DEPLOYING, SCALING, AND RUNNING GRAILS ON AWS AND VPC

LEARN THE ROPES TO MAXIMIZE YOUR APPLICATIONS POTENTIAL (AND AVOID PERIL!)

Created by Ryan Vanderwerf / @RyanVanderwerf

ABOUT ME

LEARN THE ROPES TO MAXIMIZE YOUR APPLICATIONS POTENTIAL

- Chief Architect @ ReachForce
- Co-Chair Austin Groovy and Grails User Group
- Help maintain Grails Quartz plugin
- Maintain GVPS Plugin (Grails Video Pseudo Streamer)
- Maintain Struts-1 Plugin
- Submit pull requests for others when I can (You should too!)

WHAT WE WILL COVER

- VPC
- S3
- Grails Plugins
- ElasticWolf
- Elastic Load Balancers
- Autoscaling
- Others misc tips

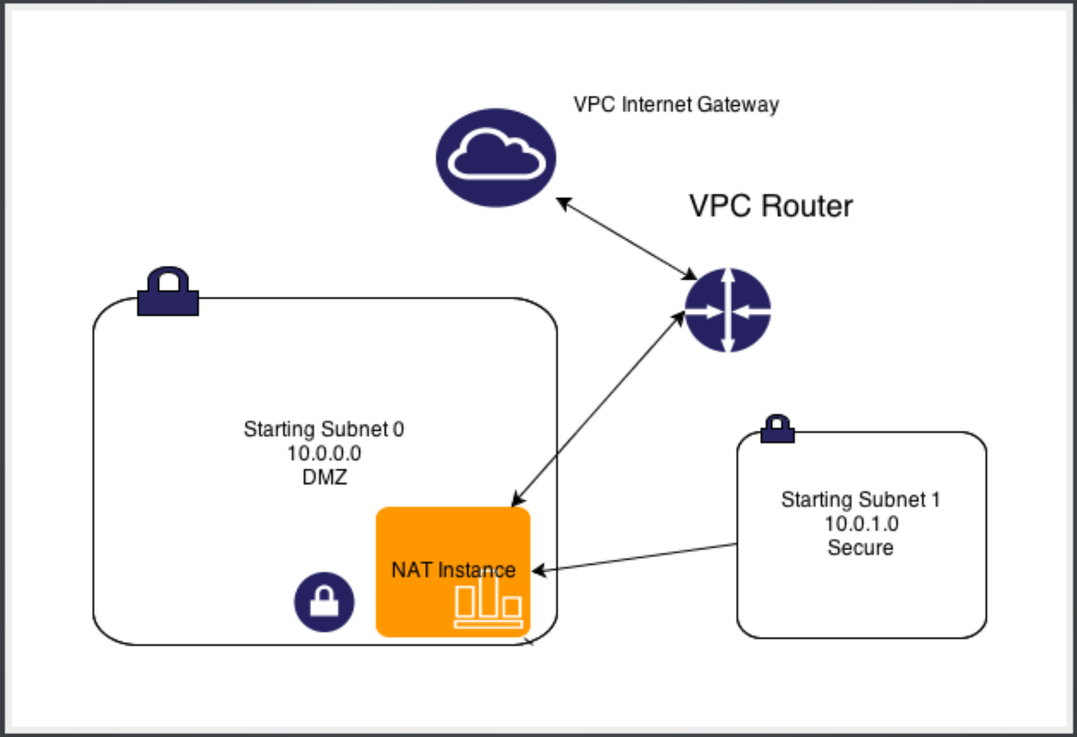
VPC OVERVIEW

Routing
NAT
ACL Firewall
Suggested Subnet Config
Security Groups
DHCP Tips
Others misc tips

