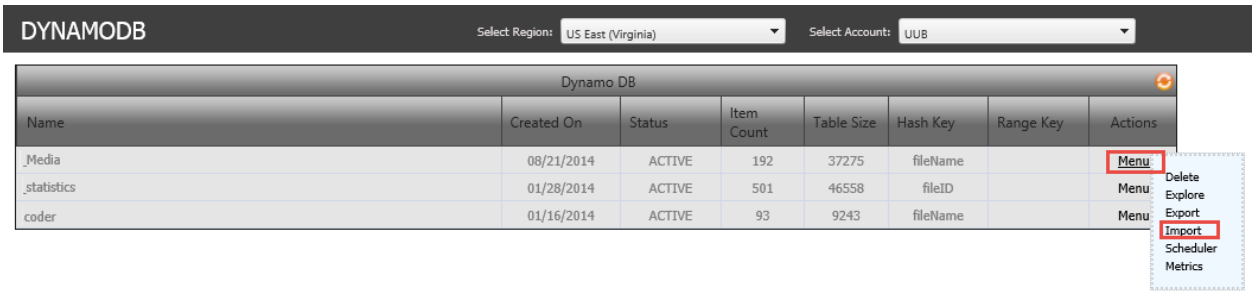
Export/Import data to DynamoDB

To import or export DynamoDB data from the main menu, select DynamoDB.

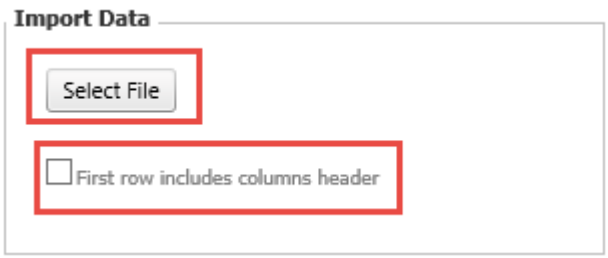
Export – To export DynamoDB data from the context menu, select Export. All data is exported to a csv file.



Import – To import data to DynamoDB from the context menu, select Import.

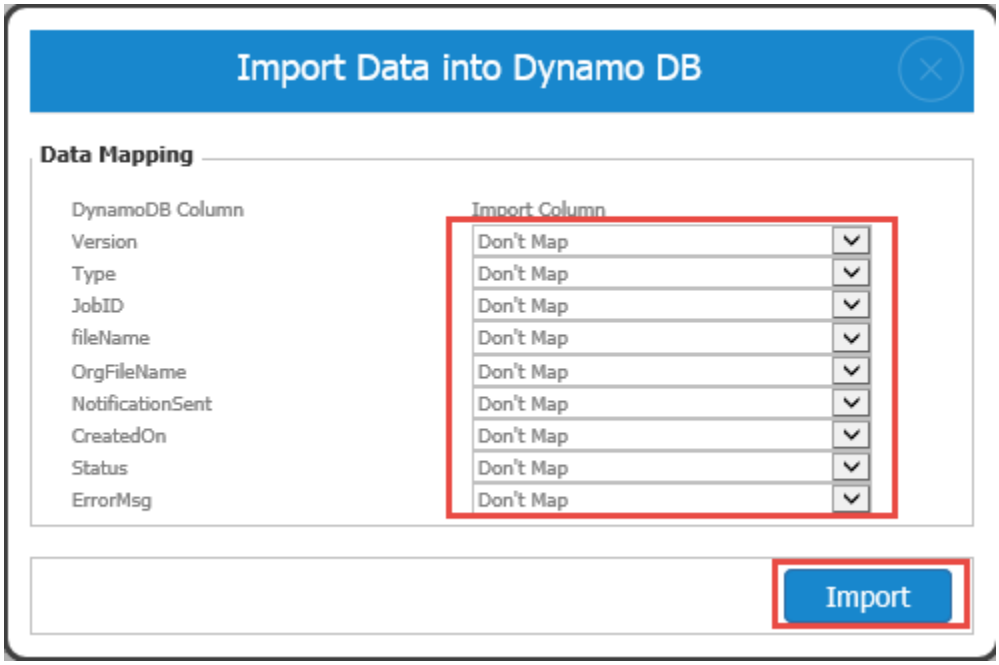


Select data file to import by clicking Select File at the top page. If the first row of import data contains column names, check the First row includes columns header checkbox.



Next: after selecting the file, map data between the import file and DynamoDB. In the new window is listed all DynamoDB columns on the left and drop down lists, with name of columns from the import file on the right. To map data from the drop down list, select the name of the column. If you do not want to map a given column, select Don't Map in the drop down list.

When you finish mapping, click Import.



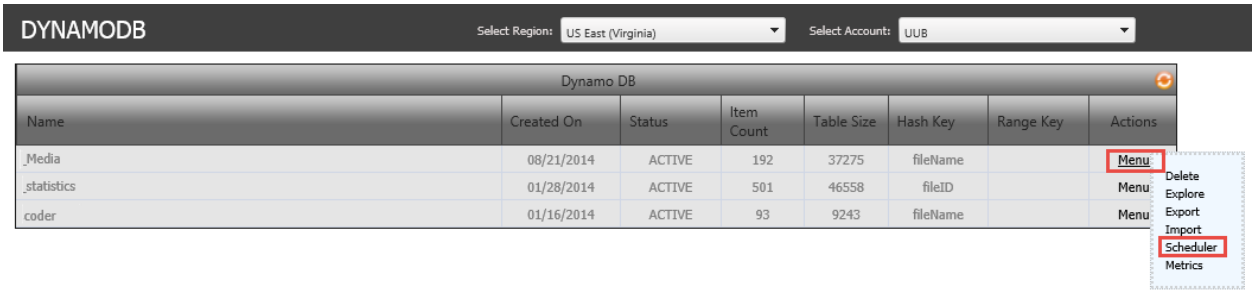
Import should start shortly. Track progress by going to Dashboard and from the Other menu, select “OnDemand Job Status”.

How to schedule export/import data to DynamoDB

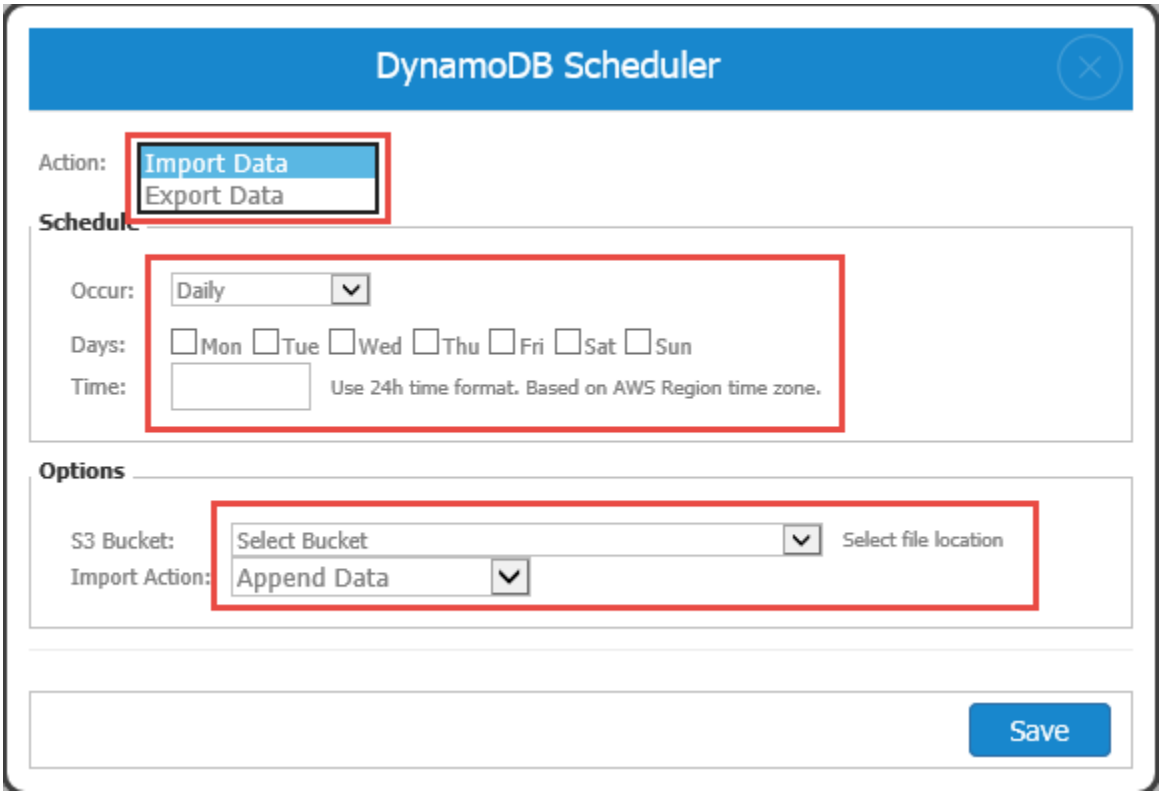
Import/Export scheduler allows scheduling of import/export DynamoDB data from/to a csv file.
When you schedule import, the csv file has to be in S3 bucket.
When you schedule export, the csv file is saved to S3 bucket.

To schedule import or export of DynamoDB data from the Main Menu, select DynamoDB.

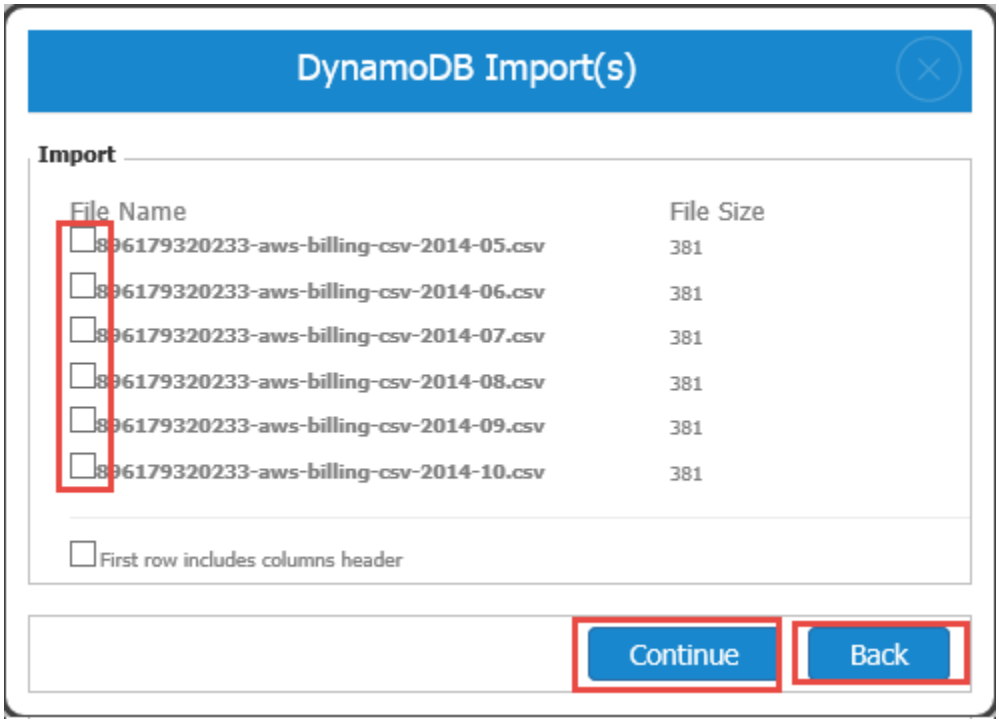
From the context menu, select Scheduler.



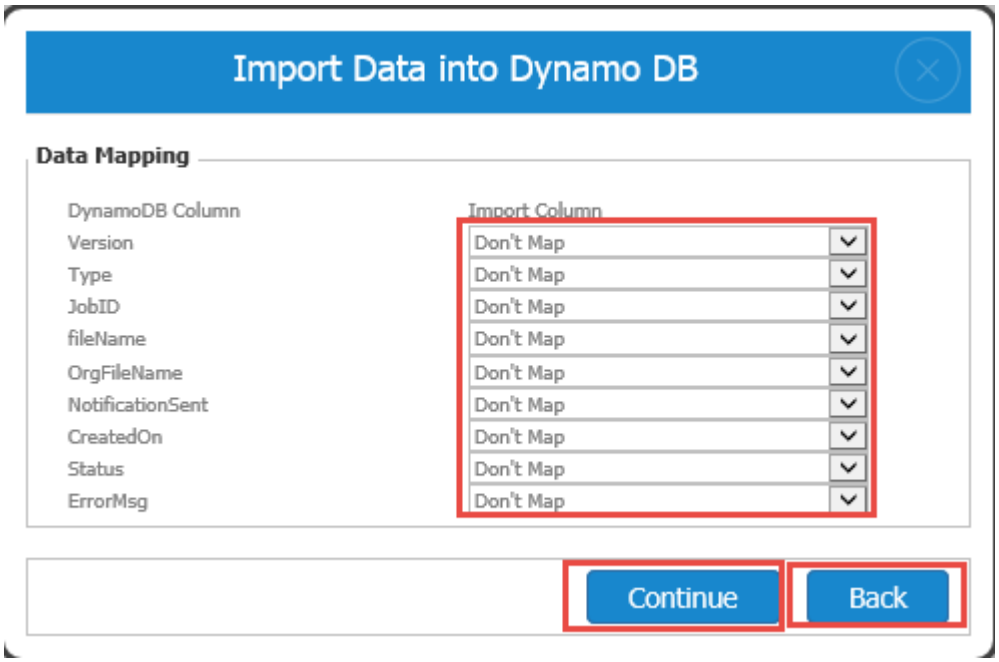
Within the scheduler windows, make the following configurations:
Action – Select either import or export data
Scheduler – Select when the action should be executed



S3 Bucket – Select S3 Bucket when the csv file is outputted. If you are scheduling import, after selecting S3 Bucket the list of files in the bucket is visible.



Check the file that contains data you want to import and click Continue. If the first row of import data contains column names, check the First row includes columns header checkbox. If you selected the wrong S3 Bucket, click Back to select a different bucket.



The next step after selecting the file is to map data between import file and DynamoDB. The new window lists all DynamoDB columns on the left and drop down lists with listed name of columns from the import file on the right. To map data from the drop down list, select the name of the column. If you do not want to map the given column, select Don't Map from the drop down list. When you finish mapping, click Continue.

Note: if the import file does not have the name of the columns in the first row, the drop down list shows Column1, Column2, etc. – the number represents the column number in your import file.
Also, keep in mind multiple files are selected to import, all of those files must have the same mapping.

Click Map button to change mapping at any time.

Import Action – This option allows selection of import data to append to the existing data: select Append Data, or Overwrite Data to select existing data to delete prior to import of the new data

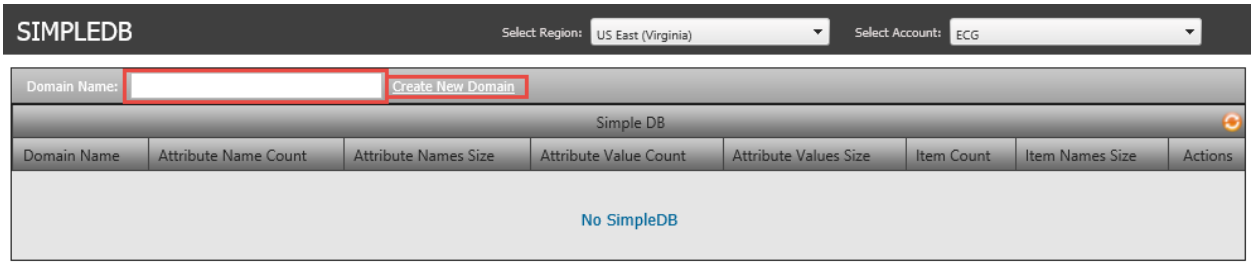
Click Save to complete configuration.

At any time, you can edit, suspend, or delete scheduler by clicking the appropriate action from the scheduler's list.

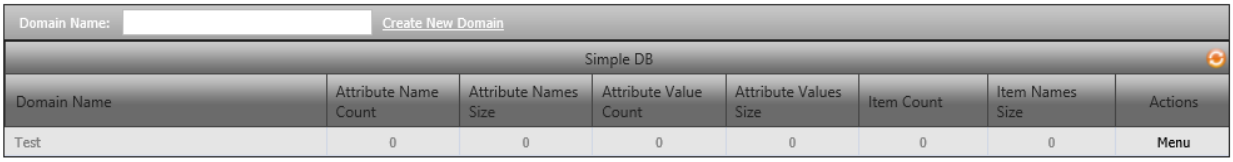
How to create SimpleDB

To create new SimpleDB domain from the Main Menu, select SimpleDB.

From the SimpleDB page, enter the new SimpleDB domain name in the Domain Name box and click Create New Domain.



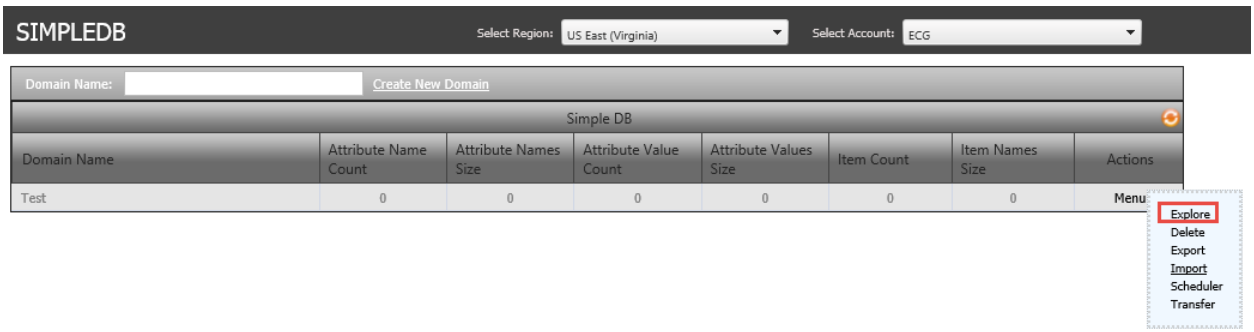
The new domain name appears on the SimpleDB domains list.



Explore SimpleDB

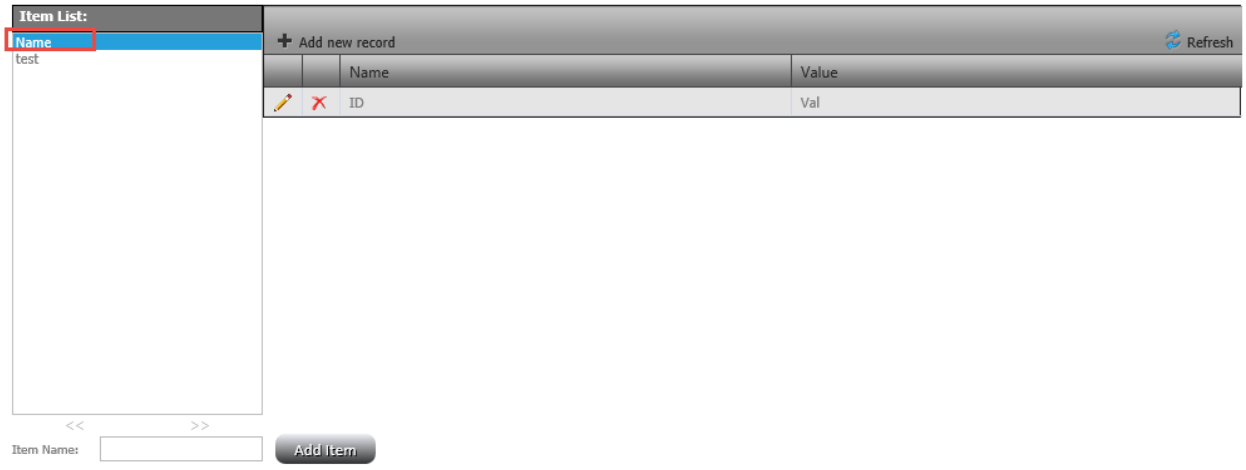
To explore SimpleDB data from the Main Menu, select SimpleDB.

From the SimpleDB page from the context menu, select Explore.

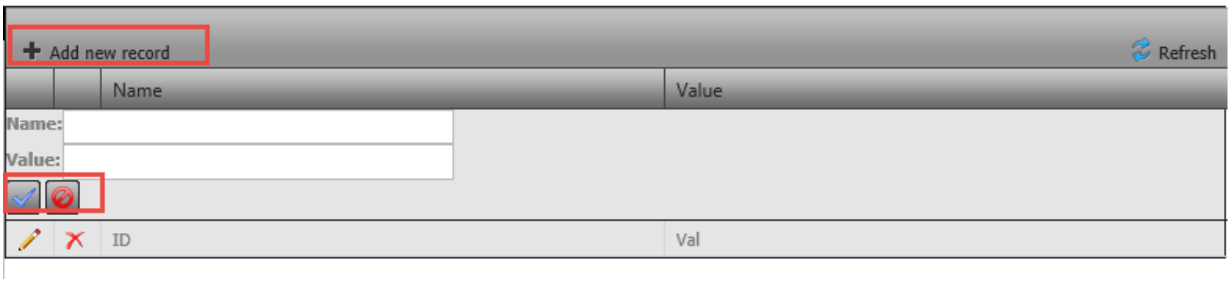


All data records are shown in the table.

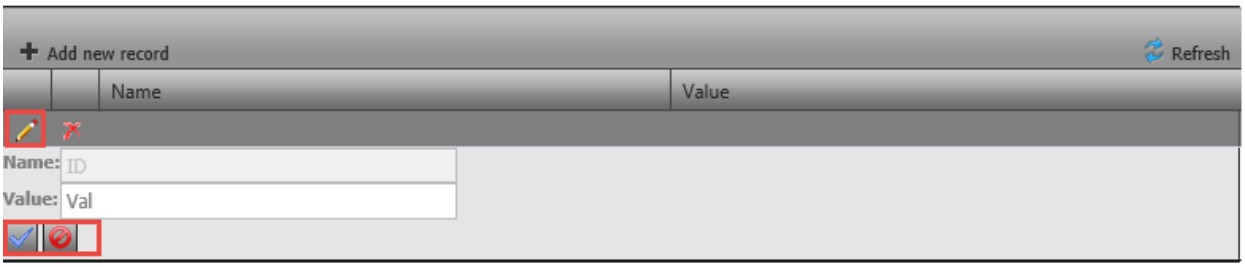
To see attributes associated with a given item, click the item name from the item list.



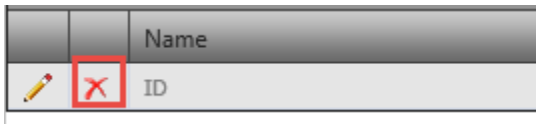
Add new attribute – To add new attribute, click Add new record, then enter attribute name and value and click Insert. To disregard this action, click Cancel.



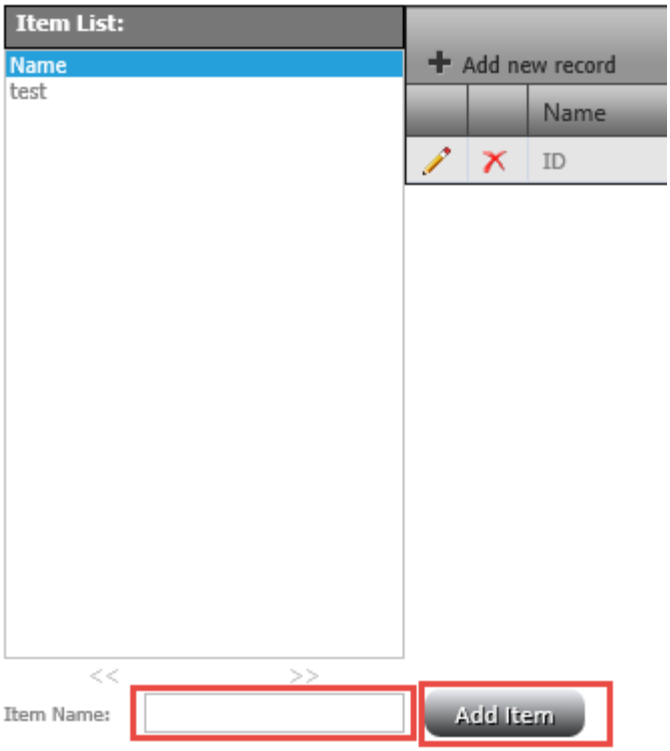
Update attribute – To update value of the given attribute, click Edit from the first column; modify the attribute value and click Update. To disregard this action, click Cancel.



Delete attribute – To delete a given attribute, click Delete from the second column.



Add new Item – To add a new item, enter the item name in the Item Name text box and click "Add Item".

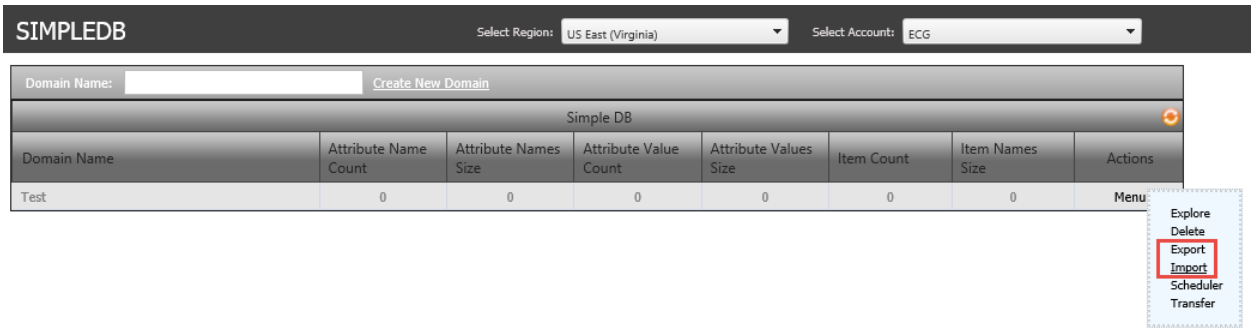


Refresh data at any time by clicking Refresh from the top panel.

Export/Import data to SimpleDB

To import or export SimpleDB data from the Main Menu, select SimpleDB.

Export – To export SimpleDB data from the context menu, select Export. All data is exported to csv file



Import – To import data to SimpleDB from the context menu, select Import. Select file to import by clicking Select File at top of page. Please ensure import file has the correct structure of three columns:

- Column 1 – item name
- Column 2 – attribute name
- Column 3 – attribute value

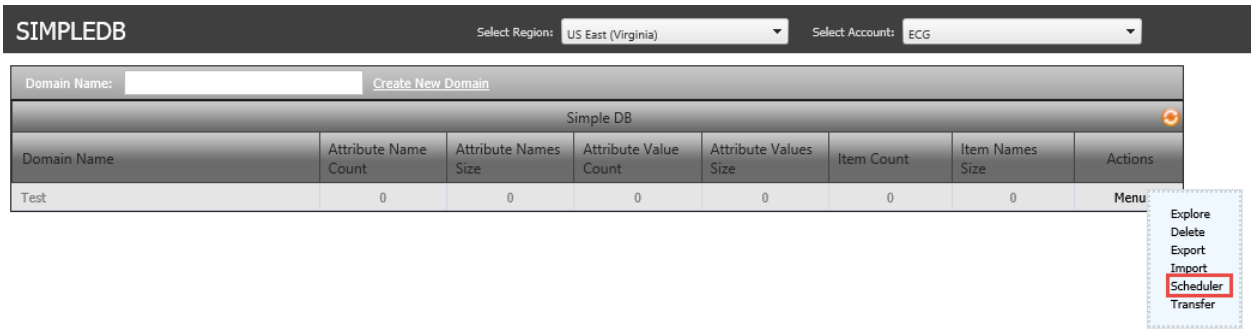
After selecting file data, start the import to SimpleDB.

How to schedule export/import data to SimpleDB

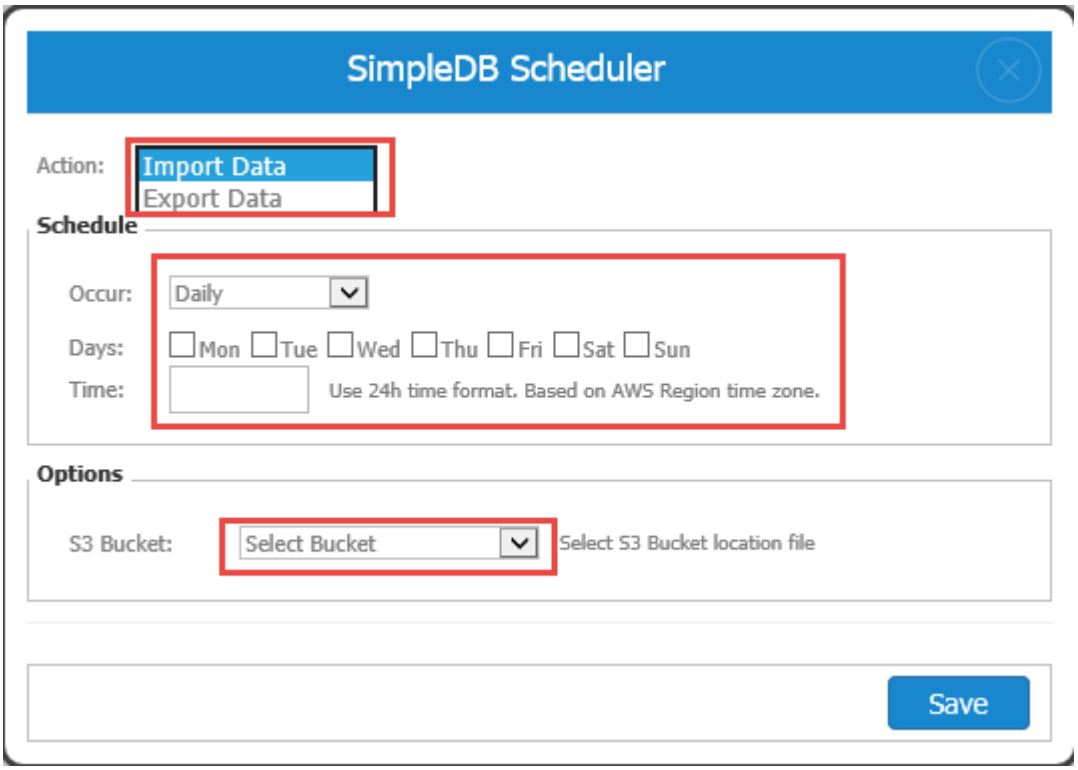
Import/Export scheduler allows scheduling of import or export of SimpleDB data from/to csv files.
To schedule import, the csv file has to be in S3 bucket.
To schedule export, the csv file is saved to S3 bucket.

To schedule import or export of SimpleDB data from the Main Menu, select SimpleDB.

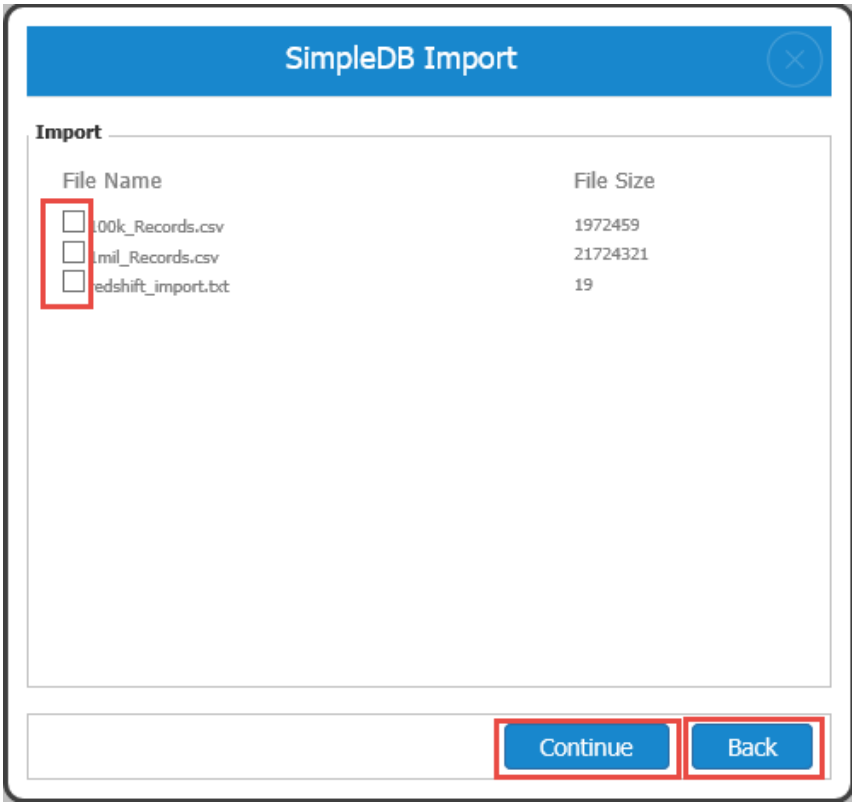
From the context menu, select Scheduler.



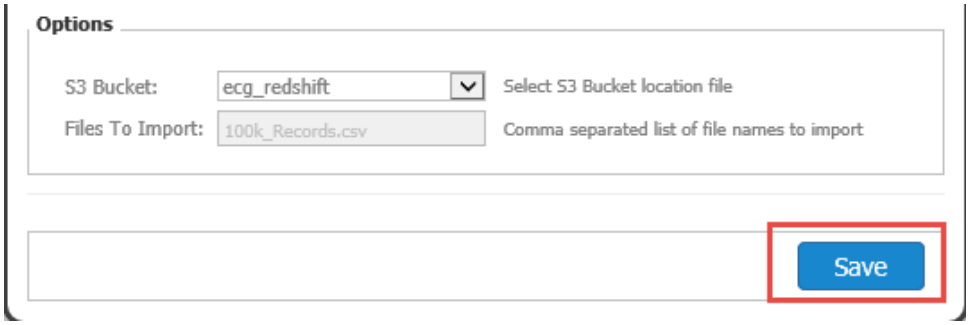
Under the scheduler windows, configure the following settings:
Action – Select either import or export data
Scheduler – Select when the action is executed



S3 Bucket – Select S3 Bucket where the csv file is outputted. If scheduling import, within selected S3 Bucket a list appears of files in the bucket.



Check the file to import and click Continue. If you selected the wrong S3 Bucket, click Back to select a different bucket.
When you finish, click Continue.
To save schedule, click Save.

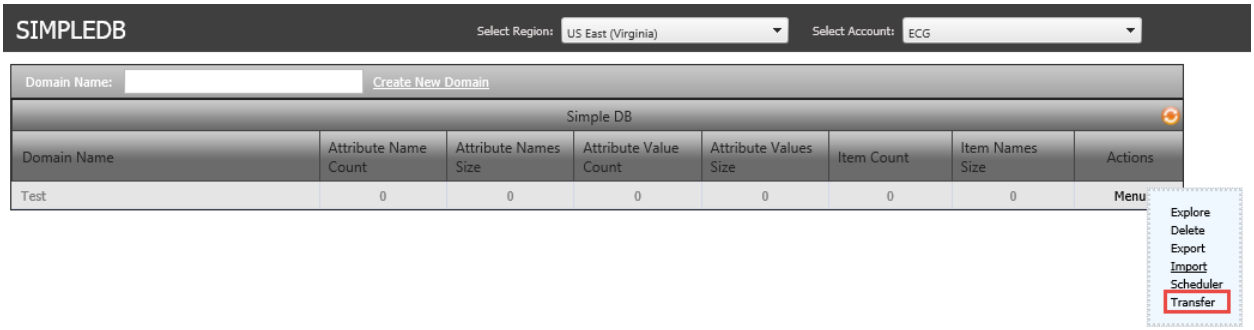


At any time, you can edit, suspend, or delete scheduler by clicking the appropriate action from the scheduler's list.

How to transfer SimpleDB to another AWS region

To transfer SimpleDB to another AWS region from the Main Menu, select SimpleDB.

Under the SimpleDB page from the context menu, select Transfer.



