

Setting up a local Appliance with Amazon S3 as storage

Hardware prerequisites:

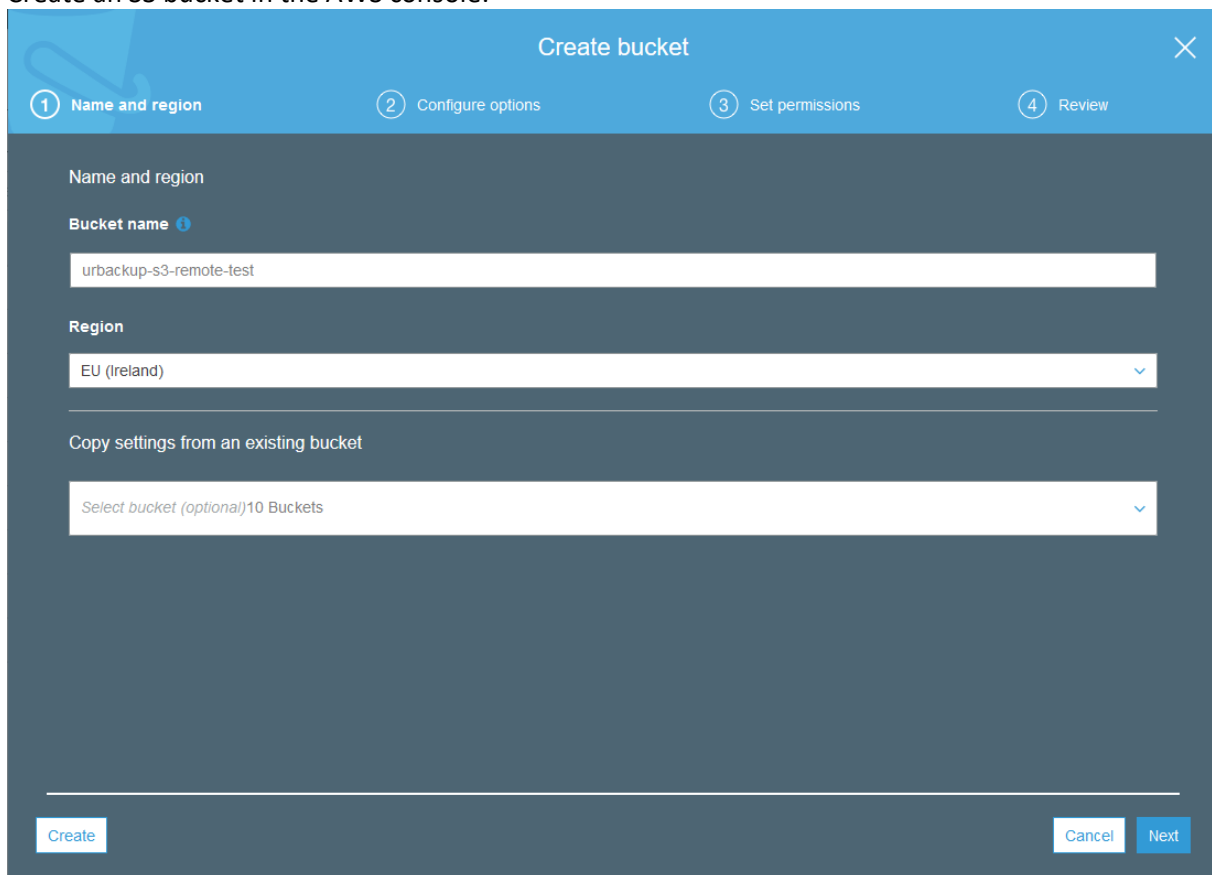
- Min. 4GB ECC RAM
- 64-bit x86 processor
- Primary disk should be flash storage (>32GB)
- Cache disk for RAID or cloud storage should be SSD/NVMe (>32GB)

Follow the installation instructions at <https://www.infscope.com/urbackup-appliance-download/> to install the Appliance.