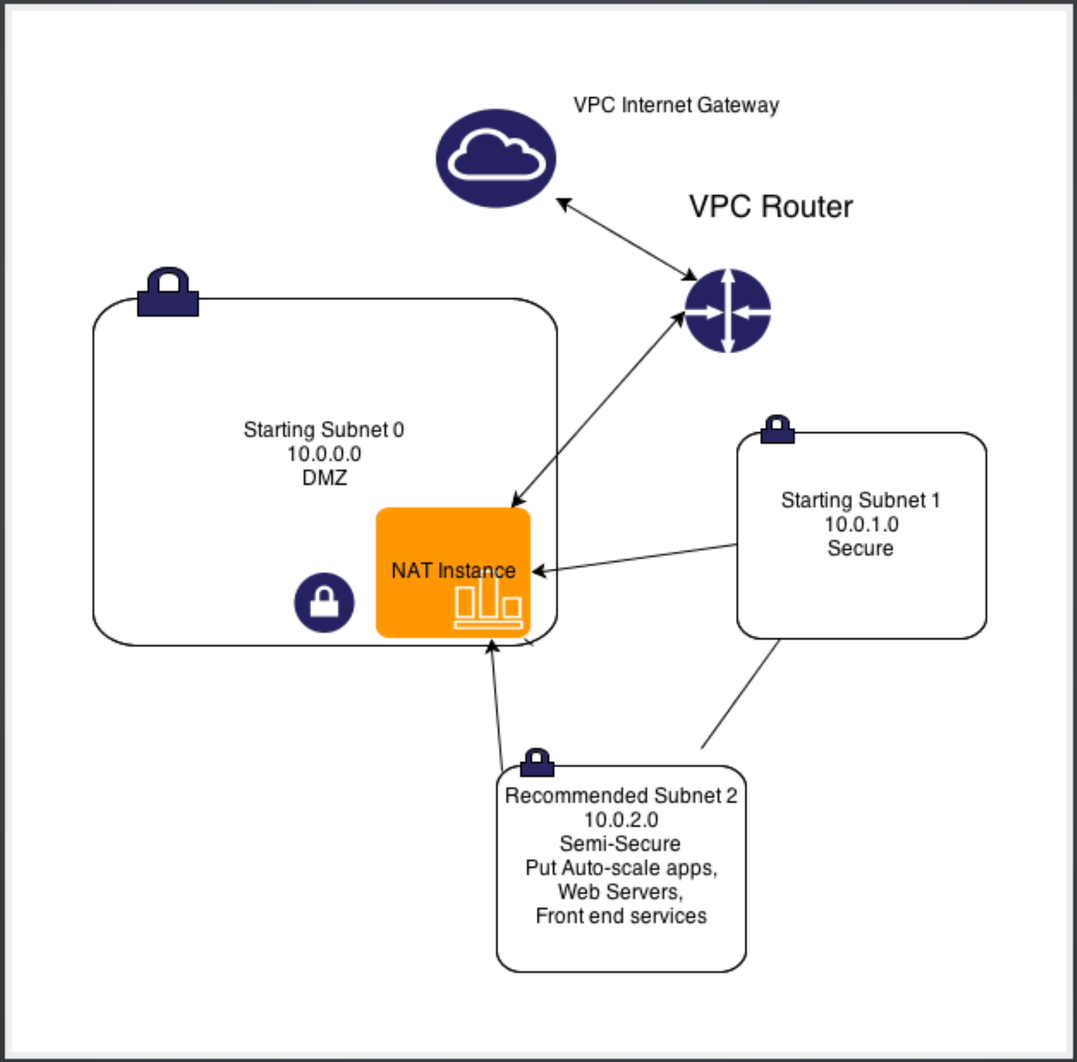
VPC OVERVIEW

Will be default and eventually required on new AWS accounts (still allows both as of last week)
Very different that EC2 'Classic' which has no private network layer or static IPs
Costs nothing extra - you have nothing to lose and everything to gain!

