

There's a hole in my bucket!



Olivier Rossi

Senior Solutions Architect
Veeam Software



Nicholas Serrecchia

Same as the other guy

Agenda

- AWS S3 Security Best Practices
- What does a hole in your bucket look like?
- Are all your eggs in the same basket?
- Setting up the S3 Bucket in AWS, Object Lock
- Bucket Policies, SCPs
- Ports, Security Groups and Network ACLs, Gateways
- IAM Policies – Apply Least Privileges



AWS S3 Security Best Practices

Security best practices for Amazon S3 - Amazon Simple Storage Service

- Disable ACLs
- Ensure that your Amazon S3 buckets use the correct policies and are not publicly accessible
- Implement least privilege access
- Encryption of data at rest – SSE-S3
- Consider S3 Object Lock
- Consider VPC endpoints for Amazon S3 access



What does a hole in your bucket look like?

- How many people/entities can list, write, read, and delete from your bucket
- How many IPs can read and write and delete from your bucket?
- Are all your Tier 1 app eggs in 1 basket?
3-2-1 rule, backup copy, archiving to a separate bucket...
- Is your bucket safe from unauthorized access or encryption and deletes?



Are all your eggs in the same basket?



Setting up the S3 Bucket in AWS

- ACLs disabled (no external account access)
- Block public access
- Enable SSE-S3
- Enable Object-Lock (Immutability)

▼ Advanced settings


Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. [Learn more](#)

☐ Disable

☒ Enable

Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

 Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Bucket Versioning.



Enabling Object Lock will permanently allow objects in this bucket to be locked

Enable Object Lock only if you need to prevent objects from being deleted to have data integrity and regulatory compliance. After you enable this feature, anyone with the appropriate permissions can put immutable objects in the bucket. You might be blocked from deleting the objects and the bucket. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten. [Learn more](#)

☒ I acknowledge that enabling Object Lock will permanently allow objects in this bucket to be locked.

Object-Lock behind the scene

Amazon S3 > Buckets > thereisaholeinmabucketveeamon2023 > Edit Object Lock

Edit Object Lock [Info](#)

Object Lock
Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. [Learn more](#)

Once Amazon S3 Object Lock is enabled, you can't disable Object Lock or suspend Bucket Versioning for the bucket.

Object Lock
Enabled

Default retention
Automatically protect new objects put into this bucket from being deleted or overwritten.

☒ Disable
☐ Enable

Cancel **Save changes**

- Veeam sets immutability per object
- Each object is locked with compliance mode
- Block-generation optimizes object re-use (i.e. lowers costs of unnecessary PUTs) (only applies to capacity tier)
- Do not use “default retention”

SCPs to protect bucket policy

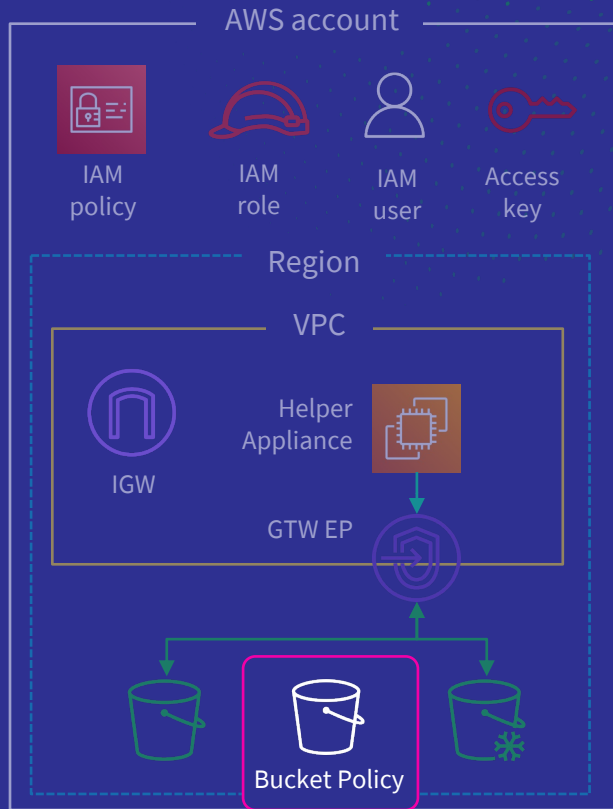
- Deny access
- To this bucket
- Except for the specified
aws:userid
- And only from this Source IP

```
orossi@morpheus:~$ aws sts get-caller-identity
{
  "UserId": "AID[REDACTED].CT3",
  "Account": "6[REDACTED]6",
  "Arn": "arn:aws:iam::6[REDACTED]:user/usr-awsprotekt21"
}
```

