My Drive Implementation (IAM)

In order to secure access of the EC2 instances to S3, an IAM role is required. Use AWS IAM service web-page.



One IAM roles is based on IAM Policies. It is required to create an IAM policy that reduce the access rights to the S3 bucket we need to use. (See S3 Bucket pages).

\rightarrow C $\textcircled{0}$	http:	s://cor	nsole	e.aws. amazon.com /iam/home?regi	on=eu-central-1#/	policies	⊠ ☆	III\ 🗉 🛎
aws Services v	٩	Searc	h for	services, features, marketplace produ	cts, and docs	[Alt+S]	D 4	▼ Global ▼ Support ▼
lentity and Access anagement (IAM)		Crea	ate p	Policy actions				2 0
Dashboard	-	Filte	r po	icies V Q Search				
Access management				Policy name 👻	Туре	Used as		Description
Groups Users			۲	AccessAnalyzerServiceRole	AWS managed	None		Allow Access Analyzer to a
Roles			►	AdministratorAccess	Job function	None		Provides full access to AWS
Policies			•	Generator Access-Amplify	AWS managed	None		Grants account administrati
Identity providers Account settings			۲	AdministratorAccess-AWSEI	AWS managed	None		Grants account administrati
Access reports			•	AlexaForBusinessDeviceSet	AWS managed	None		Provide device setup acces
Access analyzer			•	AlexaForBusinessFullAccess	AWS managed	None		Grants full access to Alexal
Archive rules Analyzers			۲	AlexaForBusinessGateway	AWS managed	None		Provide gateway execution
Settings			۲	🕴 AlexaForBusinessLifesizeD	AWS managed	None		Provide access to Lifesize
Credential report Organization activity			۲	AlexaForBusinessNetworkP	AWS managed	None		This policy enables Alexa for
Service control policies			•	AlexaForBusinessPolyDeleg	AWS managed	None		Provide access to Poly AVS

Create a new policy:

8	IAM Management (Consol × +			• • •
\leftarrow \rightarrow	C 🛈	🛛 🔒 https://con	sole.aws.amazon.com/iam/home?region=eu-central-1#/policies\$new?step= 🚥 👽 🟠	III\ 🗊	◉ 🖸
aws	Services 🔻	Q Search	for services, features, marketplace products, and docs [Alt+S]	▼ Global ▼	Support 🔻
	Create	policy	9	2 3	- 1
	A policy defines more	s the AWS permissions the	at you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using	JSON. Learn	
	Visual editor	r JSON	Import	t managed policy	
	Expand all C	collapse all			
5	✓ Select a s	service	Clone	Remove	
Documentation		Service	Choose a service		
Doc		Actions	Choose a service before defining actions		
		Resources	Choose actions before applying resources		
		Request conditions	Choose actions before specifying conditions		
			Add additional p	ermissions	
Feedbac	k English (US) ▼		© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy	Terms of Use Coo	okie preferences

Chose S3 service:

8 IA	M Management Con	isol × +				● 🖲 😣
$\leftrightarrow \rightarrow c$	° û	🗊 🔒 https://con:	sole.aws. amazon.com /iam/home?region=eu-central-1#/policies\$ne	ew?step= 🚥 🔽 🏠	lii\ 🗉	≗ 📮
aws	Services ▼	Q Search	for services, features, marketplace products, and docs [Alt+S]	D 4 🚥	▼ Global ▼	Support 🔻
	Create po	olicy		1	2 3	
	A policy defines the more	e AWS permissions th	at you can assign to a user, group, or role. You can create and edit a policy	r in the visual editor and using a	JSON. Learn	
	Visual editor	JSON		Import	managed policy	-
	Expand all Colla	pse all				
5	- S3 (All action	ns) 🛕 6 warnings		Clone	Remove	
Documentation		 Service 	S3			
Doct		- Actions	Specify the actions allowed in S3 ⑦	Switch to deny pern	nissions 🚯	
		close	Q Filter actions			
			Manual actions (add actions) All S3 actions (s3:*)			
			Access level	Expand all 0	Collapse all	
			 ✓ List (7 selected) ✓ Read (48 selected) 			
			 Tagging (10 selected) 			
_			►			
Feedback	English (US) 🔻		© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights	reserved. Privacy Policy Te	erms of Use C	ookie preferences

Check – all S3 actions (it will be filtered later per bucket)

You will need to specify the Bucket and Object resource ARN.