VPC - ROUTING/SUBNETS



VPC - ROUTING/SUBNETS

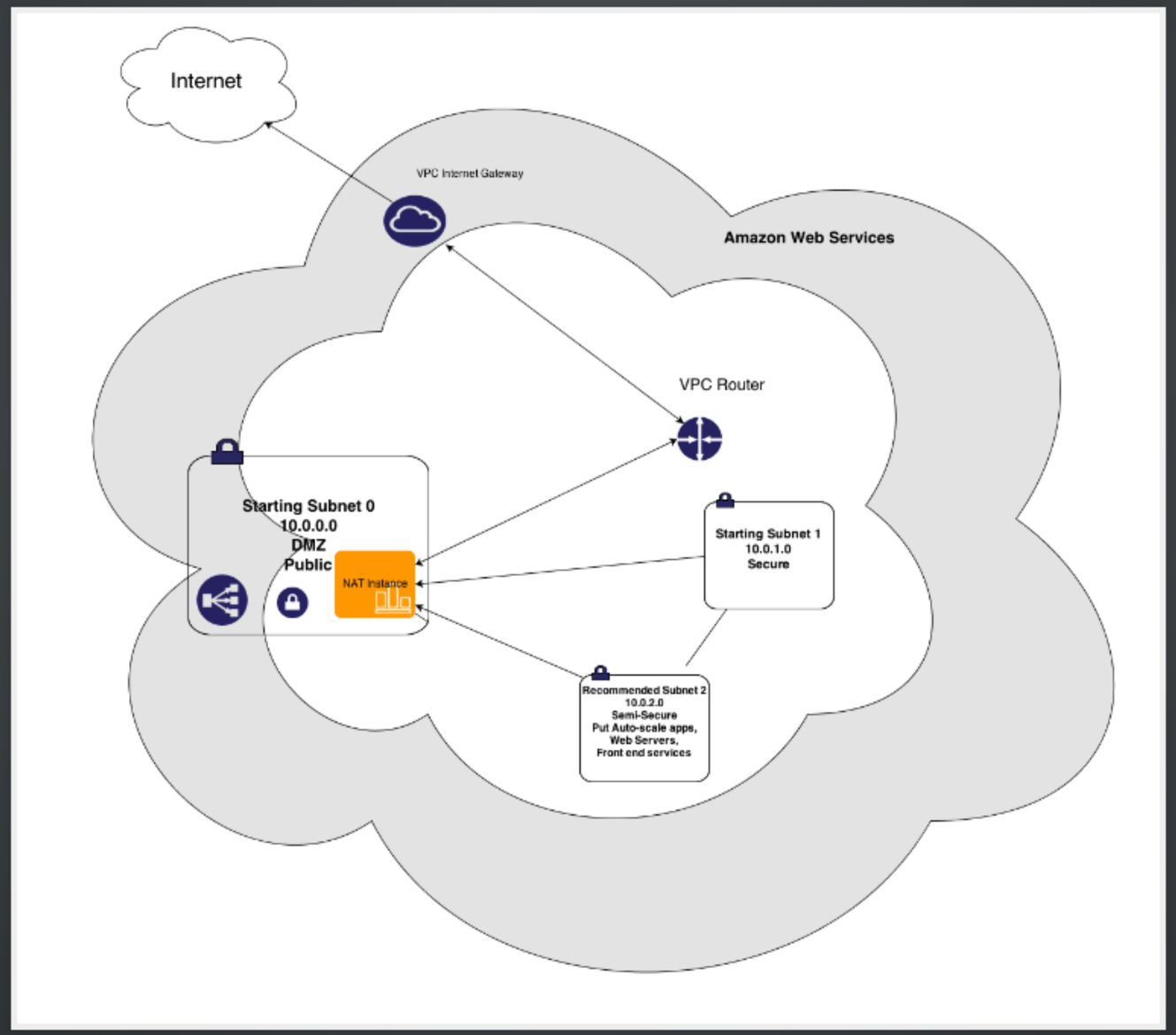


VPC - ROUTING/SUBNETS

ADDING A 3RD SUBNET - THIS GIVES A HELPING HAND

auto-scaling instances can access internet through NAT
Web Servers, Web facing apps can live behind ELB
yet be able to run OS updates
S3 Buckets accessible
can access your secure subnet as well

VPC - ROUTING/SUBNETS



VPC - ROUTING/SUBNETS

Services | Edit | RF Research | N. Virginia | Help

VPC Dashboard

VIRTUAL PRIVATE CLOUDS
- Your VPCs
- Subnets
- Route Tables
- Internet Gateways
- DHCP Options Sets
- Elastic IPs

SECURITY
- Network ACLs
- Security Groups

VPN CONNECTIONS
- Customer Gateways
- Virtual Private Gateways
- VPN Connections

Create Subnet | Delete

Viewing: All Subnets

1 to 4 of 4 Items

Subnet ID	State	VPC ID	CIDR	Available IPs	Availability Zone	Route Table	Network ACL	Default Subnet
subnet-03373a6f	available	vpc-7790c01c	10.0.3.0/24	249	us-east-1a	rtb-b87c70d4	Default	false
subnet-4890c023	available	vpc-7790c01c	10.0.1.0/24	150	us-east-1a	rtb-7590c01e	Default	false
subnet-9e1b22f5	available	vpc-7790c01c	10.0.2.0/24	246	us-east-1a	rtb-eade6186	Default	false
subnet-4e90c025	available	vpc-7790c01c	10.0.0.0/24	230	us-east-1a	rtb-4390c028	Default	false

0 Subnets selected

Select a Subnet above

© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy | Terms of Use

Feedback

VPC - ROUTING/SUBNETS

Services | Edit | RF Research | N. Virginia | Help

VPC Dashboard

VIRTUAL PRIVATE CLOUDS
- Your VPCs
- Subnets
- Route Tables
- Internet Gateways
- DHCP Options Sets
- Elastic IPs