Cache disk size: The cache disk is especially important when storing backups to remote (S3) storage. During backup, restore or running VMs every piece of data that isn't locally available needs to be retrieved from remote storage which has comparatively high latency. If this happens too often backups (or running VMs) become too slow. The cache should therefore be large enough that all data that is accessed regularly fits into it. If you plan on running a backed-up machine with a 500GB volume as VM in the appliance, your cache disk should be larger than 500GB.

Setting up S3 bucket

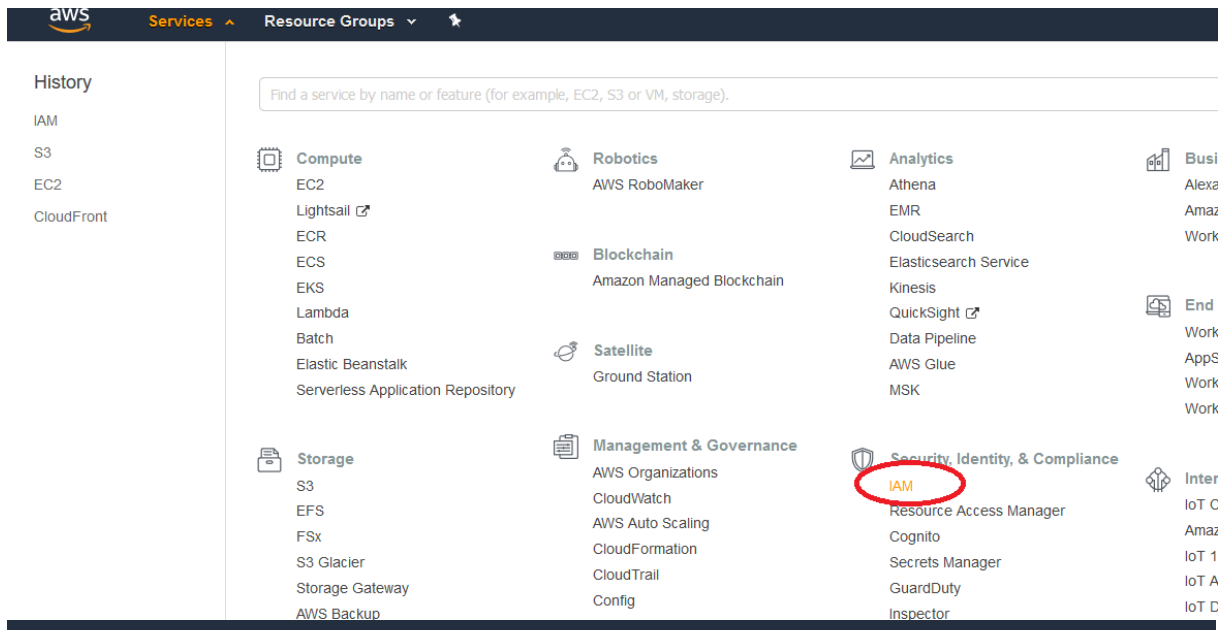
Create an S3 bucket in the AWS console:



The screenshot shows the 'Create bucket' wizard in the AWS console, specifically the 'Name and region' step. The wizard has four steps: 1. Name and region, 2. Configure options, 3. Set permissions, and 4. Review. The 'Name and region' step is active. The 'Bucket name' field contains 'urbackup-s3-remote-test'. The 'Region' dropdown menu is set to 'EU (Ireland)'. There is a section for 'Copy settings from an existing bucket' with a dropdown menu showing 'Select bucket (optional) 10 Buckets'. At the bottom, there are three buttons: 'Create', 'Cancel', and 'Next'.

Use the default options in the other steps in the “Create bucket” wizard.

