Instructions For Creating AWS Access Credentials For Grok

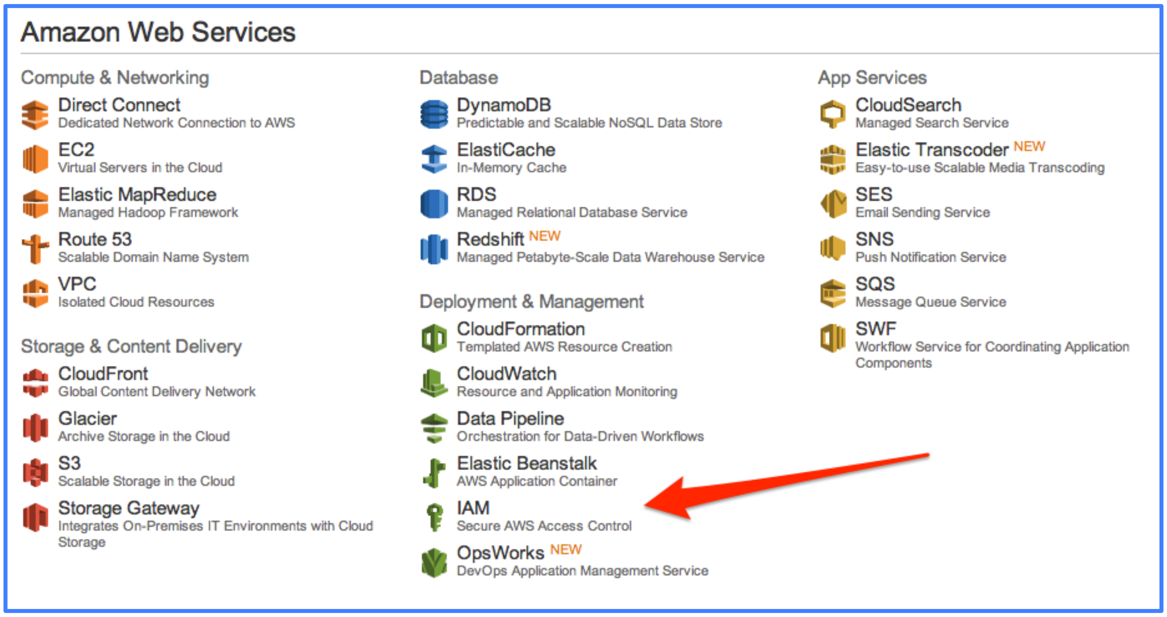
Grok can automatically discover and list your current AWS instances, load balancers, databases, etc. In addition Grok downloads Cloudwatch metrics data and automatically creates a predictive baseline for each metric.

The AWS setup involves supplying AWS access credentials. Although you can simply provide Grok your regular AWS credentials, we strongly recommend creating a separate set of credentials using the AWS IAM capability. This will allow you to specify the exact set of (read-only) permissions required by Grok. It will also allow you to disable Grok without disrupting anything else by disabling just that identity.