Within the Transfer window, the following configurations are available:

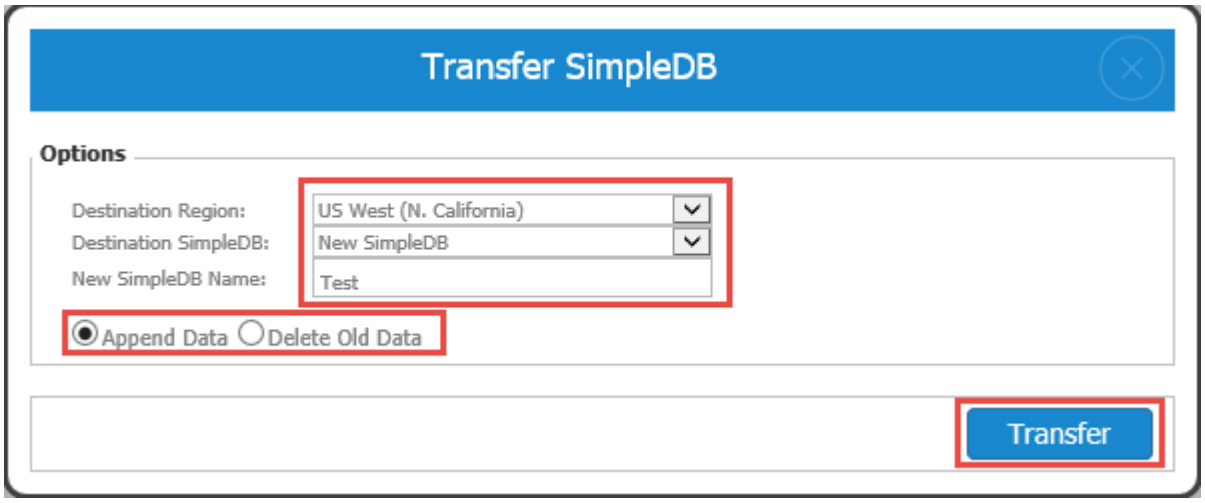
Destination Region – From the drop down list, select the AWS region you want to transfer SimpleDB domain

Destination SimpleDB – Select New SimpleDB to create a new domain, or select existing one to transfer data to existing domain

New SimpleDB – Enter the name for the new SimpleDB

If you are transferring data to the existing SimpleDB, you can choose to select either Append Data, or Delete Old Data to delete existing data before import.

Click Transfer

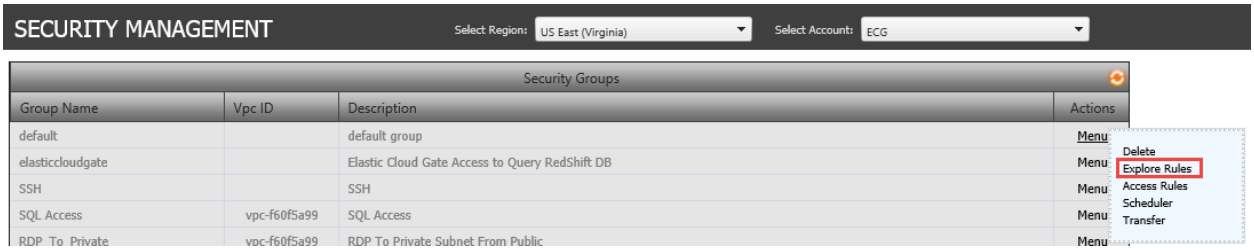


You can track progress of the transfer by going to Dashboard: from the Other menu, select "OnDemand Job Status".

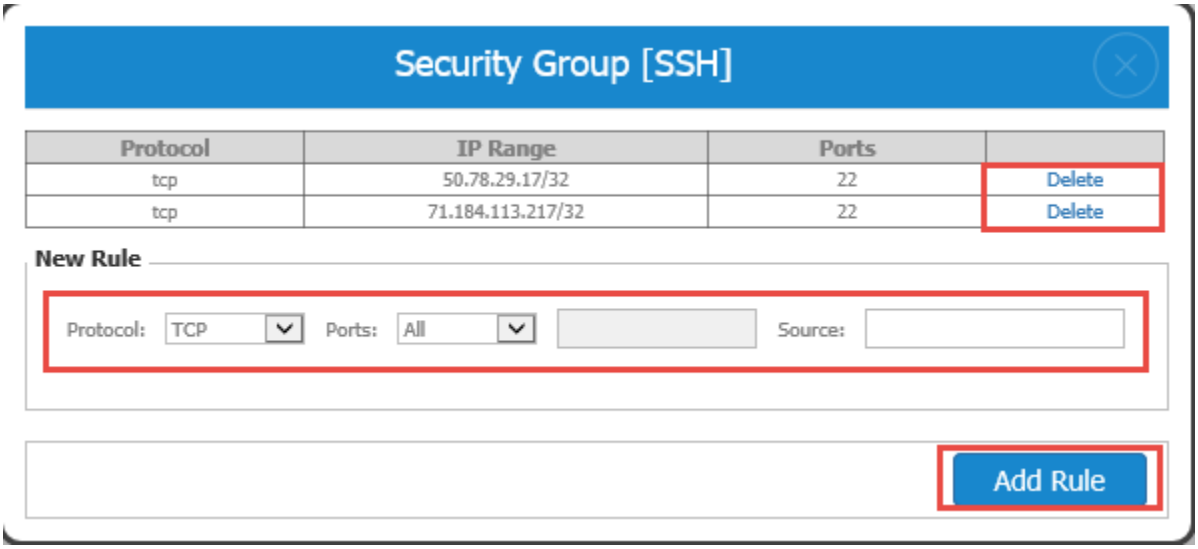
Explore and modify AWS Security Groups rules

To review current security groups from the main menu, select Security Management.

On the new page is a list of all security groups created under the selected account, in the selected region. To review or modify security group rules from the context menu, click Explore Rules.



Delete Rule – To delete rule from the security group, click Delete in the last column
Add Rule – To add new rule to security group, select protocol ports and source IP (IP has to be in CIDR format xxx.xxx.xxx.xxx/xx) and click Add Rule



How to temporarily open AWS Security Groups rules for dynamic IP

Elastic Cloud Gate provides the option to open certain ports in your security group for connections made from dynamic IP, based on the scheduler.

The flow of opening security group is:

- User who is behind dynamic IP logs-in to ECG portal
- If the current time is in the range specified in configuration and access to security group was configured without admin confirmation, the new rule is created for the IP, from user who made the connection
- If the current time is in the range specified in configuration and access to security group was configured with admin confirmation, email is sent to admin; admin must login to portal and approve the user; when user is approved, the new rule is created for IP from user who made the connection

Before you make security group configuration, you have to create a new login for the user.

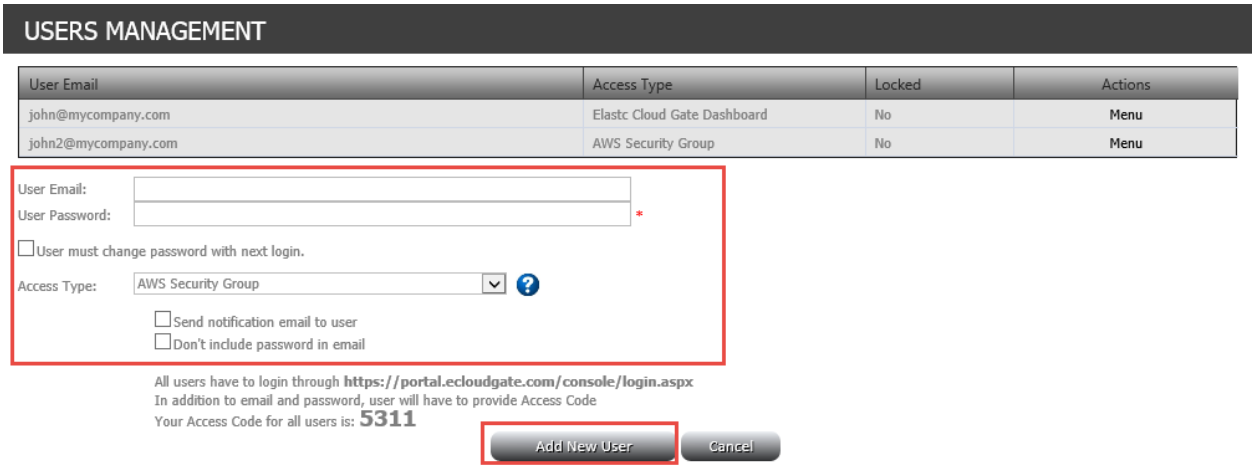
To create a new login for the user from the Settings menu, select Manage Users.
Enter user email and password.

To force user to change password with next login, check User must change password with next login.

From the Access Type drop down list, select AWS Security Group.
To send notification email to the new user, check Send notification email to user.

If for security reasons you don't want to include the password in the email, check Don't include password in email.

Click Add New User.



Note: any user created though the Users Management section must use a different URL to login to ECG portal. The URL is: https://portal.ecloudgate.com/console/login.aspx

In addition to email and password, the user is asked for the access code on the login page. You can see your access code on the Users Management page. This number is statically assigned to your account and will not change.

When the new user is created, you can configure security group: from the Main Menu select Security Management.
On the security group list, find the one to which the new rule applies and from the context menu select Access Rules.

In the configuration window from the drop down list, select User.

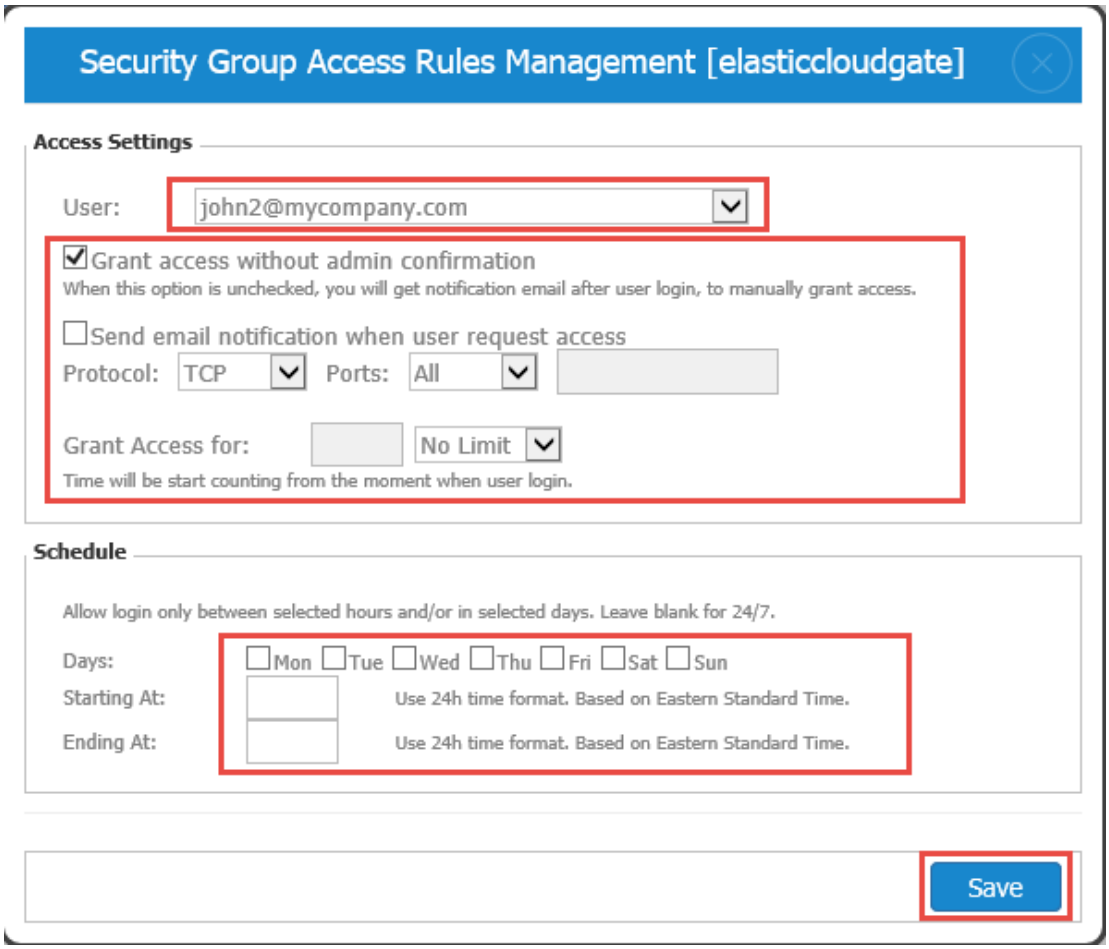
Access to the security group can be granted manually, with the administrator required to approve each user before access is granted, or automatically (without approval by administrator): this option is set by checking Grant access without admin confirmation box.

As an option, you can request a notification email whenever user requests access by checking Send email notification when user request access box.

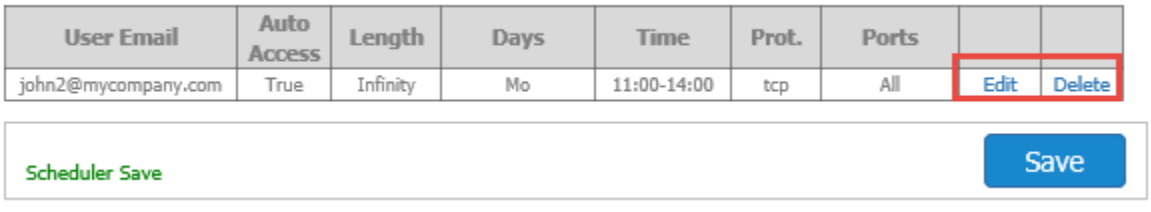
Protocol and port define the rule applied to the security group, along with user IP.

Additionally, you can limit duration the rule stays in effect: do this from the Grant Access for list, select either Hours or Days and enter the value.

Under the Schedule section, you can specify what days and time the rule applies. For access 24/7, leave blank.
When you finish configuration, click Save.



At any time, edit or delete access by selecting Edit or Delete from the access list.



Additionally, you can create multiple accesses, e.g. different time access to different days, or for different ports.

When you choose to grant access for the user after manual approval, you will receive a notification email after user's login. After that, you can grant or deny access.

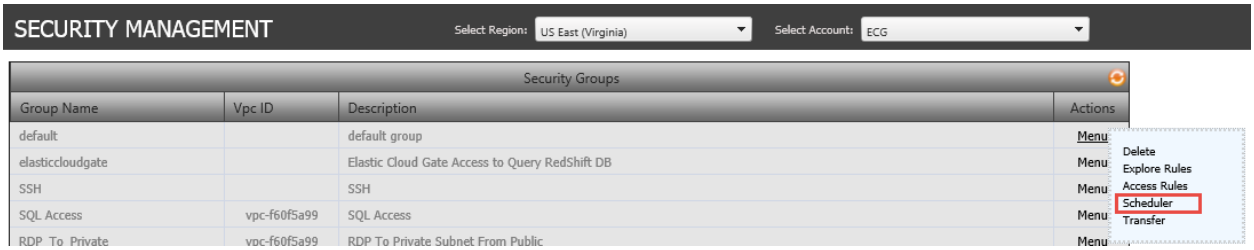
To manually confirm access login to ECG Portal, go to the Security Management section.
At the top of the page is a list of users waiting for approval; to approve or deny access, select the appropriate option from the context menu.

How to schedule grant access for selected IP

Elastic Cloud Gate provides a feature that allows adding or removing a rule to security group based on the scheduler.

To schedule security group access, go to the Security Management section.

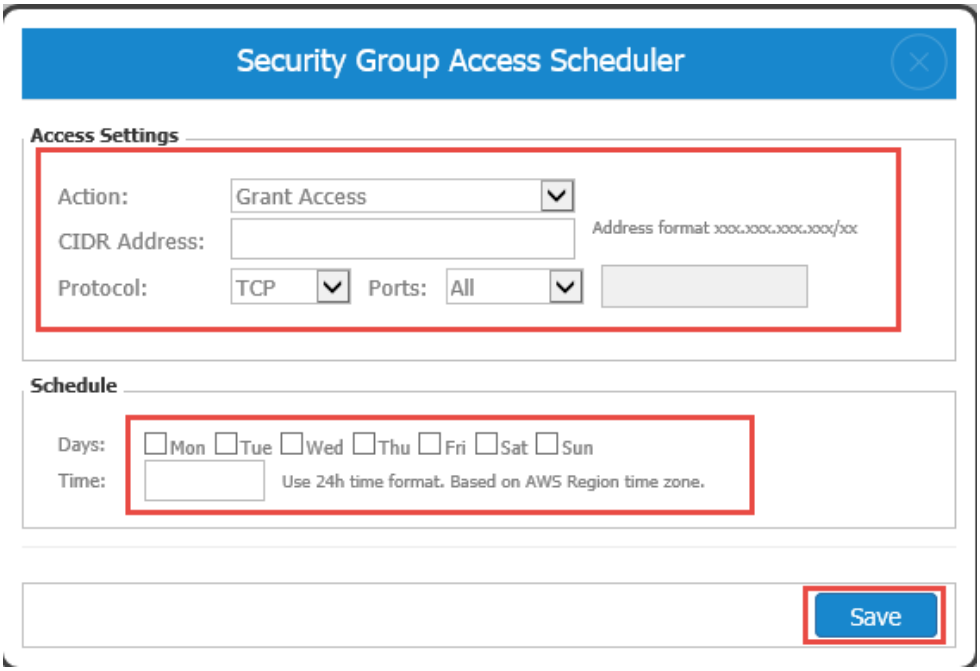
From the context menu, select Scheduler.



In the scheduler window, make the following configurations:

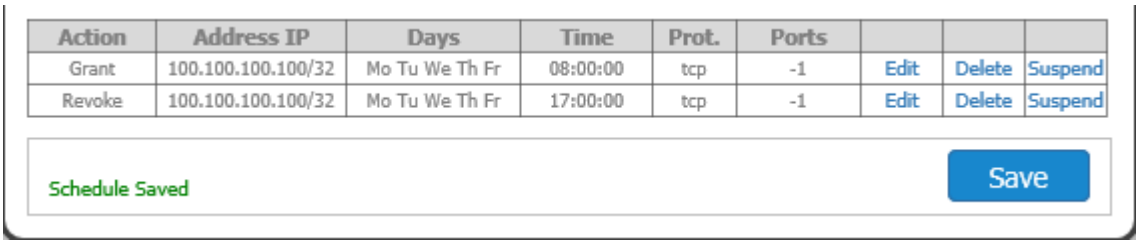
Action – Select Grant Access to add the rule or Revoke Access to remove the rule, based on the scheduler
CIDR Address – Enter IP address to grant/revoke access. Address needs to be in CIDR format (xxx.xxx.xxx.xxx/xx e.g. 10.23.1.45/32)
Protocol – Select protocol (TCP or UDP) and port

In the Schedule section, check the day(s) and time when the action should be executed.
Click Save.



You can schedule multiple actions, e.g. you can open access for given IP address only between certain hours. To do so, schedule Grant Access and Revoke Access for the same rule.

Example:

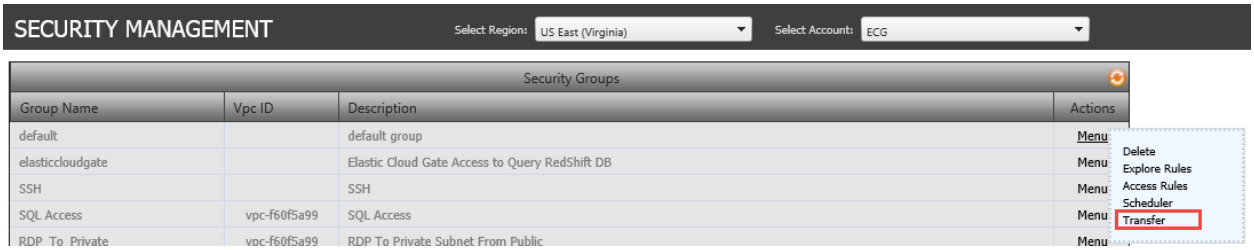


If you need to grant access to users who might try to connect from a different IP address, or if the IP address is unknown, use a more advanced scheduler – to learn more, see the previous topic How to temporarily open AWS Security Groups rules for dynamic IP

How to transfer security group to another AWS region

To transfer security group to another AWS region from the Main Menu, select Security Management.

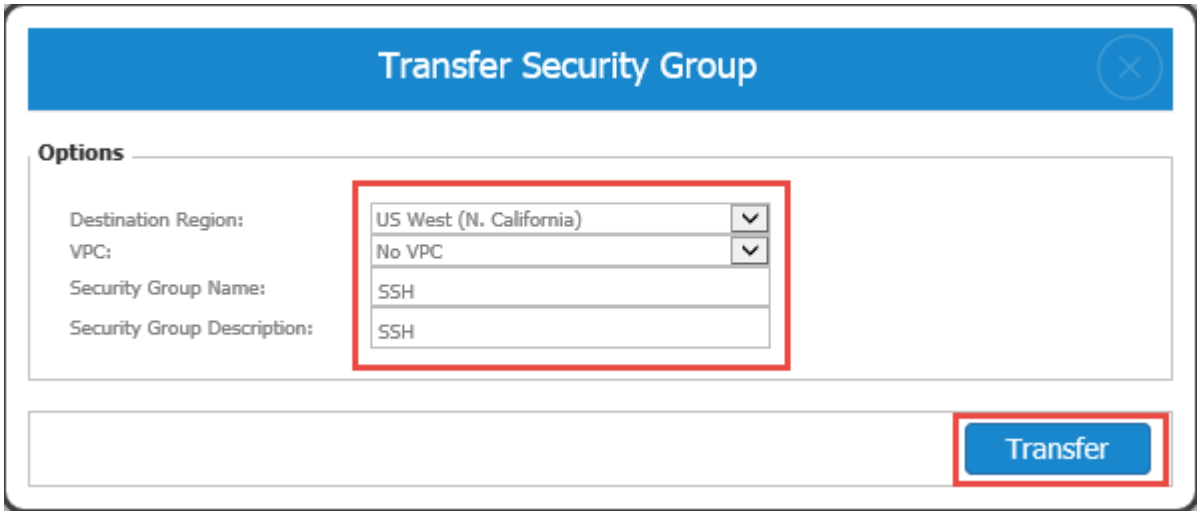
Under the Security Group list from the context menu, click Transfer.



From the new window select the following:

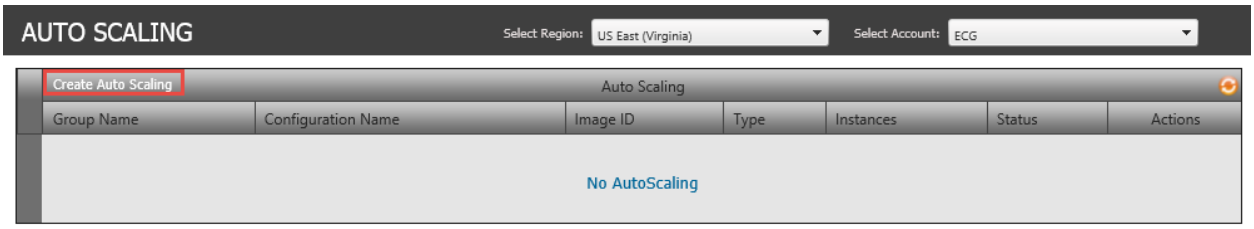
- Destination region
- VPC – To create security group outside VPC, select No VPC from the list; otherwise select VPC ID where you want to transfer security group
- Enter security group name and description

Click Transfer to recreate security group with all rules in destination region.



Auto Scaling overview

Auto Scaling allows you to scale your Amazon EC2 capacity up or down automatically, according to conditions you define. With Auto Scaling, you can ensure that the number of Amazon EC2 Instances you are using increases seamlessly during demand spikes to maintain performance, and decreases automatically during demand lulls to minimize costs. Auto scaling is particularly well suited for applications that experience hourly, daily, or weekly variability in usage.



With Auto Scaling, you can plan to configure your Auto Scaling Group to automatically scale or maintain your application. You can configure three types of plans:

Maintain a Fixed Number of Running EC2 Instances

Use this scaling plan if you would like Auto Scaling to maintain the minimum number of Instances in your Auto Scaling group at all times. You can manually change the number of running Instances in your Auto Scaling group at any time.

Scale Based on Demand

Use this scaling plan to scale dynamically in response to changes in the demand for your application. When you scale based on demand, you must specify when and how to scale using CloudWatch metrics, such as CPU or Network usage, or metrics related to Simple Queue Service.

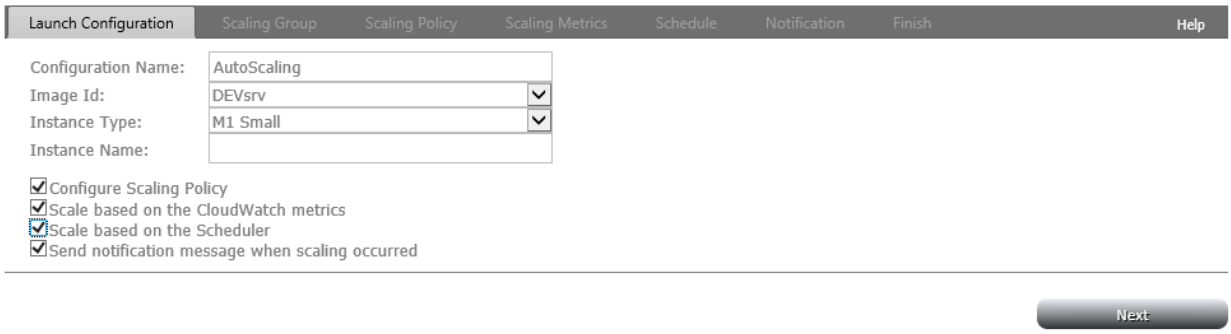
Scale Based on a Schedule

Use this scaling plan if you want to scale your application on a pre-defined schedule. You can specify the schedule for scaling one time only, or provide details for scaling on a recurring schedule.

Using Elastic Cloud Gate Auto Scaling Wizard, you can configure any of these options.

This section walks you through each tab of our wizard, explains each option, and explains what dependencies are between options.

Launch Configuration



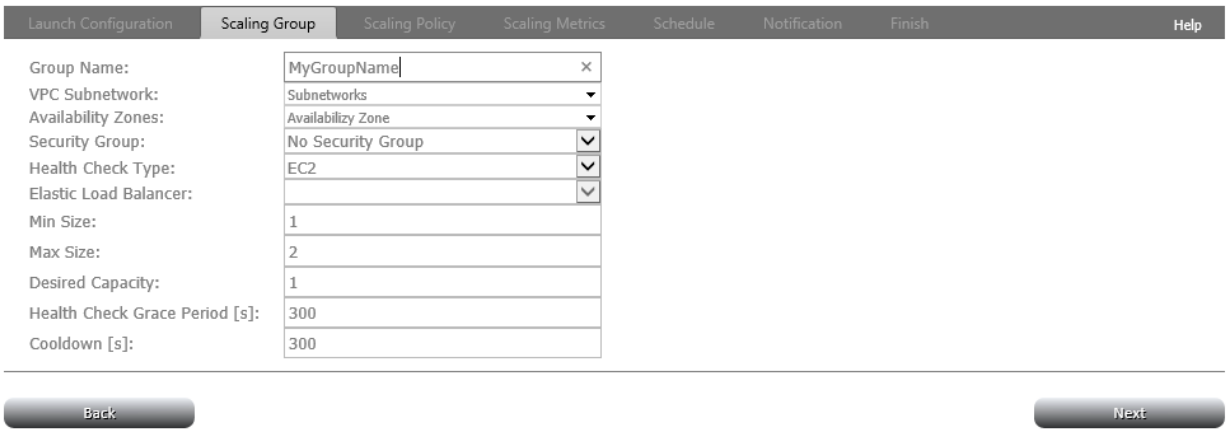
Configuration Name [required]: The name of the launch configuration

Image ID [required]: Unique ID of the Amazon Machine Image (AMI) you want to use to launch your EC2 Instances inside Auto Scaling

Instance Type [required]: The type of the Instance launch inside Auto Scaling

Instance Name [optional]: When specified, each new Instance launch in Auto Scaling is automatically assigned a tag name

Scaling Group



Group Name [required]: The name of the scaling group

VPC Subnetwork [required/optional]: List of the VPC subnetwork you prefer auto scaling to launch Instances. Either subnetwork(s) or availability zone(s) need to be specified.

Availability Zones [required/optional]: List of availability zones you prefer auto scaling to launch Instances.

Security Group [optional]: Security group associated with Instances in Auto Scaling group.

Health Check Type [required]: The type of the service used to check the health of the Instances. The allowed values can be either EC2 or ELB. When ELB is selected, you must specify the name of the Elastic Load Balancer which checks the health of Instances. Default value is EC2.

Elastic Load Balancer [optional]: The name of the Elastic Load Balancer. This property is required when Health Check Type is set to ELB.

Minimum Size [required]: The minimum count of Instances to run inside the Auto Scaling group. This value can be overwritten by Desire Capacity (see below).

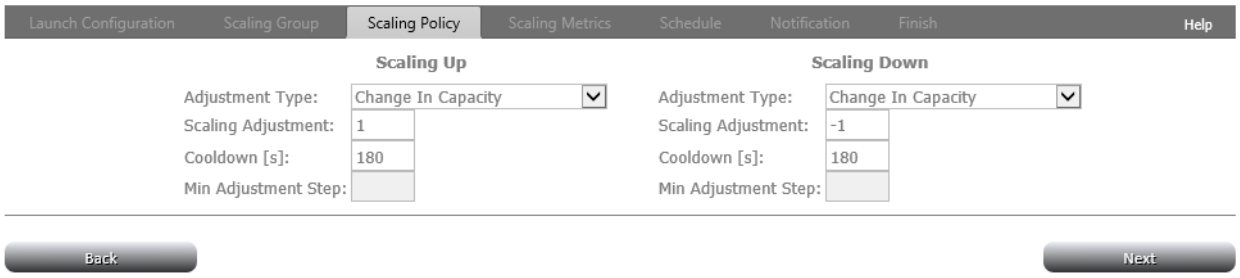
Maximum Size [required]: The maximum count of Instances created inside the Auto Scaling group. This is properly applicable when you use schedule based on demand.

Desired Capacity [optional]: The number of Amazon EC2 Instances running in the group. The desired capacity must be greater than or equal to the minimum size and less than or equal to the maximum size specified for the Auto Scaling group. When specified, it is the total number of Instances launched right after creating Auto Scaling group.

Health Check/Grace Period [optional]: Length of time (in seconds) after new Amazon EC2 Instance comes into service that Auto Scaling starts checking its health. During this time, any health check failure for that Instance is ignored. Default value is 300 seconds.

Cooldown [optional]: The amount of time (in seconds) between a successful scaling activity and the succeeding scaling activity. Default value is 300 seconds.

Scaling Policy



When Auto Scaling is used to scale on demand, you must define how to scale in response to changing conditions. For example, you have a web application that currently runs on two Instances: you want to launch two additional Instances when the load on the running Instances reaches 70 percent, and you want to terminate the additional Instances when the load goes down to 40 percent. You can configure your Auto Scaling group to automatically scale up and then scale down by specifying these conditions.

An Auto Scaling group uses a combination of policies and alarms to determine when the specified conditions for launching and terminating Instances are met. An alarm is an object that watches over a single metric (for example, the average CPU utilization of your EC2 Instances in an Auto Scaling group, or length of the queue in SQS) over a time period you specify. When the value of the metric breaches the thresholds you define, over a number of time periods you specify, the alarm performs one or more actions. An action can be sending messages to Auto Scaling. A policy is a set of instructions for Auto Scaling that tells the service how to respond to alarm messages.

Along with creating a launch configuration and Auto Scaling group, you need to create the alarms and the scaling policies and associate them with your Auto Scaling group. When the alarm sends the message, Auto Scaling executes the associated policy on your Auto Scaling group to scale the group in (that is, to terminate Instances) or scale the group out (that is, to launch Instances).

Adjustment Type [required]: Indicates whether the ScalingAdjustment is an absolute value, a constant increment, or a percentage of the current capacity.

ChangeInCapacity:

Use this to increase or decrease existing capacity. For example, the current capacity of your Auto Scaling group is set to three Instances: you then create a scaling policy on your Auto Scaling group, specify the type as ChangeInCapacity, and the adjustment as five. When the policy is executed, Auto Scaling adds five more Instances to your Auto Scaling group. You'll then have eight running Instances in your Auto Scaling group: current capacity (3) plus ChangeInCapacity (5) equals (8).

ExactCapacity:

Use this to change the current capacity of your Auto Scaling group to the exact value specified. For example, the capacity of your Auto Scaling group is set to five Instances. You then create a scaling policy on your Auto Scaling group, specify the type as ExactCapacity, and the adjustment as three. When the policy is executed, your Auto Scaling group has three running Instances. You'll get an error if you specify a negative adjustment value for the ExactCapacity adjustment type.

PercentChangeInCapacity:

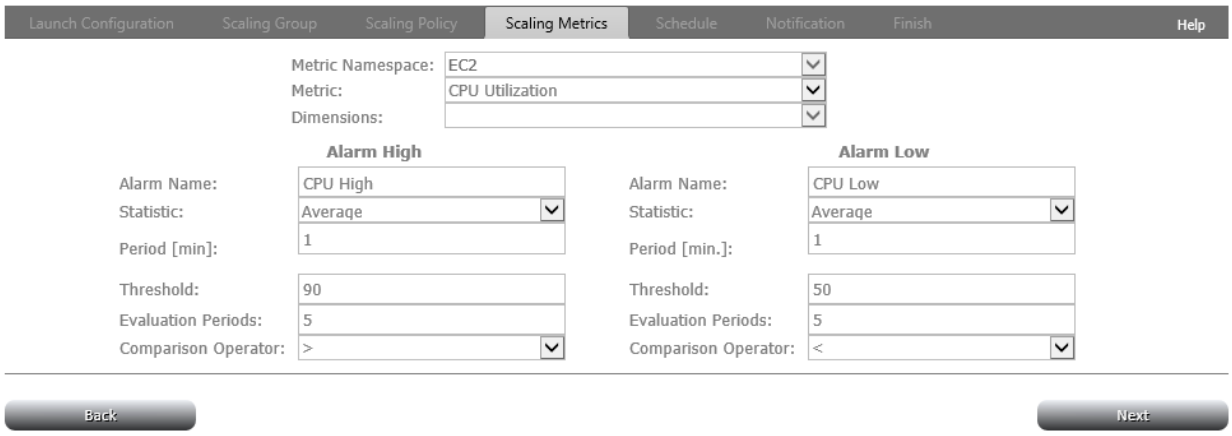
Use this to increase or decrease the desired capacity by a percentage of the desired capacity. For example, the desired capacity of your Auto Scaling group is set to ten Instances. You then create a scaling policy on your Auto Scaling group, specify the type as PercentChangeInCapacity, and the adjustment as ten. When the policy is executed, your Auto Scaling group has eleven running Instances, because 10 percent of 10 Instances is 1 Instance, and 1 Instance plus 10 Instances equals 11 Instances.

Scaling Adjustment [required]: The number of Instances by which to scale. AdjustmentType determines the interpretation of this number (e.g. as an absolute number or as a percentage of the existing Auto Scaling group size). A positive increment adds to the current capacity and a negative value removes from the current capacity.

Cooldown [optional]: The amount of time, in seconds, after a scaling activity completes before the next scaling activity begins. Default value 300 seconds.

Minimum Adjustment Step [optional]: Used with AdjustmentType with the value. PercentChangeInCapacity, the scaling policy changes the DesiredCapacity of the Auto Scaling group by at least the number of Instances specified in the value.

Metrics



Metric Namespace [required]:
Select EC2 to scale based on EC2 metrics, like CPU or Network usage.
Select SQS to scale based on the Simple Queue Service metrics, like number of sent Messages or size of sent message.

Metric [required]: Metric used for auto scaling.

Dimension [optional/required]: Active only when the SQS namespace is selected. It allows you to select a queue name to which the metric applies.

Alarm Name [required]: The name of the alarm.

Statistic [required]: The statistic to apply to the alarm's associated metric.