SECURITY
- Network ACLs
- Security Groups

VPN CONNECTIONS
- Customer Gateways
- Virtual Private Gateways
- VPN Connections

Create Subnet | Delete

Details | Tags

CIDR: 10.0.3.0/24 **VPC:** vpc-7790c01c **Availability Zone:** us-east-1a

Route Table: rtb-b87c70d4 (replace)

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	i-cdab71b1

Network ACL: Default (replace)
Inbound:

Rule #	Port (Service)	Protocol	Source	Allow/Deny
1	7	TCP	10.0.1.0/24	ALLOW
2	22 (SSH)	TCP	0.0.0.0/0	ALLOW
8	8080 (HTTP*)	TCP	0.0.0.0/0	ALLOW
100	ALL	ALL	0.0.0.0/0	ALLOW
101	ALL	TCP	5.5.0.0/24	ALLOW
102	16000	TCP	5.5.0.0/24	ALLOW

© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy | Terms of Use

Feedback

VPC - ROUTING/SUBNETS

Services | Edit | RF Research | N. Virginia | Help

VPC: All VPCs

VPC Dashboard

VIRTUAL PRIVATE CLOUDS
- Your VPCs
- Subnets
- Route Tables
- Internet Gateways
- DHCP Options Sets
- Elastic IPs

SECURITY
- Network ACLs
- Security Groups

VPN CONNECTIONS
- Customer Gateways
- Virtual Private

Create Route Table | Delete

Viewing: All Route Tables

1 to 6 of 6 Items

Route Table ID	Associated With	Main	VPC
rtb-4390c028	1 Subnet	No	vpc-7790c01c (10.0.0.0/16)
rtb-b87c70d4	1 Subnet	No	vpc-7790c01c (10.0.0.0/16)
rtb-8d7724e6	0 Subnets	No	vpc-7790c01c (10.0.0.0/16)
rtb-911a23fa	0 Subnets	No	vpc-7790c01c (10.0.0.0/16)

1 Route Table selected

Route Table: rtb-b87c70d4

Routes | Associations | Route Propagation | Tags

Destination	Target	Status	Propagated	Actions
10.0.0.0/16	local	active	No	Remove
0.0.0.0/0	eni-5894c433 / i-cdab71b1	active	No	Remove
	select a target			Add

© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy | Terms of Use

Feedback

VPC - ROUTING/SUBNETS

SECURITY ACLS

ACLs like a full stateless firewall - unlike security groups
Protects subnets instead of EC2 instances
Processed in order of rule #
ACLs are stateless - responses to inbound bound by outbound rules
To accommodate various clients and OSs open ephemeral ports 1024-65535 then block malicous ports

VPC - ROUTING/SUBNETS

SECURITY GROUPS

You can use a security group ID (starting with sgXXXXX) in blace
Processed in order of rule #
ACLs are stateless - responses to inbound bound by outbound rules
To accommodate various clients and OSs open ephemeral ports 1024-65535 then block malicous ports

VPC - ROUTING/SUBNETS

SECURITY GROUPS

VPC Security Groups are different than EC2 Groups - use different and descriptive names if both used
You can use a security group ID (starting with sgXXXXX) in blace
Processed in order of rule #
ACLs are stateless - responses to inbound bound by outbound rules
To accommodate various clients and OSs open ephemeral ports 1024-65535 then block malicous ports

VPC - ROUTING/SUBNETS

DHCP OPTIONS

Determine What DNS DHCP clients use
Can things like default domain, whether to use internal or external DNS for your VPC
From Web UI, assign only 1 option set at a time
Using amazon provided DNS, using naming scheme of 10.0.1.x, default domain ec2.internal
Can assign your own DNS server names, or even Netbios name servers or NTP servers
Options are semicolon delimited name value pairs, i.e. 'domain-name=something.com; domain-name-severs=AmazonProvidedDNSs

VPC - IAM ROLES

Don't use root account anymore. Traditional security page will be retired
Set up your IAM roles/groups for each user and use designated login url they give you
Use new resource level security with IAM to tier access to instances/resources

VPC - IAM ROLES - CONTINUED

SETUP STEPS

1. Tag your instances (like 'Env:Prod, Env:QA, Env:Dev')
2. Set up resource level IAM Policy
3. Lock down tags
4. Attach Policies to Users, Permissions, and Groups