Bucket policy
The bucket policy, written in JSON, provides access to the objects

Public access is blocked because Block Public Access is turned on
To determine which settings are turned on, check the bucket's public access settings.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "*"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3::awsprotekt21",
        "arn:aws:s3::awsprotekt21/*"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:userid": [
            "[REDACTED]6",
            "[REDACTED].CT3",
            "[REDACTED].CT3:*"
          ]
        }
      },
      "IpAddress": {
        "aws:SourceIp": "24[REDACTED].0"
      }
    }
  ]
}
```



S3 Bucket Policy

Service Control Policy

Defined at the AWS Organization level

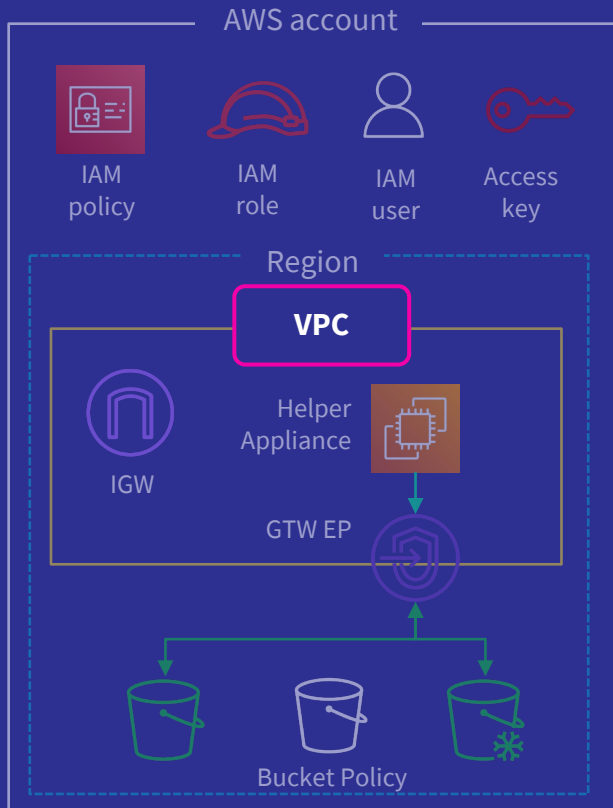
Defines a guardrail, or sets limits to the IAM users and roles in the affected accounts

Deny s3:*bucketpolicy

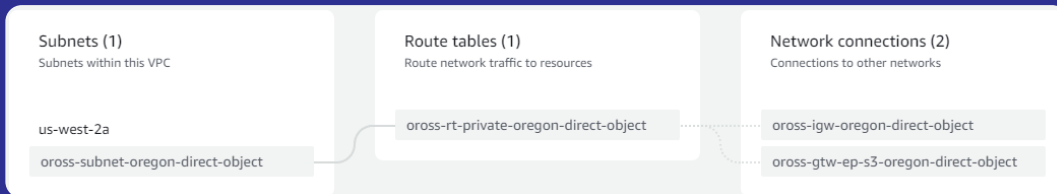
Don't have AWS Org? Use permission boundaries

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyBucketPolicyModification",
      "Effect": "Deny",
      "Action": [
        "s3:PutBucketPolicy",
        "s3:DeleteBucketPolicy"
      ],
      "Resource": [
        "arn:aws:s3:::your-bucket-name"
      ]
    }
  ]
}
```