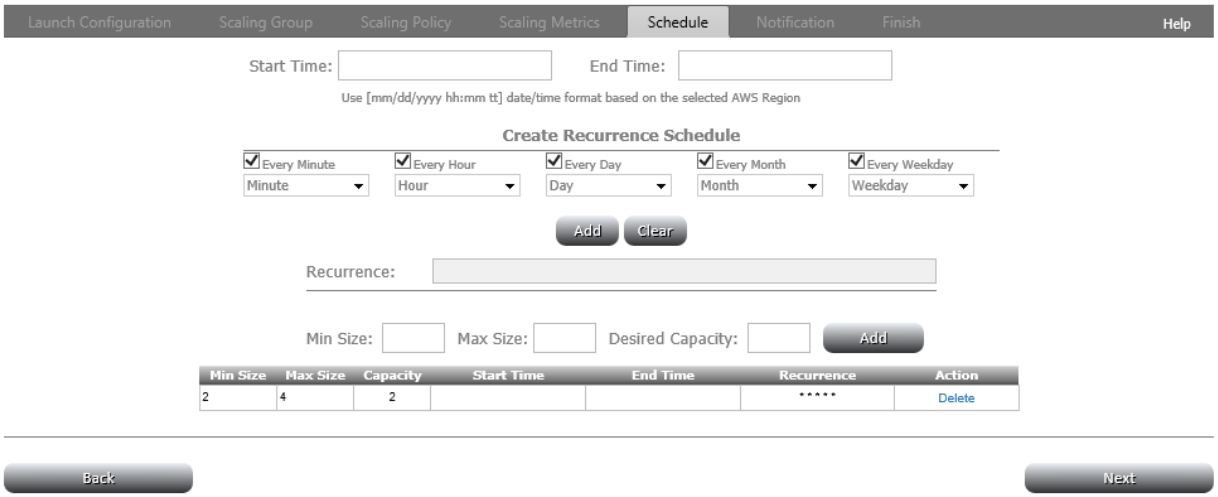
Period [required]: The period in seconds over which the specified statistic is applied. The value must be a multiply of 60. The total (Period * Evaluation Period) cannot be greater than 86400. In our wizard we use minutes instead of seconds, so the maximum combined value cannot be greater than 1440.

Threshold [required]: The value against which the specified statistic is compared.

Evaluation Period [required]: The number of periods over which data is compared to the specified threshold. The total (Period * Evaluation Period) cannot be greater than 86400.

Comparison Operator [required]: The arithmetic operation to use when comparing the specified Statistic and Threshold. The specified Statistic value is used as the first operator.

Scaling Schedule



Scaling based on a schedule allows you to scale your application in response to predictable load changes. For example, every week the traffic to your web application starts to increase on Wednesday, remains high on Thursday, and starts to decrease on Friday. You can plan your scaling activities based on the predictable traffic patterns of your web application.

To configure your Auto Scaling group to scale based on a schedule, you need to create scheduled actions. A scheduled action tells Auto Scaling to perform a scaling action at a certain time in the future. To create a scheduled scaling action, you specify the start time for the scaling action to take effect, and you specify the new minimum, maximum, and desired size you want for that group at that time. At the specified time, Auto Scaling updates the group to set the new values for minimum, maximum, and desired sizes, as specified by your scaling action. In addition, instead of using start time you can use a recurrent schedule that changes Auto Scaling options on the regular bases. E.g. assuming that the traffic to your website decreases on weekends, you can schedule two recurrent occurrences where first increases capacity on each Monday, and second decreases capacity on each Friday.

Start Time [required/optional]: The time when the scaling action occurs.

End Time [required/optional]: The time when the scaling action ends. This value applies only when Recurrence is also set, otherwise it is skipped.

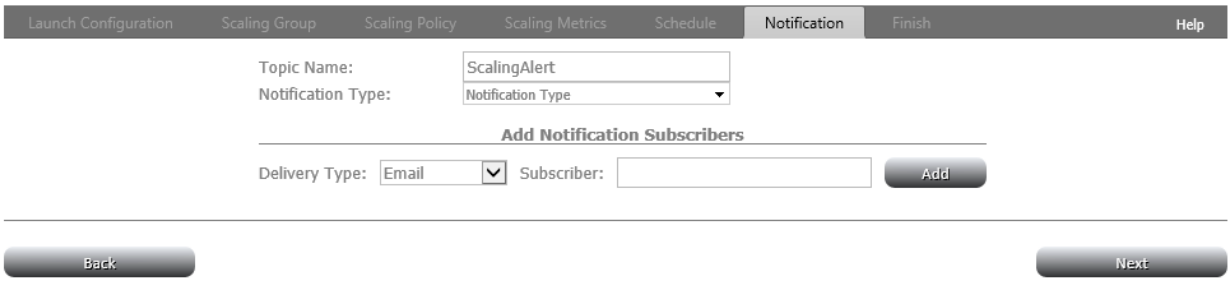
Recurrence [required/optional]: The time when recurring future actions start. When Start Time and End Time are specified with Recurrence, they form the boundaries of when the recurring action starts and stops.

Minimum Size [required]: The minimum count of Instances running inside the Auto Scaling group. This value can be overwritten** by Desire Capacity (see below).

Maximum Size [required]: The maximum count of Instances that might be created inside the Auto Scaling group.

Desired Capacity [optional]: The number of Amazon EC2 Instances running in the group. The desired capacity must be greater than or equal to the minimum size and less than or equal to the maximum size specified for the Auto Scaling group. When specified, that is the total number of Instances launched right after creating Auto Scaling group.

Notification



Topic Name [required]: Name of the topic.

Notification Type [required]: A list of Auto Scaling notification types, which are events that cause the notification to be sent. The following table lists the available notification types:

Notification Type Events:

EC2_INSTANCE_LAUNCH	Successful Instance launch by Auto Scaling
EC2_INSTANCE_LAUNCH_ERROR	Failed Instance launch by Auto Scaling
EC2_INSTANCE_TERMINATE	Successful Instance termination by Auto Scaling
EC2_INSTANCE_TERMINATE_ERROR	Failed Instance termination by Auto Scaling

Delivery Type [required]:
EMAIL – Notification is delivered via email
SMS – Notification is delivered via SMS (SMS delivery is available only in the US East Region)

Subscriber [required]: Either email address or phone number (for SMS delivery) where the message is sent; the SMS can only be delivered to US phone numbers

Finish

On the last tab of our wizard is the summary of your configuration of Auto Scaling.

From this point on, you can either create auto scaling or generate CloudFormation script.

Keep in mind that CloudFormation has a couple of limitations:
CloudFormation is not supporting schedule.
In scaling policy, CloudFormation is not supporting Minimum Adjustment Step.

How to setup and manage Disaster Recovery

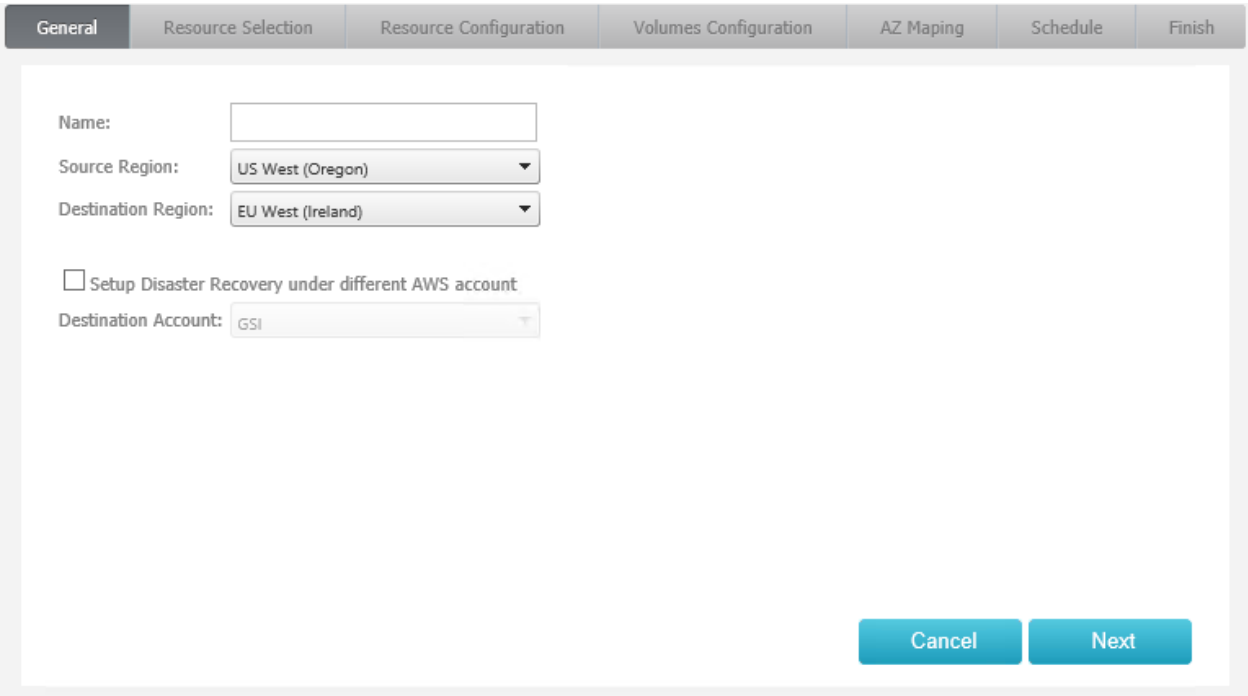
Our Disaster Recovery section gives you an option to setup and manage some aspects of the Disaster Recovery scenarios described in the AWS Disaster Recovery Overview article.

Using our wizard for Disaster Recovery, you are able to make setup across AWS Regions as well as across AWS Accounts.

Using our wizard, you are able to select source and destination regions and accounts as well as instances you want to replicate to Disaster Recovery region. Additionally, you receive options to define the Disaster Recovery parameters for each resource.

Let us review the options available under Disaster Recovery wizard step by step:

General Tab



Name – Name of your Disaster Recovery setup; the name must be unique across all of your DRs under the same account

Source Region – AWS region to replicate resources from

Destination Region – AWS region that is setup as the Disaster Recovery region; it is the region where selected resource from source region is replicated to

Setup Disaster Recovery under different AWS account – Check this option to transfer your AWS EC2 resources to different AWS account

Destination Account – AWS account you want to setup/transfer EC2 resources to.

Resource Selection Tab

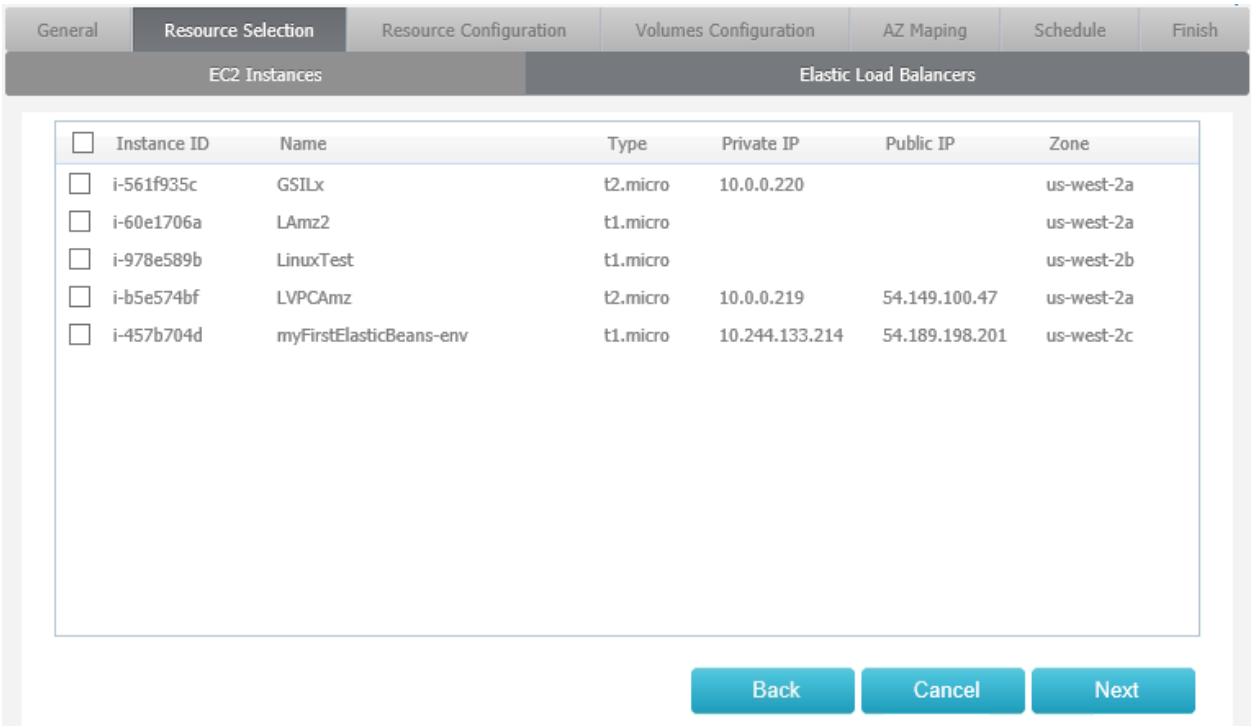
The Resource Selection tab lists all Instances and Elastic Load Balancers currently accessible in source region. You can select any Instance you want to replicate to Disaster Recovery region. Also, you can select Elastic Load Balancer you want to setup in DR region.

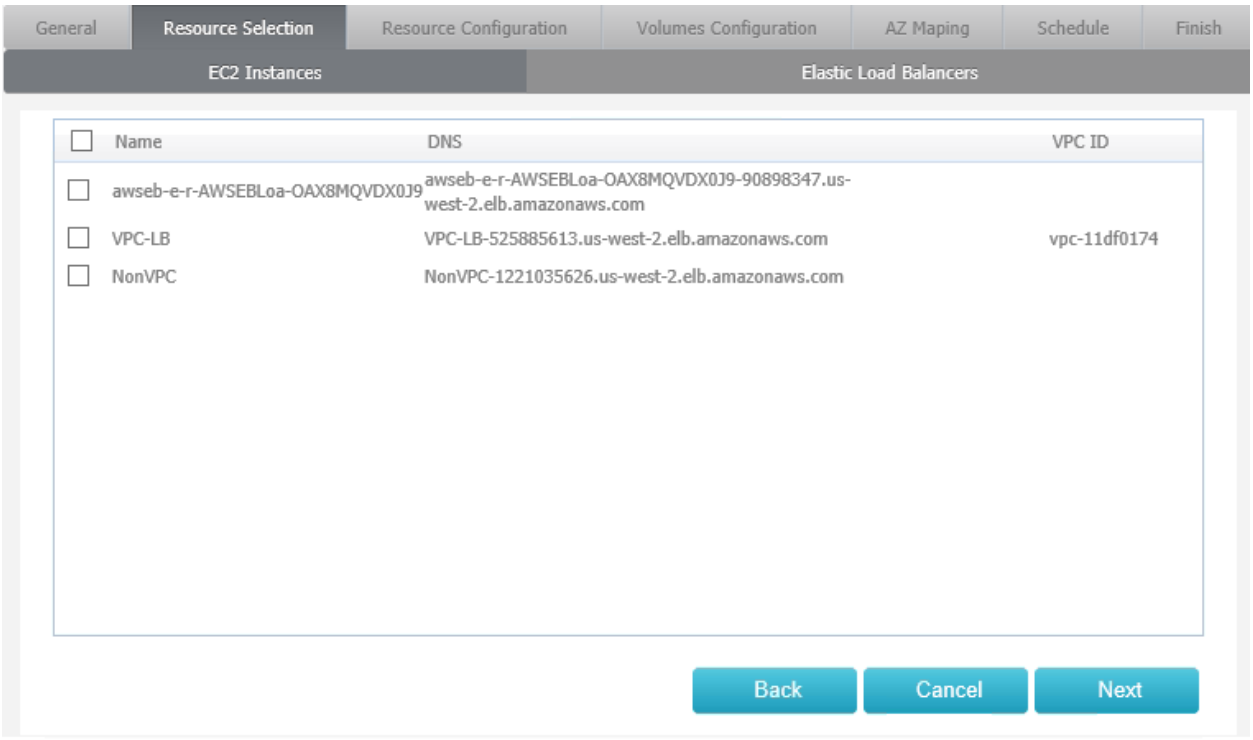
When you select ELB, you have to select at least one Instance which is currently attached to that ELB. (This option applies only to ELB, which has already attached instance(s)).

Notes:

For ELB while using SSL, all certificates need to be manually copied and setup in destination Disaster Recovery region.

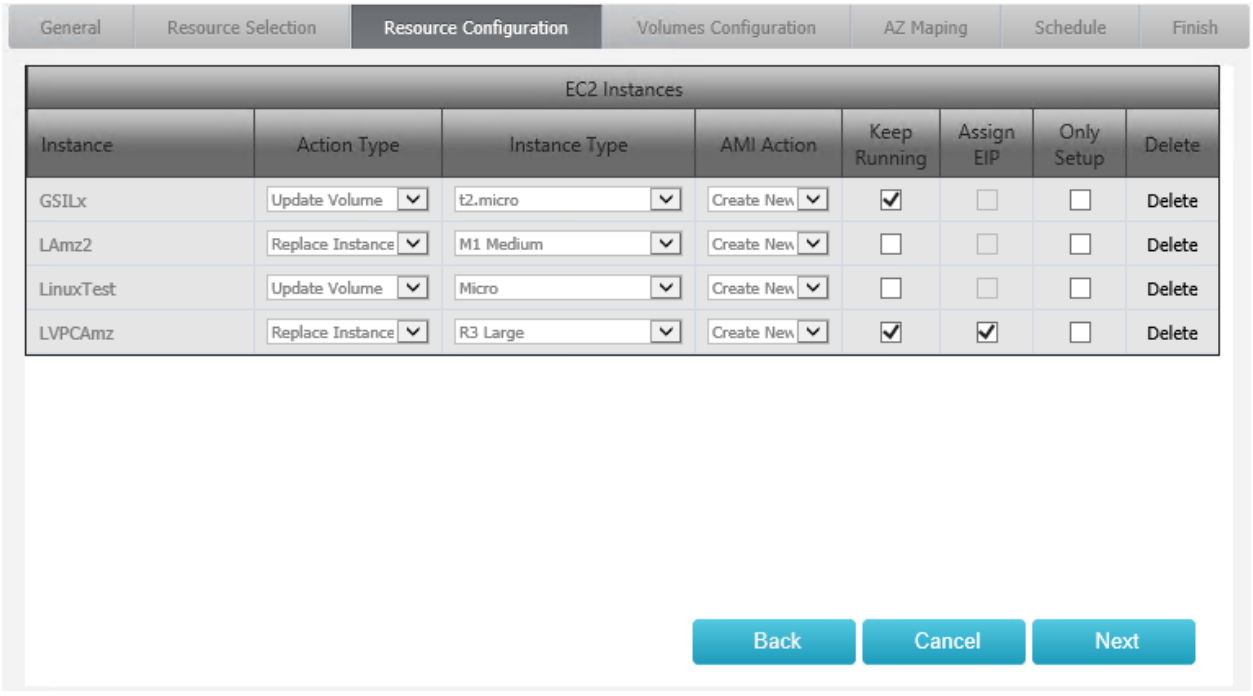
Most attributes of the Instances from source region are replicated to the destination region including: Security Groups, Local IP, Source Destination Check, and Sub-networks; along with all VPC parameters, such as Subnets, Route Tables, Internet Gateway, and DHCP Options.





Resource Configuration Tab

The resource configuration tab allows you to specify disaster recovery option for each Instance selected on previous tab.



Options that can be setup for each Instance include:

Instance Name – Identification of the Instance selected on the previous tab (not editable)

Action Type – There are three possible options to select:

-Only Copy: Initial Setup Action: this option creates AMI of the Instance from the source region and copies it over to the destination region. The new Instance is not launched from that AMI. There are additional options available for this type of replication described later in this document.
Scheduler Action: create and copy a new AMI image of the source Instance to the destination region. Deregister previous AMI image in destination region.

-Replace Instance: Initial Setup Action: this option creates the source Instance, copies it to the destination region, and launches a new Instance based on that image. The additional actions can be taken after Instance launch (if applicable), such as: register under ELB, assign EIP, stop Instance.
Scheduler Action: the process is similar to the one in initial setup with additional steps. Before the new Instance is launched, the old one will be terminated.
 if the replacing Instance was attached to ELB or was setup as NAT server, then load balancer or route table will be updated adequately.

-Update Volume: Initial Setup Action: the initial action is the same as in the Replace Instance option.
Scheduler Action: the snapshot of the volume is taken and copied over to the destination region. The old volume attached to the Instance in destination region is detached and deleted. The newly copied snapshot is converted into volume and attached to the Instance.

Instance Type – this option lets you specify the type of the EC2 Instance in destination region. The new Instance can have different size from source Instance.

AMI Action – there are two options available:
- New: this option triggers creation of new image of the source Instance and copies it to destination region.
- AMI ID: if the image of the selected Instance was already copied to the destination region, you can skip creation of the new image and use one in Disaster Recovery region.

Keep Running – this option allows you to specify if the Instance after launch is supposed to be running or be shutdown.

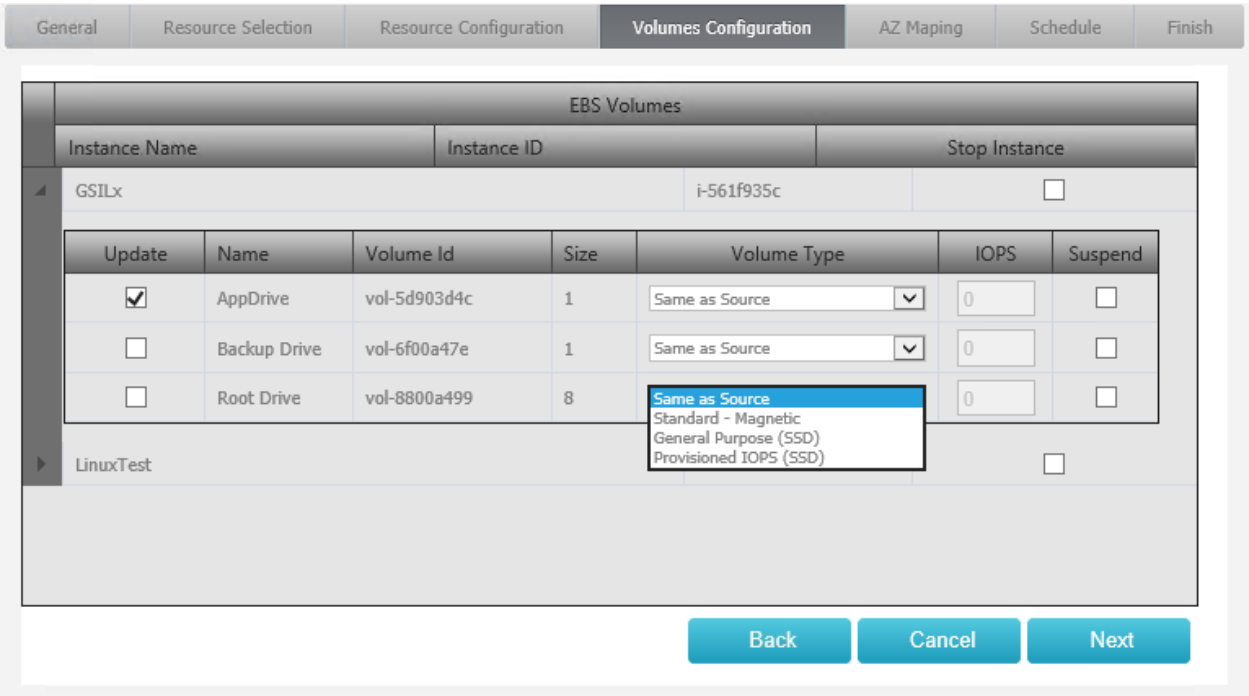
Allocate EIP – when this option is checked off, the new Elastic IP is allocated and associated with the newly launched Instance. This option is active only when selected Instance in the source region has associated EIP.

Only Setup – this option lets you specify whether the selected Instance is created only during initial disaster recovery setup or should also be updated based on the scheduler.

Delete – this option lets you delete the Instance from the list. When you edit existing setup, this option does not cause deletion of the Instance in destination region, but does remove it from scheduler list.

Volumes Configuration Tab

The volume configuration tab is active only when at least one of the Instances on previous tab has been selected as an Update Volume action type.



Instance Name – Name of the selected Instance.

Instance ID – ID of the selected Instance.

Stop Instance – This option lets you specify if you want to stop Instance before the old volume is replaced with the new one. This option should be checked when the selected volume(s) contain database or other data used by any application where sudden loss of access to hard drive could cause potential issue. When the root drive is selected (/dev/sda1) the Instance must be stopped regardless of the chosen options.

Click the arrow on the right to expand the list of the volumes attached to the given Instance.

Update – When checked, volume in Disaster Recovery region is updated based on the schedule.

Name – Name or drive path of the volume.

Volume ID – ID of the volume.

Size – Size of the volume.

Volume Type – This option lets you choose what type of EBS volume is restored during scheduled update process.

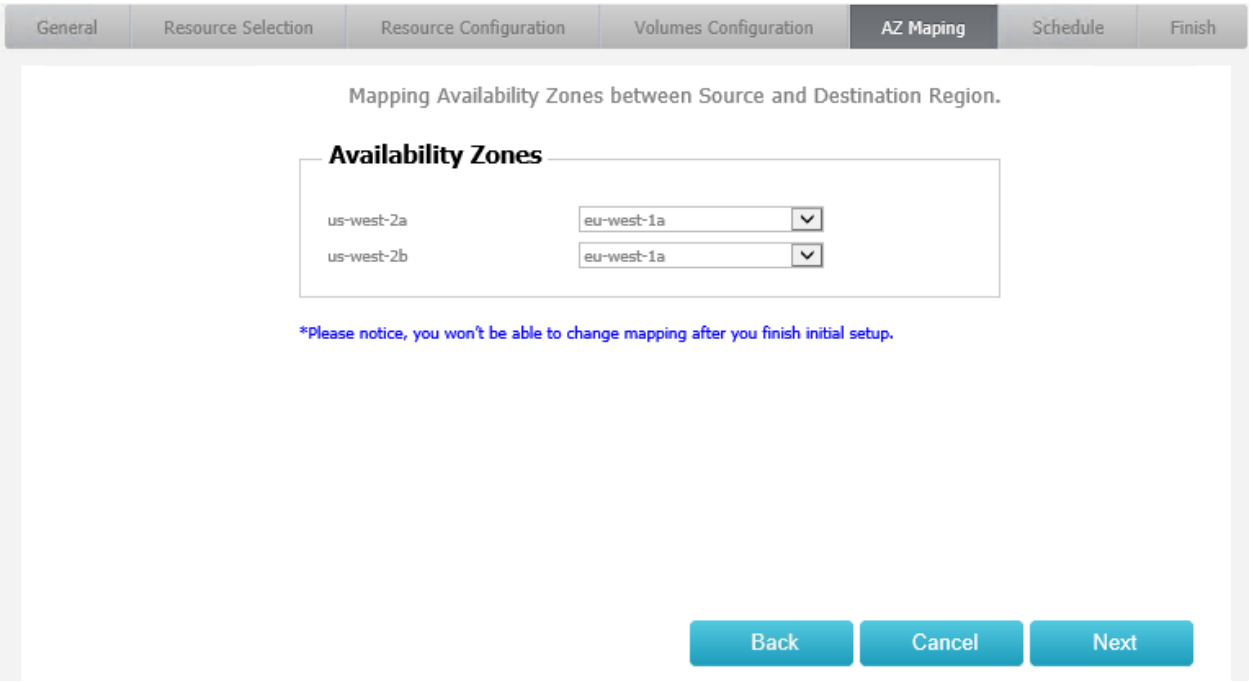
IOPS – Allows specification of new IOPS of the EBS volume. This option is active only when the selected Volume Type is Provisioned IOPS.

Suspend – This option lets you suspend scheduled update of the EBS volume.

Note: for each Instance you must check at least one volume, otherwise the wizard won't let you continue to the next step.

AZ Mapping Tab

Availability Zone mapping tab provides you an option to map zones from source region to the destination region. This feature is helpful when your source resources are spread between multiple availability zones.



Schedule Tab

The Schedule tab allows you to setup interval of how frequently you want to update your resources in Disaster Recovery region.

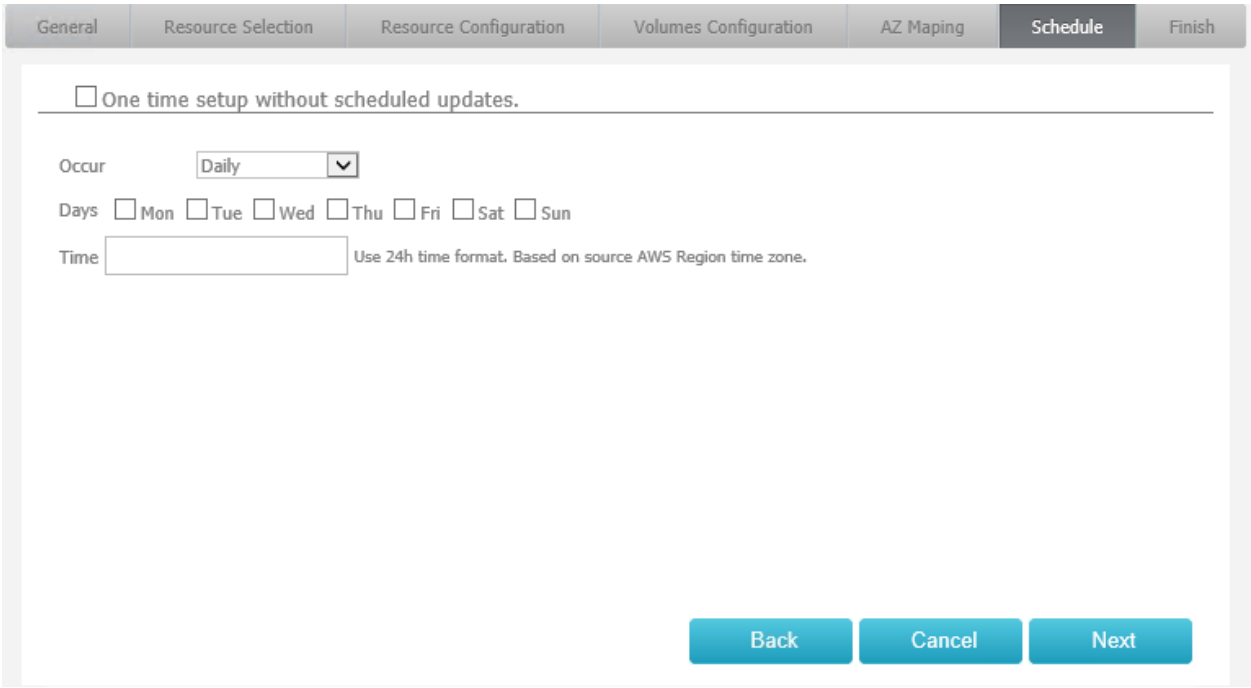
If you are planning to setup or transfer your EC2 resources as a one-time process, you can skip schedule by checking the Don't use scheduler to update Disaster Recovery resources on regular basis option.

Occur – This option allows you to select occurrence of the updates: choose Hourly, Daily, or Monthly frequency. Each of the occurrences has additional options described below:

Hourly:
Occurs Every x Hours: specify the interval of occurrence in hours
Starting At and Ending At: specify the time range when the update should take place, or leave blank for 24h range period

Daily:
Days: select days on which the update occurs
Time: select time at which the update occurs

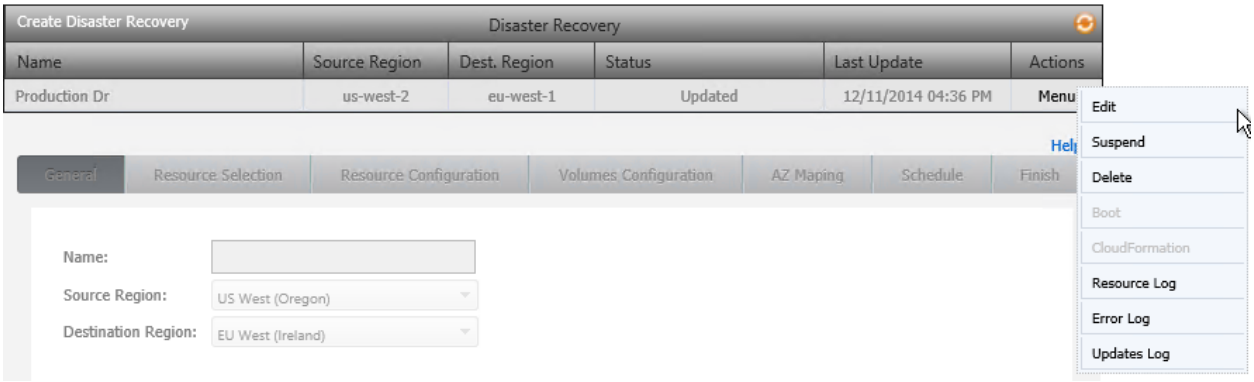
Monthly:
Occurs Every x Day of the Month: the update occurs once a month on the specified day of the month
Time: time when the update occurs



Finish Tab

After clicking the Finish button, the new setup is created. The process of initial setup of the disaster recovery region starts within 5 minutes after completion of the wizard. You cannot modify any options of your Disaster Recovery plan until the initial setup is finished.

All Disaster Recovery plans are listed above the wizard. You can track progress of the setup by refreshing the list.



For each Disaster Recovery plan, you can execute the following options:
Edit – this option allows you to change some of the parameters of the previously setup Disaster Recovery plan
Suspend/Resume – this option allows you to suspend or resume the scheduler
Delete – delete existing Disaster Recovery plan; this option does not delete any resources in destination region
Boot – this option launches Instances marked as Only Copy under Disaster Recovery plan
CloudFormation – this option outputs the CloudFormation script with setup of all Instances marked as Only Copy
Resource Log – show mapping between source and destination objects
Error Log – show list of errors during setup or update
Updates Log – show list of objects that were updated based on the schedule

Note:
Both Boot and CloudFormation options are available only if at least one Instance was marked as Only Copy on configuration tab in the wizard.
When you use Cloud Formation script, there is not an option to attach new Instance to Elastic Load Balancer.
Also, in both cases the route table is not updated even if the created Instance serves as the NAT server.

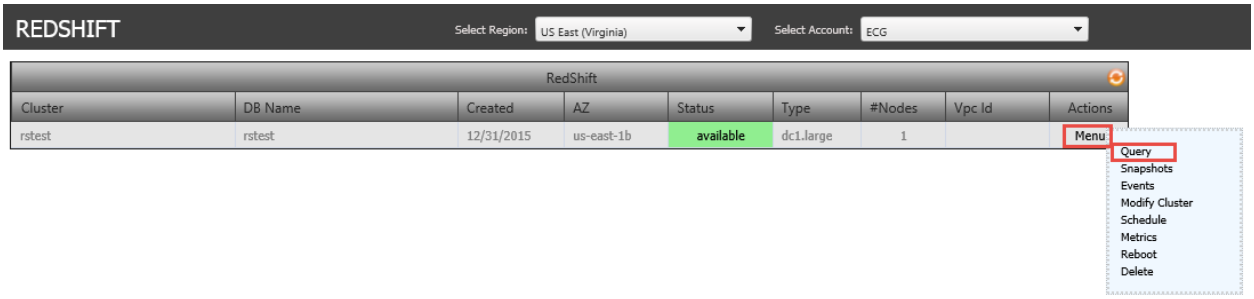
General Note:

Despite Disaster Recovery plan setup for each Instance, whenever at least one of them is inside VPC, then the entire VPC is recreated in destination region with the same attributes.

