Credentials for Amazon AWS used in Cloud Discovery

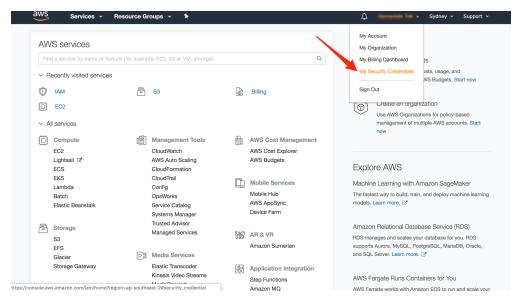
Introduction

When you are using Clouds to discover your Amazon AWS instances, you will need two credential items - key and secret key.

Your key should already be known to you and your secret key as well. Of note is that you cannot retrieve your secret key using the AWS Console provided by Amazon. If you have misplaced it, you will need to generate a new one.

Retrieving or Creating

To retrieve your key, log in to the AWS Console and select your username, then My Security Credentials.



On the next page you will be able to select Access Keys and see your key or create a new key.

aws	Servi	ces 🗸 I	Resource	Groups 🗸	*		¢	finante	in -	Global 👻	Support 👻			
Search IAM] [Your Security Credentials												
Dashboard Groups		Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the IAM Console . To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.												
Users		▲ Password												
Roles	 Multi-factor authentication (MFA) 													
Policies		 Access keys (access key ID and secret access key) 												
Identity providers Account settings Credential report		You use access keys to sign programmatic requests to AWS services. To learn how to sign requests using your access keys, see the signing documentation . For your protection, store your access keys securely and do not share them. In addition, AWS recommends that you rotate your access keys every 90 days. Note: You can have a maximum of two access keys (active or inactive) at a time.												
Encryption keys		Cre	eated	Deleted	Access Key ID	Last Used	Last Used Region	Last Used Service	Status	Ac	tions			
		Mar 29 Dec 3	1st 2010	Nov 9th 2016 Nov 9th 2016 ccess Key	-0:02F	2018-11-05 10:59 UTC+1000 N/A N/A	us-west-1 N/A N/A	ec2 N/A N/A	Active Deleted Deleted	Make Inac	ctive Delete			
		Important Change - Managing Your AWS Secret Access Keys												
		As described in a previous announcement, you cannot retrieve the existing secret access keys for your AWS root account, though you can still create a new root access key at any time. As a best practice, we recommend creating an IAM user that has access keys rather than relying on root access keys.												

Required AWS user permissions

The only required permission / policy name (in our testing) is AmazonEC2ReadOnlyAccess.

Using

Once you have those items, in Open-AudIT Enterprise you can go to menu -> Discover -> Clouds -> Create Clouds, select the "Amazon AWS" type and paste them in. Done :)

9. Open-AudIT Enterprise 2.3	Discover - Report - Manage -		Modules 🗸 Licenses 🗸 Admin 🖌 Help 👻 🚑 User: admin 🗸
Home / Clouds			II •
Clouds			≣ ?
Name		?	About
Org ID	Default Organisation		This endpoint enables you to add your cloud infrastructre details. Open-AudIT will then reach out to your clouds using their native API and return your servers, just like any other device in
Description		?	Open-AudIT.
Туре	Amazon AWS	• ?	NOTE - To use this feature, we <i>must</i> enable the configuration items match_mac (for AWS) and match_hostname (for Azure). This will be done automatically the first time a cloud
Кеу			discovery is executed. For more detailed information, check the Open-AudiT Knowledge Base.
Secret Key		· · · · · · · · · · · · · · · · · · ·	
	Submit		
Open-AudIT Enterprise 2.0.0 is Purchase a license for more no	s licensed to Opmantek for 12345 Nodes - Expires	Powered by Opmantek	