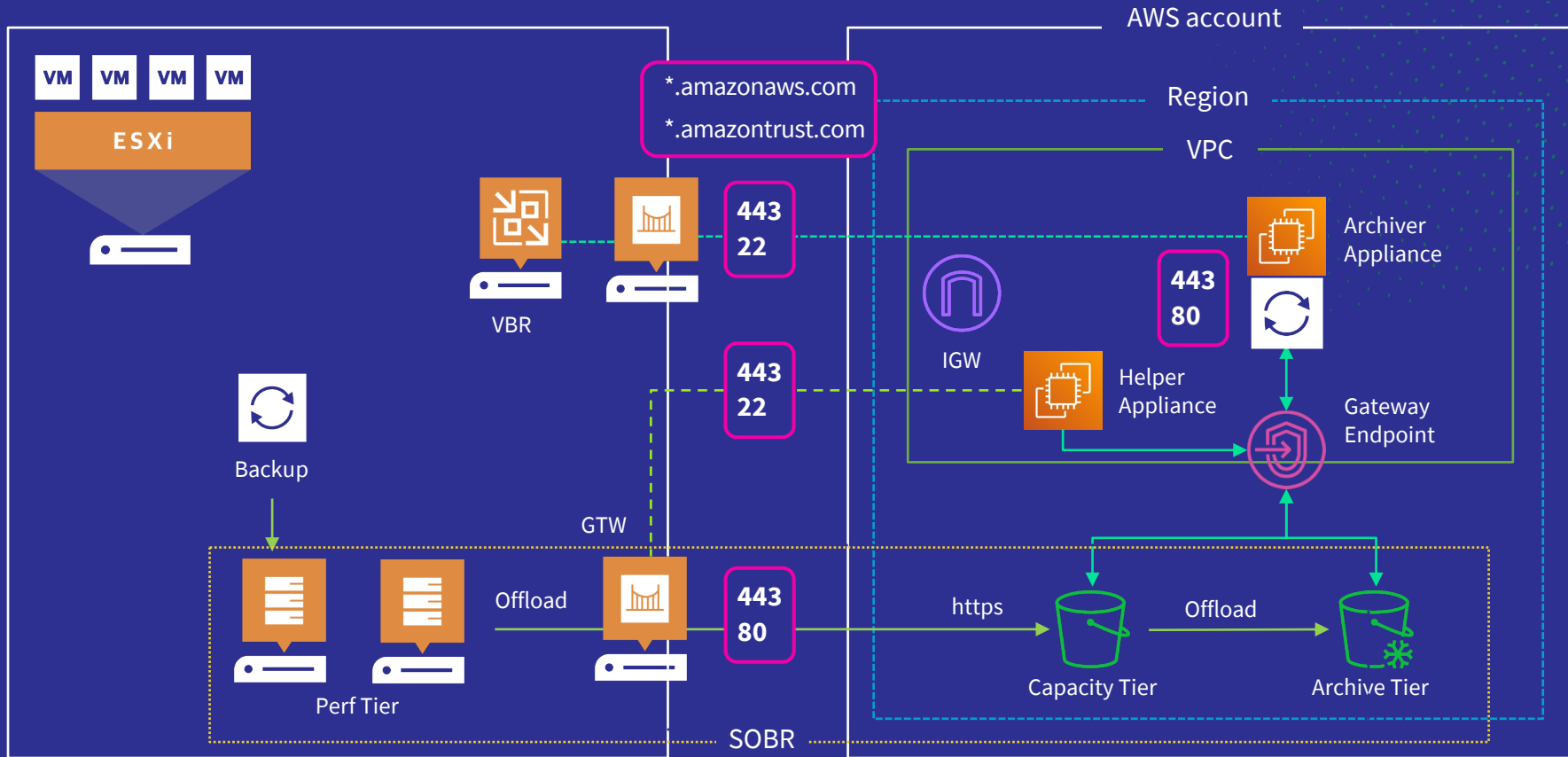
Setting up the VPC



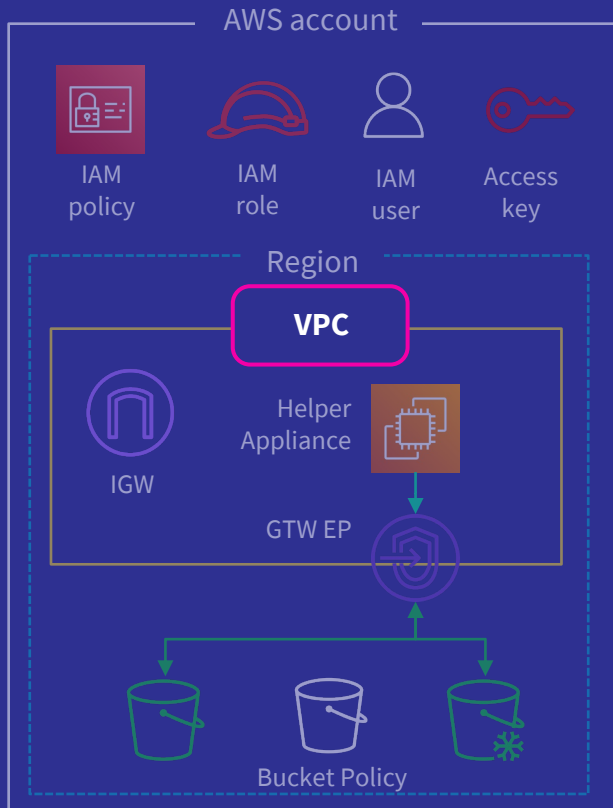
- Setup the VPC upfront (no Veeam® auto-create)
- Use a private subnet
- Don't auto assign public IPs
- Use an S3 Gateway Endpoint to keep S3 traffic internal
- Lock down the Gateway endpoint with a policy
- Restrict port access at the Security Group and Network ACL levels
- Internet access VPN, Direct Connect + Private Links – Interface Endpoint



Ports: VBR S3 access



Security Group and Network ACLs



- Only setup required ports
- Specify source IP
- Deny All – Only allow source IP

The screenshot shows the 'Edit inbound rules' page in the AWS console. The page displays a table of inbound rules for a specific security group. The table has columns for Security group rule ID, Type, Protocol, Port range, Source, and Allow/Deny. The 'Source' column shows 'My IP' and a search bar. The 'Allow/Deny' column shows 'Allow' and 'Deny' buttons.

Security group rule ID	Type	Protocol	Port range	Source	Allow/Deny
sgr-0b91bbb3d89fc1c57	HTTPS	TCP	443	My IP	Allow
sgr-032dac755f0aa2742	SSH	TCP	22	My IP	Deny

Use gateway(s)

Connection Type

Choose a connection mode for this object storage repository. For the Direct mode, ensure backup proxies and backup agents have direct network access to object storage. For the Gateway mode, we recommend having at least two gateway servers for redundancy.

☐ Direct
Backup proxies and agents will connect directly to object storage.

☒ Through a gateway server
Backup server will automatically determine the most suitable gateway server from the following list:

Name	Select All	Clear All
<input type="checkbox"/> cacherepo01.protekt.local		
<input type="checkbox"/> ec2-52-41-87-75.us-west-2.compute.amazonaws.com		
<input checked="" type="checkbox"/> fp01.protekt.local		
<input type="checkbox"/> fp02.protekt.local		
<input type="checkbox"/> ghv01.protekt.local		
<input type="checkbox"/> helper01.protekt.local		
<input type="checkbox"/> hlr01.protekt.local		
<input type="checkbox"/> hlr02.protekt.local		
<input type="checkbox"/> limp01.protekt.local		
<input type="checkbox"/> vbr12.protekt.local		
<input type="checkbox"/> winp01.protekt.local		

OK Cancel

Connection mode:
fp01.protekt.local

Specify whether object storage should be accessed directly or via selected gateway servers.

