

Quick start guide for Infscope UrBackup Appliance on Amazon Web Services

Purpose of this document

This document will give detailed step-by-step instructions on how to get Infscope UrBackup Appliance running on Amazon Web services (AWS). This document does not require any prior knowledge with AWS. You might want to follow the less detailed instruction in the administration guide if you already have prior AWS knowledge.

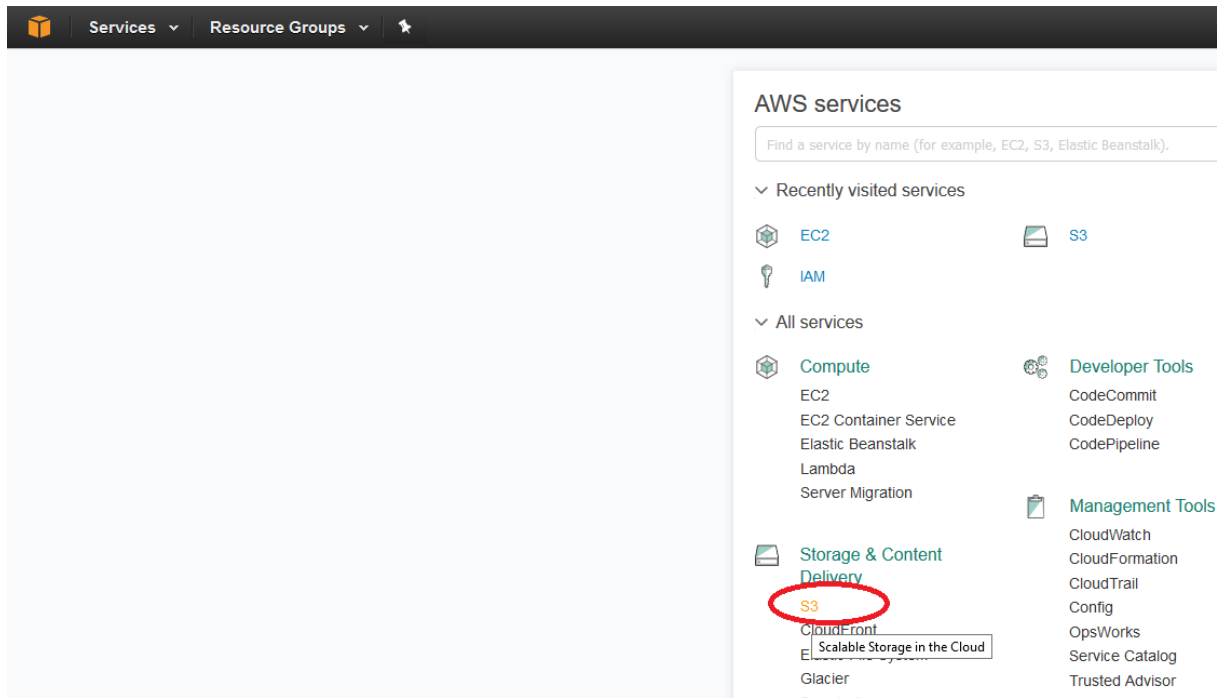
Contents

- Purpose of this document1
- Step 1: Create AWS Simple Storage Service (S3) bucket for storing backups1
- Step 2: Create an AWS Identity and Access Management (IAM) role for access to the new S3 bucket .3
- Step 3: Create Infscope UrBackup Appliance AWS Elastic Compute Cloud (EC2) instance7
- Step 4: Assign Elastic IP to new EC2 instance10
- Step 5: Setup AWS CloudFront HTTPS access to UrBackup Appliance Instance12
- Step 6: Configure Infscope UrBackup Appliance instance14