Step By Step Instructions

1. Go to your Console home (https://console.aws.amazon.com/console/home)

2. Click on IAM:



Amazon Web Services

Compute & Networking

Direct Connect
Dedicated Network Connection to AWS

EC2
Virtual Servers in the Cloud

Elastic MapReduce
Managed Hadoop Framework

Route 53
Scalable Domain Name System

VPC
Isolated Cloud Resources

Storage & Content Delivery

CloudFront
Global Content Delivery Network

Glacier
Archive Storage in the Cloud

S3
Scalable Storage in the Cloud

Storage Gateway
Integrates On-Premises IT Environments with Cloud Storage

Database

DynamoDB
Predictable and Scalable NoSQL Data Store

ElastiCache
In-Memory Cache

RDS
Managed Relational Database Service

Redshift NEW
Managed Petabyte-Scale Data Warehouse Service

Deployment & Management

CloudFormation
Templated AWS Resource Creation

CloudWatch
Resource and Application Monitoring

Data Pipeline
Orchestration for Data-Driven Workflows

Elastic Beanstalk
AWS Application Container

IAM
Secure AWS Access Control

OpsWorks NEW
DevOps Application Management Service

App Services

CloudSearch
Managed Search Service

Elastic Transcoder NEW
Easy-to-use Scalable Media Transcoding

SES
Email Sending Service

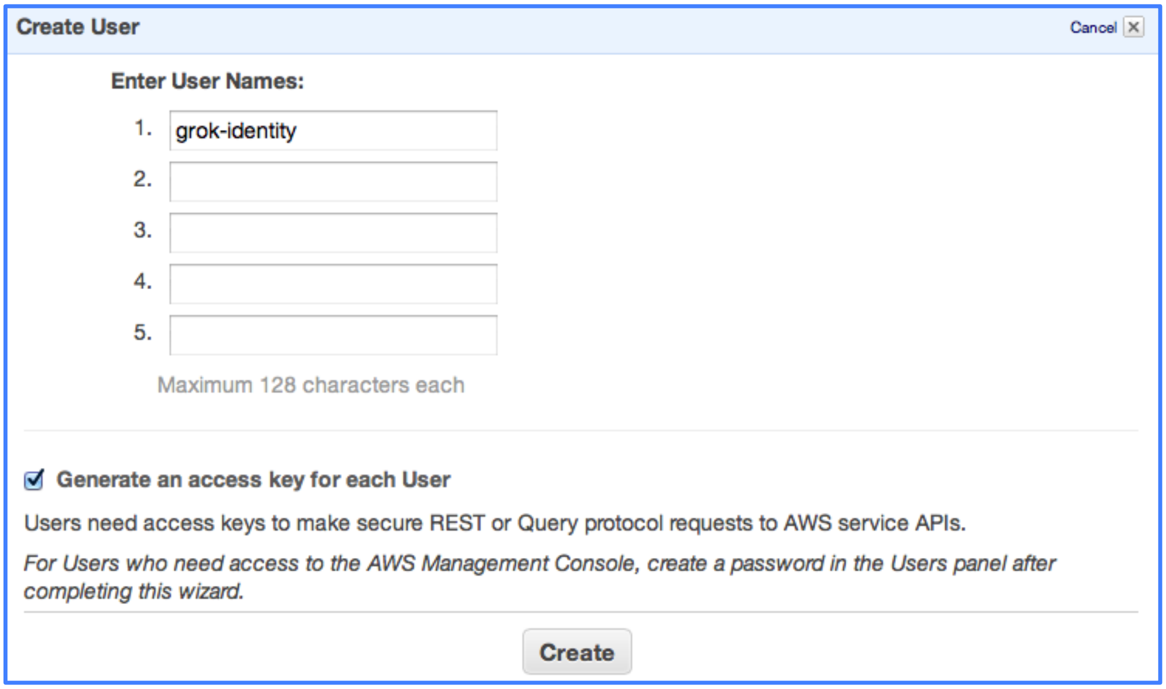
SNS
Push Notification Service

SQS
Message Queue Service

SWF
Workflow Service for Coordinating Application Components

3. On the dashboard on the left, click on "Users" and then click on the blue "Create New Users" button.

4. Enter a user name, such as "grok-identity". Ensure "Generate an access key for each User" is checked and then click on Create:



Enter User Names:

1. grok-identity
2.
3.
4.
5.