Go to IAM and create a new user and give it access to the new S3 bucket:



Add user



Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[+ Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

- Access type* **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Create a policy for accessing the S3 bucket:

Add user

1 2 3 4 5

▼ Set permissions

Add user to group Copy permissions from existing user Attach existing policies directly

Create policy

Filter policies ▾ Showing 442 results

	Policy name ▾	Type	Used as	Description
<input type="checkbox"/>	AmazonCognitoDev...	AWS managed	None	Provides access to Amazon Cognito APIs...
<input type="checkbox"/>	AmazonCognitoPow...	AWS managed	None	Provides administrative access to existin...
<input type="checkbox"/>	AmazonCognitoRea...	AWS managed	None	Provides read only access to Amazon Co...
<input type="checkbox"/>	AmazonConnectFull...	AWS managed	None	Provides full access to Amazon Connect ...
<input type="checkbox"/>	AmazonConnectRe...	AWS managed	None	Grants permission to view the Amazon C...
<input type="checkbox"/>	AmazonDMSCloud...	AWS managed	None	Provides access to upload DMS replicati...
<input type="checkbox"/>	AmazonDMSRedshi...	AWS managed	None	Provides access to manage S3 settings f...
<input type="checkbox"/>	AmazonDMSVPCM...	AWS managed	None	Provides access to manage VPC settings...

▼ Set permissions boundary

Set a permissions boundary to control the maximum permissions this user can have. This is an advanced feature used to delegate permission management to others. [Learn more](#)

- Create user without a permissions boundary
- Use a permissions boundary to control the maximum user permissions

- Select JSON and copy & paste following policy while adjusting the bucket name:

Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor JSON Import managed policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "Stmt1460057323556",
6       "Effect": "Allow",
7       "Action": [
8         "s3:ListBucket",
9         "s3:GetBucketLocation"
10      ],
11      "Resource": "arn:aws:s3:::urbackup-s3-remote-test"
12    },
13    {
14      "Sid": "Stmt1460057323557",
15      "Effect": "Allow",
16      "Action": [
17        "s3:GetObject",
18        "s3:PutObject",
19        "s3:DeleteObject"
20      ],
21      "Resource": "arn:aws:s3:::urbackup-s3-remote-test/*"
22    }
23  ]
24 }
```

Cancel Review policy

Policy:

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