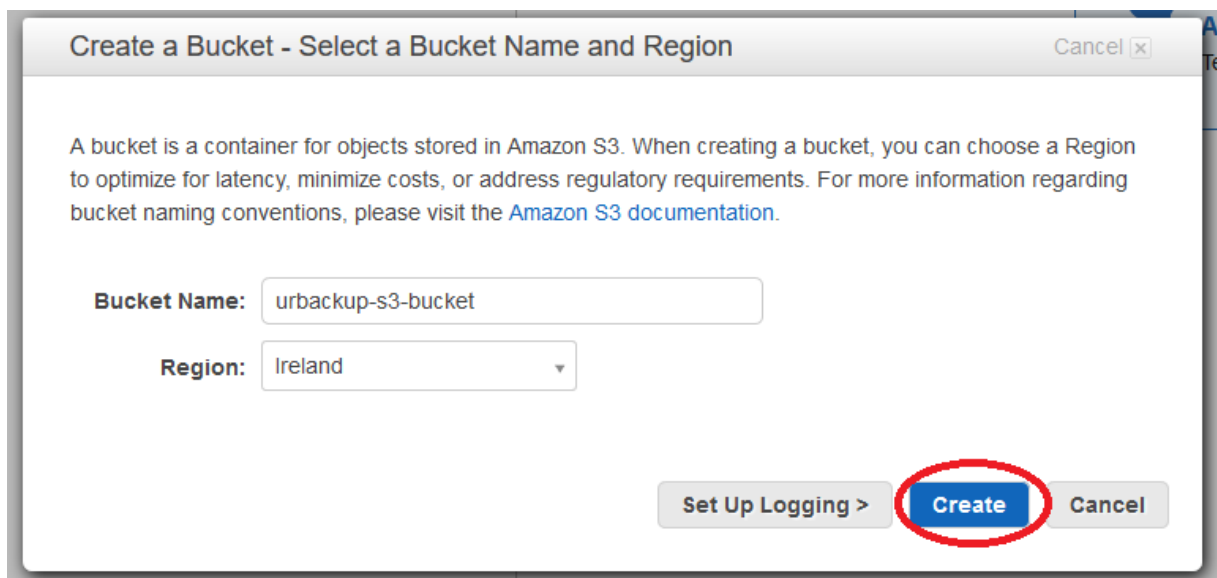
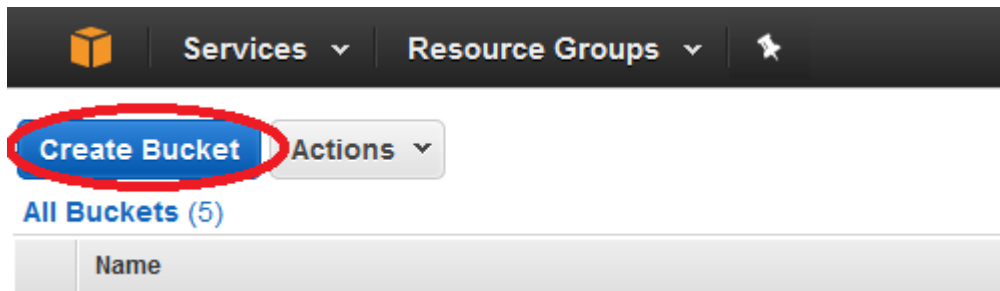
Step 1: Create AWS Simple Storage Service (S3) bucket for storing backups

Infscope UrBackup appliance stores all metadata and backups into a single AWS S3 bucket. As a first step this AWS S3 bucket needs to be created.

Go to the S3 service in your AWS management console:



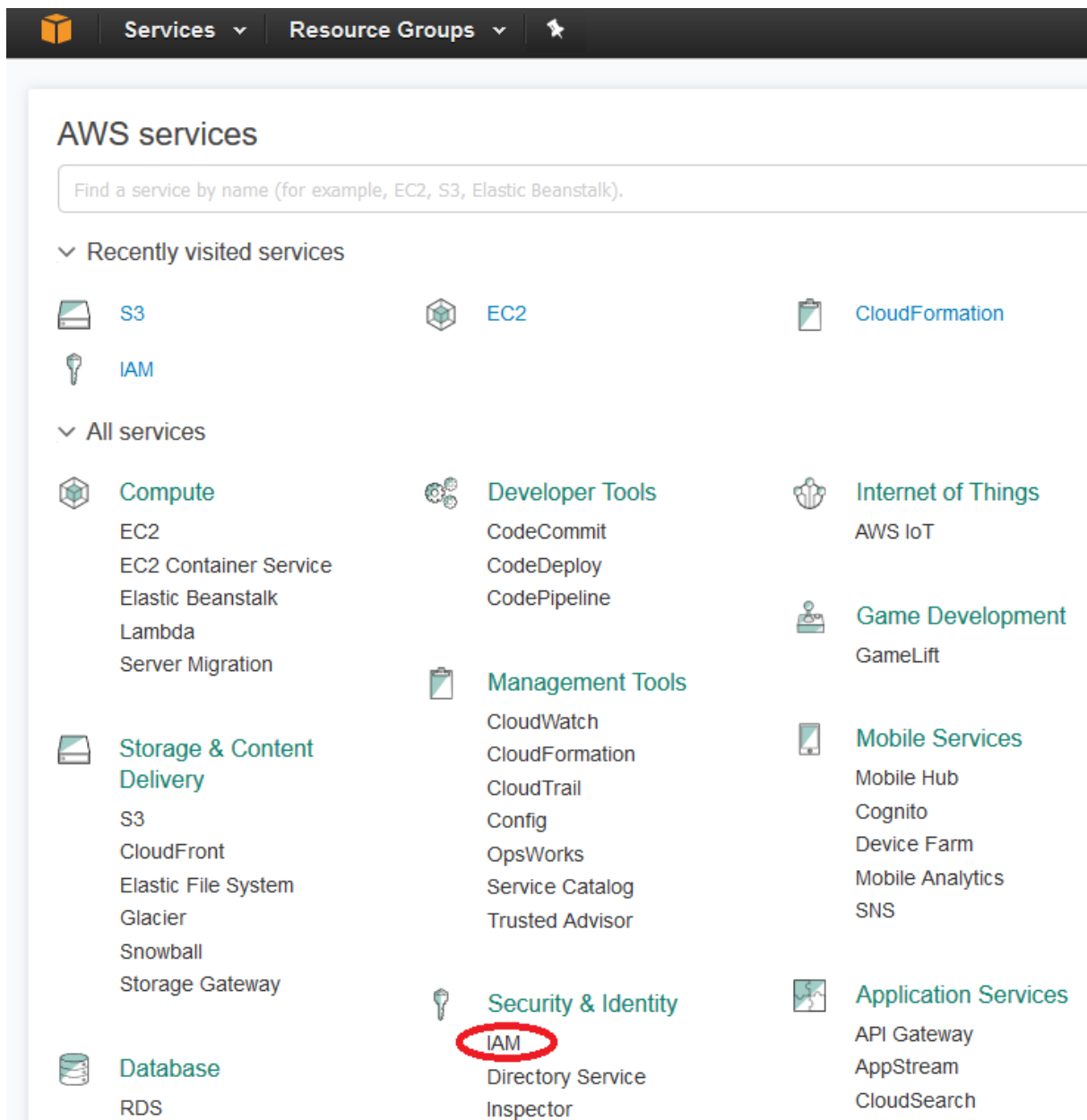
Create a bucket:



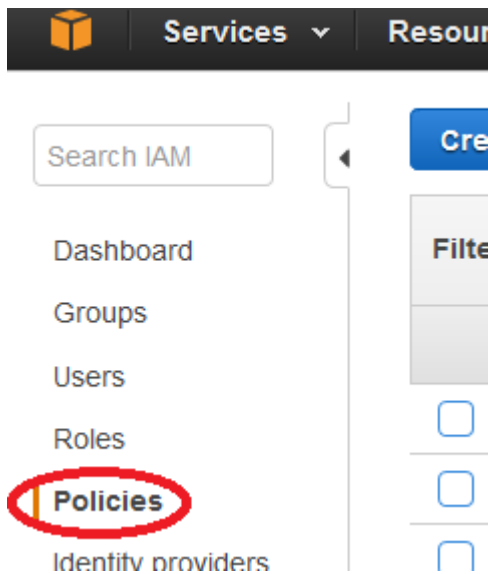
Step 2: Create an AWS Identity and Access Management (IAM) role for access to the new S3 bucket

In order to access and write to the S3 bucket an IAM role needs to be created that grants an AWS instance access to the new S3 bucket.

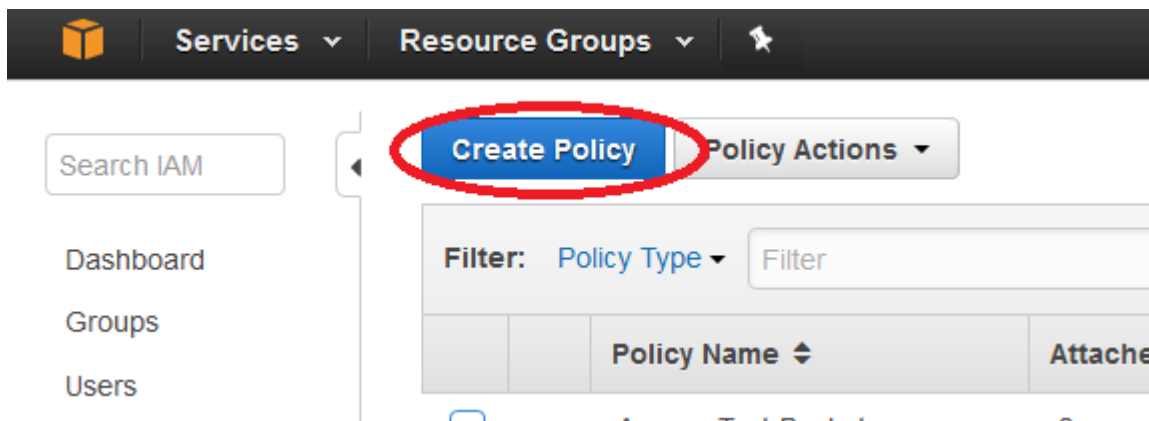
Go to IAM in the AWS management console:



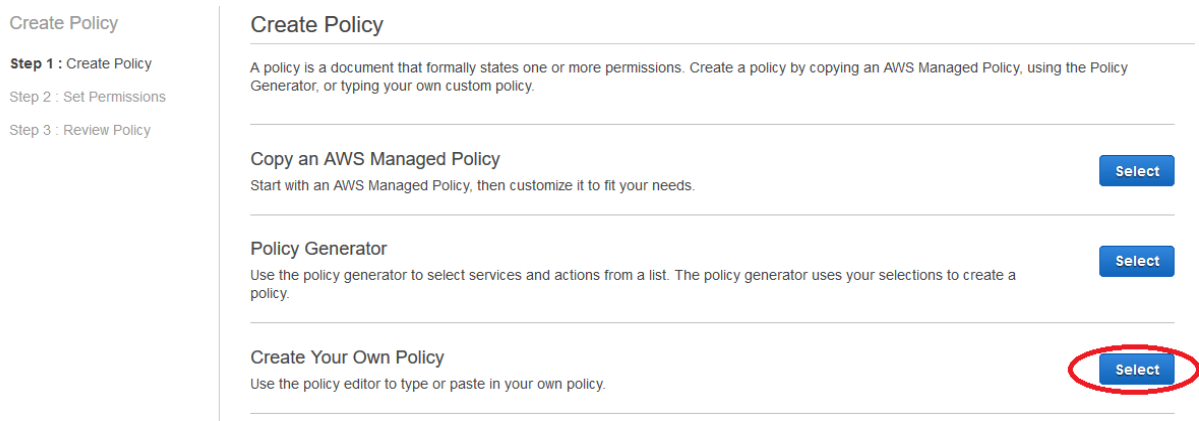
Select "Policies":



Create a new Policy:



Select "Create your own policy":



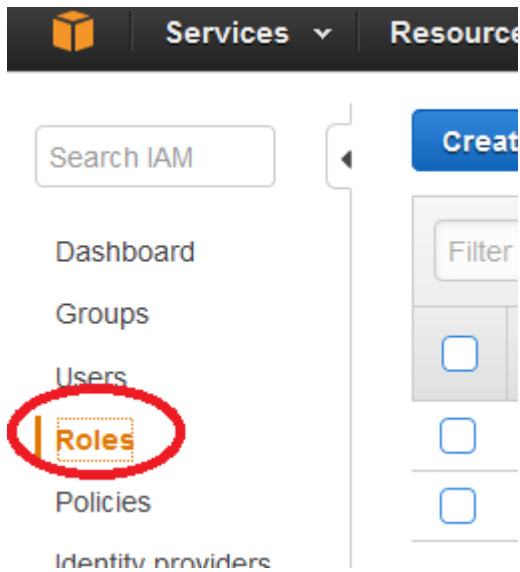
Enter a policy name. E.g. "urbackup-s3-bucket-access".