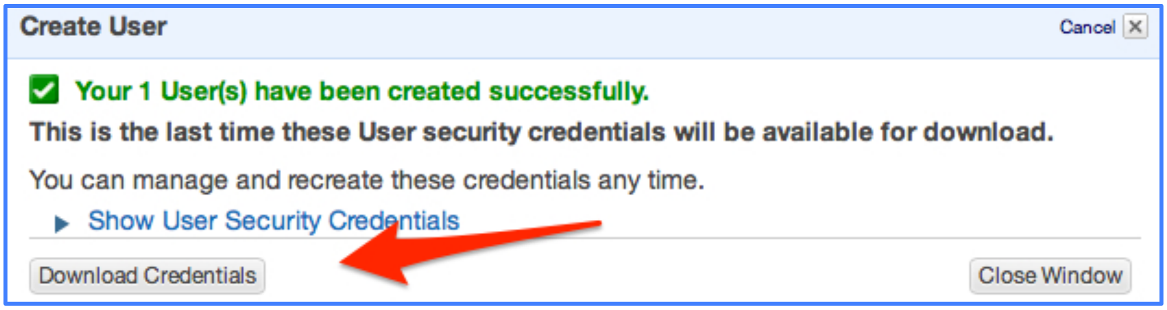
Maximum 128 characters each

☑ Generate an access key for each User

Users need access keys to make secure REST or Query protocol requests to AWS service APIs.

For Users who need access to the AWS Management Console, create a password in the Users panel after completing this wizard.

5. Click "Download Credentials" to download a CSV file with the access keys.

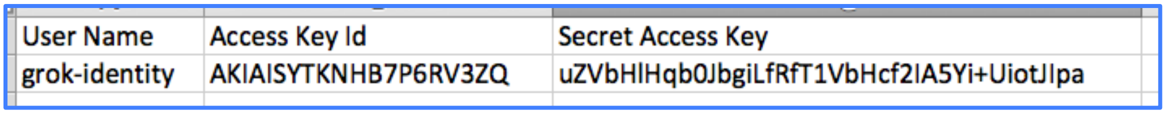


✓ Your 1 User(s) have been created successfully.

This is the last time these User security credentials will be available for download.

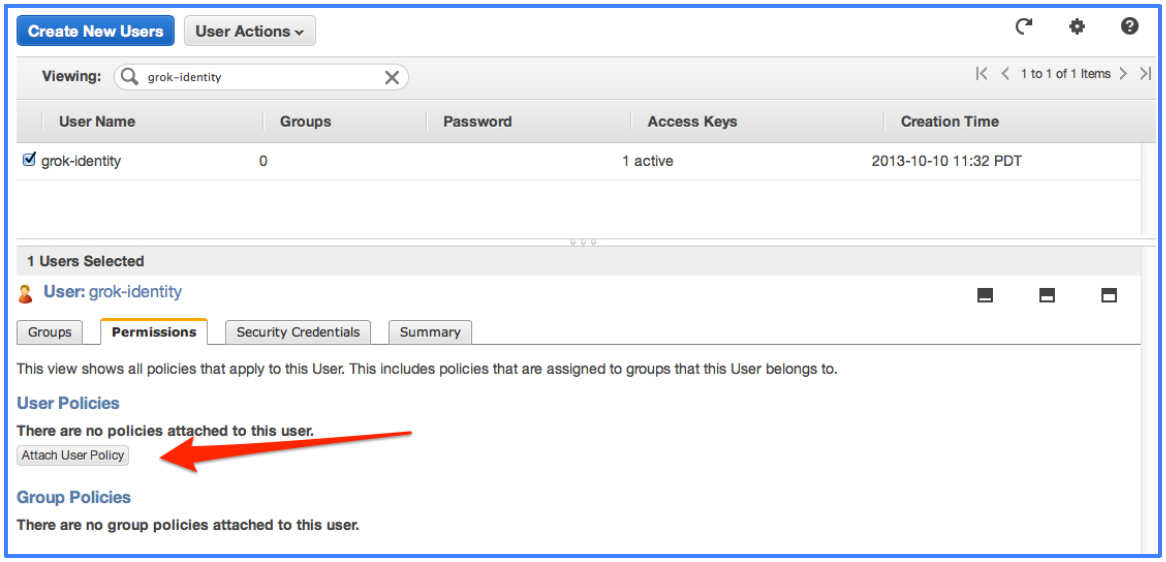
You can manage and recreate these credentials any time.