```
    ],
    "Resource": "arn:aws:s3:::urbackup-s3-remote-test/*"
  }
]
```

Name it then create the policy:

Create policy

Review policy

Name*

Use alphanumeric and '+=, @-_' characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and '+=, @-_' characters.

Summary

This policy defines some actions, resources, or conditions that do not provide permissions. To grant access, policies must have an action that has an applicable resource or condition. For details, choose **Show remaining**. [Learn more](#)

Filter			
Service	Access level	Resource	Request condition
Allow (1 of 178 services) Show remaining 177			
S3	Full: List Limited: Read, Write, Permissions management, Tagging	Multiple	None

Refresh the policy list and select the newly created policy for the user:

Add user

1 2 3 4 5

Set permissions

Add user to group Copy permissions from existing user Attach existing policies directly

Create policy Refresh

Filter policies Showing 443 results

	Policy name	Type	Used as	Description
<input type="checkbox"/>	access-app-prod-b...	Customer managed	Permissions policy (1)	
<input type="checkbox"/>	Access-Test-Bucket	Customer managed	Permissions policy (2)	
<input checked="" type="checkbox"/>	access-urbackup-s...	Customer managed	None	
<input type="checkbox"/>	AdministratorAccess	Job function	Permissions policy (1)	Provides full access to AWS services and...
<input type="checkbox"/>	AlexaForBusinessD...	AWS managed	None	Provide device setup access to AlexaFor...
<input type="checkbox"/>	AlexaForBusinessF...	AWS managed	None	Grants full access to AlexaForBusiness r...
<input type="checkbox"/>	AlexaForBusinessG...	AWS managed	None	Provide gateway execution access to Ale...
<input type="checkbox"/>	AlexaForBusinessR...	AWS managed	None	Provide read only access to AlexaForBus...

Set permissions boundary

Set a permissions boundary to control the maximum permissions this user can have. This is an advanced feature used to delegate permission management to others. [Learn more](#)

- Create user without a permissions boundary
- Use a permissions boundary to control the maximum user permissions

Continue with defaults and then copy&paste the access key and secret access key somewhere:

Add user

1 2 3 4 5

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://184104874291.signin.aws.amazon.com/console>

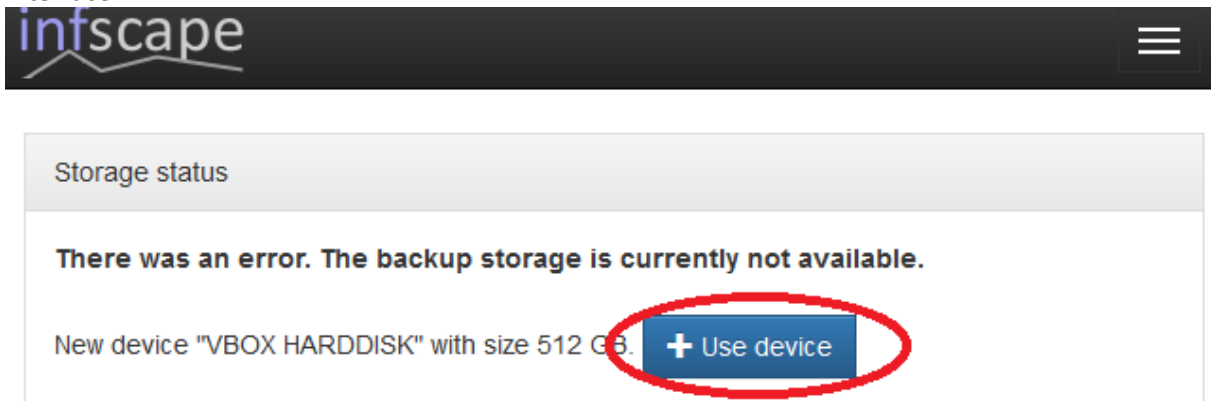
Download .csv

User	Access key ID	Secret access key
appliance-upload-test	AKIASVXMB0EZUPZBJ6P	pwG0wtW+Sh8wU1LkifTk9+ xOpU8PBJEtYF2qNe Hide

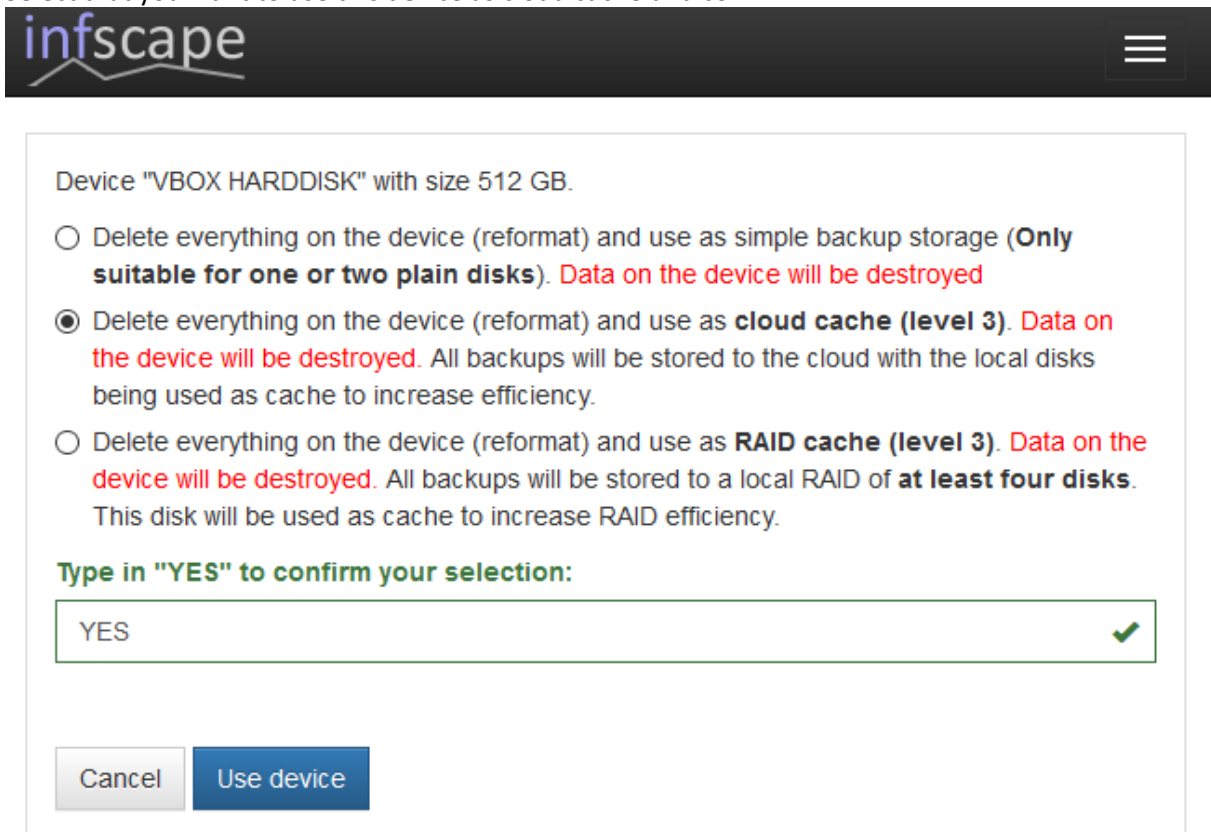