Enter following policy document, replacing the example bucket name marked in red with the name of your own, previously created bucket:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1460057323556",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::urbackup-s3-bucket"
    },
    {
      "Sid": "Stmt1460057323557",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::urbackup-s3-bucket/*"
    }
  ]
}
```

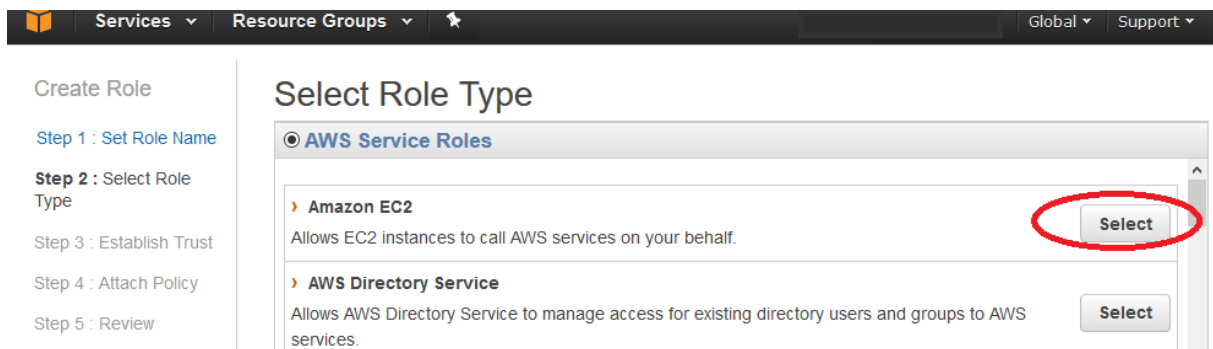
Create the new policy.

Select "Roles":



Enter a new name. E.g. "urbackup-s3-bucket-access".

Select Amazon EC2 service role:



Select the previously created policy:

Services ▾ Resource Groups ▾

Create Role

- Step 1 : Set Role Name
- Step 2 : Select Role Type
- Step 3 : Establish Trust
- Step 4 : Attach Policy**
- Step 5 : Review

Attach Policy

Select one or more policies to attach. Each role can have up to 10 policies attached.

Filter: Policy Type ▾

	Policy Name ↕	Attached Entities ↕	Created
<input checked="" type="checkbox"/>	urbackup-s3-bucket...	0	201...

Create the role.

Step 3: Create Infscope UrBackup Appliance AWS Elastic Compute Cloud (EC2) instance

Go to <http://aws.amazon.com/marketplace/pp/B01MTQ7U37> and click on continue.

Click on “Manual Launch” then “Launch with EC2 Console” in your region:

Launch on EC2: Infscope UrBackup Appliance

1-Click Launch
Review, modify and launch

Manual Launch
With EC2 Console, API or CLI

Click "Accept Software Terms" to gain access to this Software

Once you accept these terms, you will have access to this software in any supported region. You can then launch the AMIs listed below directly from the EC2 console, EC2 APIs, or with other AWS management tools.

Version

1.0, released 11/16/2016

[Usage Instructions](#)

Launch

AMI IDs

Region	ID	
Asia Pacific (Mumbai)	ami-0689fd69	Launch with EC2 Console
EU (Ireland)	ami-4e36673d	Launch with EC2 Console
Asia Pacific (Singapore)	ami-a6d271c5	Launch with EC2 Console
Asia Pacific (Sydney)	ami-ac152acf	Launch with EC2 Console

Priority

For

U

Hour

Total

EC2

t2.m

t2.sr

t2.m

m3.r

m3.l

m3.>

m3.2

cr1.i

hi1.4

hs1.

i2.xl

i2.2>

i2.4>

i2.8>

r3.la

r3.xl

r3.2

r3.4:

Choose your instance type, then click "Next: Configure Instance Details".

Select the previously created IAM role which can access the previously created S3 bucket, then click on "Next: Add Storage":

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances [Launch into Auto Scaling Group](#)

Purchasing option Request Spot instances

Network [Create new VPC](#)

Subnet [Create new subnet](#)

Auto-assign Public IP

IAM role [Create new IAM role](#)

Shutdown behavior

Enable termination protection Protect against accidental termination

Monitoring Enable CloudWatch detailed monitoring
[Additional charges apply.](#)

Tenancy
[Additional charges will apply for dedicated tenancy.](#)

Advanced Details

Increase the size of your root disk to an appropriate size. For a moderately used backup server 128 GiB is a generous starting point.