VPC - IAM ROLES - SAMPLE

```
{
    "Version": "2013-07-21",
    "Statement": [
    {
        "Action": [
            "ec2:StartInstances",
            "ec2:StopInstances",
            "ec2:RebootInstances",
            "ec2:TerminateInstances"
        ],
        "Condition": {
            "StringEquals": {
            "ec2:ResourceTag/Environment":"dev"
            }
        },
        "Resource": [
            "arn:aws:ec2:your_region:your_account_ID:instance/*"
```

VPC - MISC EC2 TIPS

Reboot != Reboot
Rebooting a machine from console will keep instance in place and ephemeral storage
If you issue an OS reboot or a 'stop' command you machine will/may move and lose ephemeral state

VPC - MISC EC2 TIPS

VPN
Use OpenVPN instead of metered AWS VPN - it runs fine on a tiny instance- save $$
Use OpenVPN client to leave remote servers connected to VPC - it auto-reconnects

VPC - MISC EC2 TIPS

EBS Based Instances
Use EBS backed instances for anything not build for cloud
If you can build server on the fly with Chef/Puppet like tools, go for ephemeral based
EBS backed instances have no swap by default - be sure to specify ephemeral disks on launch, use as swap
EBS backed instances have no ephemeral disks on by default be sure to use them on launch of instance and AMIs

S3 STORAGE

Limitations
Common tools
Regions with different functionality
Glacier
Grails S3 Plugin

S3 STORAGE

LIMITATIONS - EVENTUAL CONSISTENCY

This means after write/update it will EVENTUALLY be consistent
Make your app retry on read fail - it might not be synced yet
Different regions have different consistency rules
US-West and EU Buckets have read after write consistency - but not update or delete (and cost more)
US-East is so large it cannot handle any kind of consistency after write/update/delete - except patience!

S3 STORAGE

LIMITATIONS - LARGE FILES

Files over 5GB supported, but most tools don't handle properly
S3 Tools must support mime/multipart
s3cmd(Linux) / CyberDuck 4(Mac/Win32) / S3 Browser(Win32) / Cloudberry Explorer(PRO Win32) / Bucket Explorer
File > 5GB files work with these tools, it is EXTREMELY slow

S3 STORAGE

TOOLS

s3fs - mount as filesystem - but >5GB files broken, beware of consistency!
Make sure FUSE is in kernel
s3cmd is best free command line tools
Bucket Explorer & CloudBerry Backup are good solid windows clients that parallelize multi-part uploads to ease the pain
s3 Browser is ok free tool
For install on Ubuntu:
http://zentraal.com/docs/installing-s3fs-on-ubuntu/

S3 STORAGE

DIFFERENT FUNCTION BETWEEN DIFFERENT REGIONS

US-East-1 Cheapest for full redundancy otherwise to save $ you can use RRS (Or Glacier)
US-West and EU Buckets have read after write consistency - but not update or delete (and cost more)
US-East is so large it cannot handle any kind of consistency after write/update/delete - except patience!
Barring these limitations (and budget!), use the region closed to your VPC instances and regions

S3 STORAGE
GRAILS S3 PLUGIN

Looks unmaintained, but still works fine on latest Grails versions (no JIRA bugs pending!)
Delete Buckets (See org.grails.s3.BucketService)
Uploads and catalogs assets (will use bucket name you give as base for its bucket name)
Names files inside bucket with UUIDs to avoid collisions
Can give each asset a bucket and key pair or global
Demo - s3-demo project

GENERAL AWS-RELATED GRAILS PLUGINS

Grails AWS Plugin
AWS SDK Plugin
DynamoDB GORM Plugin - not covered
Amazon Flexible Payments - not covered
SimpleDB GORM Plugin - not convered

GENERAL AWS GRAILS PLUGINS - GRAILS AWS PLUGIN

ACTUAL GROOVY/GRAILS CODE TO MANAGE S3 STORAGE AND SES SERVICE (VS JAVA WRAPPER)

GENERAL AWS GRAILS PLUGINS - GRAILS AWS PLUGIN

HAS HANDY GANT SCRIPTS INSTALLED - USED FOR SES STATS

Aws-Ses-Get-Send-Quota
Aws-Sws-Get-Send-Statistics
Aws-Ses-List-Verified-Emails
Aws-Ses-Send-Ping-Mail
Aws-Ses-Verify-Email

GENERAL AWS GRAILS PLUGINS - GRAILS AWS PLUGIN

AWS-SES-GET-SEND-QUOTA

Gets your current Quota for Simple Email Service
Shows email limit per day, per second, # of emails
Output looks like this:
[AWS SES] The maximum number of emails the user is allowed to send in a 24-hour interval: 10000.0
[AWS SES] The maximum number of emails the user is allowed to send per second: 5.0
[AWS SES] The number of emails sent during the previous 24 hours: 15.0