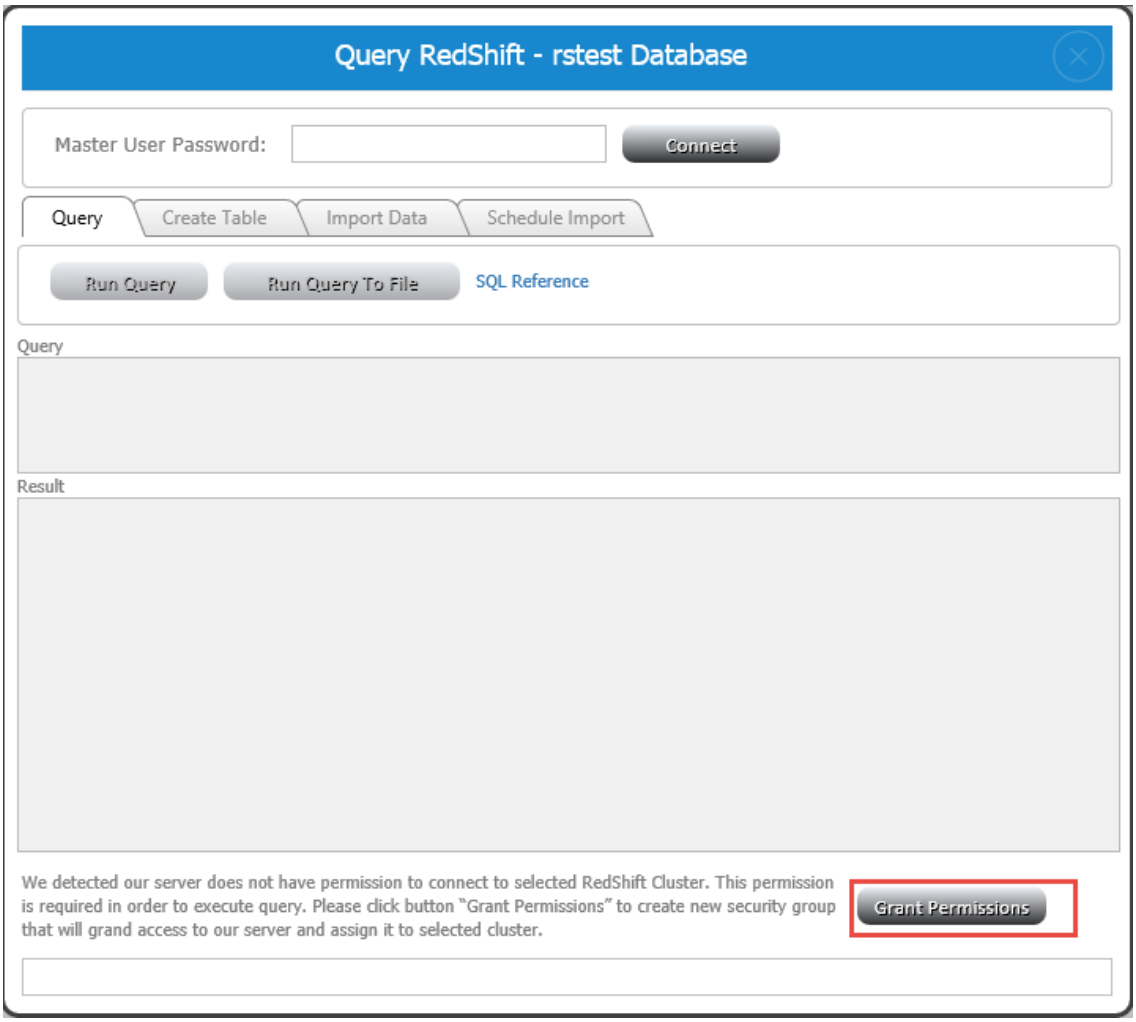
Each Elastic Load Balancer selected in the wizard is automatically recreated in the destination region. If ELB is using SSL connection, all certificates need to be manually setup under the new ELB.

How to manage RedShift data

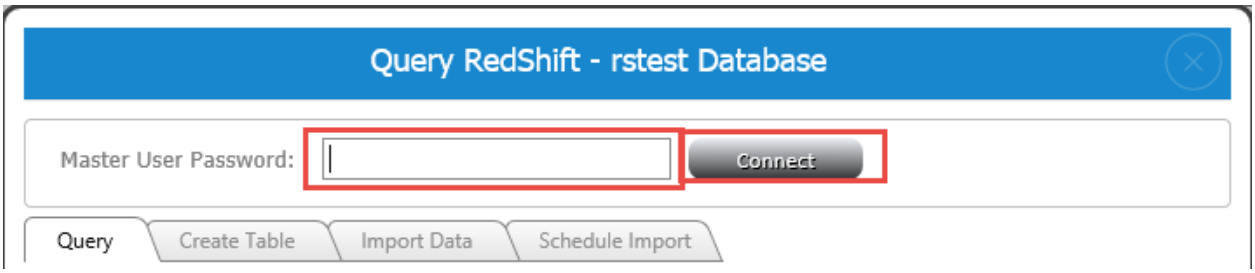
To query AWS RedShift database from the Main Menu, select RedShift.
Under the RedShift section from the context menu, select Query.



If this is the first time you query RedShift from ECG portal, a message is visible at the bottom of the Query window stating you have to grant permission to our system in order to execute the query. To grant permission, click Grant Permissions button.

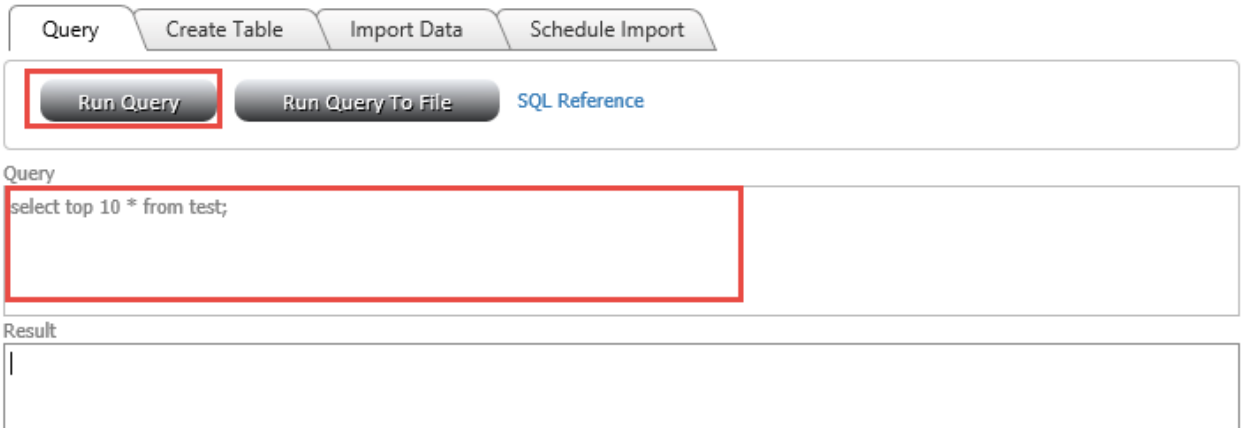


Enter the master user password and click Connect.



Query

To query RedShift database, switch to the Query tab.
Under the Query text box, enter you query statement and click Run Query.



The result is outputted to the Result panel below. Regardless of your query, only the first 1000 records are outputted to the result window.

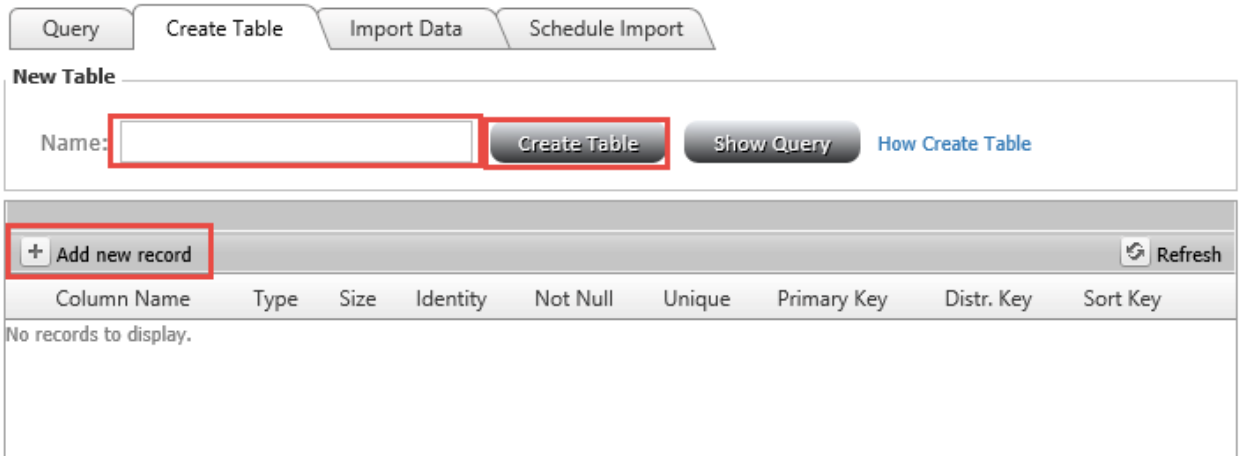
Additionally, you can export results to csv file by clicking Run Query To File; when you export results to file, all records are exported.

Create RedShift Table

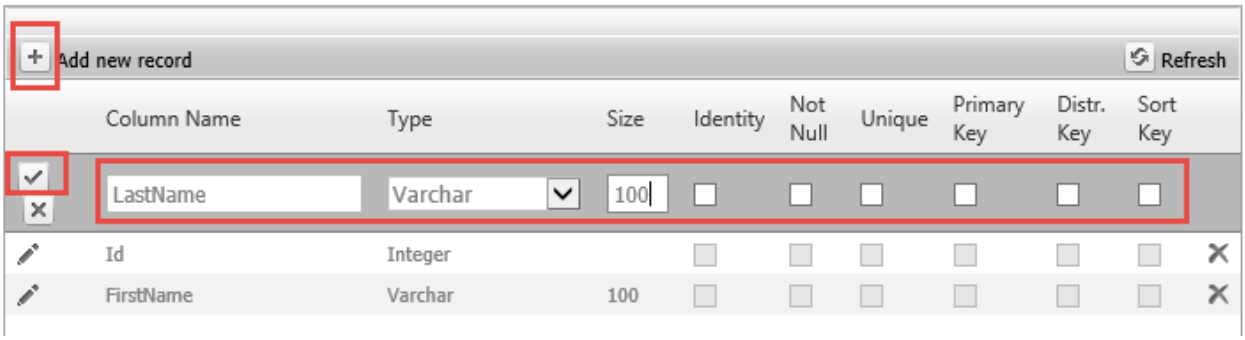
To create new table, switch to the Create Table tab.
Enter table name.
To add a column to the table:
- Click Add new record
- Enter column name
- Select column type
- Select other column property
- Click Insert from the left side, or Cancel to disregard column

Repeat these steps for all columns you want to add.

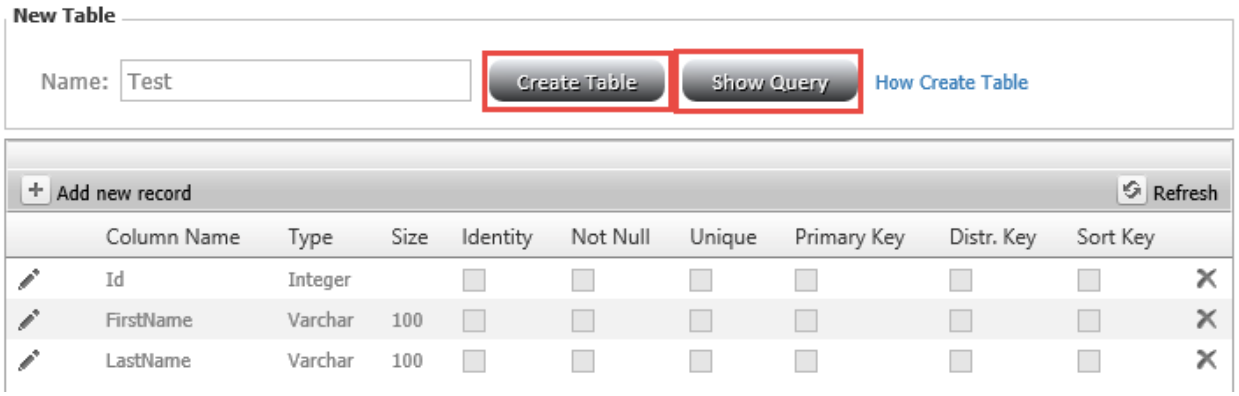
When finished, click Create Table.



If you get an error or you have to modify the column, click Edit (from the first column) or Delete (from the last column).



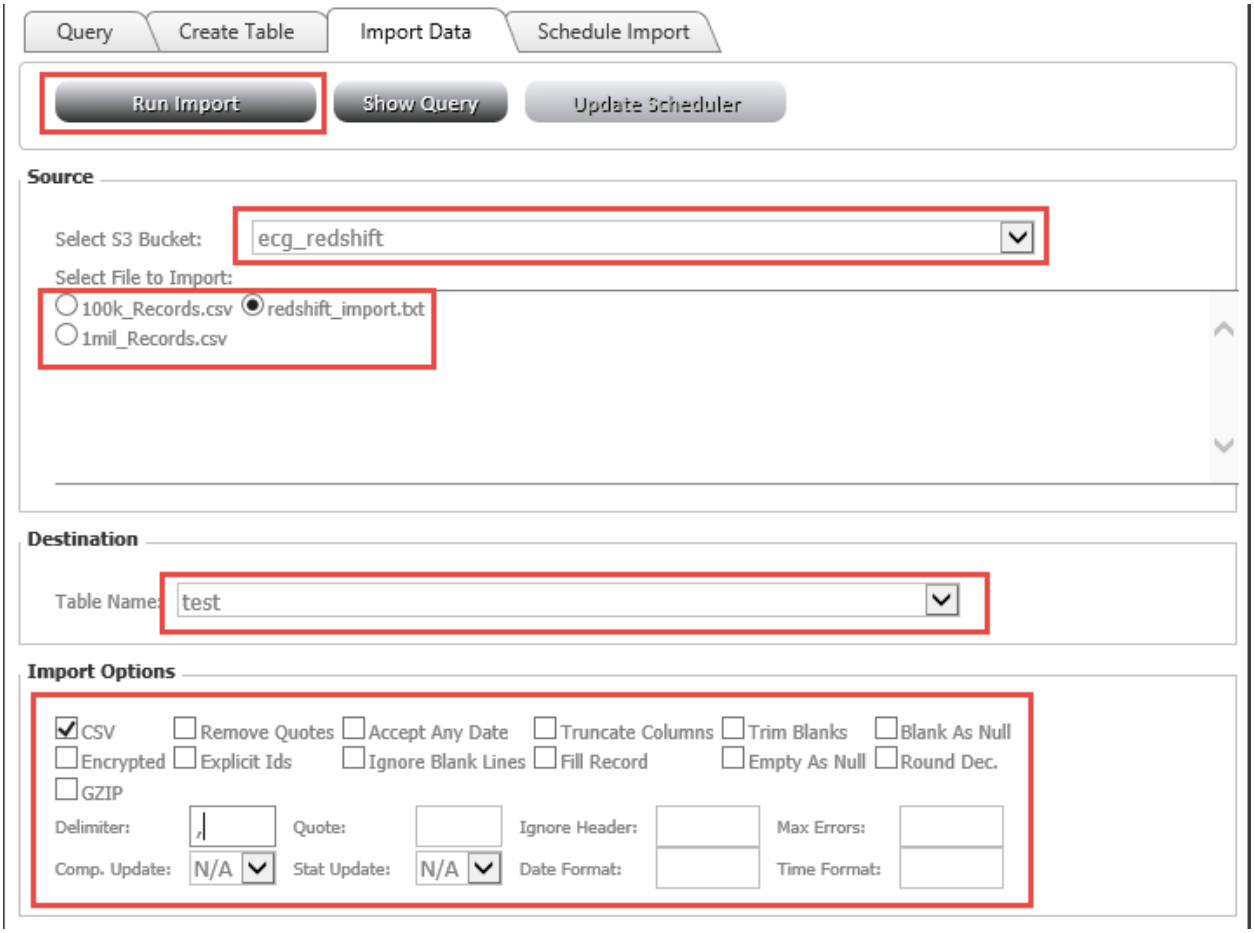
Also, you can see the query used to create the table by clicking Show Query.



Import Data to RedShift

Data can be imported from the file located in S3 bucket.

To import data to the RedShift table, switch to the Import Data tab.



From the drop down list, select S3 Bucket where the import file is located.
Select file to import.

Select table you want to import data to.

Select configure import options, if necessary.

Click Run Import.

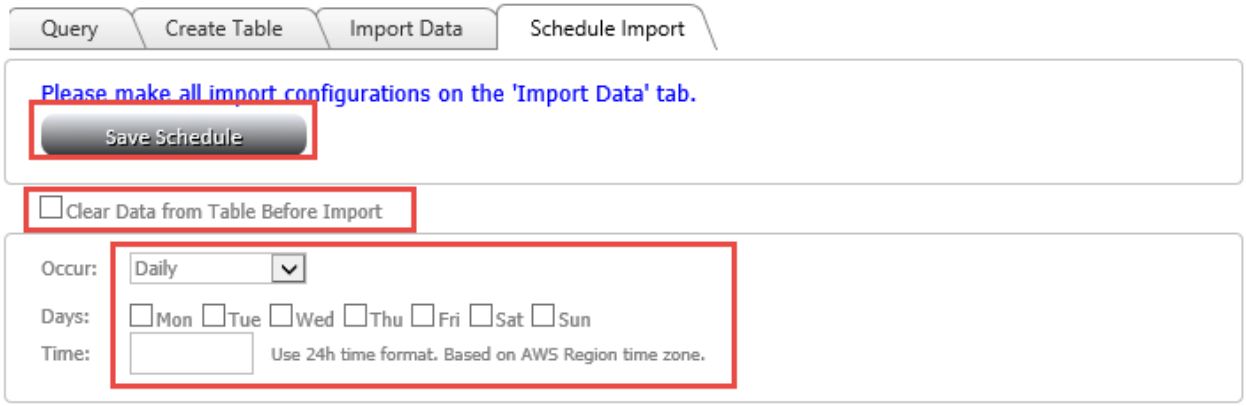
You can also see the import query by clicking Show Query.

Schedule Import

You can schedule imports to be executed on regular basis.
To schedule import, make all configurations under the Import Data tab and switch to the Schedule Import tab.

If you want to clear all data from the table before import, check Clear Data from Table Before Import.

Select occurrence of the import (e.g. Daily).
Select days and time.
Click Save Scheduler.

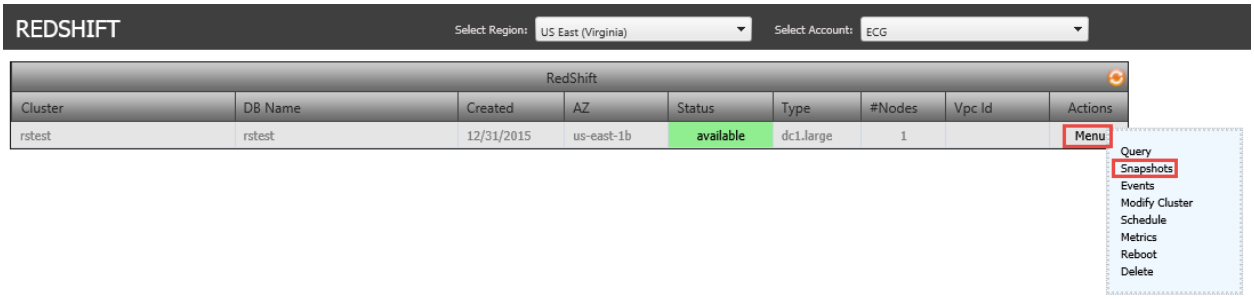


At any time you can edit, delete, or suspend schedule by clicking th appropriate action from the scheduler table.

Additionally, you can see the query that is executed by scheduler by clicking Query from the scheduler table.

How to review RedShift snapshots

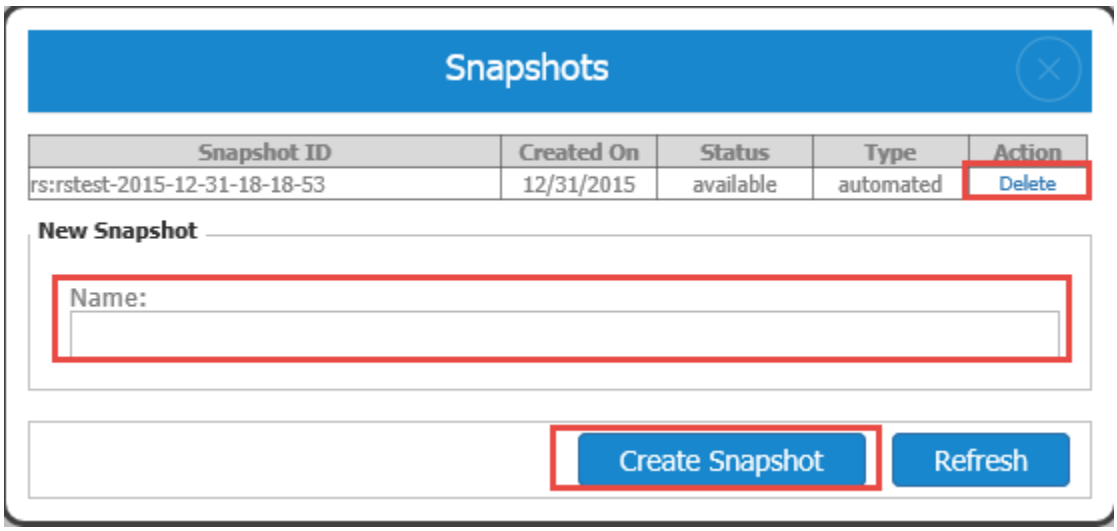
To manage snapshot from the Main Menu, select RedShift.
Under the RedShift section from the context menu, select Snapshots.



A list of all snapshots created from selected RedShift is visible.

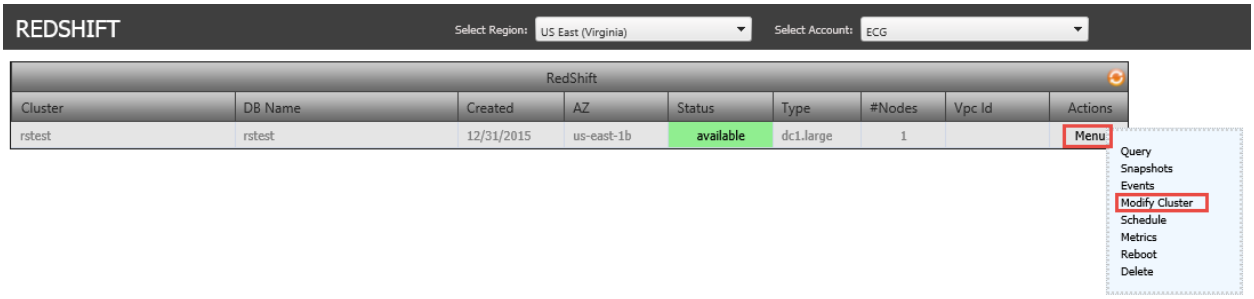
To delete snapshot, click Delete from the last column.

To create new snapshot, enter snapshot name and click Create Snapshot.

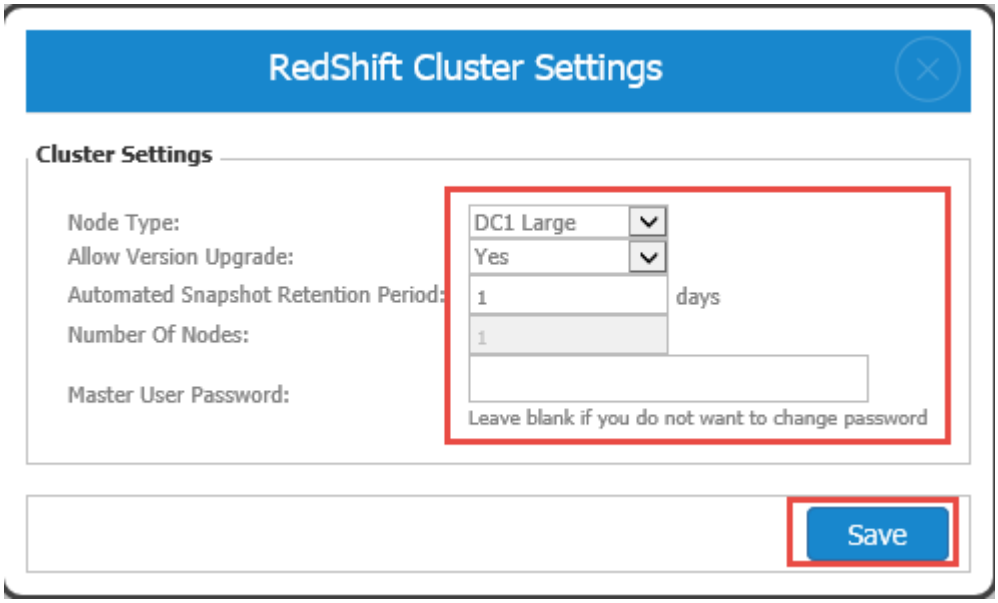


How to modify RedShift cluster

To modify some cluster settings, go to the RedShift section and from the context menu, click Modify Cluster.



Make any necessary changes and click Save.



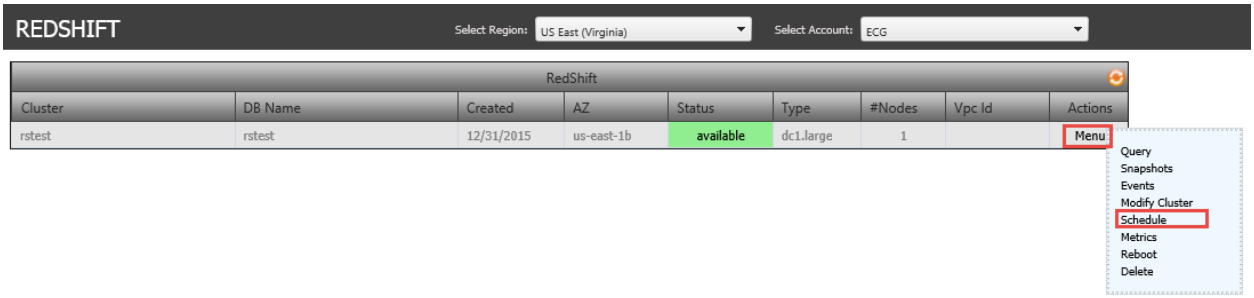
RedShift Scheduler

RedShift scheduler allows you to schedule certain actions, including:

- Take snapshot
- Modify cluster settings
- Shut down cluster
- Restore cluster from backup

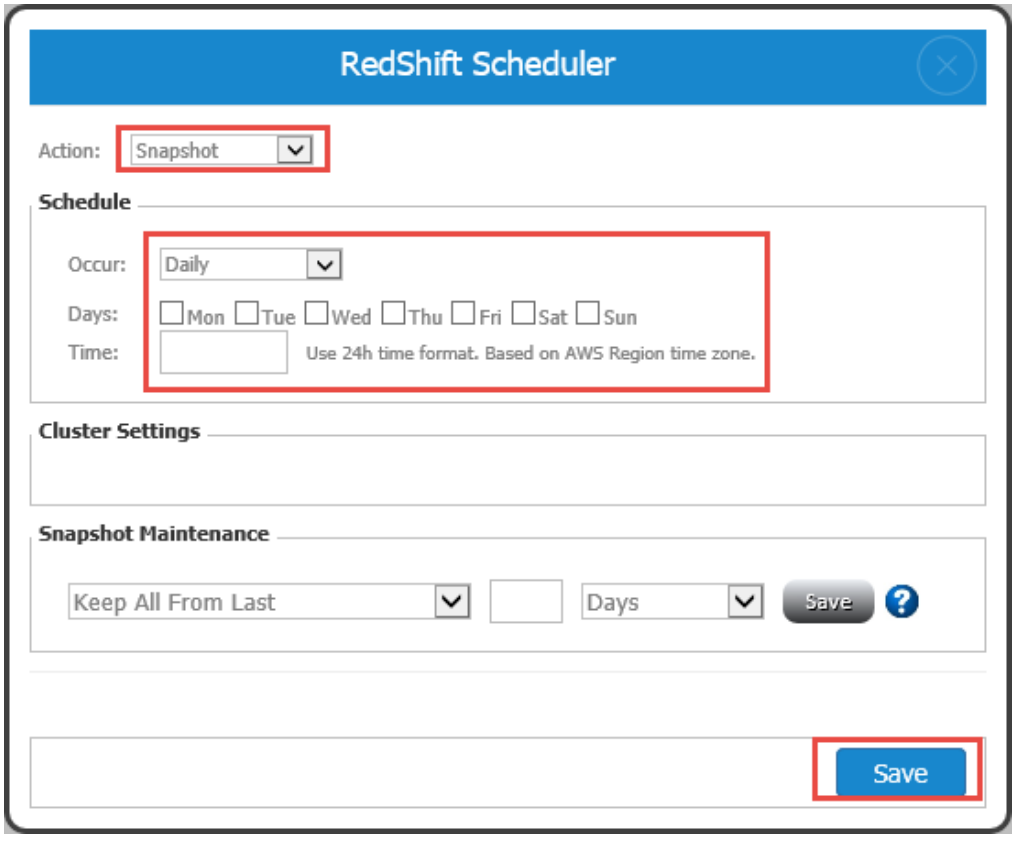
These are executed on a scheduled basis.

To schedule any of these actions go to the RedShift section, and from the context menu select Schedule.



Under scheduler windows, select the action you want to execute.

Under the Schedule section, select when the action should be executed.

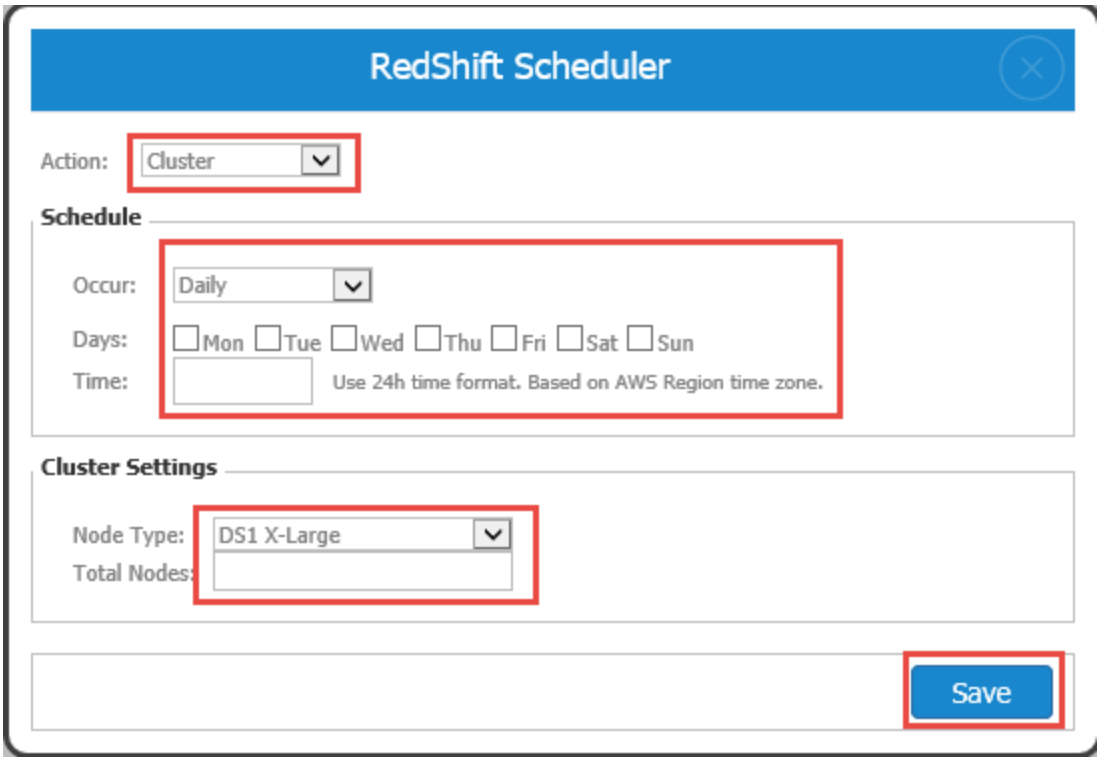


Schedule Snapshot

When you schedule snapshot, you have the option to schedule maintenance that can be used to remove old snapshots based on the selected criteria.

Schedule Cluster

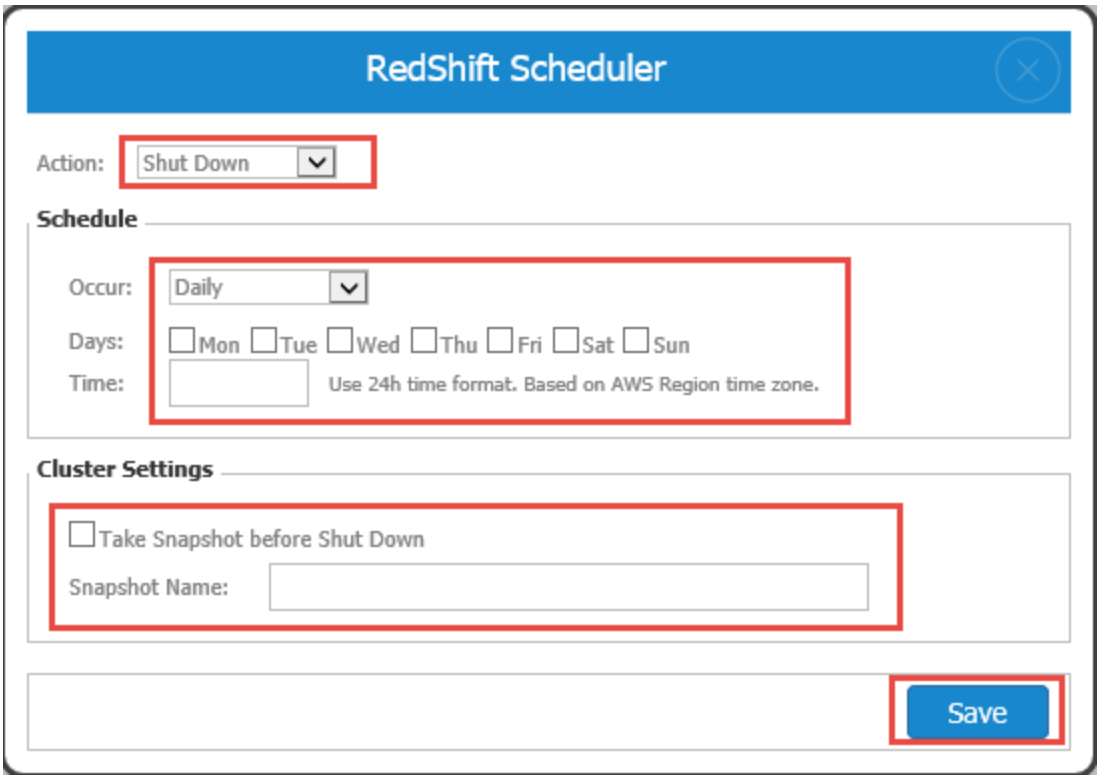
Cluster scheduler gives you the option to modify node type as well as total nodes.
Using this scheduler, you are able to change the processing power of your cluster based on needs (e.g. more power during days and less during nights or weekends).