Click on the desired line. Bucket first:

💡 IAM Management (Consol × +					008
$\overleftarrow{\leftarrow}$ \rightarrow C $\overleftarrow{0}$	🛛 🔒 https:/	/console.aws. amazon.com /ia	am/home?region=eu-central-1#/p	olicies\$new?step= ••	· ⊠ ☆	\ 🗓 😩 🧮 🗏
aws Services v	Q Se	earch for services, features, mai	rketplace products, and docs	[Alt+S]	∑ 	obal 🔻 Support 🛡
	▶ Serv	vice S3			_	
	► Ac	Add ARN(s)		×		
		Amazon Resource Names (A unique to each service. Learr	RNs) uniquely identify AWS resource	s. Resources are		
	▼ Resoι	Specify ARN for bucket		List ARNs manually		
		arn:aws:s3:::webdrive80				
E C					Any in this accord	unt
intatio		Bucket name *	webdrive80	Any	d 49 more 🛛 🖌	iny
Documentation						
Å				Cancel Add	Any in this acco	unt
			Add ARN to restrict access			
		object ⑦	Specify object resource ARN for th actions. ① Add ARN to restrict access	e PutObjectRetention a	and 29 more 🛛 A	iny
		objectlambdaacc 💿	Specify objectlambdaaccesspoint PutAccessPointConfigurationFor more actions.		Any in this accord	unt
Feedback English (US) 🔻		© 200	8 - 2021, Amazon Web Services, Inc. or its affili	iates. All rights reserved.	Privacy Policy Terms of Us	e Cookie preferences

Write the bucket name. The ARN will be completed.

₽ IAM Management Consol ×	+		
$(\leftarrow) \rightarrow C' \textcircled{a}$	tps://console.aws. amazon.con	n/iam/home?region=eu-central-1#/policies/a	
aws Services ▼ Q	Edit ARN	, ,	Global ▼ Support ▼
	Amazon Resource Names (ARI unique to each service. Learn n Specify ARN for object arn:aws:s3:::webdrive98/* Bucket name * Object name *	Ns) uniquely identify AWS resources. Resources are nore 2 webdrive98 Any * Any	
ientat			Any in this account
Documentation		Cancel Save chang	ges
	bucket 🛞	arn:aws:s3:::webdrive98 Add ARN to restrict access	EDIT O Any
	job	Specify job resource ARN for the DescribeJob and 5 more actions. Add ARN to restrict access	Any in this account
	abject @		
Feedback English (US) 🛡	© 2008 - 2021, Amaz	F con Web Services, Inc. or its affiliates. All rights reserved.	Privacy Policy Terms of Use Cookie preferences

Set the ARN for Object: (bucket name and ANY for Object name)

It should look like this:

💡 IAM Management Consol X 👘 WEB ap	p settings \times +						0	
$\leftarrow \rightarrow$ C $\textcircled{0}$ $\textcircled{0}$ $https://con$	sole.aws. amazon.com /ia	m/home?region=eu-central-1#/policies/arn:aws:ian ••	· 🛛 🖒	r	III\ 🗉		ø	≡
aws Services ▼ Q Search	for services, features, man	ketplace products, and docs [Alt+S]	D 4	••••	Global 🔻	' Su	pport	,
✓ Resources close	Specific All resources							
	accesspoint ⑦	Specify accesspoint resource ARN for the GetAccessPointPolicy and 5 more actions. Add ARN to restrict access		Any in this	account			
	bucket ⑦	arn:aws:s3:::webdrive98	EDIT	0	Any			
Documentation	job	Add ARN to restrict access Specify job resource ARN for the DescribeJob and 5 more actions. Add ARN to restrict access		Any in this	account			
	object 🕜	arn:aws:s3:::webdrive98/*	EDIT	0	Any			
	objectlambdaacc	Add ARN to restrict access Specify objectlambdaaccesspoint resource ARN for the PutAccessPointConfigurationForObjectLambda and 8 more actions. Add ARN to restrict access		Any in this	account			
	⑦ storagelensconfig	Specify storagelensconfiguration resource ARN for the DeleteStorageLensConfiguration and 5 more actions.		Any in this	account			
Feedback English (US) ▼	© 2008	8 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.	Privacy Po	licy Terms	s of Use	Cookie	oreferen	ices

You can set a tag (key and value). It is not required. Set the policy name:

PIAM Management Consol >	< +					Θ	
$\leftarrow \rightarrow $ C $\textcircled{0}$	https://console.aws.an	hazon.com/iam/home?region=eu-central-	1#/policies\$new?step= •••	⊠ ☆		۲	≡
aws Services ▼	Q Search for services,	features, marketplace products, and docs	[Alt+S]	2 4 🚥 🔹	Global 🔻	Support	•
Create polic	ÿ			1 2	3		
Review policy							
Name*	webdrive98-access						
	Use alphanumeric and '+=,.@	characters. Maximum 128 characters.					
Description							
	Maximum 1000 characters. Use	alphanumeric and '+=,.@' characters.			lh,		
Summary							
	Q Filter						
	Service 👻	Access level	Resource	Req	uest cor		- 1
	Allow (1 of 277 services) Show remaining 276					
	S3	Full access	Multiple	None	e		
Tane							
Feedback English (US) ▼		© 2008 - 2021, Amazon Web Services, Inc. or i	ts affiliates. All rights reserved.	rivacy Policy Terms of	Use Coo	kie prefere	nces

A preview, press "Create Policy"

💡 IAM	1 Management Co	nsol X	+						
€ → C	۰ û	0	https://console.aws. amazo	n.com/iam/home?region=eu-ce	ntral-1#/p	olicies\$new?step=	… ⊠ ☆	III\ 🗉	
aws	Services v		Q Search for services, feat	ures, marketplace products, and do	cs	[Alt+S]		▼ Global ▼	Support 🔻
	Descri	ption							
	Maximum 1000 characters. Use alphanumeric and '+=,,@' characters. Summary Q. Filter								
			Service 👻	Access level		Resource		Request cor	
			Allow (1 of 277 services) She	ow remaining 276					
			S3	Full access		Multiple		None	
		Tags							
		Tays	Кеу	•	Value			\bigtriangledown	
			bucket		ewbdrive	98			
	* Required					Cancel	Previous	Create policy	
Feedback	English (US) 🔻			© 2008 - 2021, Amazon Web Services	Inc. or its affilia	ates. All rights reserved.	Privacy Policy	Terms of Use C	ookie preferences

You have the policy required by the IAM role, it will allow access to the S3 bucket.

IAM Management Conso	× +						00
) -> C' 12	🔒 https	s://console	e.aws. amazon.com /iam/home	?region=eu-central-1#/	policies	⊌ ☆	III\ 🗊 🔹 🔯
aws Services ▼	٩	Search for	services, features, marketplace j	products, and docs	[Alt+S]		▼ Global ▼ Support ▼
dentity and Access Janagement (IAM)		•	webdrive98-access has	been created.			×
Dashboard		Create p	olicy Policy actions ▼				C 🗘 0
 Access management 							
Groups		Filter pol	icies ~ Q webdrive				
Users			Policy name 👻	Туре	Used as		Description
Roles		0	webdrive98-access	Customer manage	ed None		
Policies		•	weburive90-access	Customer manage	au none		
Identity providers							
Account settings							
 Access reports 							
Access analyzer							
Archive rules							
Analyzers							
Settings							
Credential report							
Organization activity							