< Previous Next > Finish

443, 80

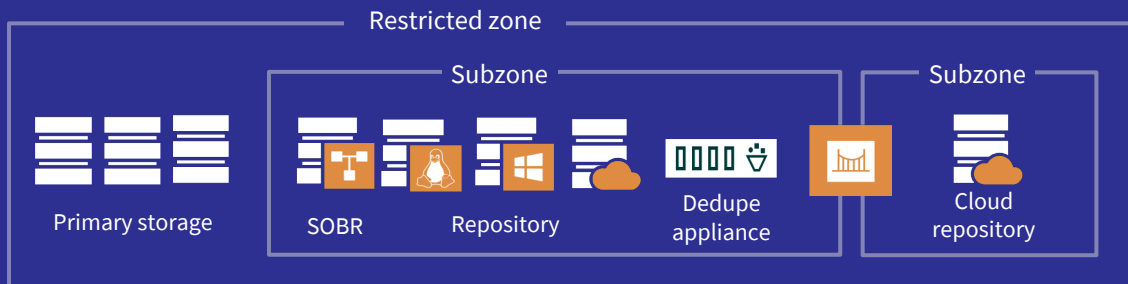
*.amazonaws.com

*.amazontrust.com

[Direct to S3](#)


[External Repositories](#)

[Getting started with direct to AWS](#)



Immutability & Encryption

Edit Object Storage Repository

 **Bucket**
Specify Amazon S3 bucket to use.

Name	Data center:
Account	US West (N. California)
Bucket	awsprotekt10
Mount Server	Folder:
Review	backups
Apply	<input type="checkbox"/> Limit object storage consumption to: 10 TB
Summary	<input checked="" type="checkbox"/> Make recent backups immutable for: 30 days

This is a soft limit to help control your object storage spend. If the already running backup offload tasks will be allowed to complete, but no new backups are made immutable for the entire duration of their retention.

Global Network Traffic Rules

Network traffic rules:

Name	Encrypt...	Throttli...	Time Per...
Internet	Enabled	Disabled	

Buttons: Add..., Edit..., Remove, Networks...

Advanced Settings

Backup Maintenance Storage Notifications vSphere Integration Scripts

Data reduction

- ☒ Enable inline data deduplication (recommended)
- ☒ Exclude swap file blocks (recommended)
- ☒ Exclude deleted file blocks (recommended)

Compression level:

Optimal (recommended)

Provides for the best compression to performance ratio, lowest backup proxy CPU usage and fastest restore.

Storage optimization:

1MB (recommended)

Delivers the optimal combination of backup speed, granular restore performance and repository space consumption.