Schedule Shut Down Cluster

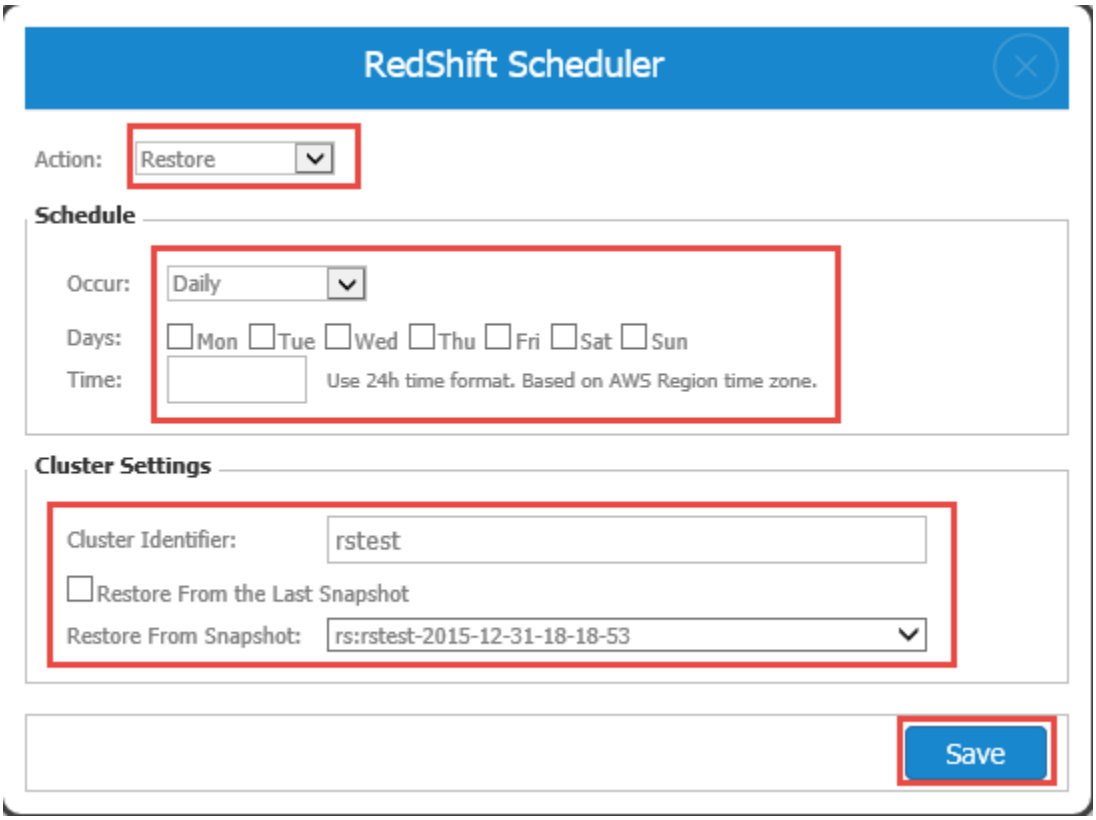
When you schedule shut down of the RedShift cluster, you have an option to create snapshot before RedShift is terminated.
To do this, check Take Snapshot before Shut Down and enter snapshot name.

This option is useful if you plan to schedule shut down and restore for the same cluster.



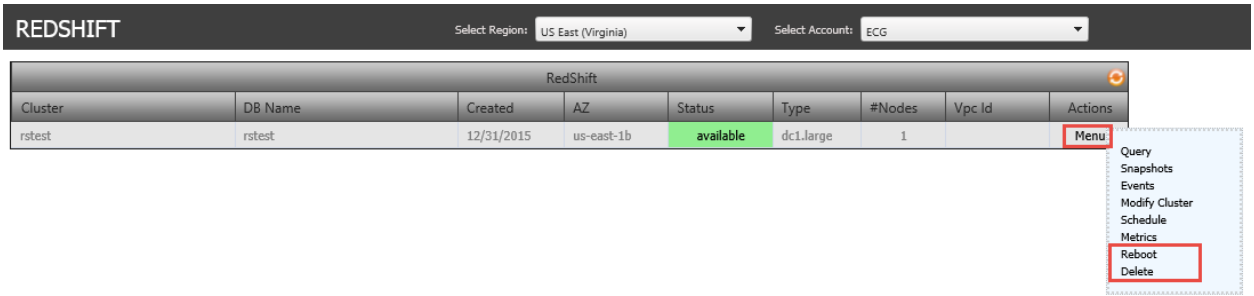
Schedule Restore Cluster

When you schedule restore cluster, you have to provide cluster name (identifier) as well as which snapshot the cluster should be restored from.
You can choose one of your existing snapshots, or restore cluster from the latest snapshot. To restore from the latest snapshot, check “Restore From the Last Snapshot”.



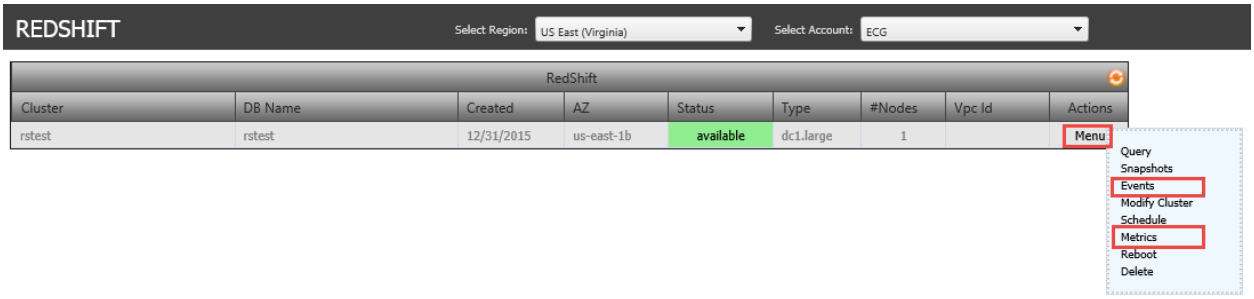
How to reboot or delete RedShift cluster

To reboot or delete RedShift cluster, go to the RedShift section and from the context menu, select Reboot or Delete.

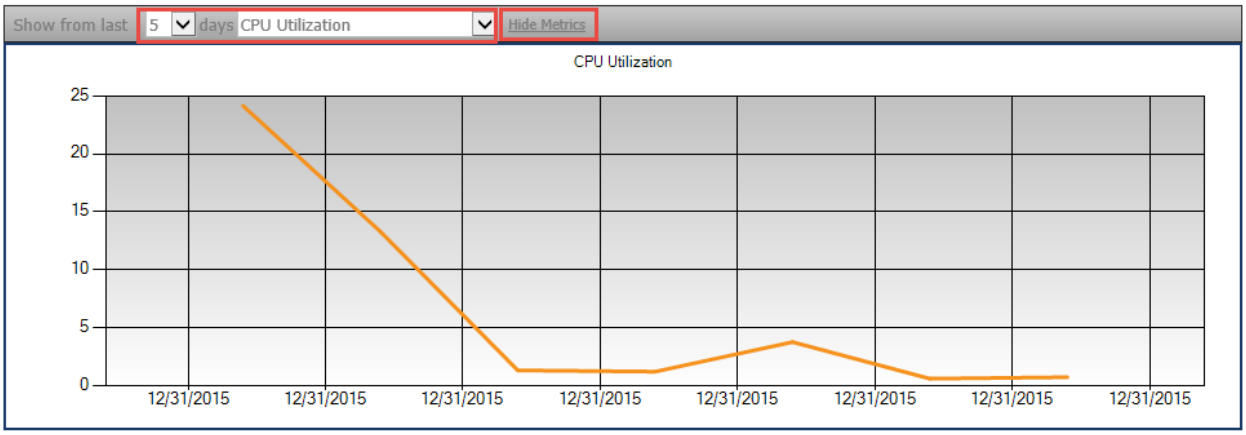


Review RedShift events and metrics

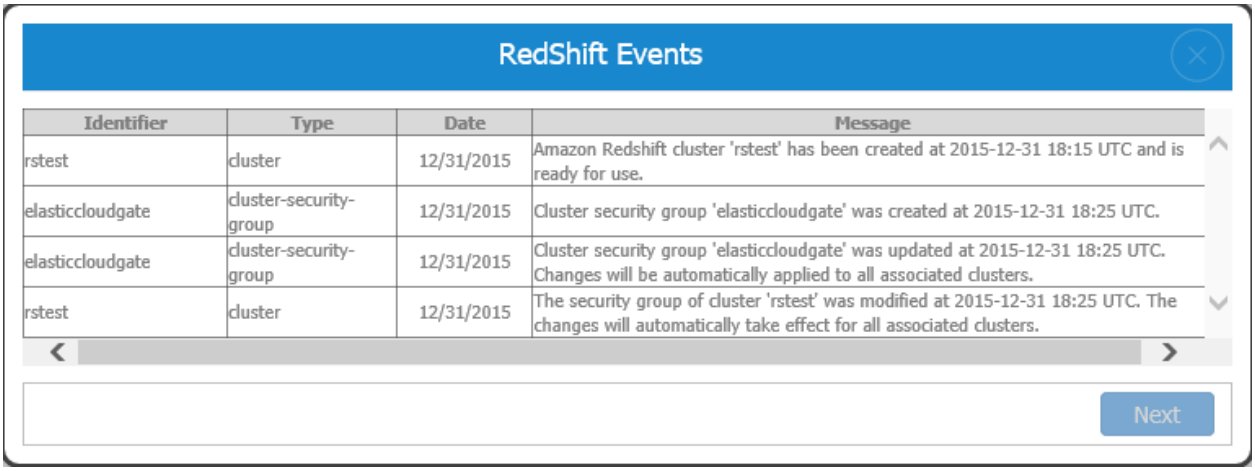
To review RedShift events or metrics, go to the RedShift section and from the context menu select Event or Metrics.



Under the Metric chart, you have options to select the period you want to see data from, as well as select the metric you want to see.



To close the metrics chart, click Hide Metrics.



Review CloudTrail

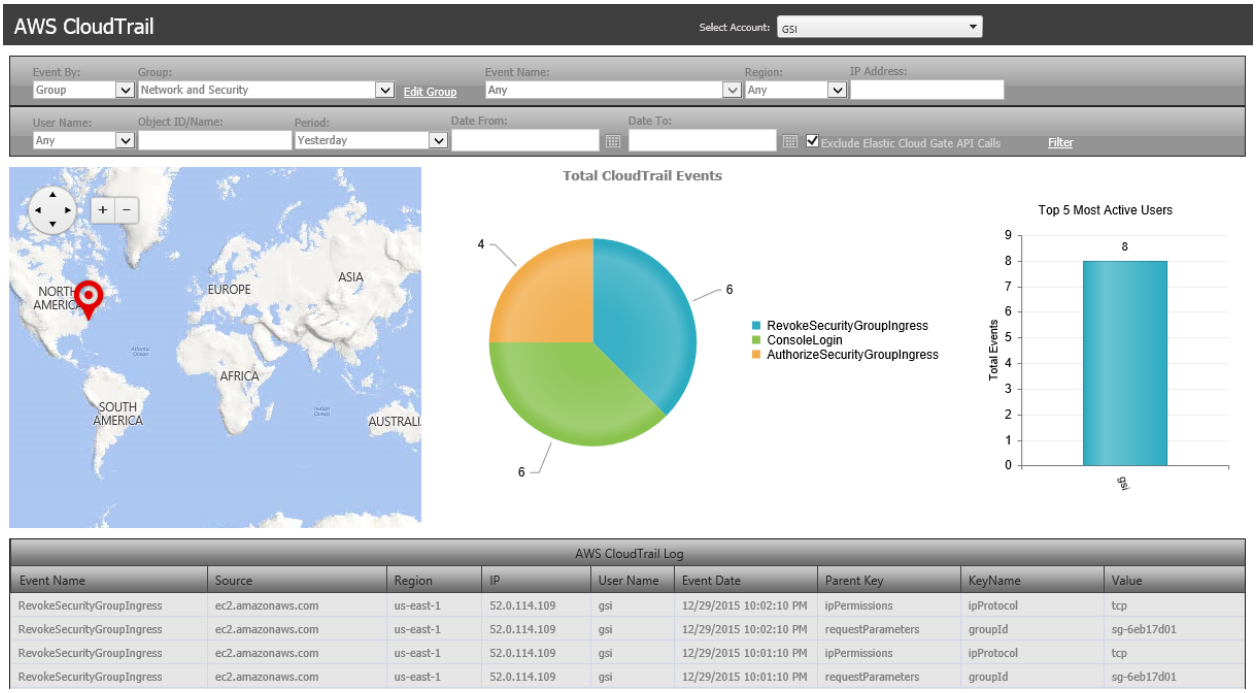
CloudTrail is a web service which effectively records AWS API calls for an account, as well as delivers log files directly to you when needed. AWS CloudTrail records the identity and IP address of the API caller, the time of the API call, the request parameters, and the response elements returned by the AWS Service.

Before you are able to review your CloudTrail logs, first you must turn on AWS as well as activate our portal under Account Management. To learn more, go to:

[How to add or manage AWS](#) Account

To review you CloudTrail log from the Main Menu, select CloudTrail.

On the CloudTrail page is information from the current day, including:
A visual map representation of the origin of the API calls, total calls per event, as well as 5 most active users.



On the bottom table are the details of CloudTrail calls.

To search CloudTrail log for specific information, use the filters on the top panel.
Simply specify you filter criteria and click Filter.

Most of the filter options are self-explanatory, however the first three require additional attention
Event By – This defines whether data is filtered by event name (Name) or by groups (Group)

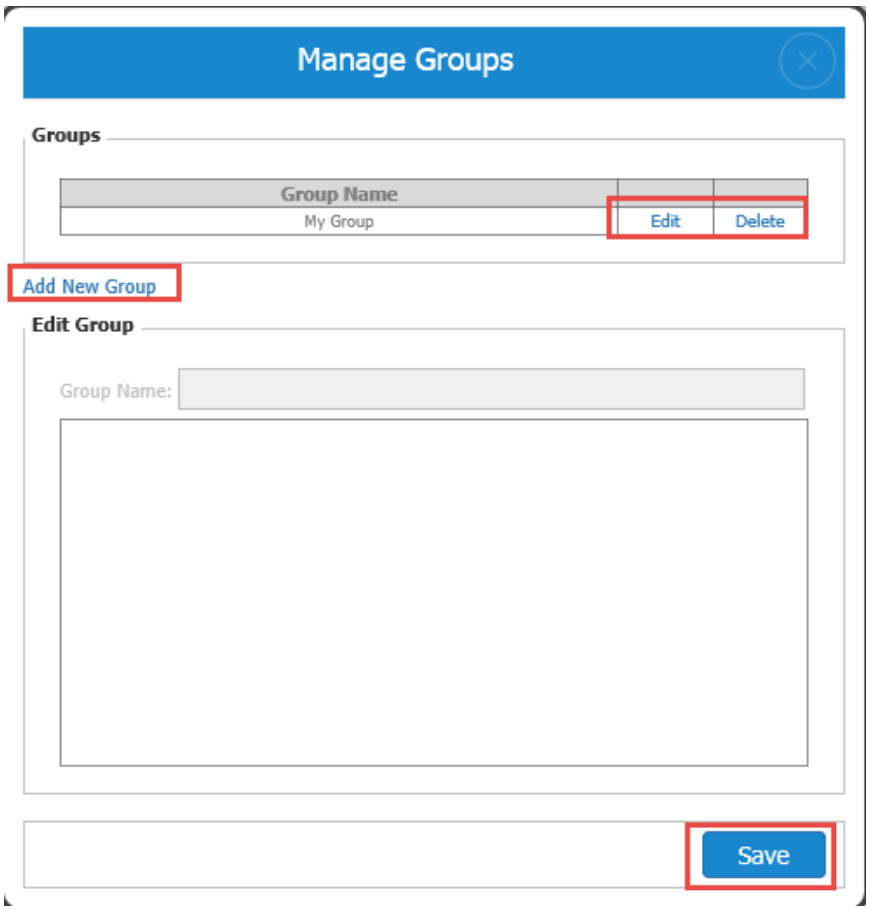
When Name is selected, the Event Name drop-down list activates. From that list, choose the event name you are looking for or leave Any to search across all events.

When Group is selected, the Group drop-down list activates. Groups are lists of actions grouped into one event. There are three predefined groups:

- Volumes, Snapshots and Images – This group displays all events related to EC2 objects (e.g. Create EBS Snapshot or AMI)
- EC2 Instance – This group displays all events related to EC2, such as Start or Stop Instance
- Network and Security – This group diplays all actions related to AWS network or security group (e.g. all information about changes to security groups)

Additionally, customized groups of actions can be created. To create a new group, click Edit Group.

To add new group, click Add New Group, enter group name, check the action to include in this group, and click Save.

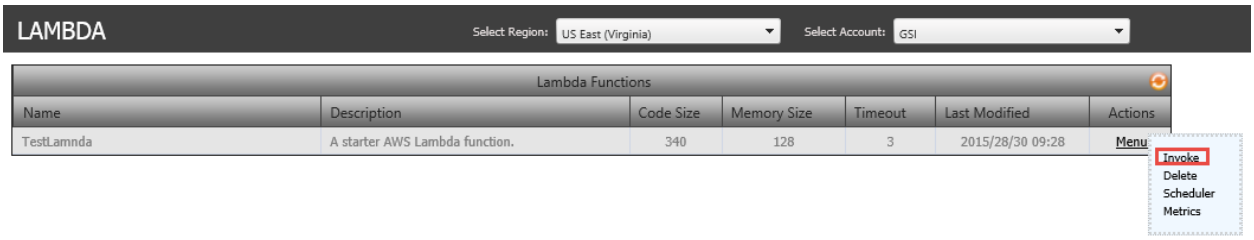


To edit or delete existing group in the top table, click Edit or Delete respectively.

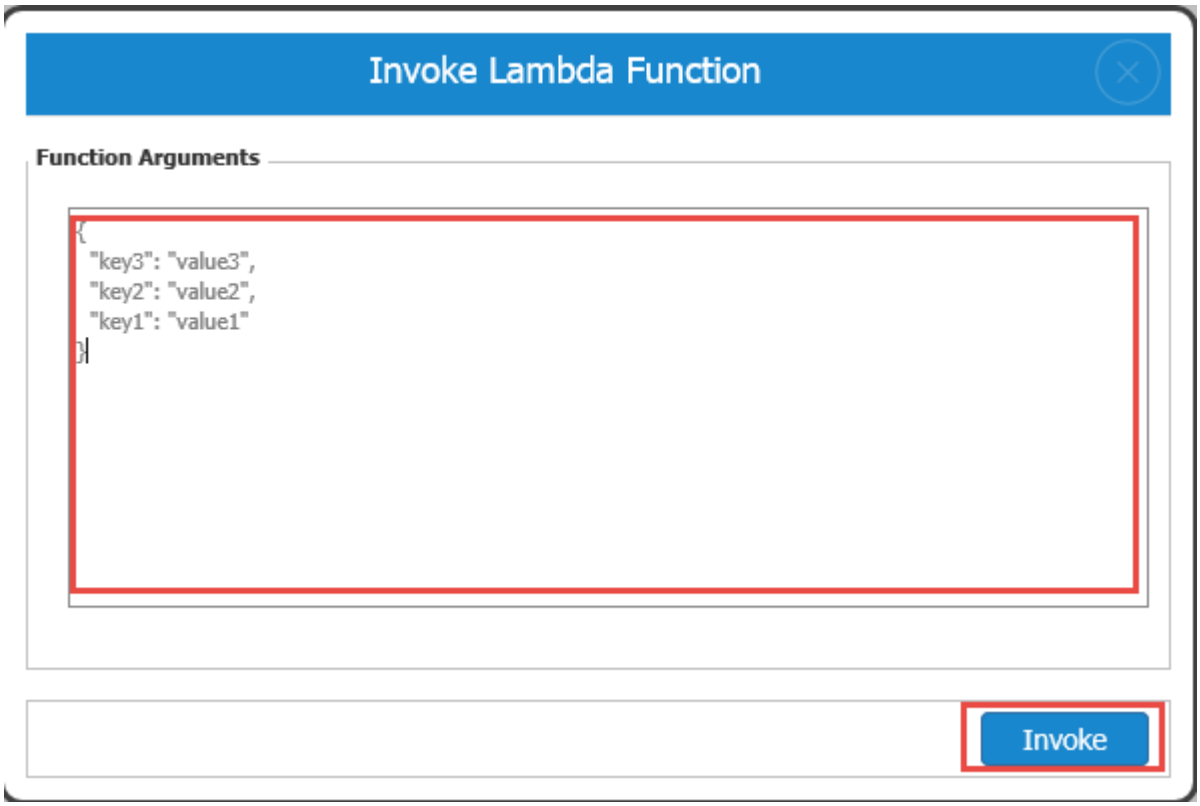
How to Invoke Lambda function

To invoke existing Lambda function from the Main Menu, select Lambda.

Under the Lambda page from the context menu, select Invoke.



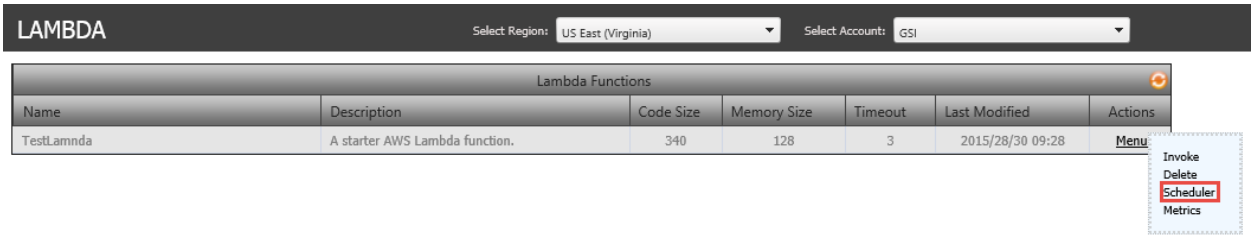
In the Function Arguments box, enter function argument.
Click Invoke.



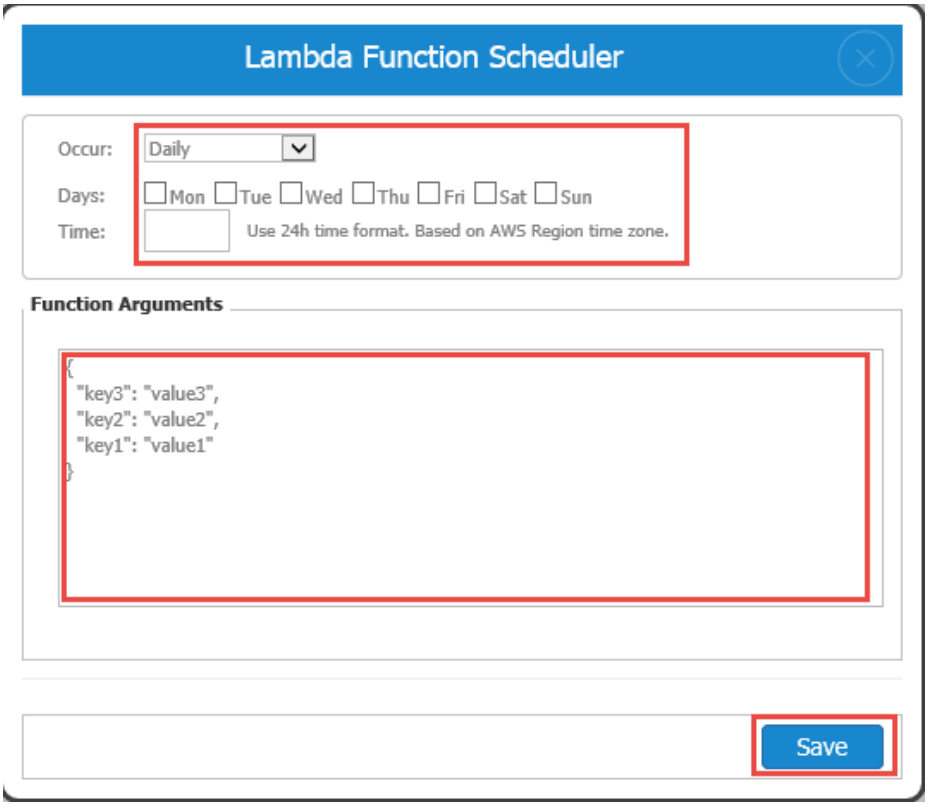
Execution status is displayed at the bottom of the window.

How to Schedule Invoke Lambda function

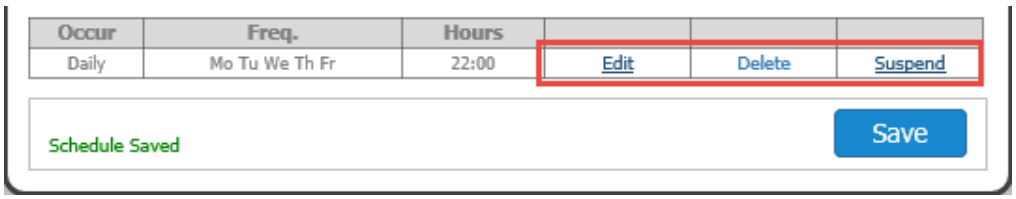
To invoke existing Lambda function from the Main Menu, select Lambda.
Under the Lambda page from the context menu, select Scheduler.



In the top section, select when to execute function.
In the bottom section, enter function arguments.
Click Save.



You can edit, delete, or suspend scheduler at any time. To do so, under the list of existing schedulers click Edit, Delete, or Suspend.



Introduction to EBS Pre-Warmer

When a new EBS volume is created or a volume from a snapshot is restored, the back-end storage blocks are allocated immediately. However, the first time you access a block of storage, it must be either wiped clean (for new volumes) or instantiated from its snapshot (for restored volumes) before you can access the block. This preliminary action requires time and can cause a 5 to 50 percent loss of IOPS for your volume the first time each block is accessed. For most applications, amortizing this cost over the lifetime of the volume is acceptable. Performance is restored after the data is accessed once.

However, you can avoid this performance hit in a production environment by writing to or reading from all of the blocks on your volume before you use them; this process is called pre-warming. Writing to all of the blocks on a volume is preferred, but is not an option for volumes restored from a snapshot, because that would overwrite the restored data. For a completely new volume created from scratch, you should write to all blocks before using the volume. For a new volume created from a snapshot, you should read all the blocks that have data before using the volume.

Elastic Cloud Gate offers a feature that allows you to pre-warm EBS volumes. It works as follows:

After selecting EBS volumes to be run by the pre-warming process, Elastic Cloud Gate will launch t1.micro Linux Instance and attach selected volumes. You might be charged for this Instance by Amazon AWS $0.02 /h.

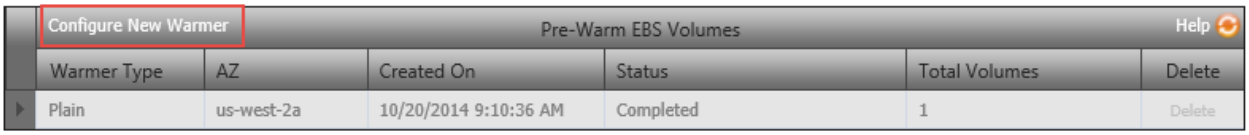
The launched Instance executes a script that pre-warms all attached volumes. This process can require from a few minutes to several hours depending on size and amount of attached volumes. For example, to pre-warm 1TB volume can take up to 30h.

The warmer Instance is launched per region and per availability zone also, either per new volumes or volumes restored from snapshot. You are not able to mix different types of EBS (new or restored from snapshot) under the same warmer server. You can attach maximum of 10 volumes per warmer.

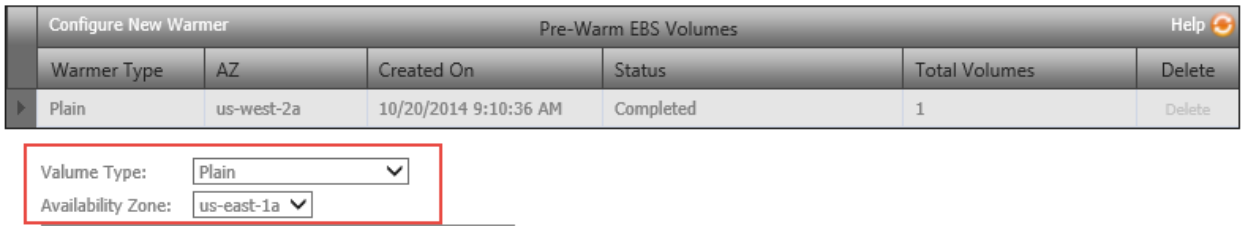
When the pre-warming process is complete, you receive a notification email and the warmer instance is terminated.

How to setup warmer:

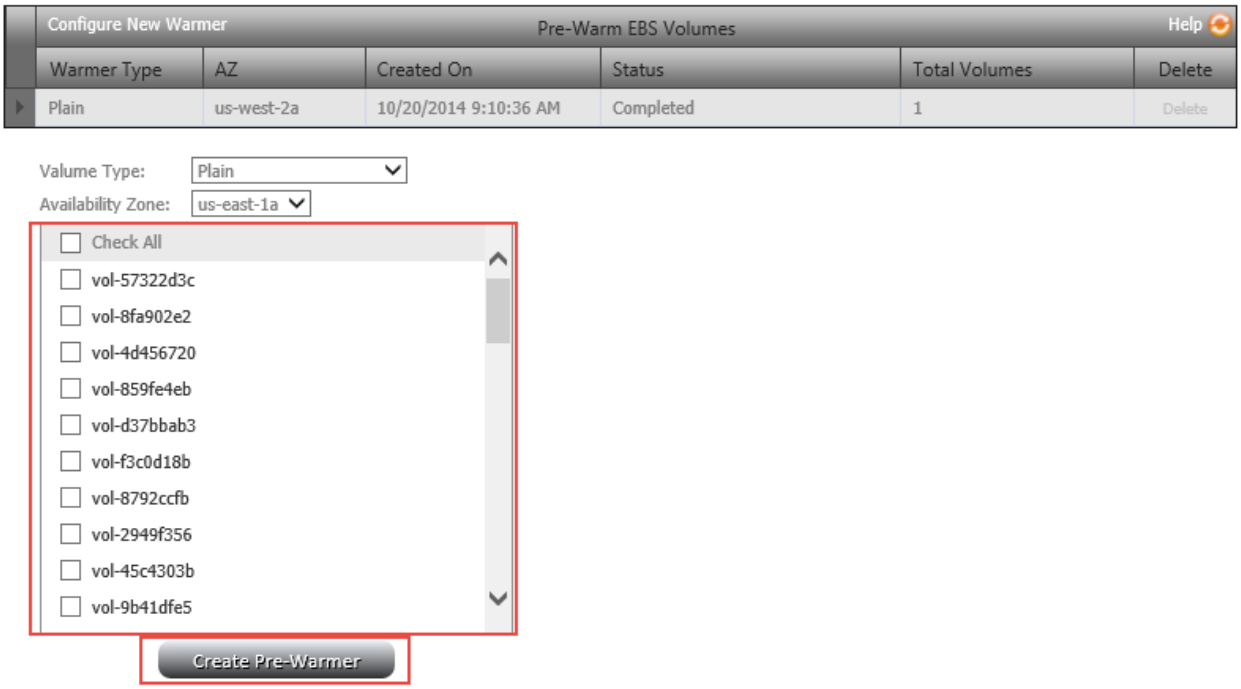
From Dashboard, click Pre-Warmer.
Click Create New Warmer.



Select Availability Zone and Volume Type; the volume must not be attached to any Instance.



Select volumes (up to 10 volumes can be attached to the same warmer).
Click Create Warmer.

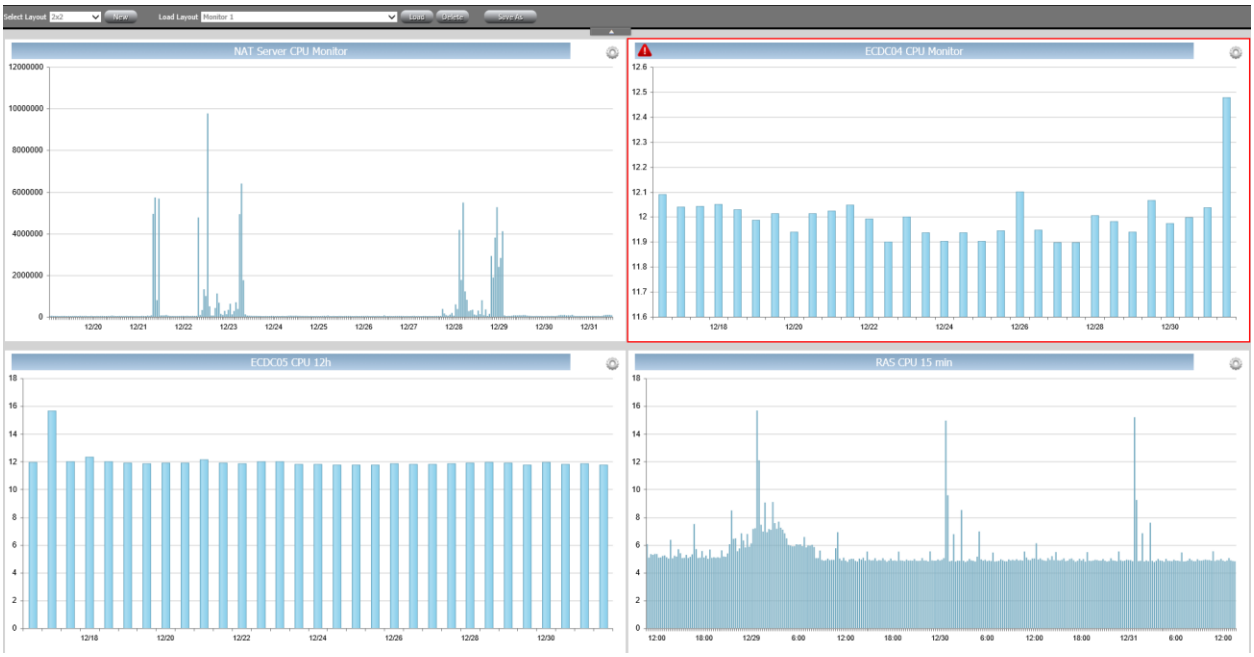


If you have more than 10 volumes or the volumes are spread across different availability zones, you can create another warmer by following steps 2 through 5.

Introduction to Monitoring Center

Monitoring Center is a tool that shows all kinds of metrics on a multi-charts page.

To open Monitoring Center from the Main Menu, select Monitoring Center.
The new page opens on a separate tab with four 2x2 charts as default.



Change the charts by selecting a new layout. Options to choose from:
2x2 (4 charts), 2x3 (6 charts) or 3x3 (9 charts).
To change the layout from the navigation bar, select Layout; charts adjust automatically on your screen.

Each chart can be configured individually by clicking the configuration icon at the right corner of the chart.

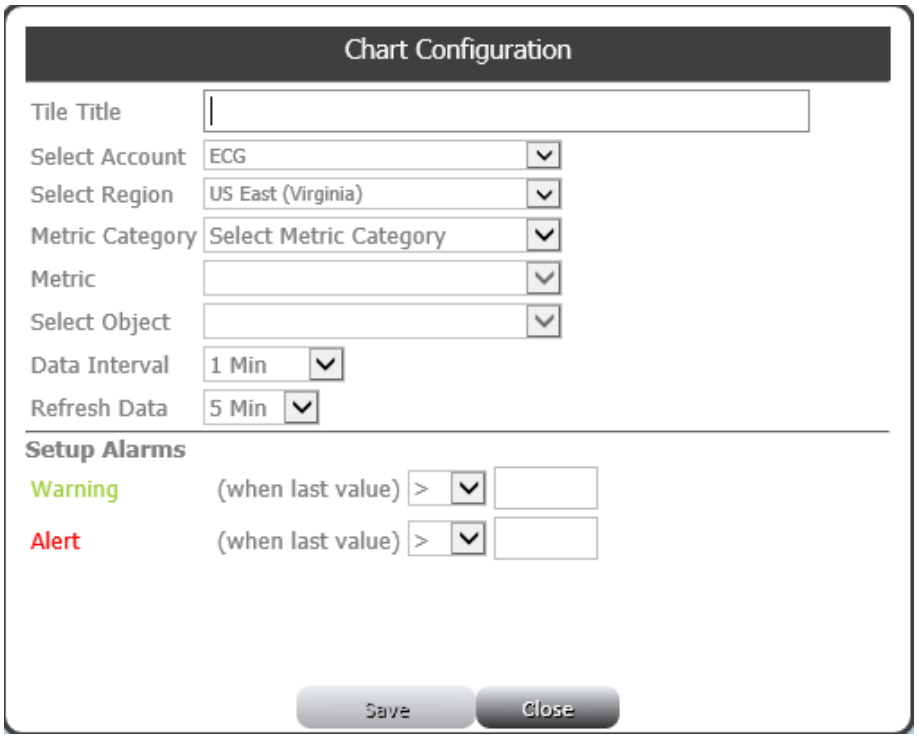
In the configuration panel you can specify:

- Chart title (displayed on the top panel of the chart)
- Account and region to pull data from
- Metric Category – Gives you an option to choose what category you want to see metrics from (e.g. EC2, EBS, ELB, etc.)