6. You should get a CSV file that looks something like this:



User Name	Access Key Id	Secret Access Key
grok-identity	AKIAISYTKNHB7P6RV3ZQ	uZVbHlHqb0JbgiLfRfT1VbHcf2lA5Yi+UiotJlpa

7. You now need to grant permissions to this identity. In the web console, locate the user name (you can type *grok-identity* in the search box). Select the username, click on the "Permissions" tab and then click on "Attach User Policy":



User Name	Groups	Password	Access Keys	Creation Time
☑ grok-identity	0		1 active	2013-10-10 11:32 PDT

1 Users Selected

User: grok-identity

This view shows all policies that apply to this User. This includes policies that are assigned to groups that this User belongs to.

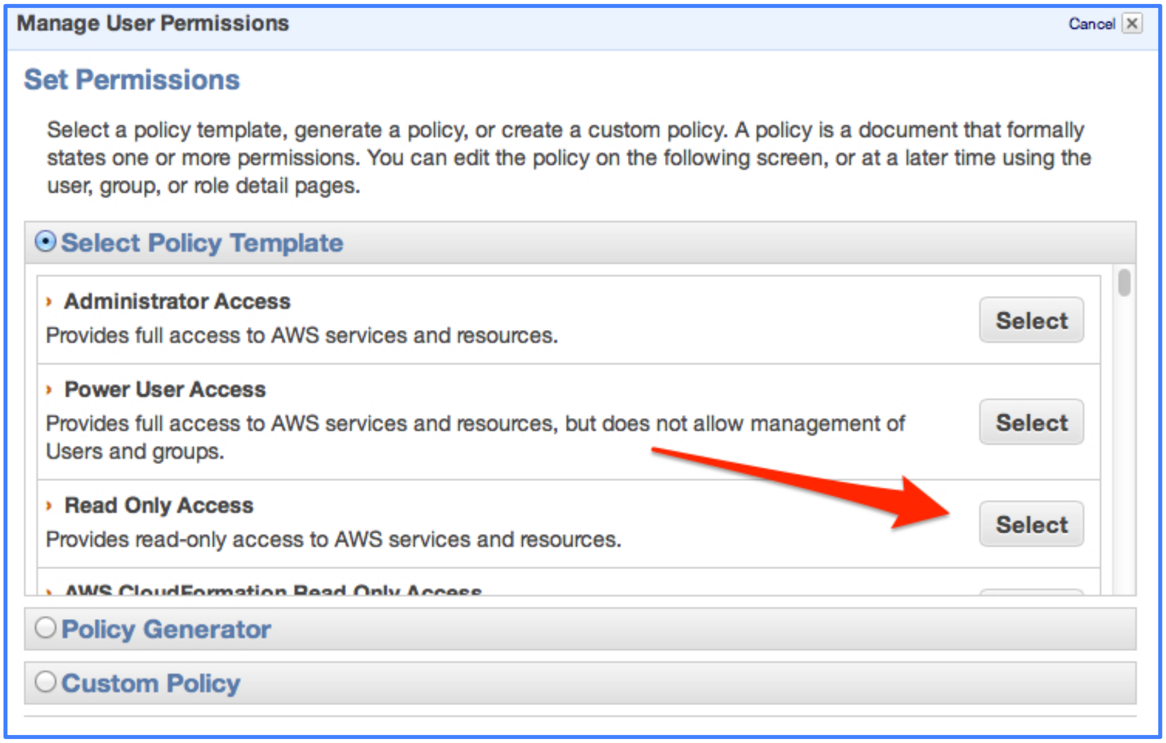
User Policies

There are no policies attached to this user.

Group Policies

There are no group policies attached to this user.

8. In the resulting dialog box, select "Read Only Access":


Manage User Permissions

Set Permissions

Select a policy template, generate a policy, or create a custom policy. A policy is a document that formally states one or more permissions. You can edit the policy on the following screen, or at a later time using the user, group, or role detail pages.

● Select Policy Template

Administrator Access
Provides full access to AWS services and resources.

Power User Access
Provides full access to AWS services and resources, but does not allow management of Users and groups.