Add a disk as cache for AWS S3. Use instance storage if available. The appropriate amount depends on the amount of data that will be stored in your S3 bucket and how the data changes during backups. You can detach the disk and attach a larger or smaller one later. Start with e.g. 256 GiB. Set the disks to delete on termination:

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encr
Root	/dev/xvda	snap-0a65afc17a98aeb8	<input type="text" value="128"/>	General Purpose SSD (gp2)	384 / 3000	N/A	<input checked="" type="checkbox"/>	Not En
<input type="text" value="EBS"/>	<input type="text" value="/dev/sdb"/>	<input type="text" value="Search (case-insensit)"/>	<input type="text" value="256"/>	General Purpose €	768 / 3000	N/A	<input checked="" type="checkbox"/>	Not E

[Add New Volume](#)

Next you will probably want give the instance a descriptive name.

Then create or select a security group which allows access on at least ports 80 and 55415:

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: Create a new security group

Select an existing security group

Security group name:

Description:

Type <small>i</small>	Protocol <small>i</small>	Port Range <small>i</small>	Source <small>i</small>	
SSH <small>v</small>	TCP	22	Custom <small>v</small> 0.0.0.0/0	<small>✕</small>
HTTP <small>v</small>	TCP	80	Custom <small>v</small> 0.0.0.0/0	<small>✕</small>
Custom TCP Rule <small>v</small>	TCP	55415	Custom <small>v</small> 0.0.0.0/0	<small>✕</small>

Add Rule

Then launch the instance and wait a bit for it to boot.

Step 4: Assign Elastic IP to new EC2 instance

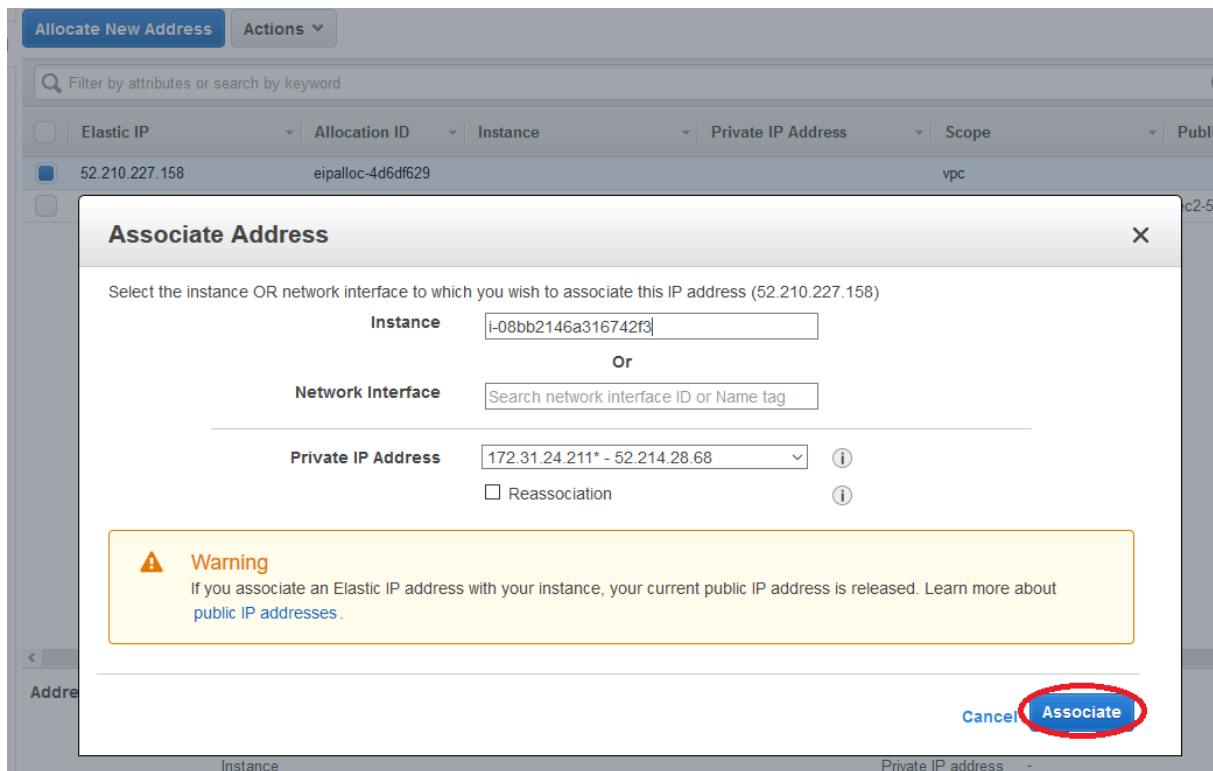
At this point you will probably want to assign an elastic IP to the Infscape UrBackup Appliance instance, such that it will always be reachable at the same address and clients are able to connect to their backup server.

You may also want to setup a DNS entry to that IP, though that is out of scope of this quick start document.

Go to “Elastic IPs” and allocate a new IP address:

The screenshot shows the AWS Management Console interface. At the top, there is a navigation bar with 'Services' and 'Resource Groups' dropdown menus. On the left side, there is a navigation pane with various categories: EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES (with sub-items: Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts), IMAGES (with sub-items: AMIs, Bundle Tasks), ELASTIC BLOCK STORE (with sub-items: Volumes, Snapshots), NETWORK & SECURITY (with sub-item: Security Groups), and Elastic IPs (highlighted with an orange bar). The main content area shows the 'Elastic IPs' page. At the top of this page, the 'Allocate New Address' button is circled in red. Below it is a search bar with the text 'Filter by attributes or search by keyword'. A table with two columns, 'Elastic IP' and 'Allocation ID', is visible. The table contains two rows, both with 'eipalloc-4' in the 'Allocation ID' column. A scroll bar is visible at the bottom of the table area.

Associate the IP address with the Infscope UrBackup Appliance instance:



Step 5: Setup AWS CloudFront HTTPS access to UrBackup Appliance Instance

We will setup AWS CloudFront such that access to the Infscope UrBackup Appliance happens via HTTPS.


Go to CloudFront in the AWS management console:

AWS services

Find a service by name (for example, EC2, S3, Elastic Beanstalk).

Recently visited services

 CloudFront

 EC2

 S3

All services

 Compute

EC2

EC2 Container Service

Elastic Beanstalk

Lambda

Server Migration

 Developer Tools

CodeCommit

CodeDeploy

CodePipeline

 Storage & Content Delivery

S3

CloudFront

Elastic File System

 Management Tools

CloudWatch

CloudFormation

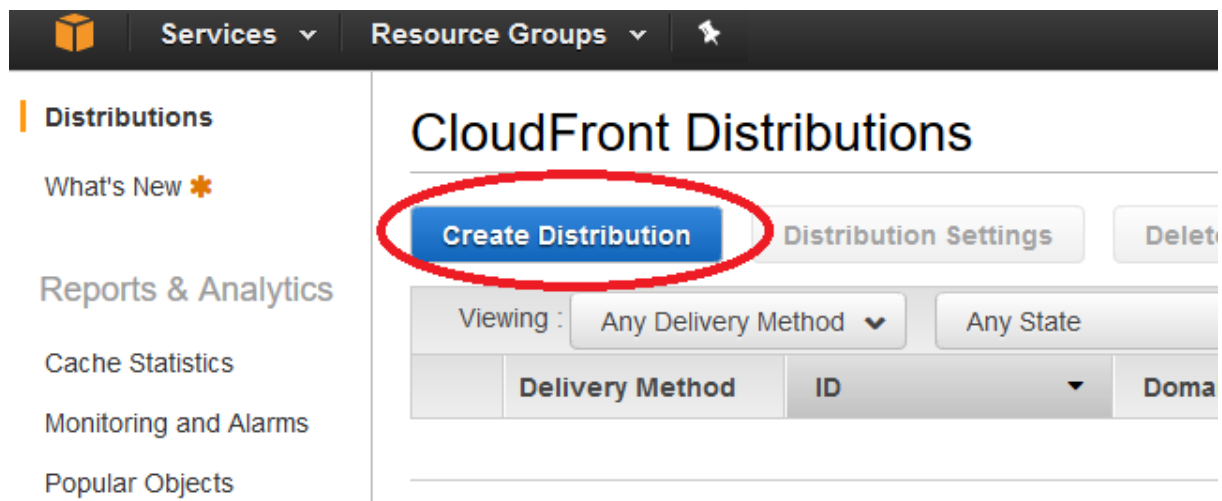
CloudTrail

Config

OpsWorks

Service Catalog

Create a new distribution:



The screenshot shows the AWS Management Console interface. At the top, there are navigation tabs for 'Services', 'Resource Groups', and a search icon. On the left sidebar, there are menu items: 'Distributions', 'What's New', 'Reports & Analytics', 'Cache Statistics', 'Monitoring and Alarms', and 'Popular Objects'. The main content area is titled 'CloudFront Distributions'. Below the title, there is a 'Create Distribution' button circled in red, followed by 'Distribution Settings' and 'Delete' buttons. Below these buttons, there are filters for 'Viewing : Any Delivery Method' and 'Any State'. At the bottom, there is a table header with columns: 'Delivery Method', 'ID', and 'Doma'.

Select "Web".

Select your Elastic IP public DNS as origin domain name. Select "HTTP only" as "Origin protocol policy". Select "GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE" as allowed HTTP methods. Set "Viewer Protocol Policy" to "HTTPS only". Set "Query String Forwarding" to "Forward all, cache based on all".

Step 1: Select delivery method

Step 2: Create distribution

Origin Domain Name	<input type="text" value="158.eu-west-1.compute.amazonaws.com"/>					
Origin Path	<input type="text"/>					
Origin ID	<input type="text" value="Custom-ec2-52-210-227-158.eu-west-1"/>					
Origin SSL Protocols	<input checked="" type="checkbox"/> TLSv1.2 <input checked="" type="checkbox"/> TLSv1.1 <input checked="" type="checkbox"/> TLSv1 <input type="checkbox"/> SSLv3					
Origin Protocol Policy	<input checked="" type="radio"/> HTTP Only <input type="radio"/> HTTPS Only <input type="radio"/> Match Viewer					
HTTP Port	<input type="text" value="80"/>					
HTTPS Port	<input type="text" value="443"/>					
Origin Custom Headers	<table><thead><tr><th>Header Name</th><th>Value</th></tr></thead><tbody><tr><td><input type="text"/></td><td><input type="text"/></td></tr></tbody></table>	Header Name	Value	<input type="text"/>	<input type="text"/>	
Header Name	Value					
<input type="text"/>	<input type="text"/>					

Default Cache Behavior Settings

Path Pattern	<input type="text" value="Default (*)"/>	
Viewer Protocol Policy	<input type="radio"/> HTTP and HTTPS <input type="radio"/> Redirect HTTP to HTTPS <input checked="" type="radio"/> HTTPS Only	If you want CloudFront either HTTP or HTTPS redirect all HTTP request want CloudFront to rec
Allowed HTTP Methods	<input type="radio"/> GET, HEAD <input type="radio"/> GET, HEAD, OPTIONS <input checked="" type="radio"/> GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE	
Cached HTTP Methods	<input checked="" type="checkbox"/> GET, HEAD (Cached by default) <input type="checkbox"/> OPTIONS	
Forward Headers	<input type="text" value="None (Improves Caching)"/>	
Object Caching	<input checked="" type="radio"/> Use Origin Cache Headers <input type="radio"/> Customize Learn More	
Minimum TTL	<input type="text" value="0"/>	
Maximum TTL	<input type="text" value="31536000"/>	
Default TTL	<input type="text" value="86400"/>	
Forward Cookies	<input type="text" value="None (Improves Caching)"/>	
Query String Forwarding and Caching	<input type="text" value="Forward all, cache based on all"/>	
Smooth Streaming	<input type="radio"/> Yes <input checked="" type="radio"/> No	

Create the distribution and wait a bit for AWS to create the resources.

Step 6: Configure Infscape UrBackup Appliance instance

Access the Infscape UrBackup Appliance instance via CloudFront (<https://d3uk77p4xxxxx.cloudfront.net>). Enter the instance id found on the EC2 console (i-xxxxxxx) as the first step.

Setup - login

Welcome to your new AWS UrBackup Appliance instance!
Please enter the Amazon EC2 Instance Id to proceed. This is a security measure to prevent unauthorized access.

Amazon EC2 Instance Id

[Next](#)

Review the storage setup, then click next.

Enter the name of the previously created AWS S3 bucket:

Step 1 of 3 - Setup cloud storage

Infscope UrBackup Appliance stores all backups deduplicated, compressed and encrypted to a S3 bucket. If the S3 bucket was previously used as backup storage, it will import existing backups given the correct encryption key. Do not use the same S3 bucket from multiple instances simultaneously.

S3 storage encryption key (leave empty to generate one)

S3 bucket name



Current storage limit (can be increased later)



S3 storage class

[Next](#)

Enter an administrator password, an instance name and review the appliance URL and IP address. If you setup a DNS entry pointing to the IP address in step 4 change the IP address to the DNS name:

Step 2 of 3 - Setup UrBackup Appliance account and select UrBackup Appliance name

An UrBackup Appliance account allows you to reset your password, access your UrBackup Appliance over the Internet and to use external UrBackup Appliance monitoring.

- Continue without UrBackup Appliance account
- Register a new UrBackup Appliance account
- I have an existing UrBackup Appliance account

Password

Repeat password

Please also select a name for your UrBackup Appliance:

UrBackup Appliance name

Please select/confirm your timezone:

Timezone

America	▼
New_York	▼

UrBackup Appliance public IP address/hostname:

Public IP address/hostname to which clients can connect

UrBackup Appliance access URL:

UrBackup Appliance URL to which clients can connect

After finishing the initial setup, you can login as administrator and create your first client.