GENERAL AWS GRAILS PLUGINS - GRAILS AWS PLUGIN

AWS-SWS-GET-SEND-STATISTICS

Gets your email sending statistics
The output is a list of items, for the last two weeks of sending activity.
Example output:
[AWS SES] ----------
[AWS SES] | time range | attemps | rejects (SES) | complaints (recipient) | bounces |
[AWS SES] |----------|
[AWS SES] | 2013/06/26 22:42 | 1 | 0 | 0 | 0 |

GENERAL AWS GRAILS PLUGINS - GRAILS AWS PLUGIN

AWS-SES-LIST-VERIFIED-EMAILS

Shows a list of all verified emails with
The output is a list of emails authorized to send email FROM
Example output:
[AWS SES] 1) support@yourcompany.com

GENERAL AWS GRAILS PLUGINS - GRAILS AWS PLUGIN

AWS-SES-SEND-PING-MAIL

Script will verify a given email has been 'verified' by Amazon

GENERAL AWS GRAILS PLUGINS - GRAILS AWS PLUGIN

AWS-SES-VERIFY-EMAIL

Script will submit an email for verification to amazon, and send an email to that address

GENERAL AWS GRAILS PLUGINS - GRAILS AWS PLUGIN

AWS-SES-VERIFY-EMAIL

Script will submit an email for verification to amazon, and send an email to that address

GENERAL AWS GRAILS PLUGINS - GRAILS AWS PLUGIN

S3 FILE MANAGEMENT

Demo

GENERAL AWS GRAILS PLUGINS - GRAILS AWS PLUGIN

S3 FILE MANAGEMENT

Handy for storing existing assets into S3

```
Convert local File to S3 Storage

def s3file = new File("/tmp/test.txt").s3upload {
    path "folder/to/my/file/"
 }
```

Upload directly from Stream:

```
    def file = request.getFile('photo')
    def uploadedFile = file.inputStream.s3upload(file.originalFile
           bucket "file-upload-from-inputstream"
    }
```

GENERAL AWS GRAILS PLUGINS - GRAILS AWS PLUGIN

SES MANAGEMENT

AFAIK skip this - the mail plugin handles all of this

```
// settings for mail plugin to work with SES
    grails {
        mail {
            host = "email-smtp.us-east-1.amazonaws.com"
            port = 25
            username = "SESUsername"
            password = "SESPassword"
            props = ["mail.smtp.starttls.enable":"true",
            "mail.smtp.port":"587","mail.debug":"true","mail.smtp.auth":
            // uncomment to force all emails to one address
            // grails.mail.overrideAddress="test@address.com"
            grails.mail.default.from = "support@yourcompany.com"
        }
    }
```

GENERAL AWS GRAILS PLUGINS - AWS SDK PLUGIN

Wrapper for AWS Java SDK
This is the one to use for most powerful work of services - can access almost all of AWS services that JDK supports
Uses AWS Web Service API wrapped in a Java Library
Error handing can be more difficult than using web service api directly

GENERAL AWS GRAILS PLUGINS - AWS SDK PLUGIN

SERVICES SUPPORTED

EC2 - ELB,CloudWatch, Elastic Beanstalk
RDS - Elastic Mapreduce, SDB, Dynamo, Redshift, SimpleDB
S3/Glacier
SES (us-east-1 only)
SQS, SWF
CloudFormation,CloudFront
Elastic Beanstalk, Transcoder, Opsworks(Old Chef)
Cloudformation, CloudSearch, Elasticache

GENERAL AWS GRAILS PLUGINS - AWS SDK PLUGIN

EC2

Grails service wrapper is 'amazonWebService'
Call amazonWebService.ec2. - for default region, call amazonWebService.getEc2('region'). for others
RunInstancesRequest class defines parameters to launch an instance (It seems picky about nulls)
use amazonWebService.runInstances() to start instances
Complete docs at:
http://docs.aws.amazon.com/AWSJavaSDK/latest/javadoc/

GENERAL AWS GRAILS PLUGINS - AWS SDK PLUGIN

RDS

Not sure why you would spin up entire databases, but you can!
Most practical use would be to automate snapshots of the database
If you have a small simple database, service is good
Cannot start/top RDS instances, and pay premium to use their licenses if using commercial DBs
If you have the skill or have large DB requirements, set up your own database - there is probably an AMI for it
Has good multi-az failover (but pricey!) with PIOPS EBS Volumes (You can raid your own PIOPS drives!)