- Metrics – This list is populated after selecting category and contains metrics relevant to the selected category
- Select Object – List of objects related to the selected category, e.g. if you select EC2 as a category, the object list, contains EC2 Instances from the selected account and region
- Data Interval – Interval of data to be shown on the chart
- Refresh Data – Interval of frequency to refresh data on the chart

Additionally, you can configure alarms. When the alarm is triggered, the color of the chart's border is changed to light green if a warning is triggered, or red if an alert is triggered.
To setup alarm, select operator and enter value.

When you finish configuration, click Save.

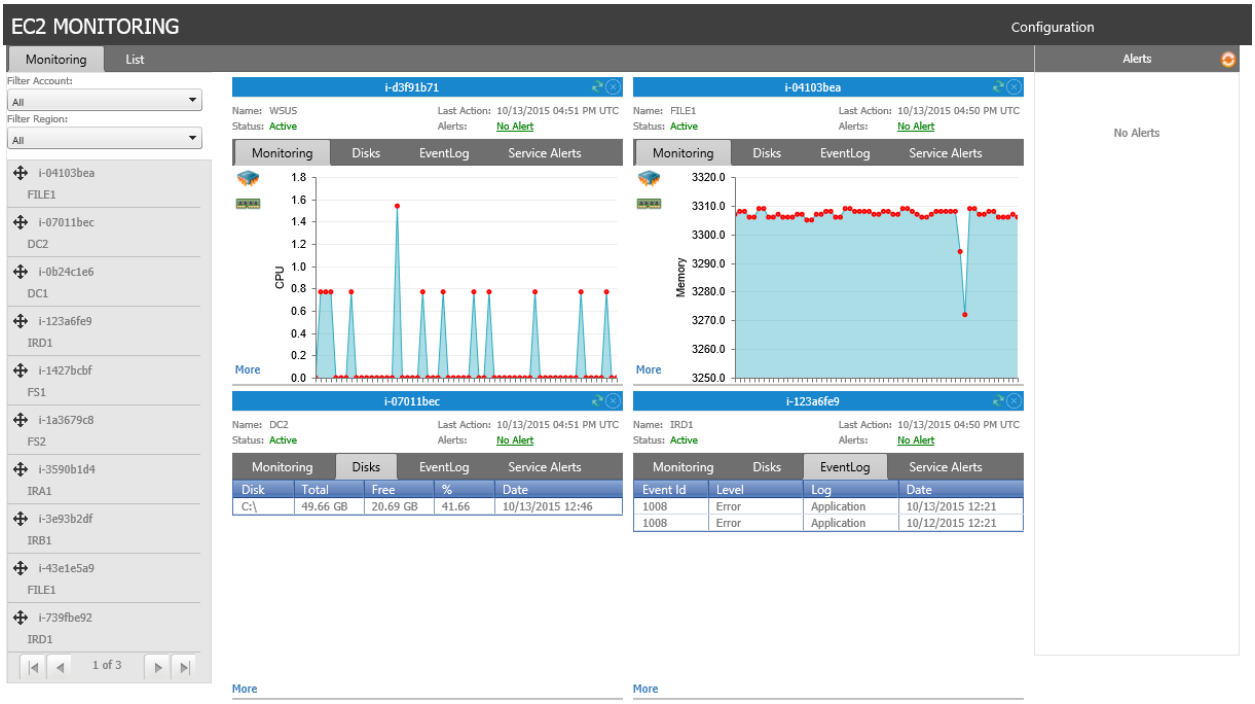


When you finish configuration of charts, you can save the layout (including configuration of all charts under given name). To save layout, click Save As from the navigation panel.
Enter name and click Save.

The new layout is displayed on the Load Layout drop down list.
To load layout from the list, select layout and click Load.
At any time, you can remove layout from the list by selecting Layout and clicking Delete.
To create a new layout, click New.

Introduction to EC2 Monitoring

EC2 Monitoring is a tool to monitor resources on Windows Server.

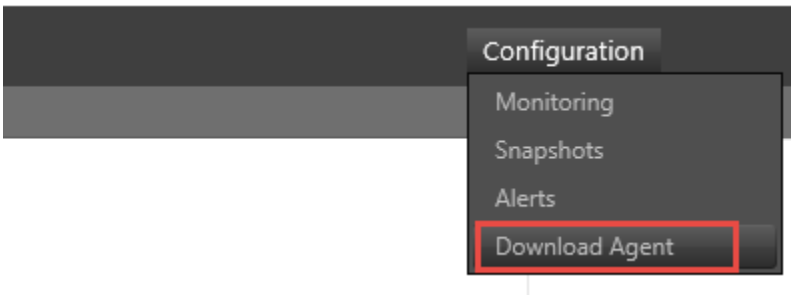


EC2 Monitoring requires installation of Monitoring Agent.

Monitoring Agent requirements:
- Windows Server 2008 or later, 64 bit
- .NET 4.5

Installing Agent:

Go to the EC2 Monitoring section, from the configuration menu select Download Agent.



Unzip file on your Windows Server and run AWSMonitoringService.
This installs Monitoring Agent as Windows Service. When installation is complete, the Authenticator application opens.

Enter your Elastic Cloud Gate user and password and click Verify.
After successful verification of credentials, Monitoring Agent tries to connect to ECG system to pull configuration.

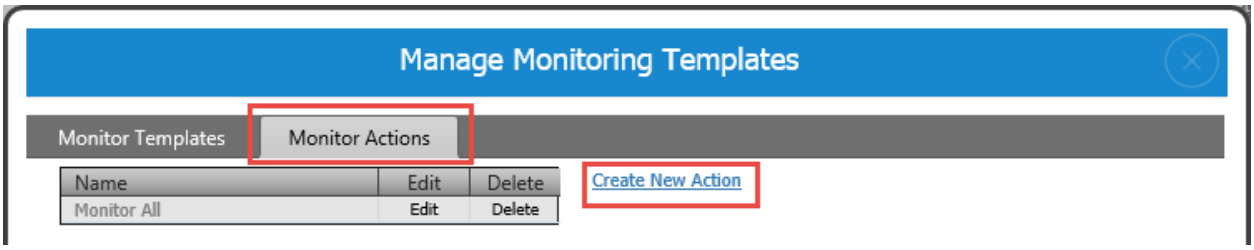
To schedule update of Monitoring Agent, once installation is finished logout and log back in. After logging back in, Agent Installer will start again. Click Yes to minimize installer to notification area. Click on installer icon and follow wizard to schedule update.

Note: Monitoring Agent pulls configuration every hour, therefore any configuration changes may take up to an hour to take effect. We recommend creating configuration for EC2 Instance before installing the agent – see next section for more information.

Configurations

Agent Configuration:

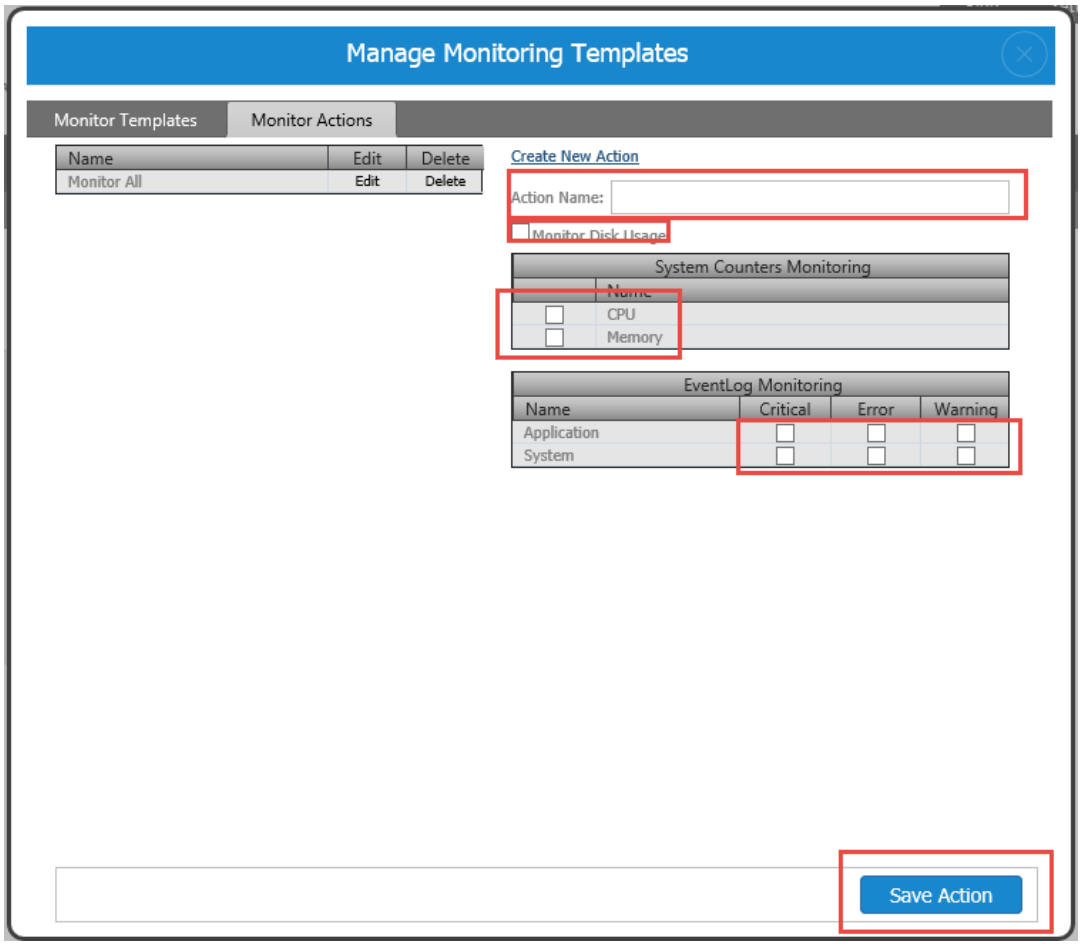
To configure agent from the Configuration menu, select Monitoring.
In the new window, go to the Monitor Actions tab and click Create New Action.



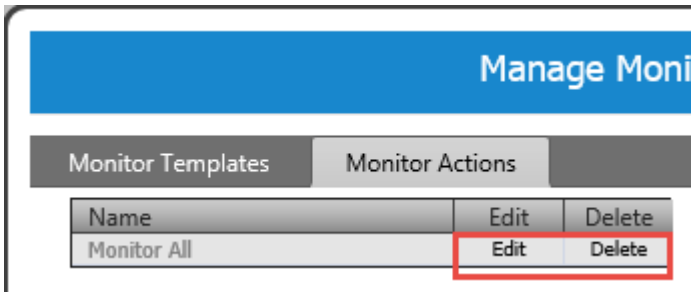
Enter action name; additionally, you can make the following configurations:

1. To monitor disk usage, check Monitor Disk Usage: this option sends information about total space and space available on every logical disk on the monitoring Windows, every 10 minutes.
2. System Counters Monitoring – Select resource to monitor: this sends value of the monitoring resource every 1 minute.

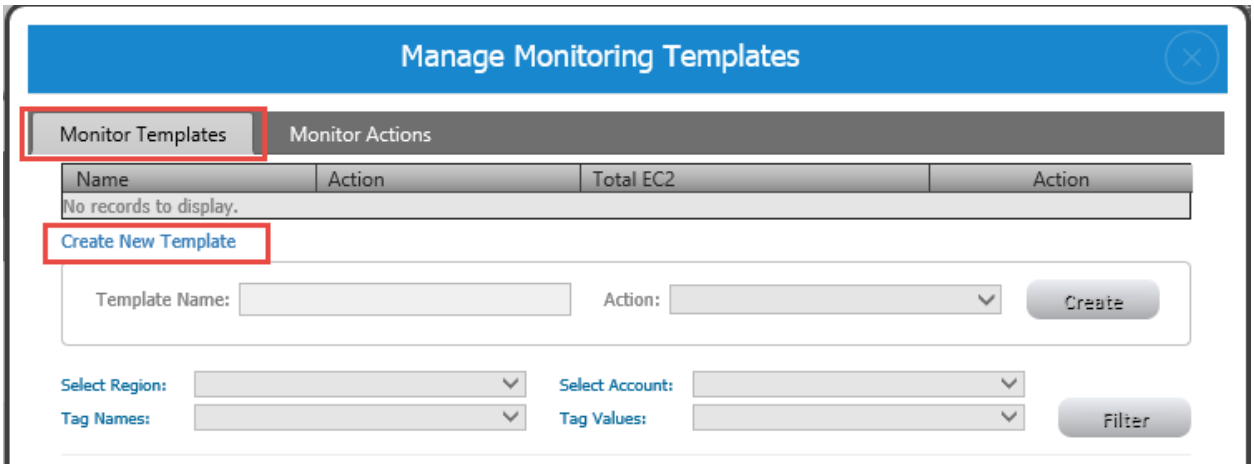
3. EventLog Monitoring – Allows you to specify event log and log level to be read by agent and sent back to our portal for review by users.



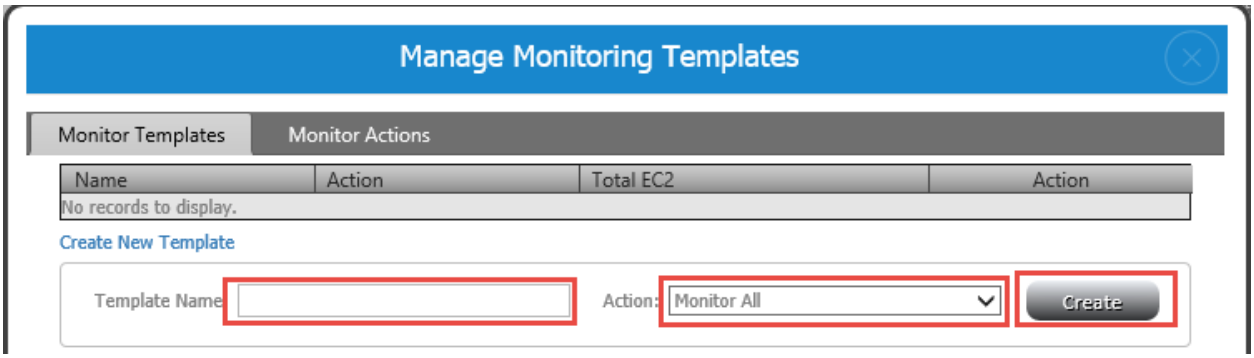
When configuration is complete, click Save Action.
You can create multiple configurations based on your needs.
Actions can be modified or deleted at any time: select Edit or Delete in the table on the left.



After creating action(s), switch to the Monitor Templates tab and click Create New Template.

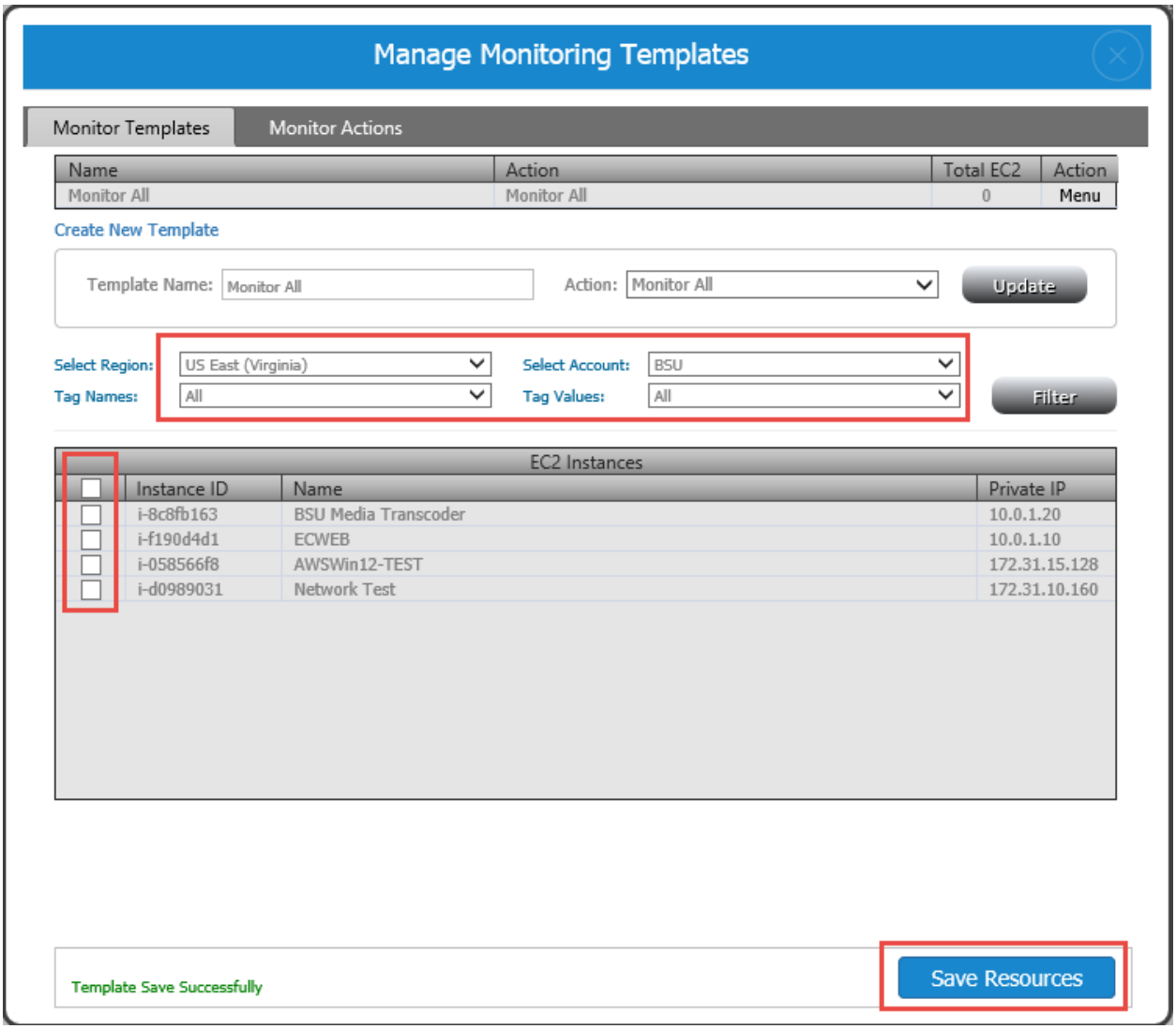


Enter template name, select action from the drop down list, and click Create.



From the EC2 Instances list, check Instances you want associated with the template and click Save Resources.

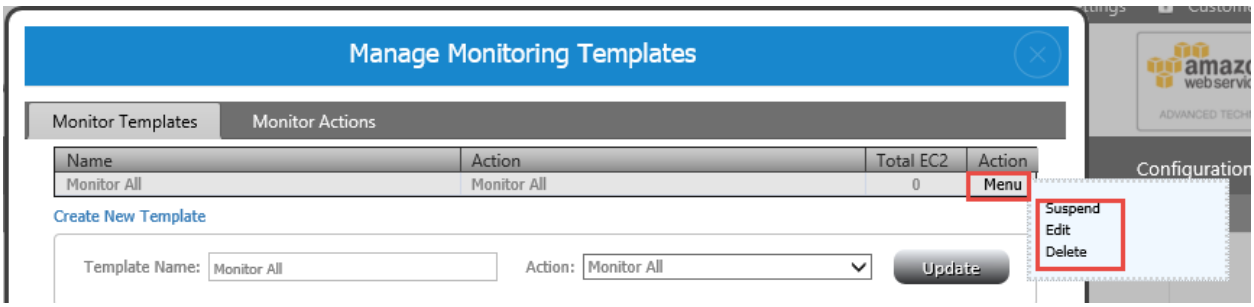
Filter Instances by region and AWS account, as well as by tag assigned to Instance.



Any given EC2 Instance can be associated with a template and action only once.

To modify template from the menu, select Edit.
To temporarily suspend monitoring, select Suspend. Please remember configuration is pulled by agent once every hour, so it might take up to one hour before your change takes effect. To resume suspended monitoring from the menu, select Resume.

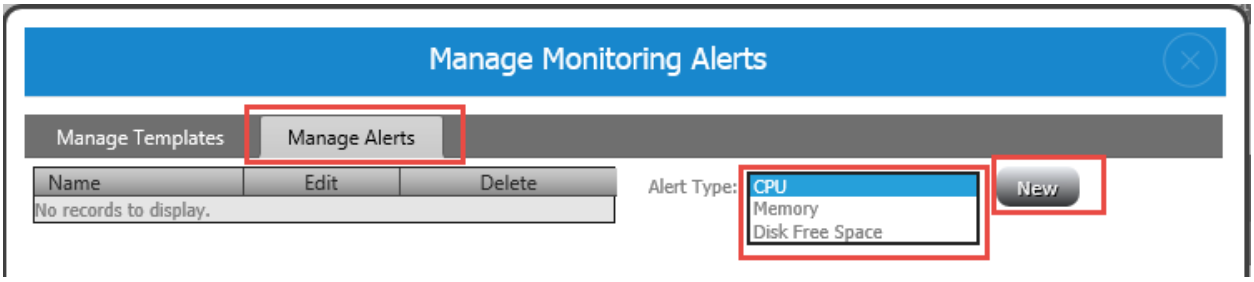
To delete template from the menu, select Delete.



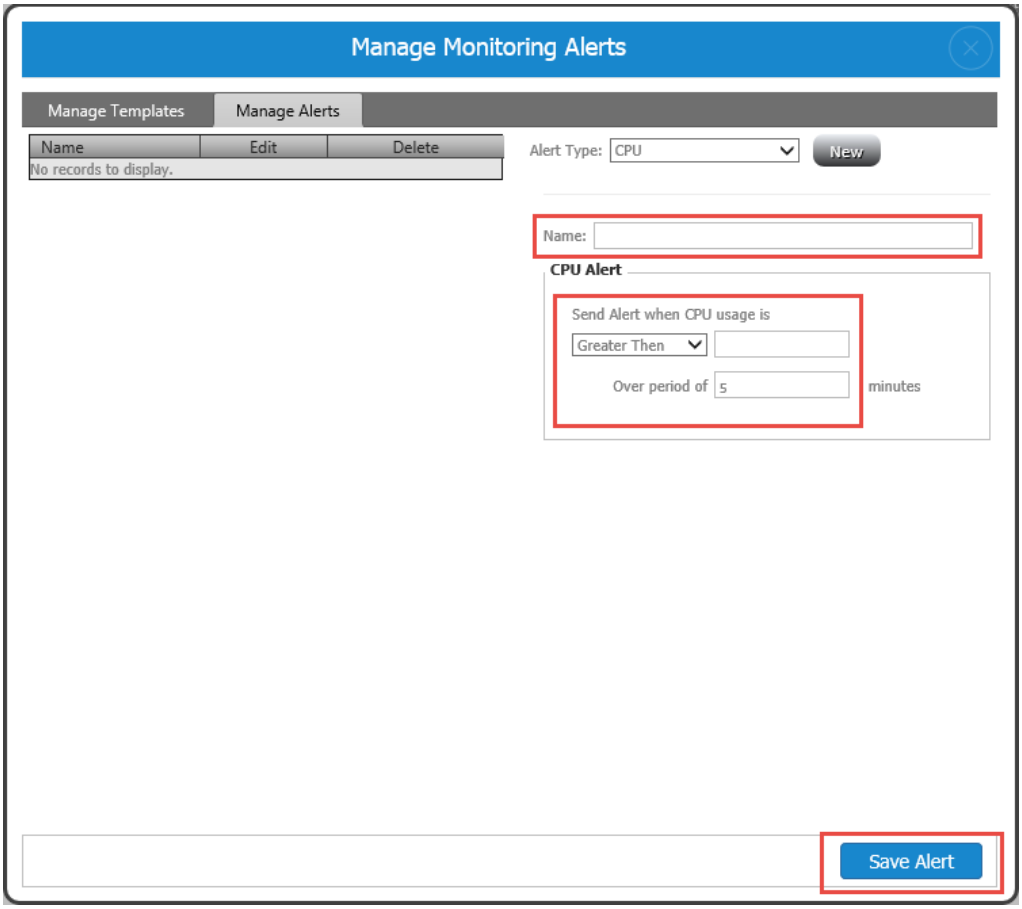
Note: If you plan to use Agent only for consistent backup, you can create an empty action.

Alerts Configuration:

From the Configuration menu, select Alerts.
In the new window, go to Manage Alerts. From the Action Type drop down list, select which resource you want to create the alert for and click New.

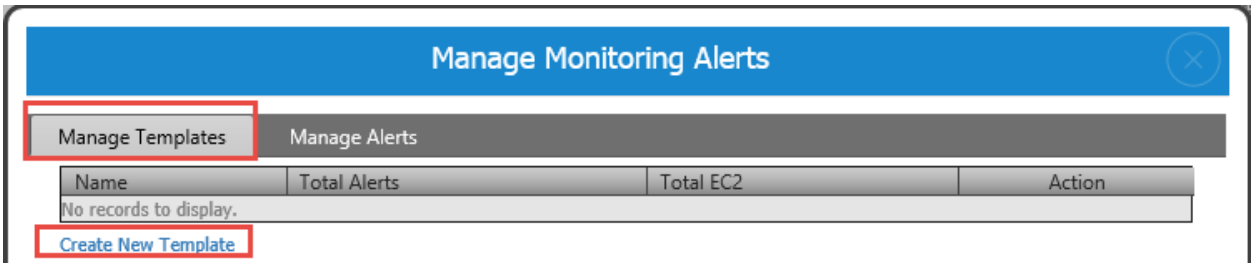


Enter all conditions to trigger the alert and click Save Alert.
Over period of – This value specifies how long (in minutes) the condition needs to persist to trigger an alert. The values range from 5 to 60 minutes, e.g. if you create an alert for CPU with condition Greater Than 90 Over period of 5 minutes, this means alert triggers if the average CPU usage over the last 5 minutes was larger than 90%.

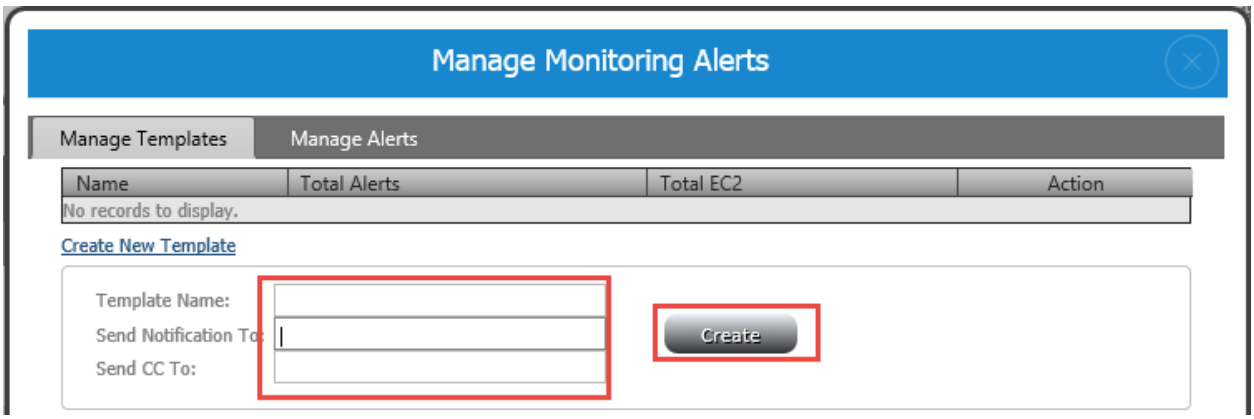


To edit or delete alert from the table on the left, click Edit or Delete.

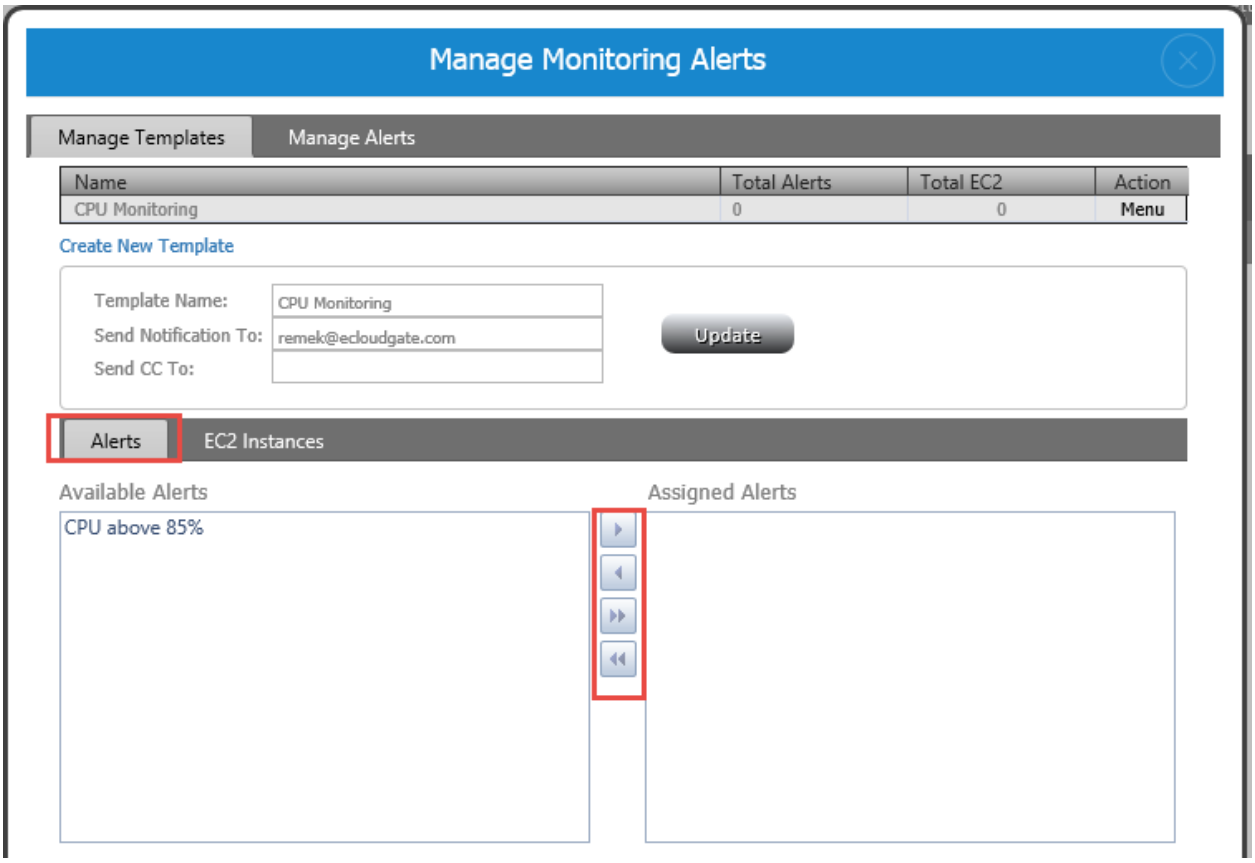
To assign alert with instance(s), go to the Manage Templates tab and click Create New Template.



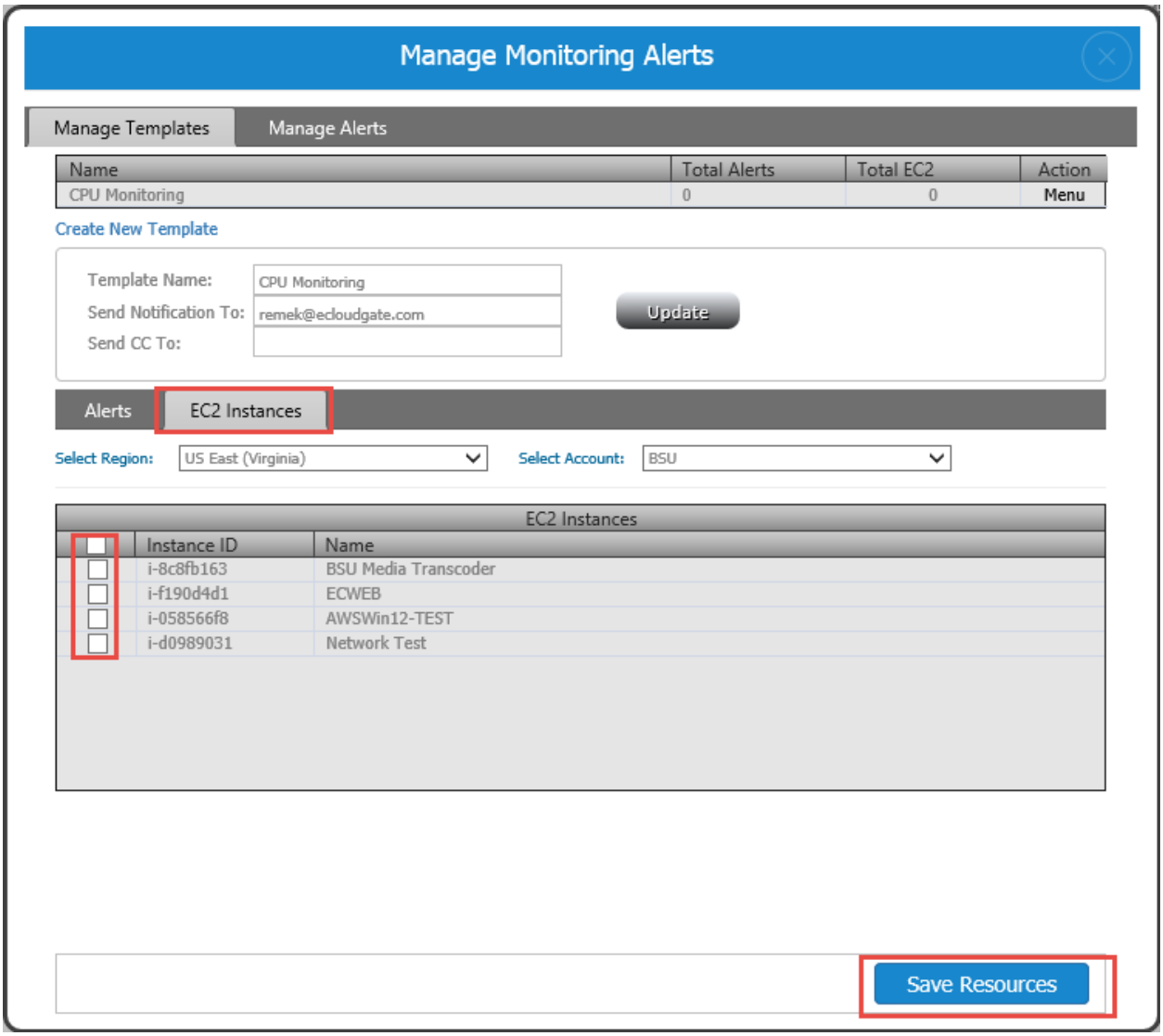
Enter template name and email of the user alert notifications should be sent.
If you want the alert sent to multiple emails, add them under “Send CC To” (use a comma separator). When you are done, click Create.



To associate or disassociate alert(s) with template, use arrows under the Alerts tab.
Available Alerts shows the list of alerts you created, but didn’t associate with the current template.
Assigned Alerts shows the list of alerts that are currently associated with the given template.

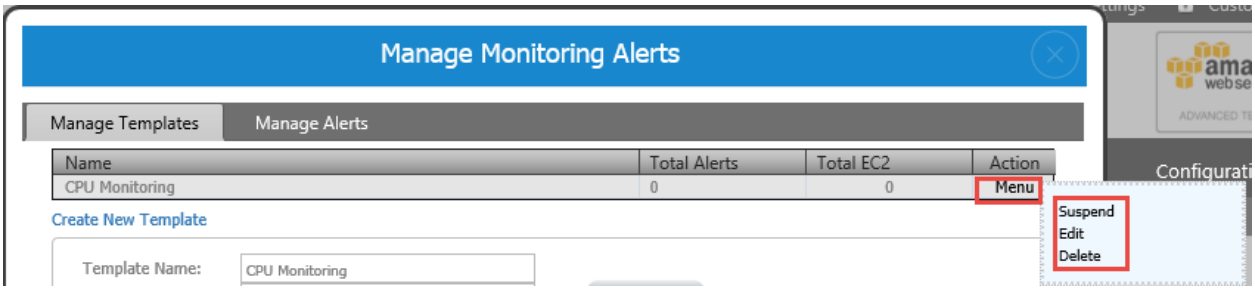


To assign Instances to template, switch to the EC2 Instances tab and check the Instance(s) you want to associate with template, then click Save Resources.
You can filter Instances by Account and Region.



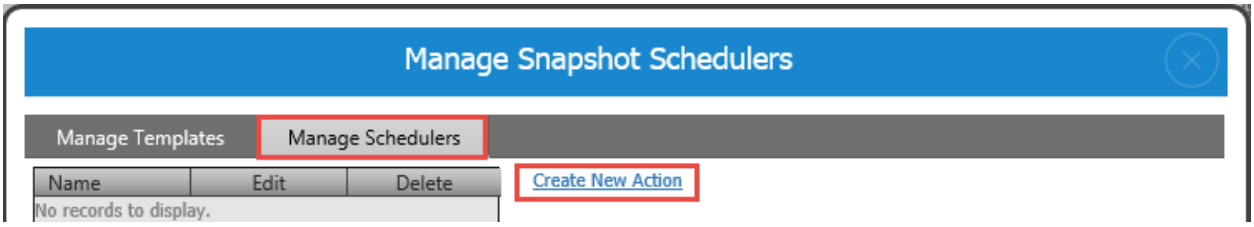
Note: only Instances currently set up under monitoring are accessible on the list.

At any time, you can edit, suspend, resume, or delete a template by selecting the option from the Action menu.



Schedule Consistent Snapshot:

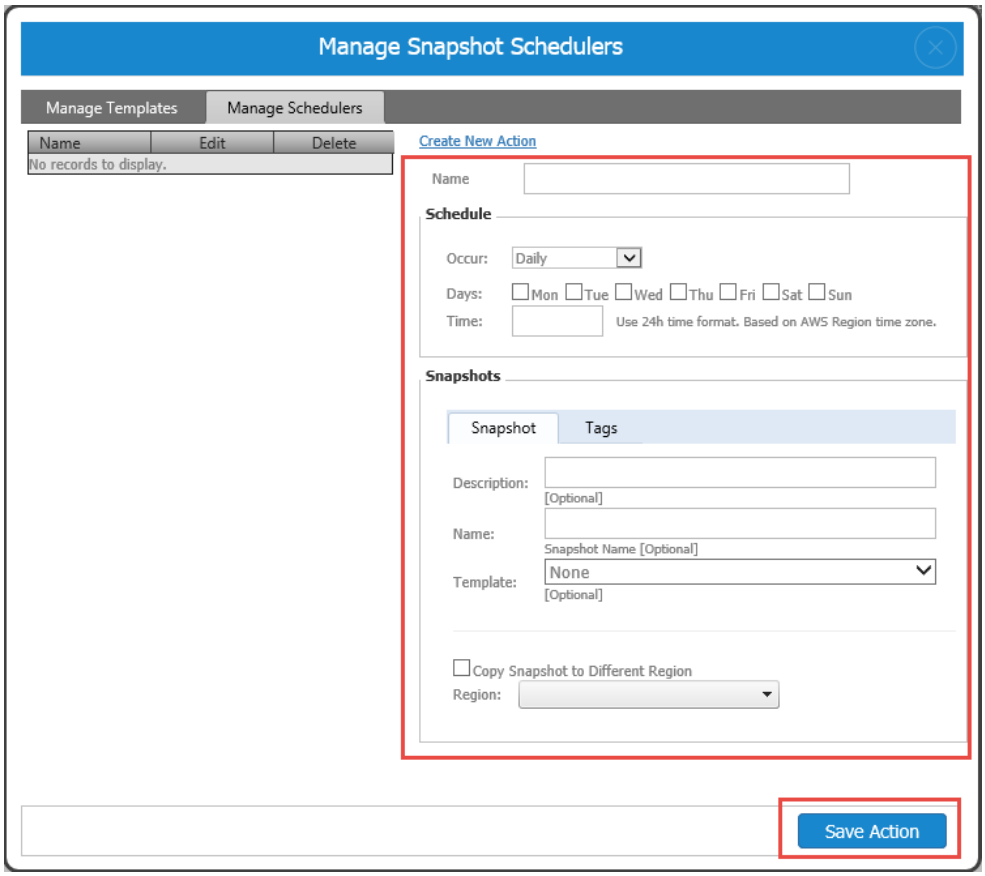
To schedule consistent snapshots from the Configuration menu, select Snapshots.
In the new window, go to Manage Schedulers and click Create New Action.



Enter the scheduler name as well as time/date of when the snapshot of the EBS should be taken.

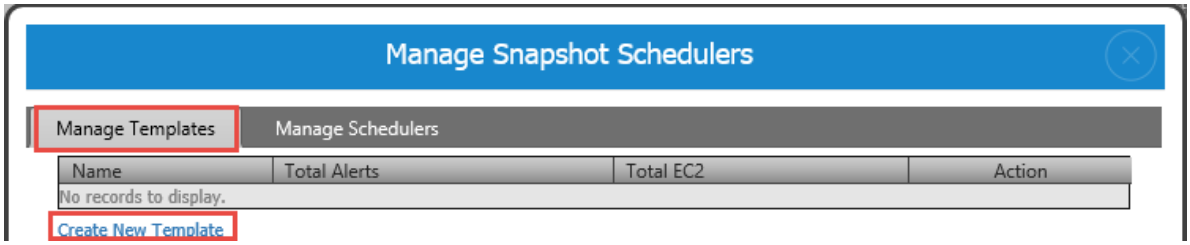
You can enter (optional): Description and name of the snapshot.
Select description template.
If you want to copy this snapshot to multiple regions, check Copy snapshot to Different Region and select destination regions from the list.
In addition, you have an option to assign custom tags to the snapshot.

When done, click Save Action.

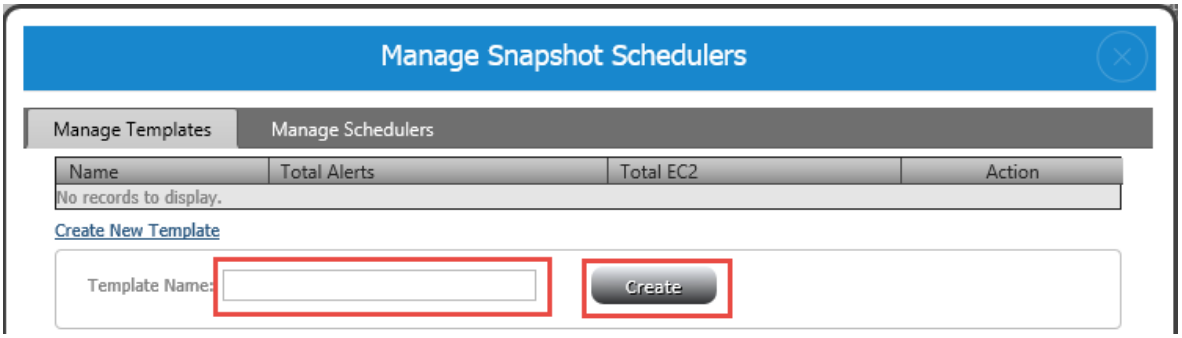


Note: Maintenance of the snapshot must be set up under the EC2 section, just like regular snapshots.

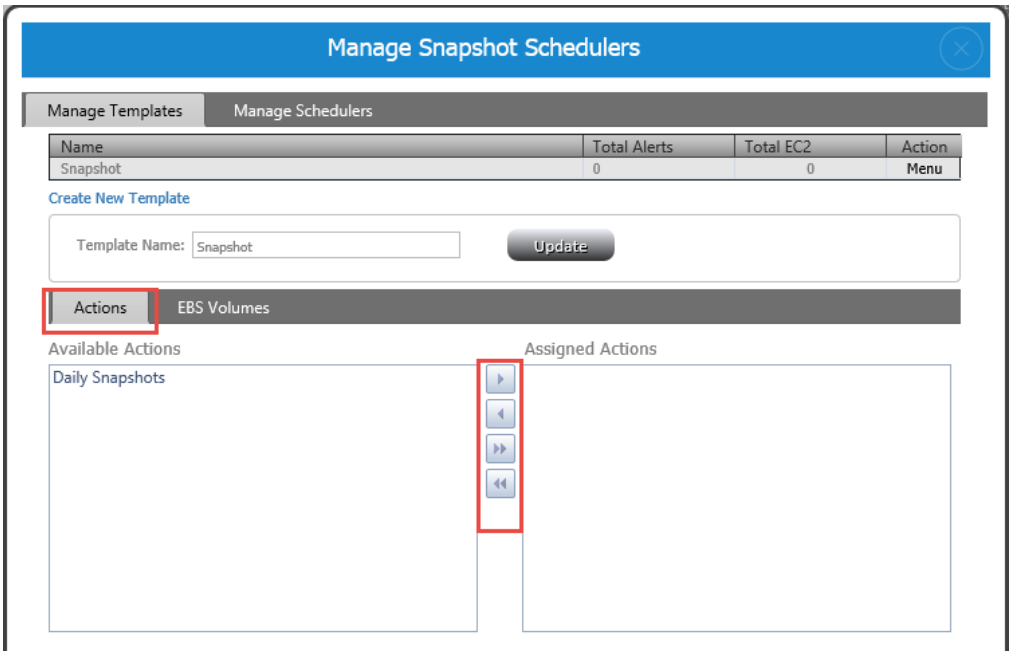
To associate snapshot schedulers with EBS volume, switch to Manage Templates and click Create New Template.



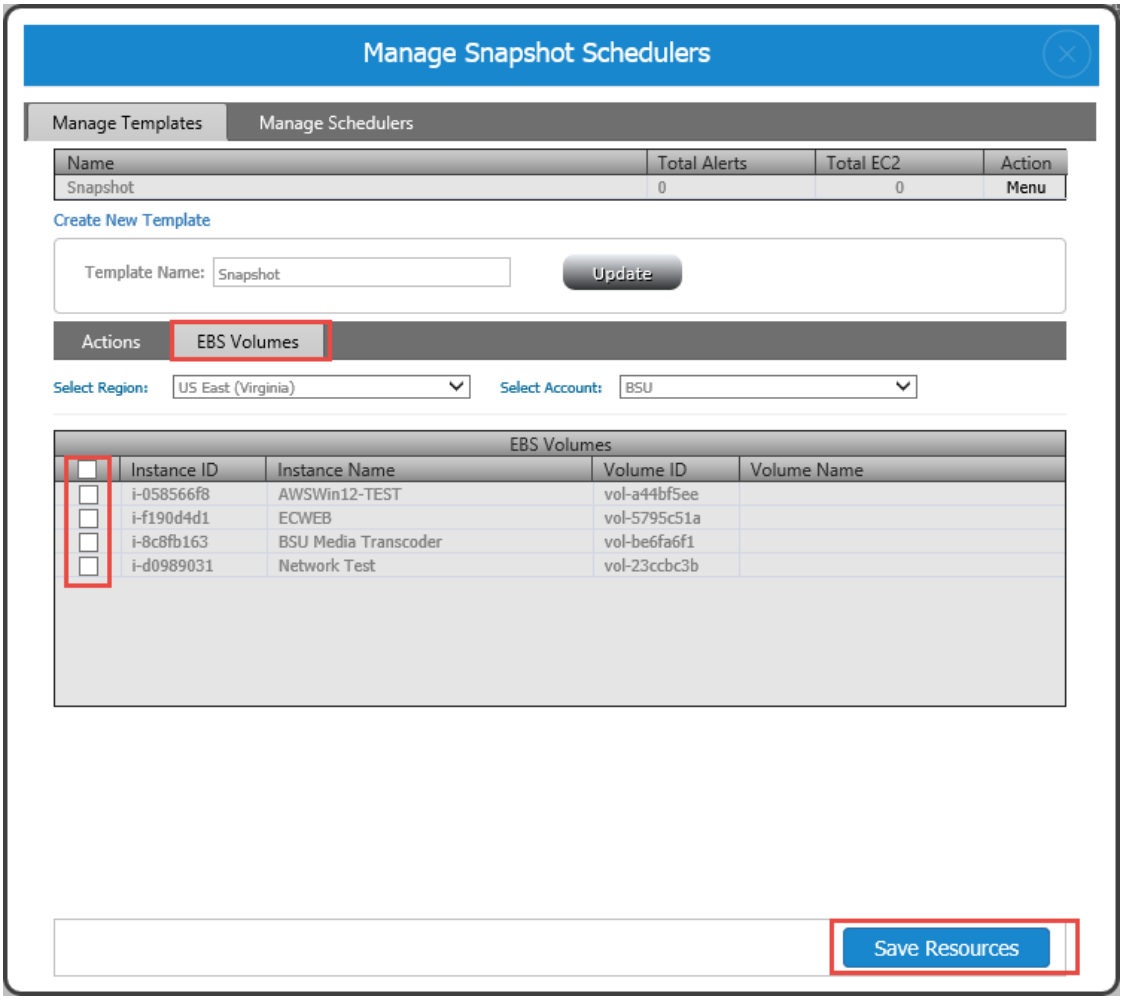
Enter template name and click Create.



To associate or disassociate action(s) with template, use arrows the under the Actions tab.
Available Actions shows the list of actions you created but didn't associate with the current template.
Assigned Actions shows the list of actions that are currently associated with the given template.



To assign volume to template, switch to the EBS Volumes tab and check the volume(s) you want to associate with template. After that, click Save Resources.



Note: Only EBS volume(s) associated with the instances currently set up under monitoring are accessible on the list.

UI

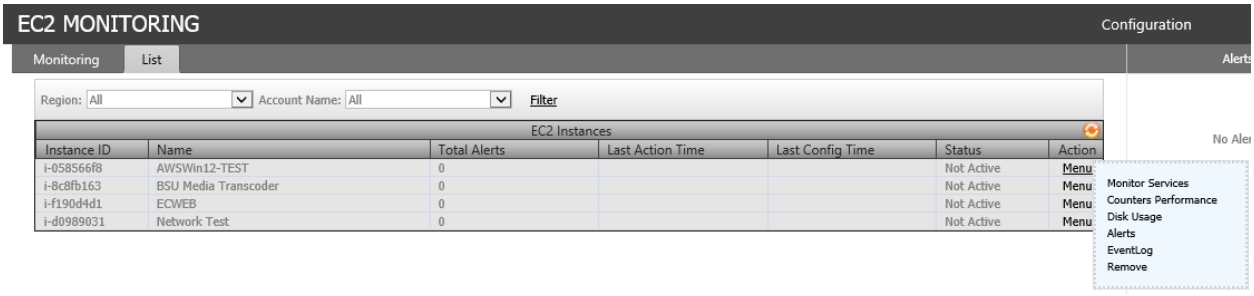
Monitoring Panel

Monitoring panel allows you to take a quick look at the current status of up to four Instances. To add an Instance to monitor panel, drag Instance from the left hand side list and drop it to the panel.

Alerts

The list of alerts within the last 10 minutes is found on the right hand side.

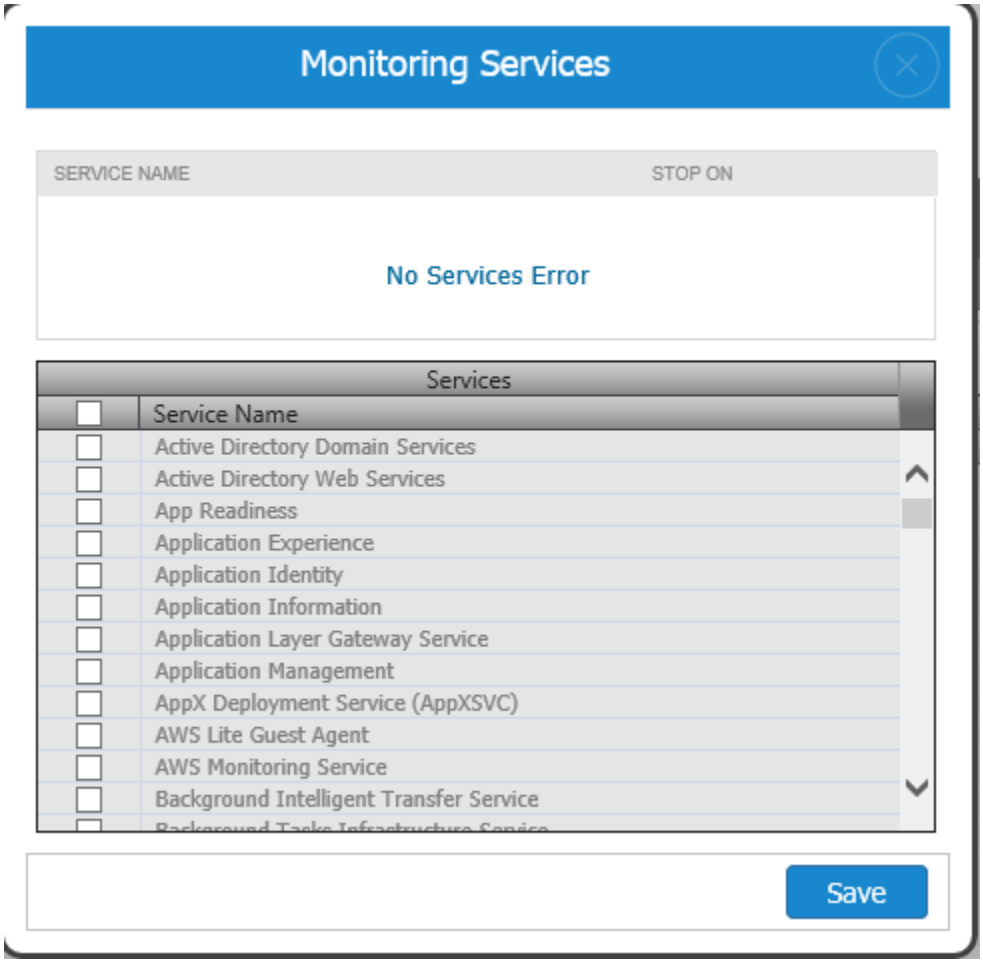
List Tab



On the List tab is visible all Instances configured under monitoring. For each Instance, you can select the following options from the menu:

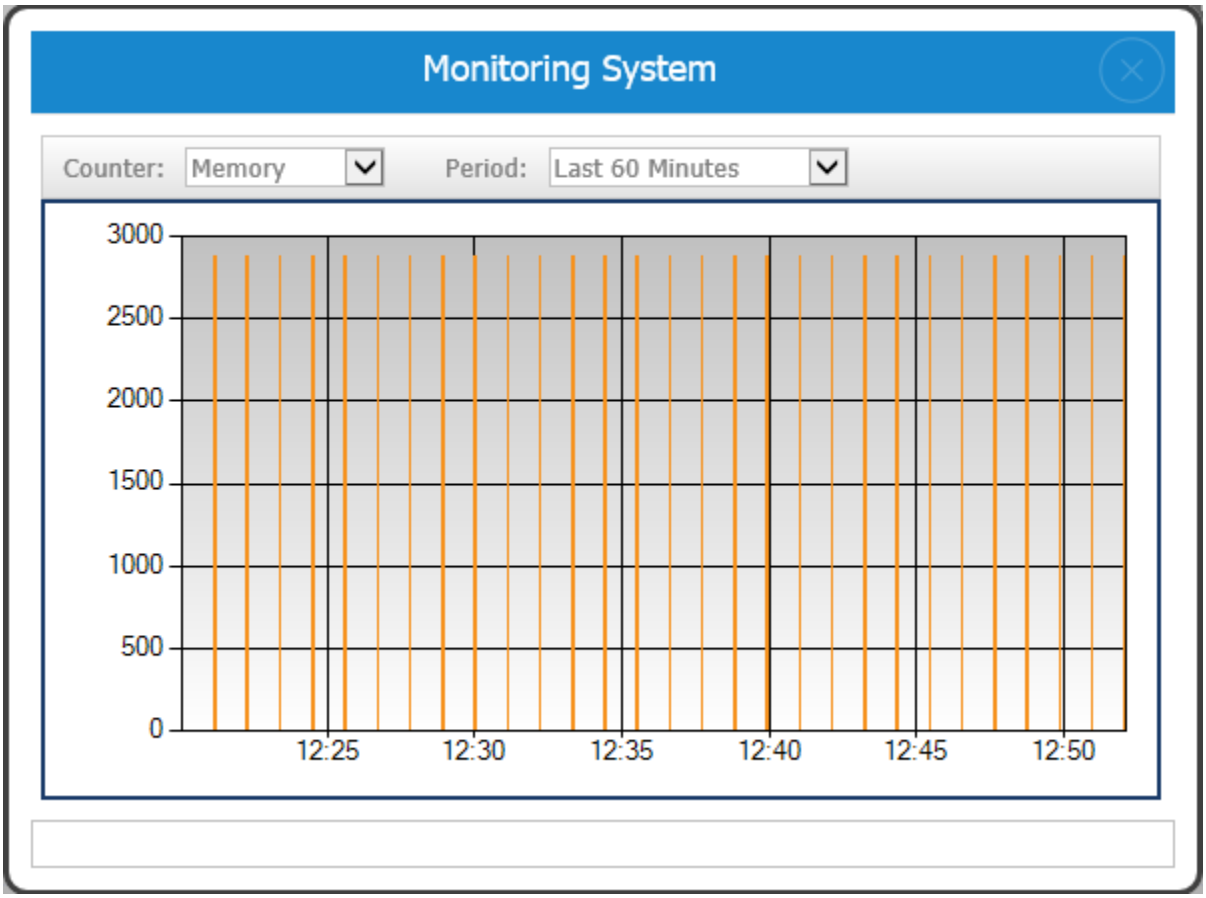
Monitoring Service

Monitoring service allows you to select Windows Service to monitor. If agent detects that selected service is not running, it attempts to start it.
To select services to monitor, switch to the List tab and under given Instance from the menu select Monitor Services. On the bottom of the list, check services to monitor.
On the top table is visible a list of services that stopped running.



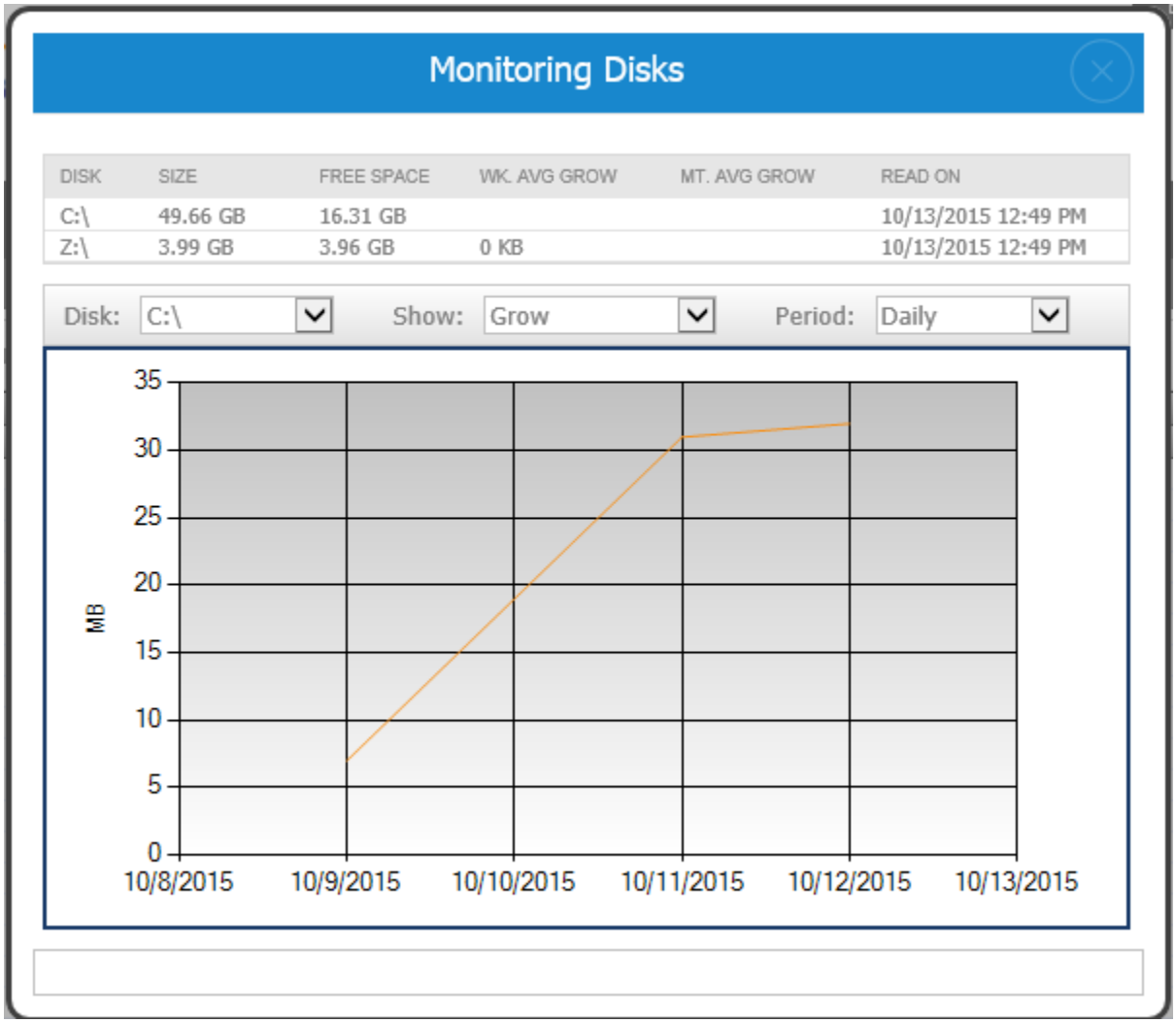
Counters Performance

This option shows the chart for selected counter from selected period.



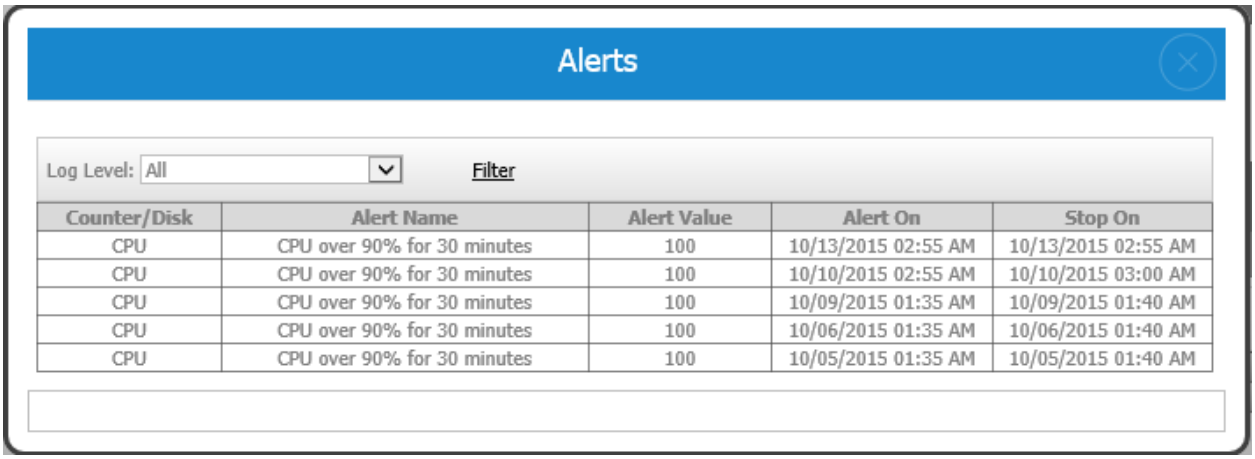
Disk Usage

This chart shows current disk usage, along with average growth rate. Use this feature to estimate when you need to expand your EBS volume.



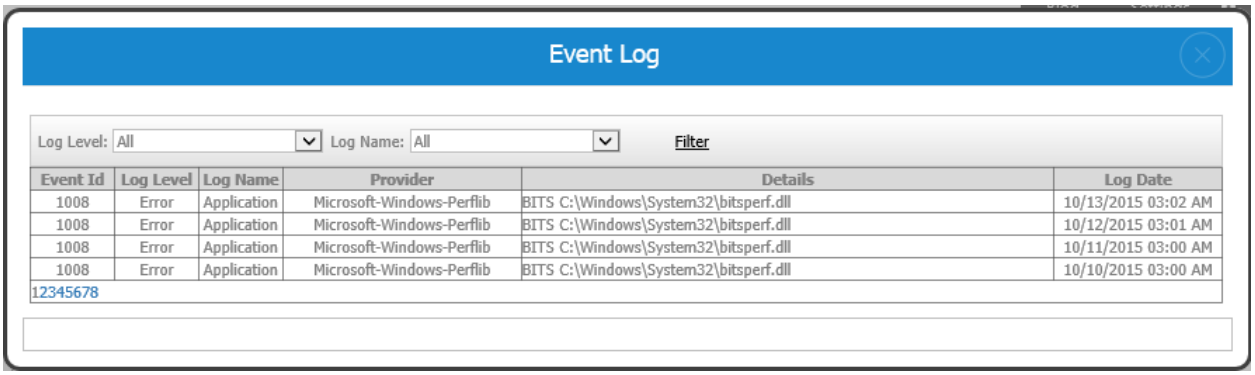
Alert

This option shows all alerts currently active, regardless when first occurrence happened.



EventLog

This option lists records from Windows EventLog, per your configuration.



Remove

This option allows you to quickly remove a given Instance from monitoring. It removes the selected Instance from all configurations.

How to setup and manage federated users

Elastic Cloud Gate provides an option to setup federated users who are able to access AWS Management Console directly from ECG portal, without knowing AWS credentials.

The ECG federated user works the same as AMI user, with one exception: under ECG portal, you can specify days and time when user can access the AWS Management Console.

To create a federated user from the Settings menu, select Manage Users.

Enter user email and password.

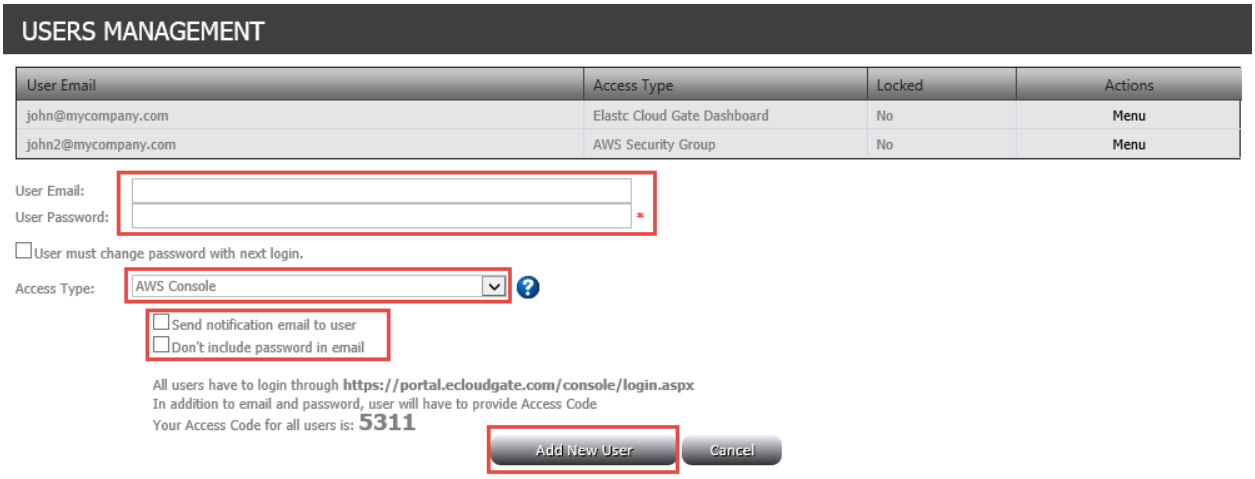
To force the user to change password with next login, check User must change password with next login.

From the Access Type drop down list, select AWS Console.

To send notification email to the new user, check Send notification email to user.

If for security reasons you do not want to include the password in the email, check Don't include password in email.

Click Add New User.

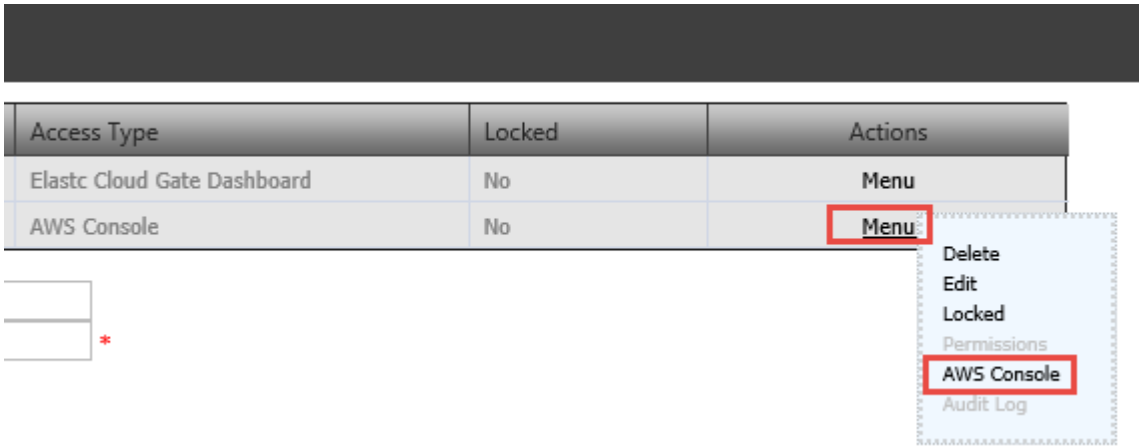


Note: Any user created though the Users Management section has to use a different URL to login to ECG portal. The URL is: https://portal.ecloudgate.com/console/login.aspx

Additionally, beside email and password, the user is asked for the access code on the login page.
You can see your access code on the Users Management page. This number is statically assigned to your account and does not change.

Once the new user is created, you must grant him permission to select AWS account as well as to choose what permission he will have on AWS Management Console.

To grant permission under users table from the context menu, select AWS Console.

