Accounts as a Service

Why we have 50+ AWS accounts, and why you should too

Keith Gregory AWS Practice Lead, Chariot Solutions



About Chariot Solutions

50-person application-development consulting firm

Created this conference!

Offers training and developer workshops

AWS Consulting Partner



Why we did this

Reduce friction for workshop attendees

They might not have (or be able to use) an existing account

They could create an account, but this takes time

Support project teams



Why you might want to do the same

Allow developers/teams space to experiment

Ensure that they don't harm others

Centralizes control, billing

Good practice for managing/promoting workloads



Approaches we considered

Single account, segregated by region/VPC/naming

Manually create/manage independent accounts

Manually create/manage accounts within organization

AWS Control Tower



Goals

Limit the likelihood of unexpected (big) bills

Identify who is responsible for creating what

Automate all the things!



Setting Up Your Organization



Control Tower

Amazon's enterprise-scale multi-account solution

Account Factory to create child accounts

Predefined "guardrails" based on AWS best practices

Accounts for Application and Audit (CloudTrail) logs

Too heavyweight?



AWS Organizations

Supports a hierarchy of accounts

Individual accounts are assigned to an "organizational unit," which allows controls to applied to entire group

Accounts can be invited or created

Each child account needs a unique email address ("+name" FTW)

You will need to increase your account limit

Default limit is 4 accounts per organization

AWS won't increase limits on new accounts



Organizing Accounts

-		AWS Organizations - Mozilla Firefox		- + ×			
<u>File Edit View History Bookmarks</u>	<u>I</u> ools <u>H</u> elp						
← → C ŵ		/browse/ou-easily and a second s					
aws Services +	Resource Groups 🗸 🧍 IAM 🌐 Cloud	dFormation 🦺 CloudWatch 順 EC2 🎼 El	astic Container Service 🎁 Lambd 🖌 🗘 👦	agory @ chariotsolutions 🔹 Global 👻 Support 👻			
☆ AWS Organizations							
Accounts Organize accounts	Policies			Invitations Settings			
	<	< Sandboxes					
O Root O Sandboxes • WorkshopUsers	TREE VIEW Organizational units (0) + New organizational unit No organizational units are present in the current Accounts (12) developer-sandbox Developer Sandbox #3 Developer Sandbox #4	Developer Sandbox #4 Developer S Developer Sandbox #8 Developer S kgregory-sandbox Fall Marketin	(Charotochik	ARN ID Accounts > POLICIES Service control policies > Tag policies >			

aws organizations create-account \
 --email sandbox+1@example.com

Creating a child account

Can only be invoked from organization root account

Each child account must have a unique email address

Also creates OrganizationAccountAccessRole



User Management

Option 1: Create IAM users in each child account

Easiest for users ... as long as they only have one account

Option 2: Create IAM users in parent account

Users log-in and then assume role; better for multiple accounts

Option 3: AWS Single Sign-On

Uses an existing Active Directory server to manage users

AD User \Rightarrow AD Group \Rightarrow SSO Permission Set \Rightarrow IAM Role



ProTip: use multi-factor authentication

Goal: weak/leaked password != big bill

AWS supports several options

Virtual TOTP (Google Authenticator, Authy, ...)

Physical TOTP (Gemalto)

Hardware key (Yubikey)



Organization Account Access Role

Administrator role in each child account

Created automatically when child is created inside organization

Must be manually created for invited accounts

Default name: OrganizationAccountAccessRole

Damaging or deleting this role is a Bad Idea™



"Guardrails"



Service Control Policies

IAM-like policy that limits what a child account can do

If an SCP prevents an activity, it doesn't matter if the account allows it – root user notwithstanding!

Does not replace IAM: accounts must define own policies Can be applied to account or organizational unit



Allow versus Deny SCPs

Allow lets you do something, Deny prevents it

Example: Allow EC2

Gets tricky when multiple SCPs apply to an account

Example: Allow-All, Deny EC2

Allow applies only to accounts in specific organizational unit

Deny applies to all descendents, overrides Allow

Don't apply Deny-All at root of organization!