Create the IAM role:

IAM Management Const	iol × +			•							
$) ightarrow$ C' $rac{1}{2}$	🗊 🔒 http	s://console.aws. amazon.com /iam/home?region=eu-central-1#/roles	··· ≥ ☆	III\ 🗉 🙁 🔛							
aws Services ▼	٩	Search for services, features, marketplace products, and docs [A	lt+S]	Global ▼ Support ▼							
dentity and Access Management (IAM)		Roles									
Dashboard		What are IAM roles?		×							
 Access management 		IAM roles are a secure way to grant permissions to entities that you trust	t. Examples of entities include the follow	ing:							
Groups		IAM user in another account	AM user in another account								
Users		Application code running on an EC2 instance that needs to perform actions on AWS resources									
Roles		An AWS service that needs to act on resources in your account to pro	An AWS service that needs to act on resources in your account to provide its features								
Policies		Users from a corporate directory who use identity federation with SAM	ΛL								
Identity providers		IAM roles issue keys that are valid for short durations, making them a me	ore secure way to grant access.								
Account settings		Additional resources:									
		IAM Roles FAQ									
Access reports		IAM Roles Documentation									
Access analyzer		Tutorial: Setting Up Cross Account Access									
Archive rules		Common Scenarios for Roles									
Analyzers											
Settings											
Credential report		Create role Delete role		2 0							
Organization activity		Q Search		Showing 2 result							
Service control policies											
edback English (US) 🔻		© 2008 - 2021, Amazon Web Services, Inc. or its affiliates.	All rights reserved. Privacy Policy Term	ns of Use Cookie preferen							

Press "Create role"

Chose EC2 service for the new role:

💡 IAM Management Co	nsol× +			●
← → ♂ ☆	🗊 🔒 https://console.aws.amazon.	com /iam/home?region=eu-central-1#/	roles\$new?step=typ 🚥 🗵 🏠	III\ 🖸 🛎 🖻 🗏
aws Services ▼	Q Search for services, featur	es, marketplace products, and docs	[Alt+S]	Global 🔻 Support 🔻
Create	role		1 2 3	4
Select ty	pe of trusted entity			
EC2		r AWS account g to you or 3rd party Web identifi Cognito or any provider		
Choose	a use case			
Common use EC2 Allows EC2 in	e cases stances to call AWS services on your beha	lf.		
Lambda Allows Lambd	a functions to call AWS services on your b	ehalf.		
Or select a se	ervice to view its use cases			
API Gateway	CodeBuild	EMR IoT S	iteWise RDS	
AWS Backup	CodeDeploy	EMR Containers IoT T	hings Graph Redshift	
AWS Chatbo	t CodeGuru	ElastiCache KMS	Rekognition	
* Required			Cancel Next: Permi	ssions
Feedback English (US) ▼		© 2008 - 2021, Amazon Web Services, Inc. or its aff	iliates. All rights reserved. Privacy Policy Terms	of Use Cookie preferences

Attach the required policy (one created earlier):

R IAM Management C						● 🛛 😣
$\overleftarrow{\leftarrow}$ \rightarrow \overleftarrow{c}	🛛 🗎 https://console.aws. amazon.com /ia	n/home?region=eu-central-1#/roles\$n	ew?step=pei	⊌ ☆	lii\ C	I 🔍 🖸 🗏
aws Services v	Q Search for services, features, man	etplace products, and docs [Alt+	S]		Global 🖲	▼ Support ▼
Create				1 2	3 4	
	permissions policies					
Choose one	or more policies to attach to your new role.					
Create pol	icy				C	
Filter polic	es v Q webdrive			Sh	owing 1 result	
	Policy name 🔻		Used a	as		
✓ ▶	webdrive98-access		None			
* Required			Cancel	Previous	Next: Tags	
Feedback English (US) ▼	© 2008	- 2021, Amazon Web Services, Inc. or its affiliates. All	rights reserved.	Privacy Policy	Terms of Use	Cookie preferences