- Created user appliance-upload-test
- Attached policy access-urbackup-s3-remote to user appliance-upload-test
- Created access key for user appliance-upload-test

Connect Appliance to S3 bucket

Click on the "Use device" button of your cache disk on the status page on your appliance web interface:



Select that you want to use this device as cloud cache and confirm:



Select "Amazon S3", copy & paste the s3 access key and secret access key shown previously and enter your bucket name. Also copy your cloud storage encryption key and keep it somewhere save (it will be needed to recover from system disk loss) and configure the maximum size of your s3 backup storage:

Please select/confirm your underlying cloud storage settings.

Cloud storage encryption key

fd168ddba9b7c3cac6c4

Current storage limit (can only be increased)

1024 GB

Default cloud storage

Error retrieving information about existing cloud drives in your account. If you continue a new cloud drive will be created.

Amazon S3

S3 access key

AKIASVXMB0EZUPZBJI6P

S3 secret access key

pwGOwfW+Sh8wUILkifTk9j+xOpU8PBJEtYF2qNe

S3 bucket name

urbackup-s3-remote-test

S3 endpoint URL (leave empty for Amazon)

S3 storage class

Standard

Azure Blob Storage

Select/confirm and S3 will be used as backup storage.

Please note, that while the “Cloud synchronization window” is empty the appliance will only upload to s3 after a nightly cleanup, i.e. once at night:

The screenshot shows the infscape Settings page. The top navigation bar includes Status, Activities, Backups, VMs, Replication, Logs, Statistics, and Settings. The main navigation bar includes General, Mail, LDAP/AD, Users, System, Networking, Storage, and a button to Add new group. The sub-navigation bar includes Server, File Backups, Image Backups, Permissions, Client, Archive, Alerts, and Internet. The Advanced tab is selected, showing the following settings:

- Server URL: http://192.168.1.111
- Do not do image backups:
- Do not do file backups:
- Autoupdate clients:
- Max simultaneous backups: 100
- Max recently active clients: 10
- Cleanup time window: 1-7/3-4
- Total max backup speed for local network: - MBit/s
- Cloud storage synchronization window: (empty field, highlighted with a red oval)

A warning message is displayed at the bottom: "Warning: The settings configured on the client will overwrite the settings configured here. If you want to change this behaviour do not allow the client to change settings. Force reset of client settings with server settings once". A Save button is located at the bottom right.