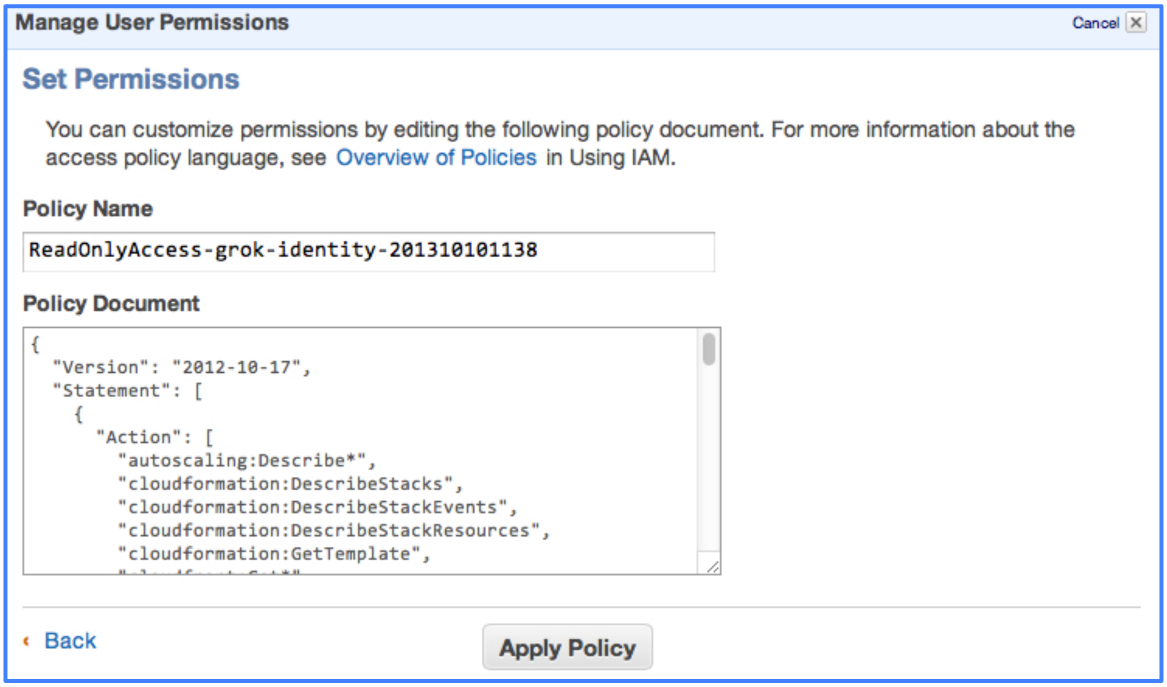
Read Only Access
Provides read-only access to AWS services and resources.

AWS CloudFormation Read Only Access

○ Policy Generator

○ Custom Policy

and then select "Apply Policy":



Manage User Permissions

Set Permissions

You can customize permissions by editing the following policy document. For more information about the access policy language, see Overview of Policies in Using IAM.