Encryption

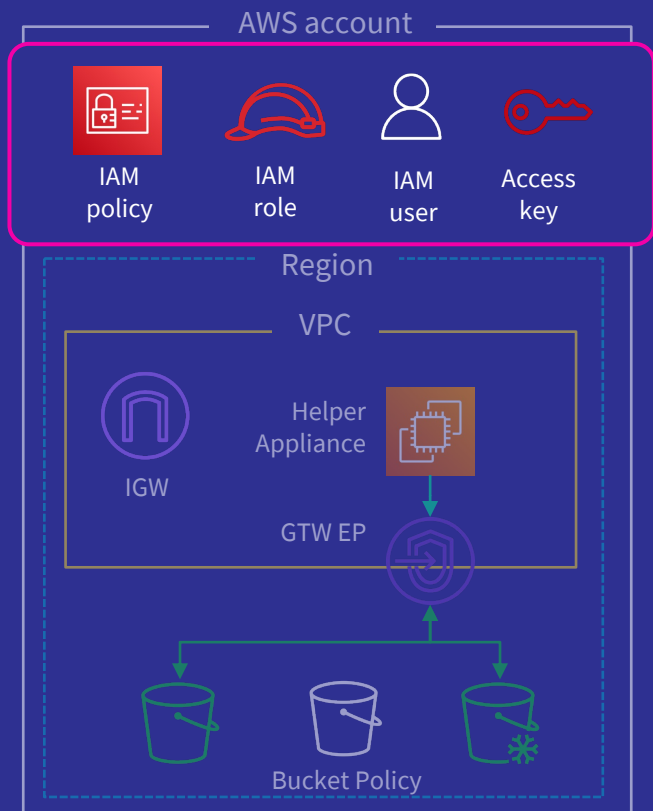
- ☒ Enable backup file encryption

Password:

SuperSecretEncryption (Last edited: less than a day ag)

Add...

IAM Policies – Apply Least Privileges



Only apply what is required

- Pre-created resources

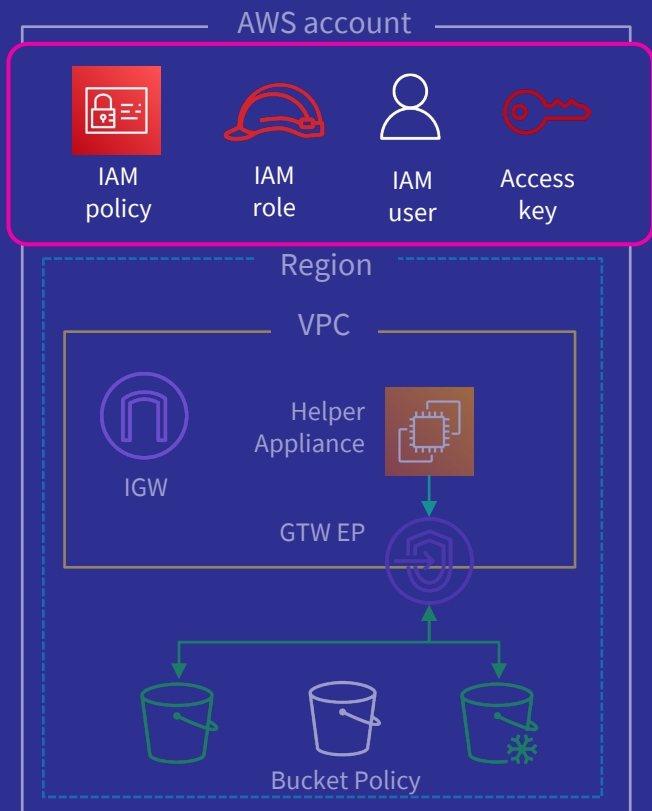
Veeam Backup & Replication™:

- Read/Write to S3
- Launch EC2 Helper/Archiver Appliances

Veeam Backup *for* AWS:

- Launch EC2 Worker Appliances
- Read/Write to S3
- Backup/Restore (EC2, RDS, EFS, VPC)

IAM Policies – Apply Least Privileges



pol-usr-awsprotekt10

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "SecureBucketPolicy0",  
6       "Effect": "Allow",  
7       "Action": [  
8         "s3:PutObject",  
9         "s3:GetObject",  
10        "s3:DeleteObject",  
11        "s3:GetBucketLocation",  
12        "s3:GetBucketVersioning",  
13        "s3:GetBucketObjectLockConfiguration"  
14      ]  
15      "Resource": [  
16        "arn:aws:s3:::awsprotekt10/*",  
17        "arn:aws:s3:::awsprotekt10"  
18      ]  
19    }  
20  ]  
21 }
```


AWS S3 Security Best Practices

Security best practices for Amazon S3 - Amazon Simple Storage Service

- Disable ACLs
- Ensure that your Amazon S3 buckets use the correct policies and are not publicly accessible
- Implement least privilege access
- Encryption of data at rest – SSE-S3
- Consider S3 Object Lock
- Consider VPC endpoints for Amazon S3 access



Thank you!

veeAMON2023