GENERAL AWS GRAILS PLUGINS - AWS SDK PLUGIN

S3

manage buckets, upload/download and delete files
Transfer Manager - handles multipart uploads (big files, batch, fas
full docs here:
http://docs.aws.amazon.com/AWSJavaSDK/latest/javadoc/com/ama
summary.html
s3browser demo

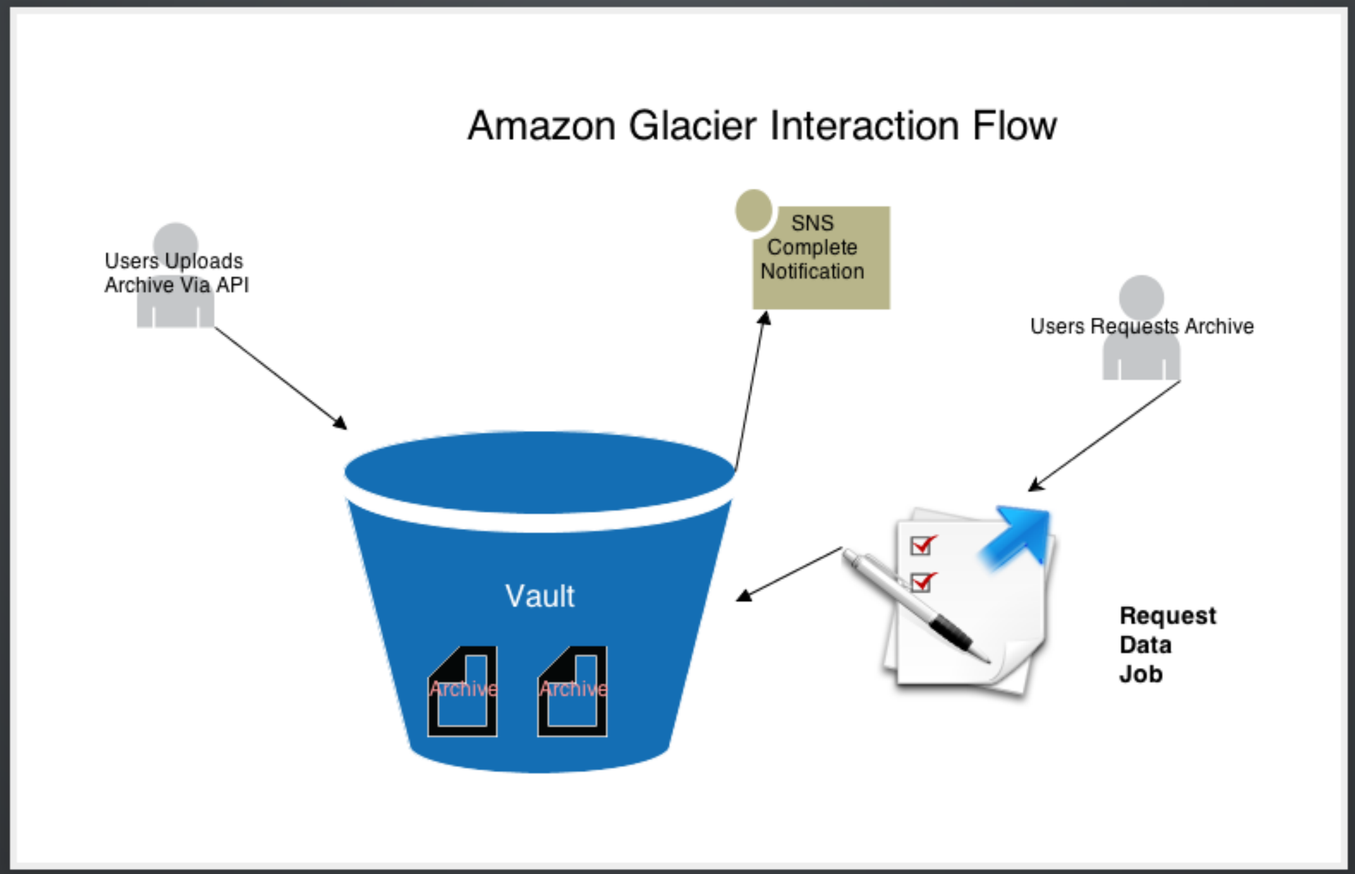
GENERAL AWS GRAILS PLUGINS - AWS SDK PLUGIN