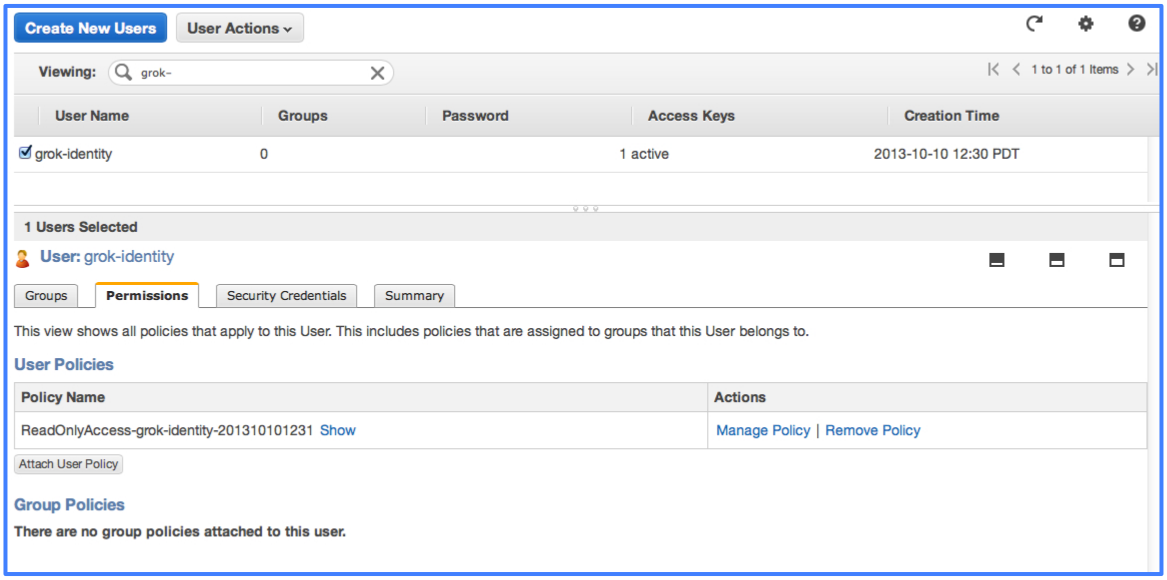
Policy Name

ReadOnlyAccess-grok-identity-201310101138

Policy Document

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "autoscaling:Describe*",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplate",
```

9. You should now see something like this:



Viewing: grok-

1 to 1 of 1 Items

User Name	Groups	Password	Access Keys	Creation Time
☑ grok-identity	0		1 active	2013-10-10 12:30 PDT

1 Users Selected

User: grok-identity

This view shows all policies that apply to this User. This includes policies that are assigned to groups that this User belongs to.

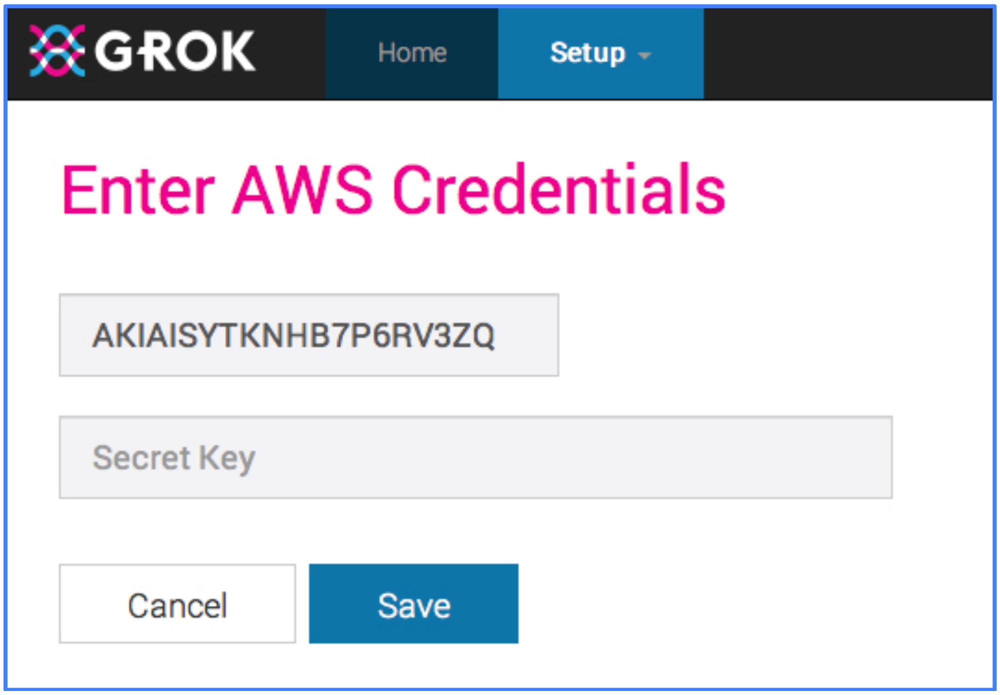
User Policies

Policy Name	Actions
ReadOnlyAccess-grok-identity-201310101231 Show	Manage Policy | Remove Policy

Group Policies

There are no group policies attached to this user.

10. You can now enter the Access Key Id and Secret Access Key you downloaded earlier into Grok:



Enter AWS Credentials

AKIAISYTKNHB7P6RV3ZQ

Secret Key