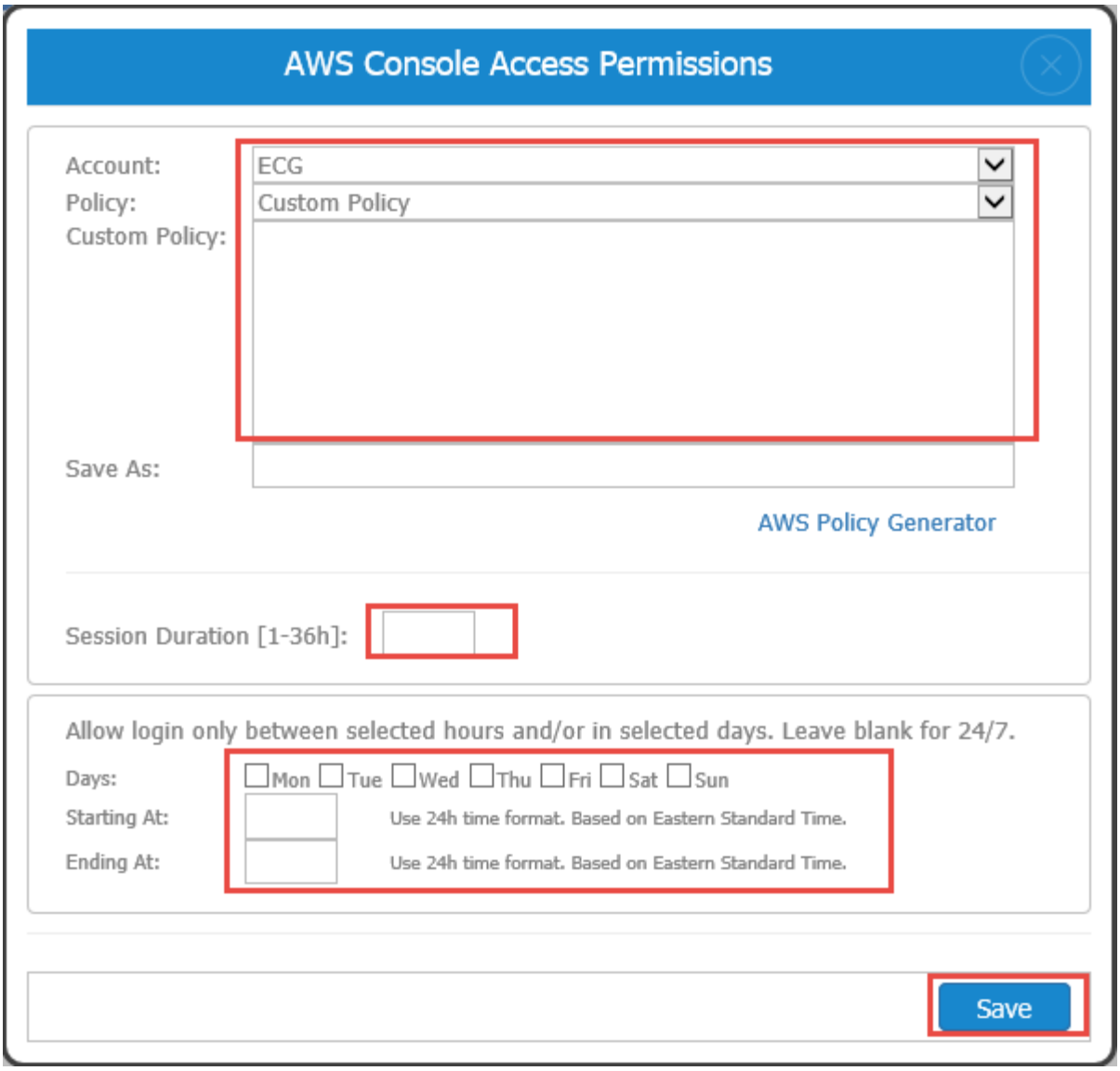


Under new windows, the selected account user has permission to specify AWS policy. You can choose either one of the pre-defined policies, or enter a customized policy.

Under Session Duration, enter how long the user is allowed to stay logged in to AWS Management Console.

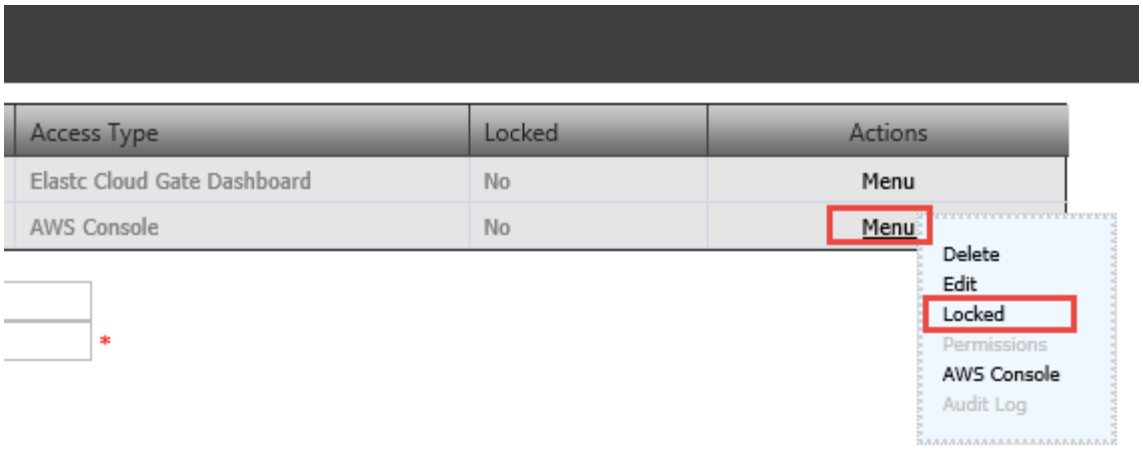
To limit days and hours the user can login to AWS Management Console, check days or enter start and end hours. For 24/7 access, leave all blank.

Click Save.



At any time, you can edit or delete user by selecting the appropriate option from the context menu.

If you need to temporarily prevent user from logging in, from the context menu select Locked. To unlock the user account, select Unlocked from the context menu.



How to setup and manage console users

Elastic Cloud Gate provides options to create multiple users (console users) who can access ECG portal under your primary account. For each user, you can specify permission on the action as well as on the object level.

For example, you can grant access to start only a single EC2 Instance.

To create a console user from the Settings menu, select Manage Users.

Enter user email and password.

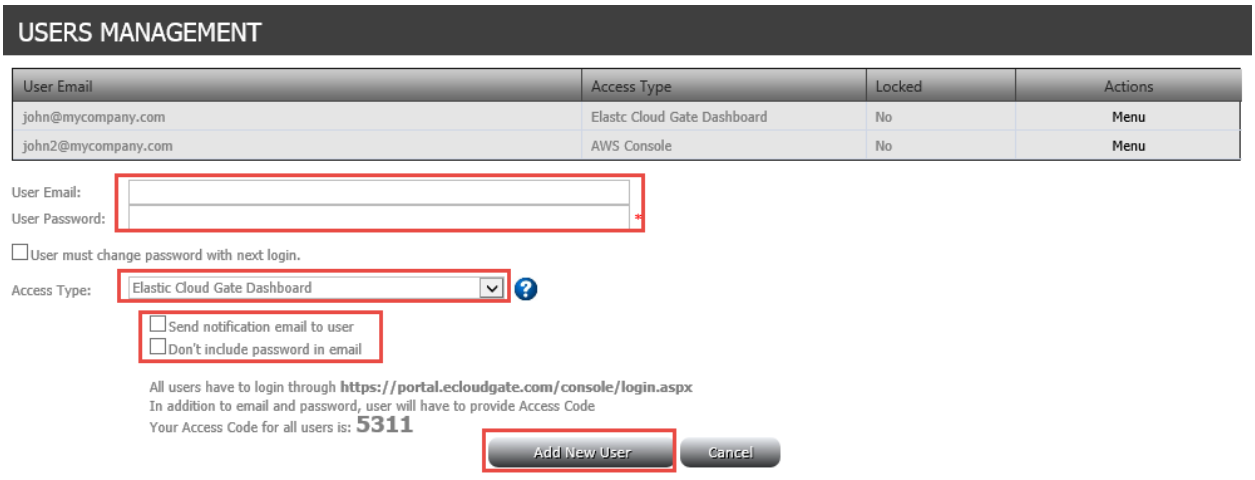
To force the user to change password with next login, check User must change password with next login.

From the Access Type drop down list, select either Elastic Cloud Gate Dashboard or Security Group & Dashboard. To learn more about Security Group access type, go to:
How to temporarily open AWS Security Groups rules for dynamic IP
How to temporarily open AWS Security Groups rules for dynamic IP

To send a notification email to the new user, check Send notification email to user.

If for security reasons, if you do not want to include the password in the email, check Don't include password in email.

Click Add New User.



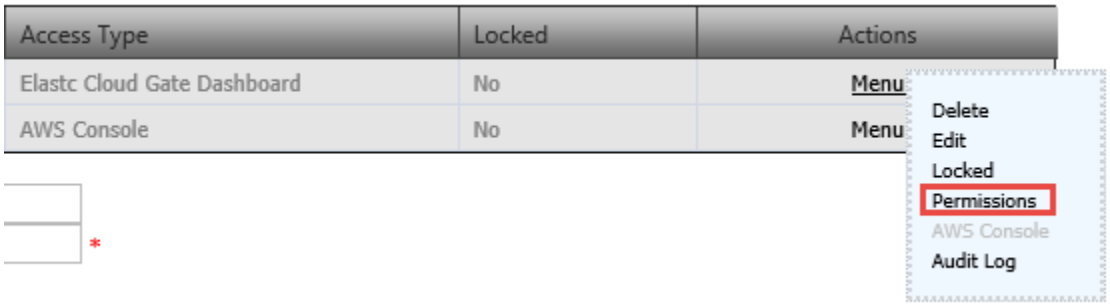
Note: Console user has to use different URL to login to ECG portal. The URL is:
https://portal.ecloudgate.com/console/login.aspx

In addition, beside email and password, the user is asked for the access code on the login page.

You can see your access code on the Users Management page. This number is statically assigned to your account and does not change.

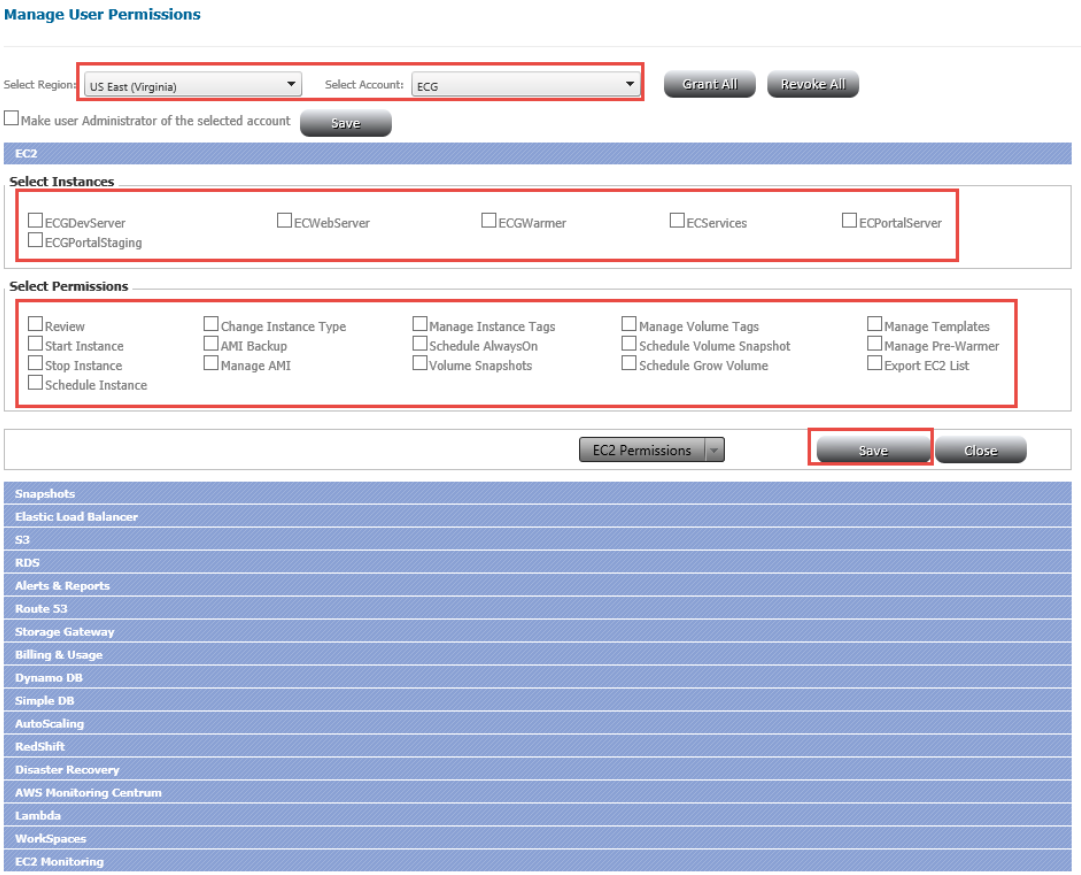
When the new user is created, you can grant him permission to actions and objects available in ECG portal.

To grant permission, within the users table from the context menu, select Permissions.



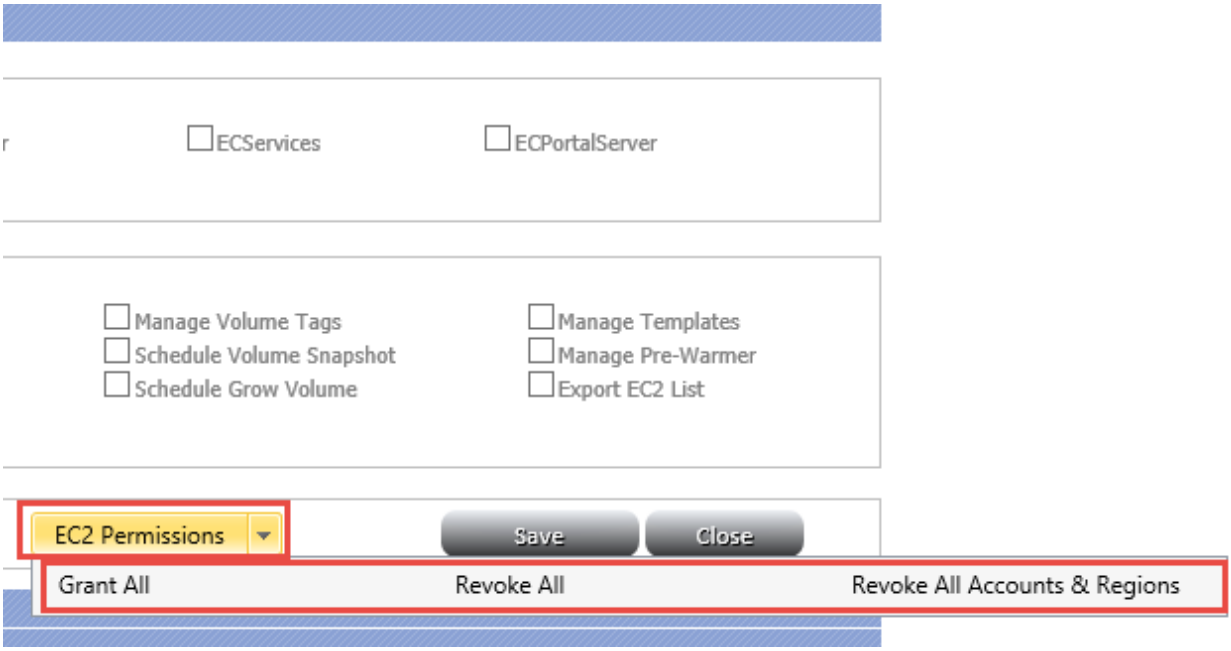
You can grant permissions as follows:

1. To grant access for individual actions and objects, review each section and make the appropriate selection; to apply changes, click Save under each section.

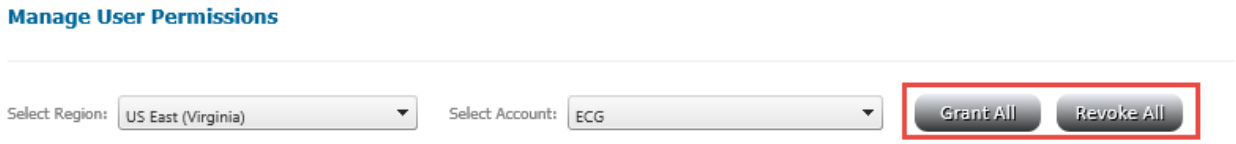


Permissions are applied only to actions and objects under the selected account and region.

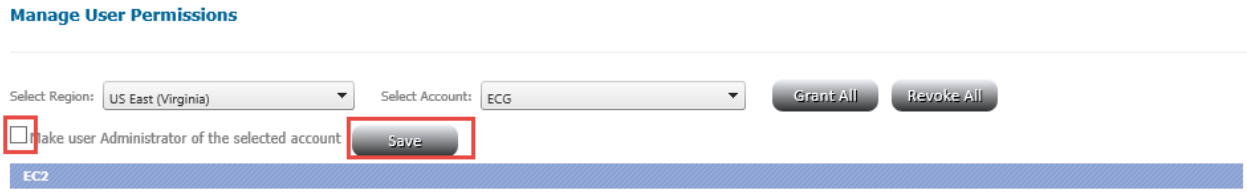
2. To apply or revoke permission to all actions and objects under the selected account, region, and section, click the down arrow on the Permissions button and select either Grant All or Revoke All. If you want to revoke permissions to the given section from all accounts and region, choose Revoke All Accounts & Region.



3. To grant permission to all actions and objects in all sections under the selected account and region, click Grant All on the top panel. In the same way, you can revoke all permissions by clicking Revoke All.



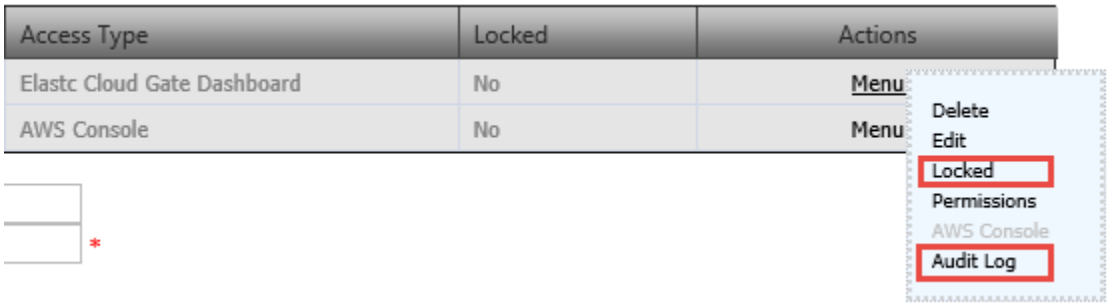
4. To grant permission to all actions and objects under the selected account, regardless of region or section, make the user an administrator. To make user an administrator, check Make user Administrator of the selected account and click Save.



At any time, you can edit or delete the console user by selecting the appropriate option from the context menu.

If you need to temporarily prevent the console user from logging in, from the context menu select Locked. To unlock user account, select Unlocked from the context menu.

All actions taken by the console user are recorded. You can review those actions by selecting Audit Log from the context menu.



How to update profile

To update your profile from the Settings menu, select Update Profile.

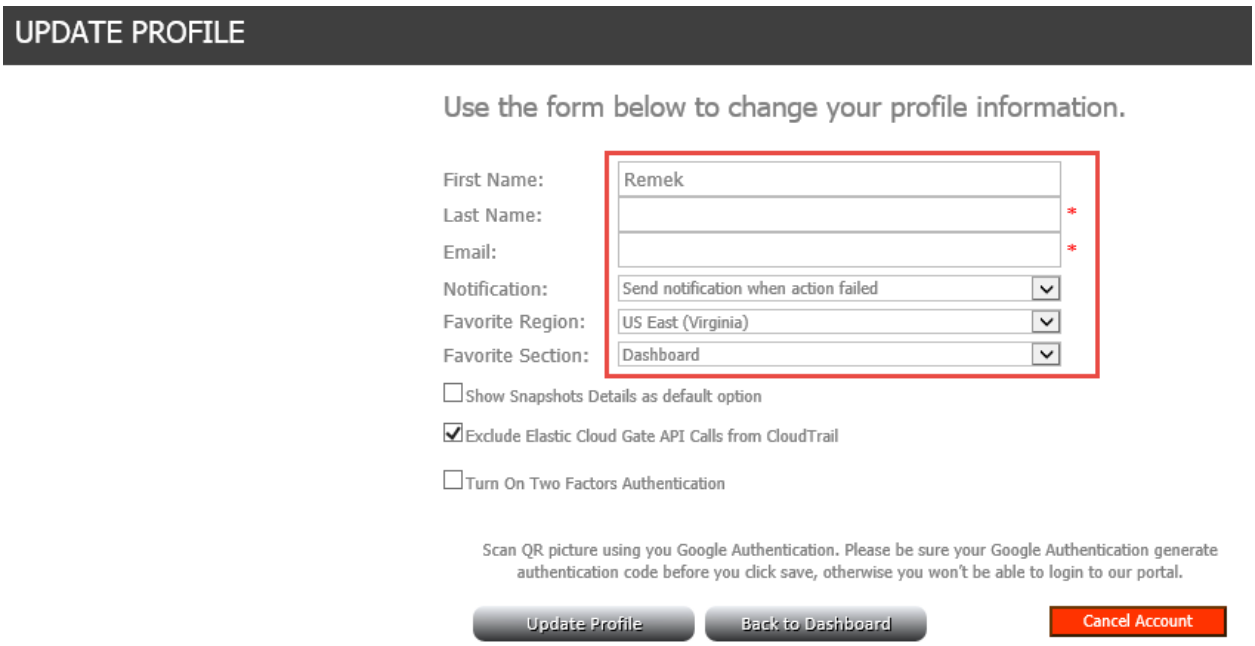
On the profile page, in addition to name and email, you can change:

Notification – Select how you want to be notified about execution of your schedulers. The options to choose from are:

- Send notification when action failed – Receive notification email only if the scheduled task failed
- Send notification when action success or failed – Receive notification email if the execution of the task was a success or failure
- Don't send notification – You will not receive any notifications about execution of your tasks

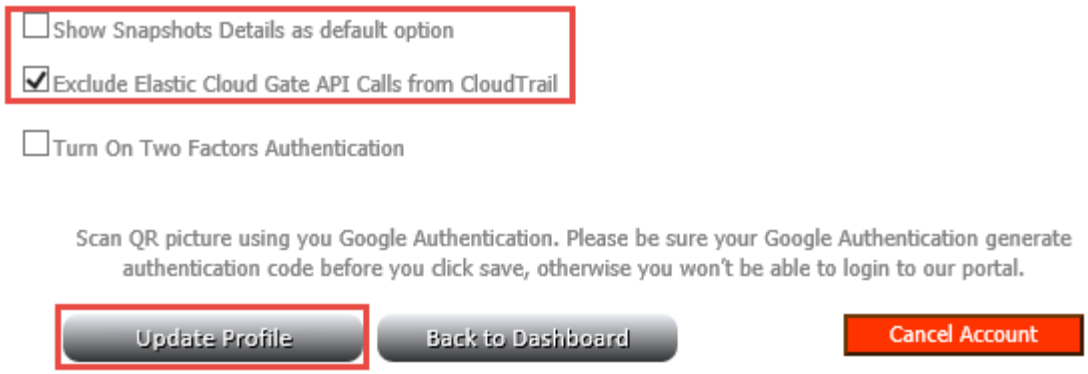
Favorite Region – From the drop down list, select region set as default after you login to portal.

Favorite Section – From the drop down list, select the default section of our portal you are automatically redirected after login.



Show Snapshot Details as default option – When checked, whenever you open the Snapshot section, snapshot details information, including Instance Name, Volume Name, and Attachment are automatically populated.

Excluded Elastic Cloud Gate API Calls from CloudTrail – When checked, all calls to your AWS made by our system are excluded from the CloudTrail list.



Turn On Two Factor Authentication – Enables multi factor authentication. Learn more about this option here: [How to turn on multi factor authentication (MFA)]
How to turn on multi factor authentication (MFA)

After changing your profile settings, click Update Profile to apply changes.

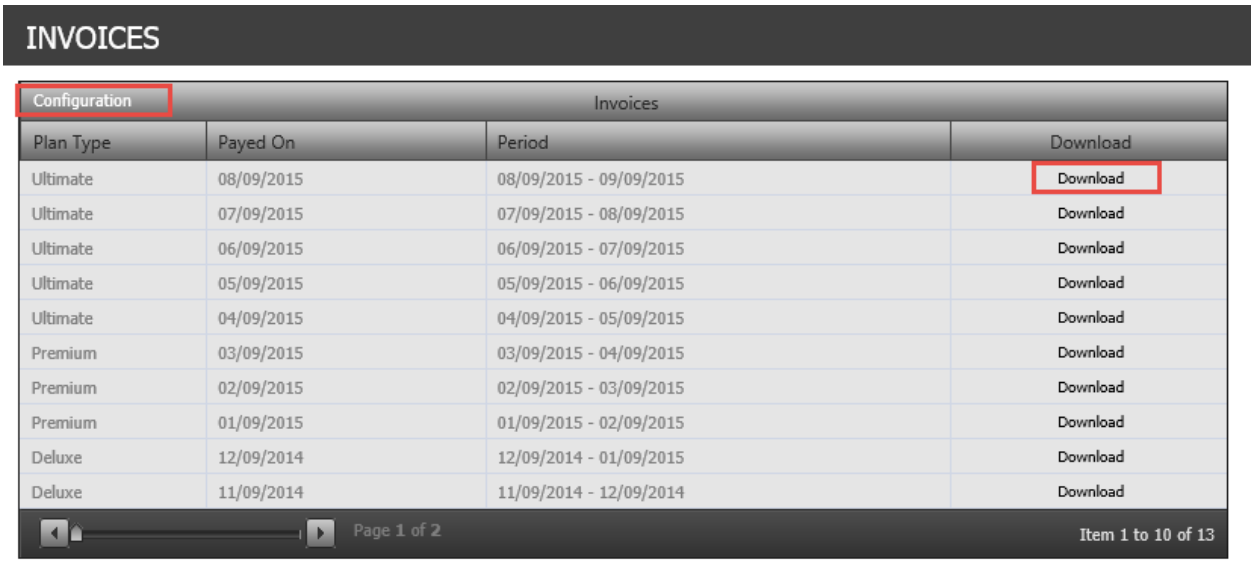
Additionally, on the profile page you can cancel your ECG account: to do so, click Cancel Account.

Manage Invoices

To review your invoices from the Settings menu, select Invoices.

Visible on the new page is a list of all invoices already processed.

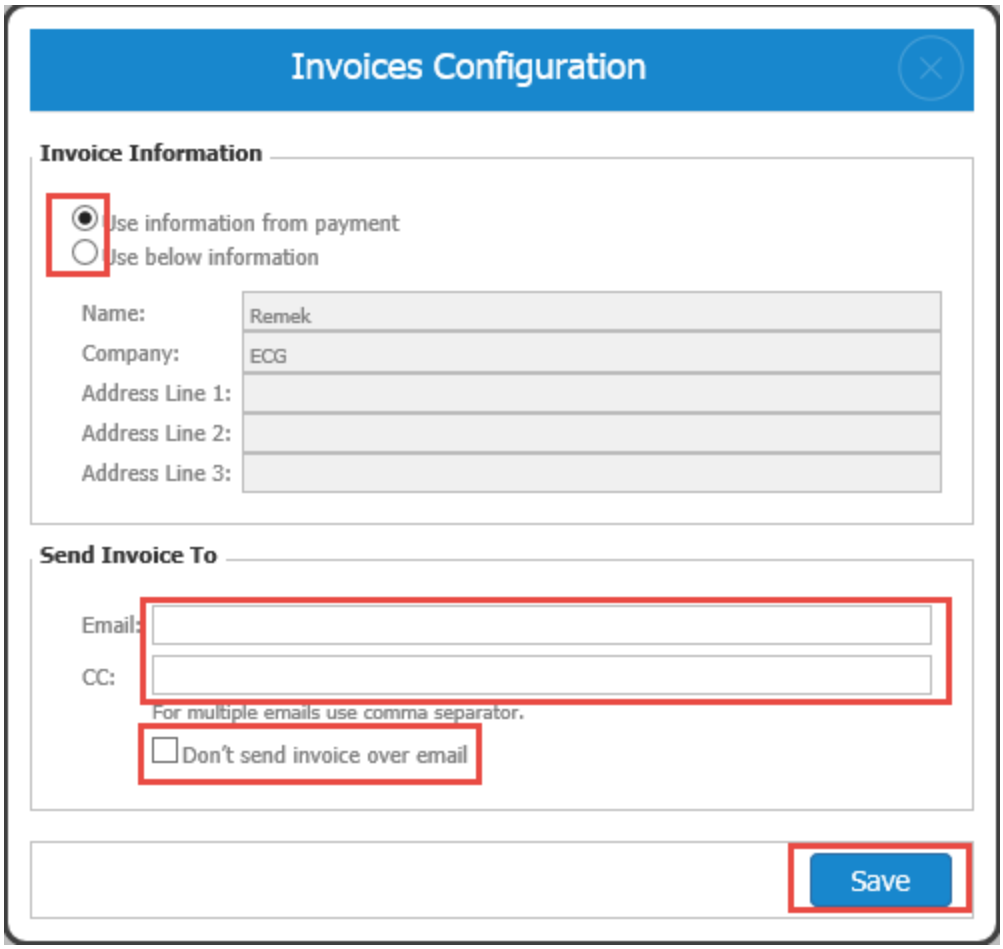
To download invoice from a given period, click Download on the last column.



The name and address on the invoice are taken from your payment information.
To change this, click Configuration at the top of the panel.
In the new window, check Use below information and enter new information you want on the invoice.

As default, invoices are sent to your login user email. You change this by modifying the information in the Send Invoice To section. You can specify additional email(s) where you want the invoice to be sent in the CC box (for multiple emails, use a comma separator).

If you don't want to receive invoices by email, check the Don't send invoice over email checkbox.

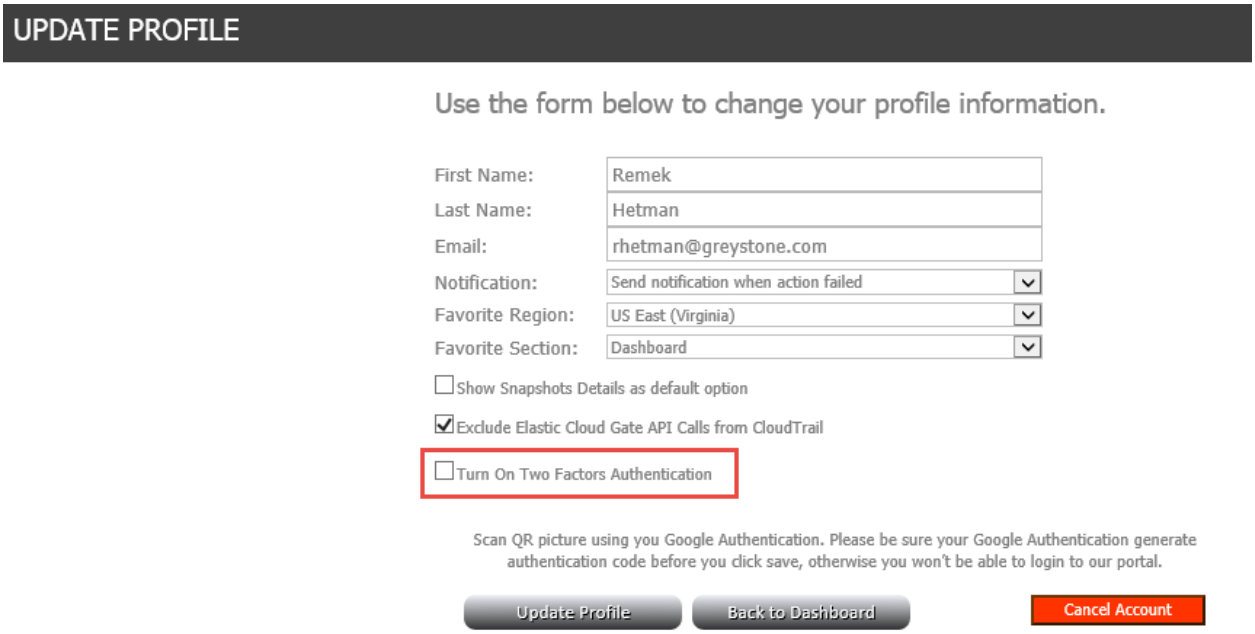


How to turn on multi factor authentication (MFA)

Elastic Cloud Gate provides the option to use MFA (Multi Factor Authentication) to access your account.

To use MFA, you must install Google Authenticator on your smart phone.

To turn on MFA, from the Setting menu select Update Profile.
On the profile page, check Turn On Two Factor Authentication.



After that, you are shown a QR picture.
Scan this picture using Google Authenticator.

Click Update Profile.

When you login, in addition to your regular user name and password, you are asked for the number generated by Google Authenticator. This number is generated every 30 seconds.

Please remember, when this feature is turned on you cannot login to our portal without entering the correct authentication number.

Turn this option off at any time by unchecking Turn On Two Factor Authentication and clicking Update Profile.

Email Notification Settings

Most schedulers provide option to select how the user can be notified about execution of the task.

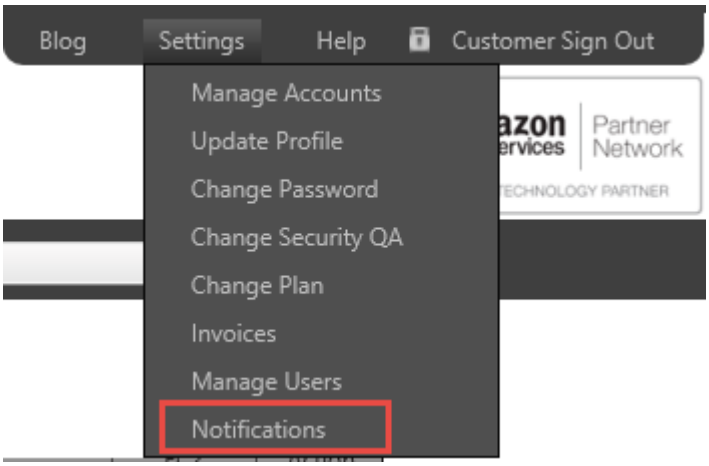
The options to choose from are:

"Use Global Notification Settings" (default) – When selected, user will be notified based on the global notification settings configured under user profile. For more information about user profile visit: How to update profile

"Do Not Send Notification" – When selected, no notification will be sent to user.

Custom (Notification Name):
When selected, notification will be sent based on the custom settings. User can create multiple different notifications and assign them to different schedulers. For instance, one can create different notification that will be sent to different email addresses.

To create custom notification from the Settings menu, select "Notifications"

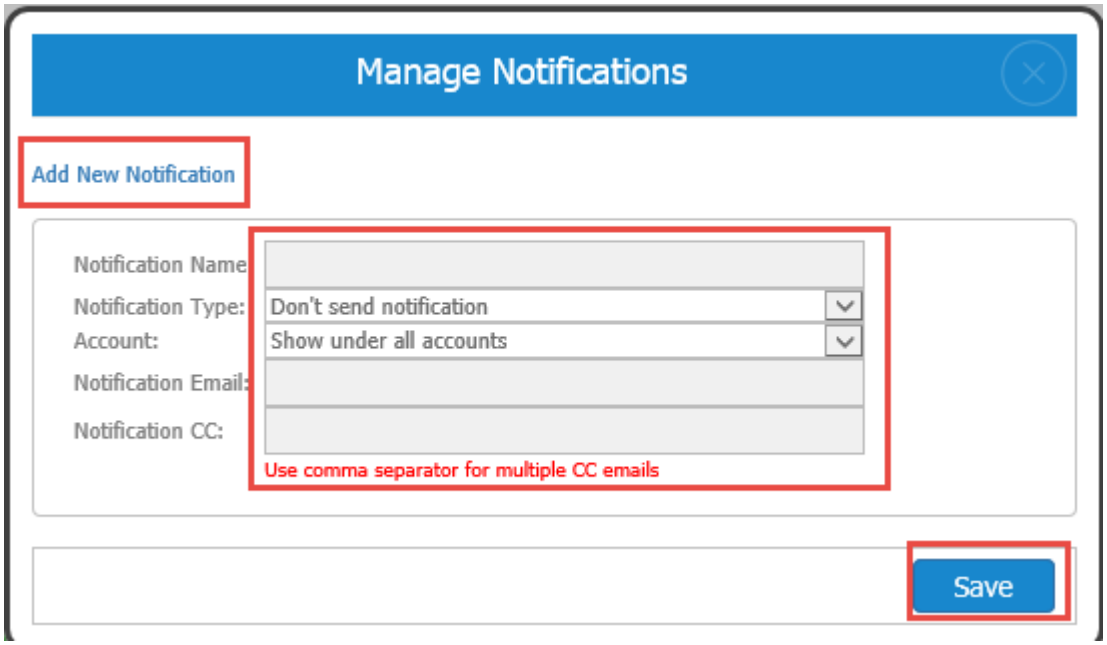


To create new notification:
Click "Add New Notification"
Enter notification name and notification type.
Account

- "Show under all accounts" – When selected, this notification will appear under scheduler regardless of selected account
- Account name – notification will appear under scheduler only for selected account.

Notification Email – email to which notification will be sent.
Notification CC (optional) – additional email(s) (comma separated) where notification will be sent.

Click “Save”



To edit or delete existing notification, click appropriate option in the table.