GLACIER

cold storage for data - not immediately available on demand
vaults - organize your archives and policies (where your files go)
Upload files via amazonWebService.glacier.uploadArchive(UploadArchiveRequest uploadArchiveRequest) or UploadMultiPart
Files are retrieved via 'initiateJob'
Call 'listJobs' until your job is done.
Can use Amazon SNS to notify you when jobs are complete
When done get files from your vault via GetJobOutput

GENERAL AWS GRAILS PLUGINS - AWS SDK PLUGIN

GLACIER



GENERAL AWS GRAILS PLUGINS - AWS SDK PLUGIN

SQS

Simple queue service
Create / Delete Queues
Receive Message
Can also assign permissions and batch messages
Messages can remain in queue for 12 hours

ELASTIC LOAD BALANCER

With VPC more options can be internal or external LB
60s timeout on idle max - can file ticket for extension to 15+ minutes(but screws up UI!)
Quick and easy - be up and running with scale in minutes!
Use Haproxy or nginx for anything very advanced, can accommodate many options

ELASTIC LOAD BALANCER

You can install your own SSL cert - this avoids having to install certs on each server
Supports sticky source IPs which many webapps need
Balancing HTTP only supports 80, 443 - only straight TCP LB works on 1024-65535
On VPC, the ELB takes one of your IP addresses
Use Route 53 health checks to provide DNS failover of ELB endpoints(Sorry server pages)
Works with multiple AZs - if on AZ is down it will auto route to instance in the other

ELASTIC LOAD BALANCER

Use with autoscaling for tremendous power!
Can't load balance paid AMIs with ELB (argh)
Simple port mapping allowed
On VPC, internal load balancing rocks - no maintenance or fuss
Beware of 60 second idle limit. This solution doesnt work well with long-running idle connections
Do NOT register the IP of your endpoint in DNS!
CNAME only - IPs can and do change

ELASTICWOLF

More powerful than web console gui
Can control things like auto-scaling
Created partly for new GovCloud because they had no UI at all initially
Managed by sales organization instead of IT
Actively Maintained on Github

ELASTICWOLF

Demo

AUTOSCALING OVERVIEW

Autoscaling can be used for fault-tolernance (min 1)
Most efficient user of instance
Set Policies using templates for how more servers created/terminated
Control Spot instance bid price
You app must be able to handle 'sudden death'
Make sure your debug your AMI BEFORE adding to a autoscale group (debugging failed autoscaled instances is no way to go through life son!)

AUTOSCALING SETUP

Step 1: Create Launch Config(Just like launching instance but a ter
Step 2: Create Autoscale Group
Step 4: Create Policies (Scale Up and Scale Down)
Step 3: Create CloudWatch Alarms (Assign to Topic of your policie
Scheduled Actions - scale up or down based on pre-set cron like se
Failover - if you have even 1 instance, you can set min servers to
another
Custom CloudWatch Metrics - Create and associate to autoscaling
http://docs.aws.amazon.com/AmazonCloudWatch/latest/Developer
Current docs:
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/W
Demo with ElasticWolf

ELASTIC BEANSTALK

Bobby Warner's Blog:
http://www.bobbywarner.com/2011/10/14/grails-on-aws/
Elastic Beantalk in 3 simple steps:
http://malderhout.wordpress.com/2011/02/18/deploy-grails-apps-in-3-simple-steps-to-amazon-beanstalk

USEFUL RESOURCES

Elastic Beanstalk Intro @ Bobby Warner's Blog:
http://www.bobbywarner.com/2011/10/14/grails-on-aws/
Another Beanstalk:
http://malderhout.wordpress.com/2011/02/18/deploy-grails-apps-in-3-simple-steps-to-amazon-beanstalk/
Sample Beanstalk app:
https://github.com/4np/grailsOnAWS
Try out free beta of StackDriver.com - auto scans your assets and monitors

USEFUL RESOURCES - CONTINUED

Oracle, EBS, and other Tips from AWS Architect Tom Laszewski http://cloudconclave.blogspot.com/
Building an S3 Browser in Grails http://aws.amazon.com/articles/Amazon-S3/4000
Autoscaling with Amazon Web Services - Part 1 http://www.cardinalpath.com/autoscaling-your-website-with-amazon-web-services-part-1/
Autoscaling with Amazon Web Services - Part 2 http://www.cardinalpath.com/autoscaling-your-website-with-amazon-web-services-part-2/

QUESTIONS?

THANK YOU!

Follow me on Twitter @RyanVanderwerf
Blog: http://rvanderwerf@blogspot.com
Storm picture used under Creative Commons license. http://www.flickr.com/photos/jumpyjodes/