Your First SCP

The organization access role is your way to manage the account without an explicit login; don't let it get damaged!

```
"Version": "2012-10-17",
"Statement": [
    "Sid": "ProtectOrgAccess",
    "Effect": "Deny",
    "Action": [
      "iam:DeleteRole",
      "iam:DeleteRolePolicy",
      "iam:DetachRolePolicy",
      "iam:UpdateRole"
    ر ا
    "Resource": [
      "arn:aws:iam::*:role/OrganizationAccountAccessRole",
```



Limit the regions you allow

You can be more clever, and allow read-only access, but probably not worth it.

```
"Version": "2012-10-17",
"Statement": [
    "Sid": "RestrictRegion",
    "Effect": "Deny",
    "Action": [ "*" ],
    "Resource": [ "*" ],
    "Condition": {
      "StringNotEqualsIfExists": {
        "aws:RequestedRegion": [
          "us-east-1",
          "us-east-2",
          "us-west-1",
          "us-west-2"
```



Limit expensive resources

You'll also need to do this for RDS, Redshift, Elasticsearch, and others.

Some services (eg, Private Certificate Authorities) should be disabled entirely.

```
"Version": "2012-10-17",
"Statement": [
    "Sid": "LimitEC2InstanceType",
    "Effect": "Deny",
    "Action": [
      "ec2:RunInstances"
    ر ا
    "Resource": [
      "arn:aws:ec2:*:*:instance/*"
    و ا
    "Condition": {
      "StringNotLike": {
        "ec2:InstanceType": [
          "t2.*",
          "t3.*",
          "m5.large",
          "m5d.large"
```



Turning Your Users Loose



Have "The Talk" about security

Review AWS Shared Responsibility Model

Example: security groups

Long random passwords + multi-factor auth FTW

Access keys

"Keep them secret, keep them safe!"

Assumed roles (and SSO) make them less vulnerable

Don't fire up random AWS Marketplace AMIs



Tag Resources

Start with a simple strategy

CreatedBy: username of person who created resource

DeleteAfter: how long they expect to need it

Implement a Lambda to look for missing tags

Send an SNS notification, or just delete the resource

This is actually a complex task: multi-service, multi-region, multi-account



Cost Explorer is your new BFF

le <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmar	ks Tools Halp		Cost Reports - Mozilla Firef	ox			-
	Cost Reports X +						
-) → C û	⑦ ▲ S https://console.aws.amazon	.com/cost-reports/home?#/custom	?groupBy=Service&forecastTime	RangeOption=None&hasBlende	d=false&hasAmortized=false&exclud	e ••• 🛛 🕁	III\ 🗉 🔮
aws Services -	Resource Groups 🗸 🦹 IAM	CloudFormation	👢 CloudWatch 🛛 🎁 EC:	e 🕼 ECS 🎁 Lami	bda 🖈 🗘 kgregoi	y @ chariotsolutions 👻 Glol	bal 🕶 Support 👻
AWS Cost Management	Saved Reports > Worksho						🌣 Settings 🕜
Home							¥
C. CARCARDA	Save Save as R	eports O New report					
Cost Explorer	Workshop Accounts	. <i>P</i>				▲ FILTERS	CLEAR ALL
Saved reports	Nov 05, 2019 - Nov 12, 20				liı, Bar 👻	Service	Include all 👻
Budgets						Linked Account	Include only -
Recommendations	Group by: Service ×	Linked Account Region In	stance Type Usage Type	Resource Cost Category	Tag ▼ More ▼		38
Savings Plans	Costs (\$) 1.0					Region	Include all 👻
Overview						Instance Type	Include all 💌
Inventory	0.8					Usage Type	Include all 💌
Recommendations	0.6					Usage Type Group	Include all 🝷
Purchase Savings Plans	0.4					Resource (Include all 🔻
Utilization Report	0.2					Cost Category	
Coverage Report	0.2					Tag	
Reservations	0.0 Nov-05	Nov-06 Nov-07	Nov-08 Nov-09	Nov-10 Nov-1	1 Nov-12	More filters 💌	
Overview	-	Kinesis Kinesis Analytic	s 📕 loT 🔡 S3 📕 lo ⁻	Device Management	Others	ADVANCED OPTIO	NS 🚯
ve with Savings Plans						Show costs as ()	
ngs Plans offer significant savings in nange for an hourly commitment to	To s	ee usage data, filter by "Usage T	ype" or "Usage Type Group" fil	ters with matching units (e.g	J., hours).	Unblended costs	•
pute usage. Savings Plans matically apply to any applicable					Download CSV	Include costs related to	
pute usage across regions, regardless ze, tenancy, and OS.	Service	Nov-05	Nov-06	Nov-07	Nov-08	Show only untagged re Show only uncategoriz	
Purchase Savings Plans	Total cost (\$)	0.02	1.37	0.00	0.00	Show forecasted value	

Along with AWS Budgets

e Edit View History Bookmarks Tools Help		Billing Man	agement Console - Mozilla Firefo	x	
Billing Management Console × +					
) → C û	nsole.aws. amazon.com /billing/home?region=	us-east-1#/budgets/details?name=Sandb	ox monthly budge		□10% … ▽ ☆
aws Services - Resource G	roups 🗸 🌐 CloudFormation	🔒 CloudWatch 🧍 🖡	M 🌓 EC2 🌓 Lar	mbda 🔸	众 kgregory @ chariotsolutions ▾ Global ▾ Support ▾
andbox monthly budge st Updated Apr 10, 2020					Edit Budget
Current vs. budgeted		Forecasted vs. budgeted			Alerts
21.02% Current \$52.56	Budgeted amount \$250	4 Forecasted \$115.81	5.33%	Budgeted amount \$250	Alert 1 @ Forecasted costs exceed 150% (\$375) <pre> 1 contact @chariotsolutions.com </pre>
ldget History (\$)			☑ ⁴ View in AWS Cost Exp	plorer 🕹 Download CSV	Budget details
600					Budget period Monthly
500					Budget type Cost
300					Start Date 11/01/2019
200		•		•	End Date
100				_	Filters Linked Account:
Apr May Jun 2019 2019 2019		2019 2019 2019 2	lan Feb Mar 020 2020 2020	Apr 2020 (MTD)	Advanced filters
	Actual 😑	Budgeted			Include: Upfront reservation fees, Recurring reservation charges, Other
< Monthly EC2 Budget			2 of 2 budgets		

And CloudTrail + Search Engine

	<u>E</u> dit <u>V</u> iew Hi <u>s</u> t	Discover - Kibana - Mozilla Firefox tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp	- + ×
	scover - Kibana	x +	
$\langle \boldsymbol{\epsilon} \rangle$	→ C' û	🖸 🔒 https://search-cloudtrail-events-ef6yajsd2dttvnwj72qakdln5i.us-east-1.es.amazonaws.com/_plugin/kibana/app/kibana#/discover?_g=(refreshInte 🚥 🖂 🏠) ◎ 📅 =
	kibana		Last 1 year 🔉
		>_ 0a7badded743619b6 Options	C Refresh
Ø		eventName: "RunInstances" Add a filter +	Actions •
î	Visualize	January 17th 2019, 12:42:31.278 - January 17th 2020, 12:42:31.278 - Auto •	
50	Dashboard	1	
Ø	Timelion	ti 0.6	
A	Alerting	0.2 -	
₿	Dev Tools	0 2019-01-31 2019-02-28 2019-03-31 2019-04-30 2019-05-31 2019-06-30 2019-07-31 2019-08-31 2019-09-30 2019-10-31 2019-11-30 eventTime per week	2019-12-31
÷	Management	Time - userIdentity.accountId awsRegion eventSource eventName userIdentity.invokedBy userIdentity.us	serName
		January 3rd 2020, 09:41:10.000 us-west-2 ec2.amazonaws.com RunInstances signin.amazonaws.com kgregory	
÷	Collapse		

If You're Running a Workshop



Getting Ready

Identify the services used by the workshop and craft an Explicit-Allow SCP that allows all of them

Test-run the workshop to ensure you've caught them all!

Create a "workshop" IAM user for each account, with login profile and randomly-generated password

Attach a "deny all" SCP until the day of the workshop



Wrapping-up

Attach an SCP that prevents creating new resources

Run a script to delete all resources for the accounts

First thing to delete: user access keys, login profiles, non-standard users

There will be some cases where manual intervention is needed

Attach a "deny all" SCP until next time



ProTip: Excel is Your Friend

Keep track of all of your accounts in one sheet

Randomly generate passwords

=TRUNC(100000000*RAND())

No, this isn't secure, but it's a limited-duration vulnerability

Use additional sheets to produce CLI commands



Really, Cost Explorer is your BFF

•			Cost Reports - Moz	lla Firefox				- +
Eile Edit View History Bookmarks	ools <u>H</u> elp							
	₽₩ https://console.aws.amazon.com/cost-reg	oorts/home?#/custom?groupBy=Servic	&forecastTimeRangeOption=Nc	ne&hasBlended=false&hasAmortiz	ed=false&excludeDiscounts	=true&excludeTaggedResou	(110%) ♡☆	III\ 🗊 🔹 =
aws Services - I	Resource Groups 👻 💡 IAM	🕼 CloudFormation 🛛 🛔	CloudWatch 🏻 🍈 E	C2 🏾 🌔 Elastic Contain	ner Service 🏾 🌔 L	ambd 🛠 🗘® kgr	egory @ chariotsolutions 👻 G	lobal 🕶 Support 🕶
& AWS Cost Management >	Saved Reports > Workshop /	Accounts						🌣 Settings 🔞 🗸
A Home	Save Save as Repo	rts - O New report						
Q Cost Explorer								
Saved reports	Workshop Accounts 🌶						▲ FILTERS	CLEAR ALL
Budgets	Mar 06, 2020 - Mar 20, 2020	▼ Daily ▼ 🚯				III ∎ Bar ▼	Service	Include all 👻
Recommendations	Group by: Service × Lir	iked Account Region Instar	ice Type Usage Type	Resource Cost Category •	 Tag < API Operation 	ation More 🕶	Linked Account	Include only
Savings Plans	Costs (\$)						Region	Include all
Overview			- 1 1				Instance Type	Include all 👻
Inventory	150						Usage Type	Include all 👻
Recommendations	100						Usage Type Group	Include all 👻
Purchase Savings Plans	100						Resource 0	Include all 🔻
Utilization Report	50							
Coverage Report							Cost Category	
	0			h h			Tag	
T		r-08* Mar-10*		r-14* Mar-16*	Mar-18*	Mar-20*	More filters 💌	
Overview		Kinesis Relational Data		33 Killesis Pileliose	Oulers		ADVANCED OPTION	IS
Recommendations	-	data filma ha mitana	- T		· (Show costs as ()	
Utilization Report		see usage data, filter by "Usage	r Type or Usage Type Gro	up miters with matching units	s (e.g., nours).		Unblended costs 👻	
Coverage Report						Download CSV	Include costs related to	
My Billing Dashboard	Service	Mar-06*	Mar-07*	Mar-08*	Mar-09*	Mar-1	Show only untagged reso Show only uncategorized	
 Save with Savings Plans 	Total cost (\$)	0.23	1.24	0.75	0.04	<u>í</u>	Show forecasted values	

Questions?



About Me



AWS Practice Lead at Chariot Solutions

Programming since 1977, professionally since 1984, on AWS since 2008



https://www.kdgregory.com/

https://github.com/kdgregory/

@ChariotKGregory





Technology in the Service of Business.

Chariot Solutions is the Greater Philadelphia region's top IT consulting firm specializing in software development, systems integration, mobile application development and training.

Our team includes many of the top software architects in the area, with deep technical expertise, industry knowledge and a genuine passion for software development.

Visit us online at chariotsolutions.com.