Add tags (not required)

💡 IAM Management C	ionsol × +							•••
\leftrightarrow > C' $$	🛛 🔒 https://console	aws. amazon.com /iam/home?reg	gion=eu-central-1#/rc	oles\$new?step=ta	♥ ☆			
aws Services ▼	Q Search for	ervices, features, marketplace prod	ucts, and docs	[Alt+S]	$\Sigma \Leftrightarrow$	▼ Global ▼	Suppo	ort 🔻
Create Add tag	e role s (optional)				1 2	3 4		
IAM tags are	e key-value pairs you can ad	d to your role. Tags can include user ack, or control access for this role. L		email address, or c	can be descriptive	e, such as a job		
Кеу		Value (optional)				Remove		
Add new	key							
You can ac	dd 50 more tags.							
				Cancel	Previous	Next: Review		
Feedback English (US) ▼		© 2008 - 2021, Amazon	Web Services, Inc. or its affilia	ates. All rights reserved.	Privacy Policy	Terms of Use	Cookie pre	ferences

Set the IAM role name:

IAM Management Consol	× +					● • ×
\leftrightarrow > C $\textcircled{0}$	https://console.aws.ama	zon.com/iam/home?region=eu-central-1#	t/roles\$new?step=rev	… ⊠ ☆	III\ 🗉) 🙁 🙋 😑
aws Services v	Q Search for services, fe	atures, marketplace products, and docs	[Alt+S]	D 4	🔻 Global 🔻	Support 🔻
Create ro	le			1 2	3 4	
Review						
Provide the require	ed information below and review	•				
	Role name*	webdrive98-role				
		Use alphanumeric and '+=,.@' characters. Maximu	im 64 characters.			
	Role description	Allows EC2 instances to call AWS services	on your behalf.		ĺk.	
		Maximum 1000 characters. Use alphanumeric and '-	+=,.@' characters.			
	Trusted entities	AWS service: ec2.amazonaws.com				
	Policies	webdrive98-access 🖸				
	Permissions boundary	Permissions boundary is not set				
No tags were adde	ed.					
* Required			Cancel	Previous	Create role	
Feedback English (US) ▼		© 2008 - 2021, Amazon Web Services, Inc. or its a	affiliates. All rights reserved.	Privacy Policy	Terms of Use C	Cookie preferences

That is, you have set the required IAM role:

IAM Management Cor	nsol 🗙 🕂							•	• •
← → ♂ ŵ	🛛 🗎 https	://console.aws. ar	mazon.com/iam/hor	ne?region=eu-central-1#/roles	🗵 ☆		III\ 🗊	۹	≡
aws Services v	٩	Search for services	, features, marketplac	e products, and docs [Alt+S]	D 4	•	Global 🔻	Support	•
Identity and Access Management (IAM)		The ro	le <u>webdrive98-r</u>	ole has been created.				×	:
Dashboard ▼ Access management		Create role	Delete role				0	¢ 0	
Groups		Q Search					Showir	ıg 3 resul	ts
Users Roles		Role name	•	Trusted entities		Last activ	vity 👻		
Policies		AWSService	RoleForSupport	AWS service: support (Service-Linked role)		None			
Identity providers		AWSService	RoleForTrustedA	AWS service: trustedadvisor (Service-Linked		None			
Account settings	-	webdrive98-	role	AWS service: ec2		None			
Access analyzer									
Archive rules									
Analyzers									
Settings									
Credential report									
Organization activity									
Service control policies									
https://console.aws.amazon.cor	n/iam/home?r	egion=eu-central-	1#/roles/webdrive9	B-role Web Services, Inc. or its affiliates. All rights reserved.	Privacy Polic	y Terms o	f Use Co	okie prefere	nces

Notes: