

**Deloitte.**



**AWS Training Workshop Guide**

18 October 2018

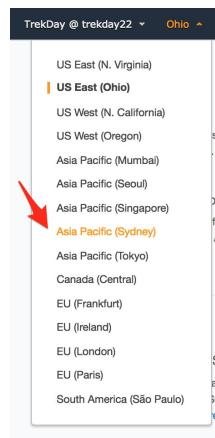
# Session 1 - Introduction

In this session we will get introduced to AWS and create our first virtual server.

Take the following steps, one at a time. There is plenty of time to complete the session and ask any questions along the way.

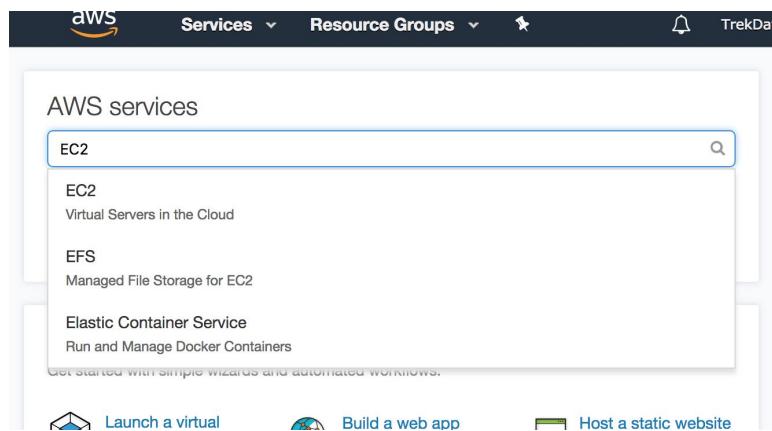
## Getting Started

- Log into the AWS console using the details provided on your Credentials Note
- Set the region to Sydney (stay in this region today, check from time to time)



## Create a Virtual Server - EC2 Instance

- Navigate to EC2



**- Click “Launch Instance”**

Resources

You are using the following Amazon EC2 resources in the Asia Pacific (Sydney) region:

0 Running Instances	0 Elastic IPs
0 Dedicated Hosts	0 Snapshots
0 Volumes	0 Load Balancers
0 Key Pairs	1 Security Groups
0 Placement Groups	

Learn more about the latest in AWS Compute from AWS re:Invent 2017 by viewing the [EC2 Videos](#).

Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

**Launch Instance**

Note: Your instances will launch in the Asia Pacific (Sydney) region

**- Step 1: Select an Amazon Machine Image (AMI)**

Take a look at all the different Amazon Machine Images that are available. There are many variants of Windows and Linux.

**- Select "Microsoft Windows Server 2016 Base"**

1. Choose AMI    2. Choose Instance Type    3. Configure Instance    4. Add Storage    5. Add Tags    6. Configure Security Group    7. Review

**Step 1: Choose an Amazon Machine Image (AMI)**

**Cancel and Exit**

Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Root device type: ebs    Virtualization type: hvm

**Are you launching a database instance? Try Amazon RDS.**

**Amazon RDS**

Amazon Relational Database Service (RDS) makes it easy to set up, operate, and scale your database on AWS by automating time-consuming database management tasks. With RDS, you can easily deploy **Amazon Aurora, MariaDB, MySQL, Oracle, PostgreSQL, and SQL Server** databases on AWS. **Aurora** is a MySQL- and PostgreSQL-compatible, enterprise-class database at 1/10th the cost of commercial databases. [Learn more about RDS](#)

**Launch a database using RDS**

<b>Microsoft Windows Server 2016 Base - ami-48d6122a</b>	<b>Select</b>
Windows	64-bit
<small>Free tier eligible</small>	
Microsoft Windows 2016 Datacenter edition. [English]	
Root device type: ebs    Virtualization type: hvm	
<hr/>	
<b>Deep Learning AMI (Ubuntu) Version 4.0 - ami-e223985</b>	<b>Select</b>
Deep Learning AMI (Ubuntu) Version 4.0	64-bit
<small>Free tier eligible</small>	
Latest versions of deep learning frameworks pre-installed in separate virtual environments: MXNet, TensorFlow, Caffe, Caffe2, PyTorch, Theano, CNTK, Keras	
Root device type: ebs    Virtualization type: hvm	
<hr/>	
<b>Deep Learning AMI (Amazon Linux) Version 4.0 - ami-46c23924</b>	<b>Select</b>
Deep Learning AMI (Amazon Linux) Version 4.0	64-bit
<small>Free tier eligible</small>	
Latest versions of deep learning frameworks pre-installed in separate virtual environments: MXNet, TensorFlow, Caffe, Caffe2, PyTorch, Theano, CNTK, Keras	
Root device type: ebs    Virtualization type: hvm	

## - Step 2: Choose an Instance Type

Take a look at all the different Instance Types available. There are sizes for almost any workload.

### - Select "t2.micro"

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
General purpose	<b>t2.micro</b>	1	1	EBS only	-	Low to Moderate	Yes
General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
General purpose	m5.large	2	8	EBS only	Yes	Up to 10 Gigabit	Yes
General purpose	m5.xlarge	4	16	EBS only	Yes	Up to 10 Gigabit	Yes

Cancel Previous **Review and Launch** Next: Configure Instance Details

### - Select “Review and Launch”, then “Launch”

Step 7: Review Instance Launch

AMI Details

Microsoft Windows Server 2016 Base - ami-48d6122a

Free tier eligible Microsoft Windows 2016 Datacenter edition. [English]  
Root Device Type: ebs Virtualization type: hvm

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups

Security group name: launch-wizard-1  
Description: launch-wizard-1 created 2018-02-23T09:01:22.258+10:00

Type	Protocol	Port Range	Source	Description
This security group has no rules				

Instance Details

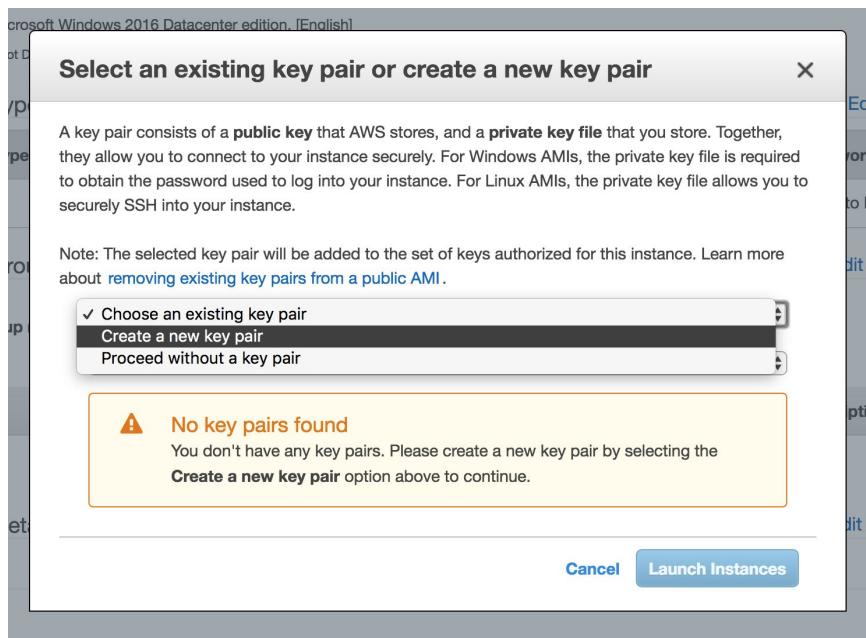
Storage

Tags

Cancel Previous **Launch**

- Popup: "Select an existing key pair or create a new key pair"

- Select: "Create a new key pair"



- Provide: Type a name, then "Download Key Pair" and keep it safe, we will use this a couple of times today.

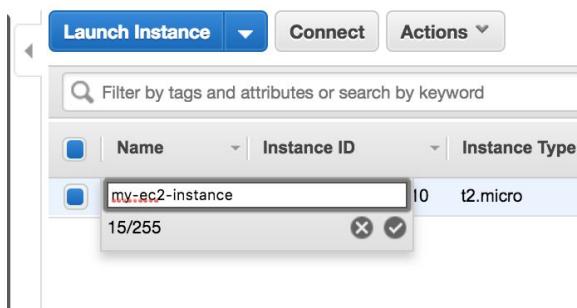
- Select: "Launch instances"

- Scroll down and select "View Instances"

- Review the "Instances" page.

This is where you will see all the instances you have launched. We will be coming back to this list several times today.

- Set the name of the instance, by clicking the pencil in the Name column. Set the name to "my-ec2-instance".



*Tip: Make sure you select the 'tick' when changing the name, else it won't take.*

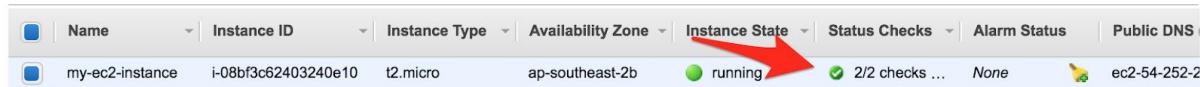
- Review the "Description" tab for the running instance.
- Look at the "Tags" tab, notice that the name is set as a tag.

The screenshot shows the 'Tags' tab of the AWS CloudWatch Metrics interface. At the top, there are tabs for 'Description', 'Status Checks', 'Monitoring', and 'Tags'. The 'Tags' tab is selected, indicated by an orange underline. Below the tabs is a button labeled 'Add/Edit Tags'. The main area displays a table with two columns: 'Key' and 'Value'. A single row is present, showing 'Name' in the Key column and 'my-ec2-instance' in the Value column. There is also a 'Hide Column' link next to the Value column header.

Key	Value	
Name	my-ec2-instance	<a href="#">Hide Column</a>

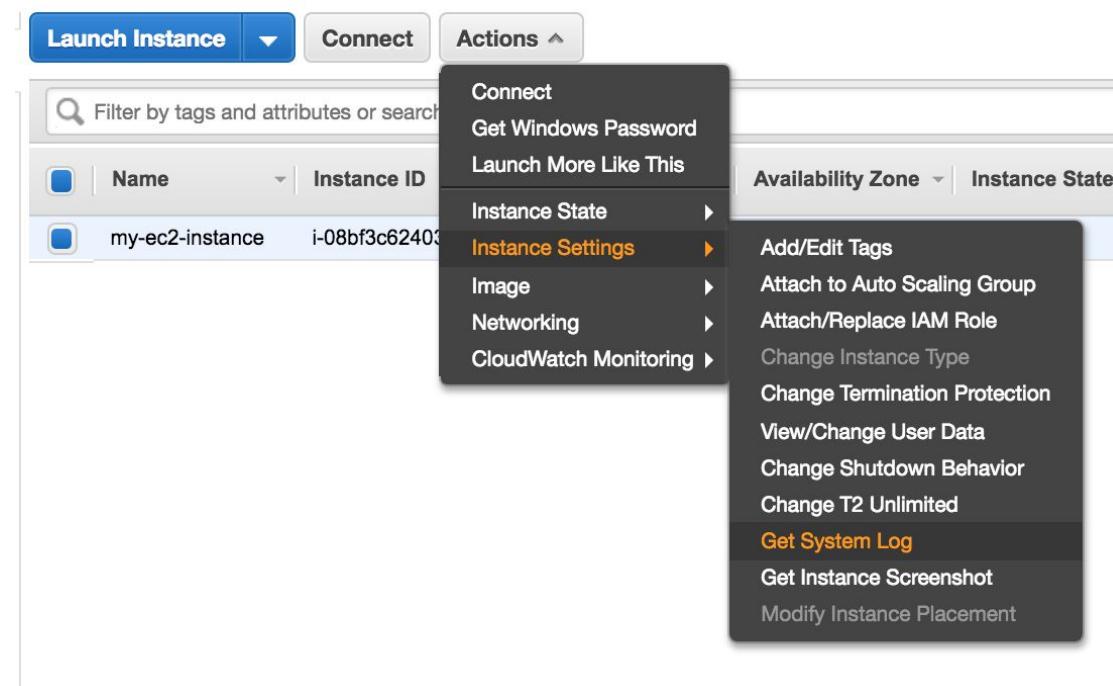
## Connect to the Virtual Server - EC2 Instance

- Wait for the "Status Checks" 2/2. This means that the host and guest OS's are passing status checks.

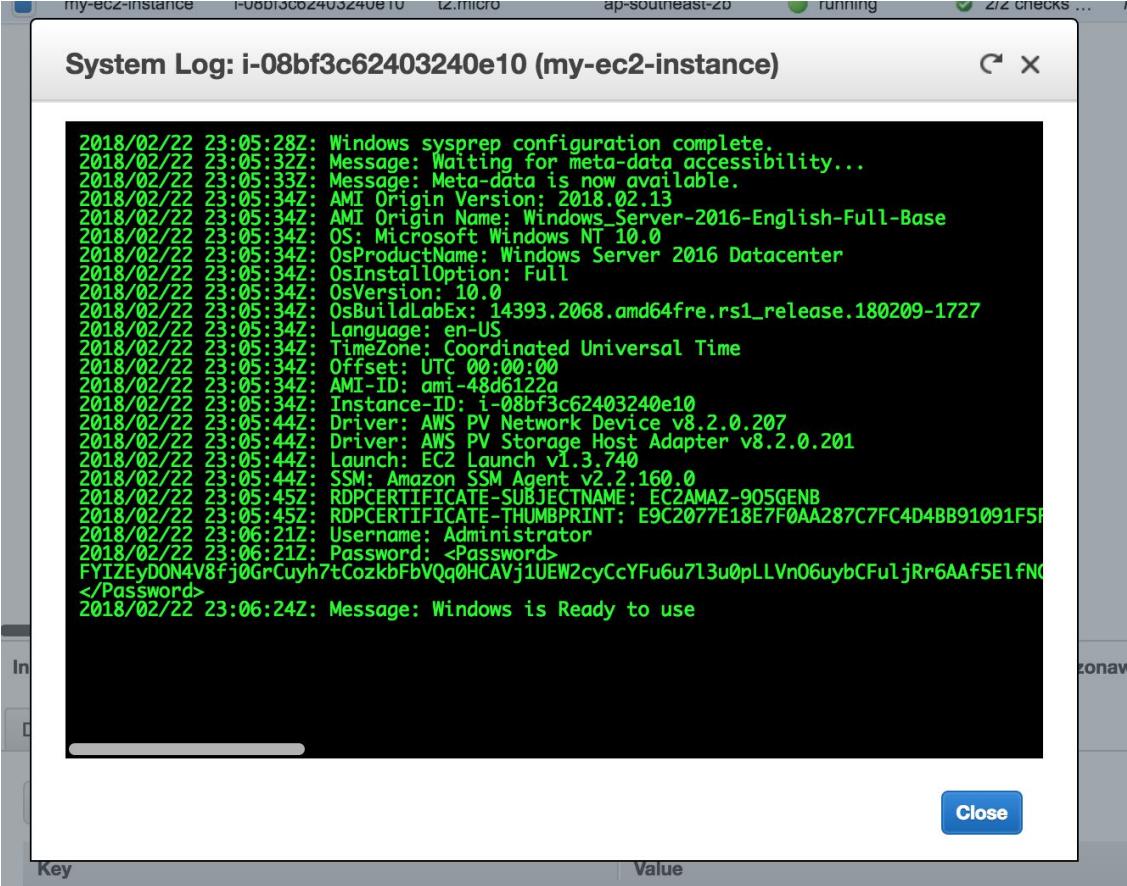


- Let's check that the Windows server is up and running:

- With the instance selected, select "Actions", "Instance Settings", "Get System Log"



- You should be able to see system logs sent from the server.

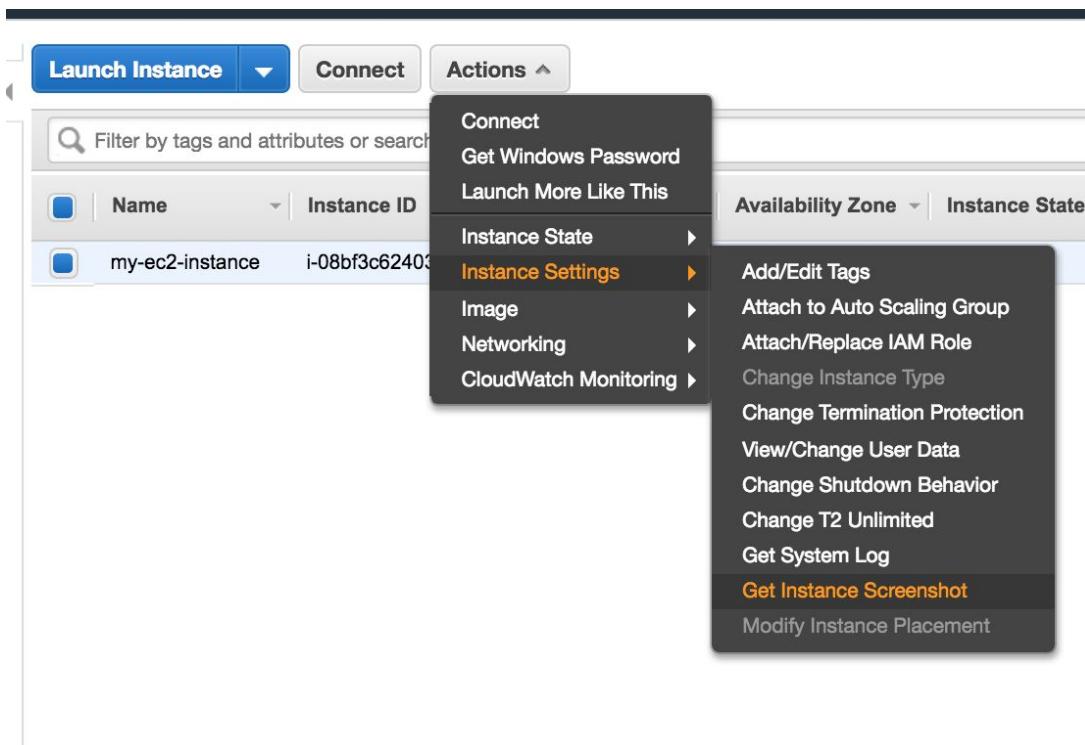


The screenshot shows a modal window titled "System Log: i-08bf3c62403240e10 (my-ec2-instance)". The log output is displayed in a monospaced font. The log entries are as follows:

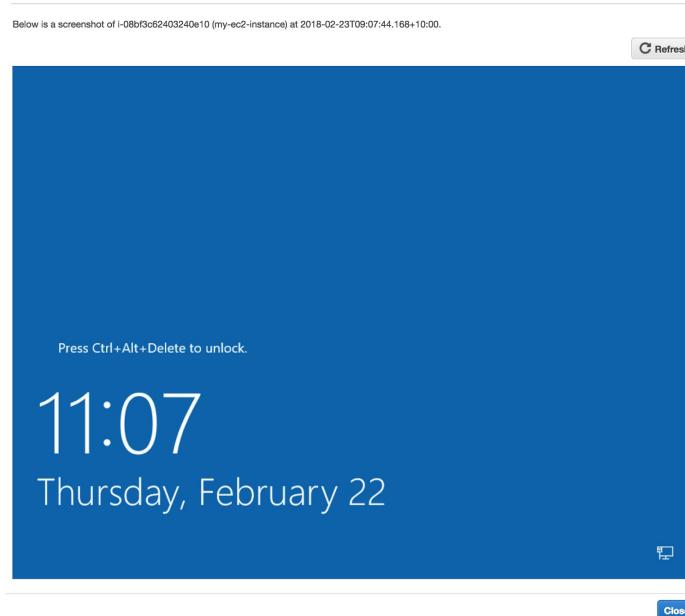
```
2018/02/22 23:05:28Z: Windows sysprep configuration complete.
2018/02/22 23:05:32Z: Message: Waiting for meta-data accessibility...
2018/02/22 23:05:33Z: Message: Meta-data is now available.
2018/02/22 23:05:34Z: AMI Origin Version: 2018.02.13
2018/02/22 23:05:34Z: AMI Origin Name: Windows_Server-2016-English-Full-Base
2018/02/22 23:05:34Z: OS: Microsoft Windows NT 10.0
2018/02/22 23:05:34Z: OsProductName: Windows Server 2016 Datacenter
2018/02/22 23:05:34Z: OsInstallOption: Full
2018/02/22 23:05:34Z: OsVersion: 10.0
2018/02/22 23:05:34Z: OsBuildLabEx: 14393.2068.amd64fre.rs1_release.180209-1727
2018/02/22 23:05:34Z: Language: en-US
2018/02/22 23:05:34Z: TimeZone: Coordinated Universal Time
2018/02/22 23:05:34Z: Offset: UTC 00:00:00
2018/02/22 23:05:34Z: AMI-ID: ami-48d6122a
2018/02/22 23:05:34Z: Instance-ID: i-08bf3c62403240e10
2018/02/22 23:05:44Z: Driver: AWS PV Network Device v8.2.0.207
2018/02/22 23:05:44Z: Driver: AWS PV Storage Host Adapter v8.2.0.201
2018/02/22 23:05:44Z: Launch: EC2 Launch v1.3.740
2018/02/22 23:05:44Z: SSM: Amazon SSM Agent v2.2.160.0
2018/02/22 23:05:45Z: RDPCERTIFICATE-SUBJECTNAME: EC2AMAZ-905GENB
2018/02/22 23:05:45Z: RDPCERTIFICATE-THUMPRINT: E9C2077E18E7F0AA287C7FC4D4BB91091F5F
2018/02/22 23:06:21Z: Username: Administrator
2018/02/22 23:06:21Z: Password: <Password>
</Password>
2018/02/22 23:06:24Z: Message: Windows is Ready to use
```

- Notice the Password field is encrypted
- Is there a line that says: "Message: Windows is Ready to use"?
- Select "Close"

- With the instance selected, select "Actions", "Instance Settings", "Get Instance Screenshot":



- You should see an image of the screen output of the server.

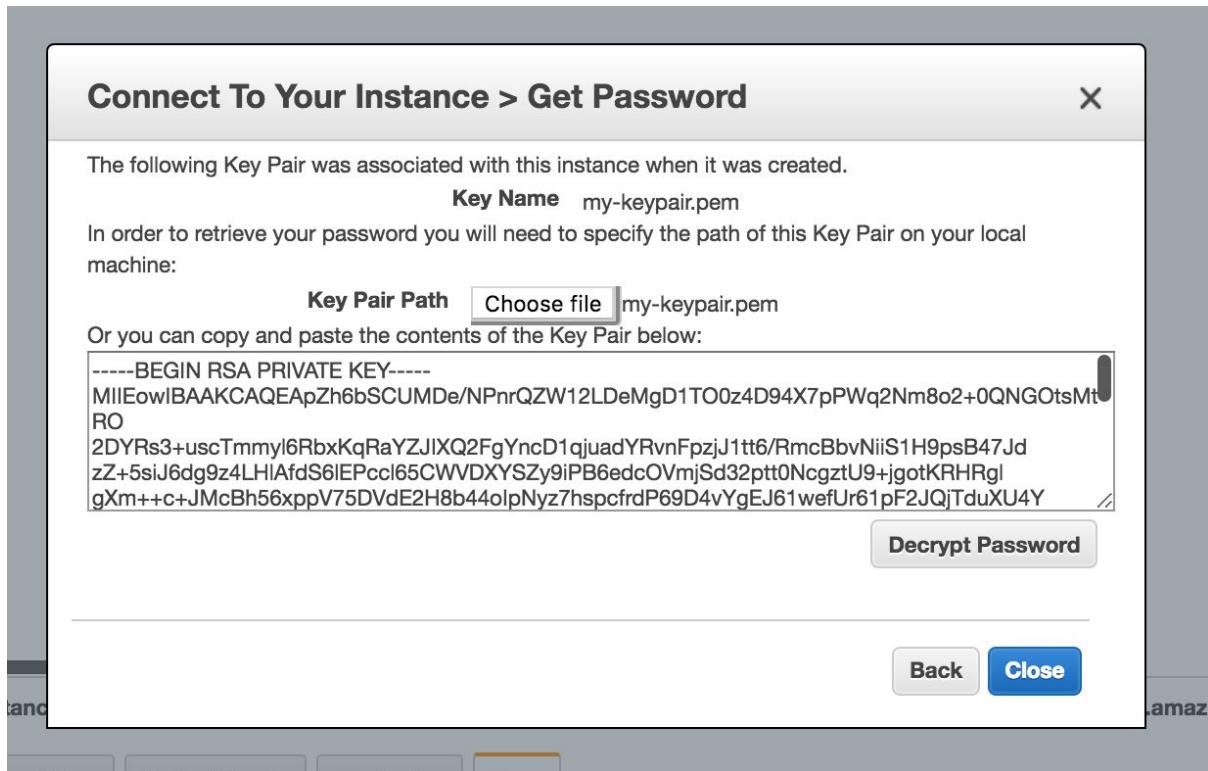


- You can't interact with this image, so lets log in to the server.

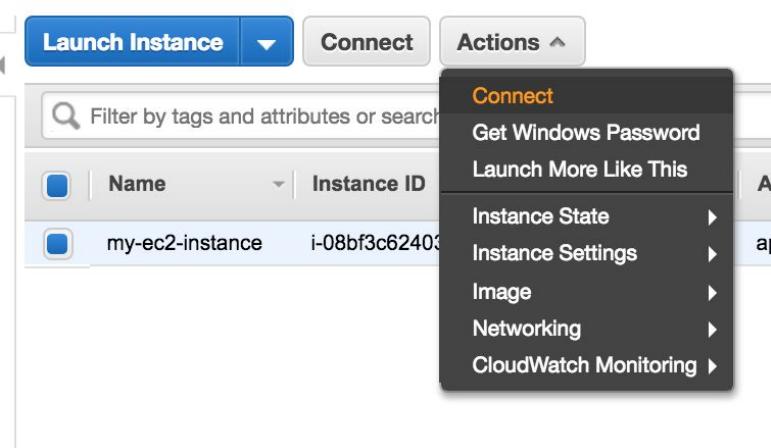
- Select "Close"

- Let's decrypt the Windows Administrator password:

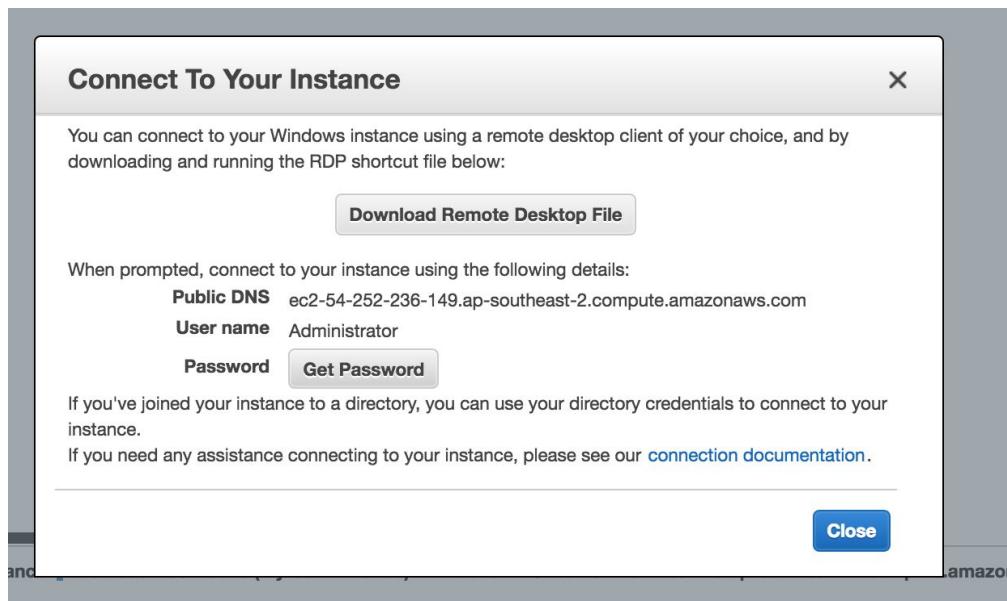
- With the instance selected, select "Actions", "Get Windows Password"
- Select “Choose file” and browse to the key file you downloaded earlier in this section.
- Select "Decrypt Password"



- Keep the details safe somewhere.
- Again with the instance selected, click "Actions" and select "Connect"



- Popup: "Connect To Your Instance" select "Download Remote Desktop File"



- This should download, automatically open, and configure a Remote Desktop Protocol client to connect to your instance.

*If clicking the "Download Remote Desktop File" didn't work for you:*

- Open your RDP client, enter the DNS value into the address field
- When prompted enter the username and password.

- Note: when you connect you may be prompted by security warnings. This is not a production environment, these warnings are ok.

- Back in the AWS console, let's take a look at how our server is doing.

You might want to open this next link in a new tab, it helps to have different AWS services open in different tabs to save time when switching back and forth.

- Navigate to CloudWatch

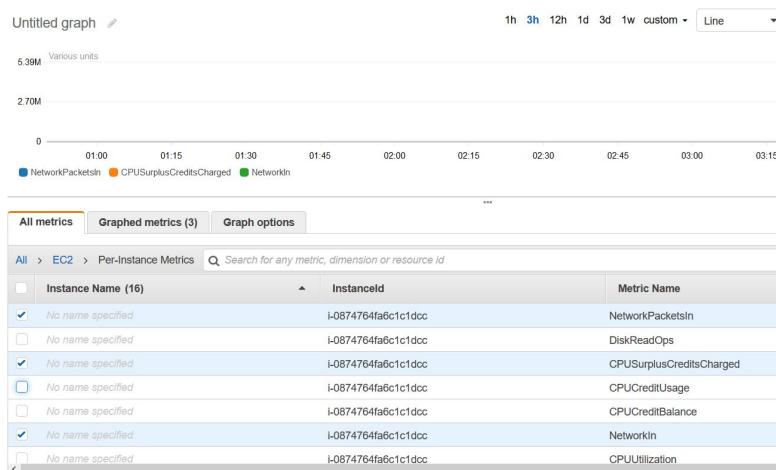
- CloudWatch is the central location of all monitoring and logging in AWS.

- Select “Browse Metrics”

- Towards the bottom, with the tab “All metrics” selected, select “EC2” then “Per-Instance Metrics”

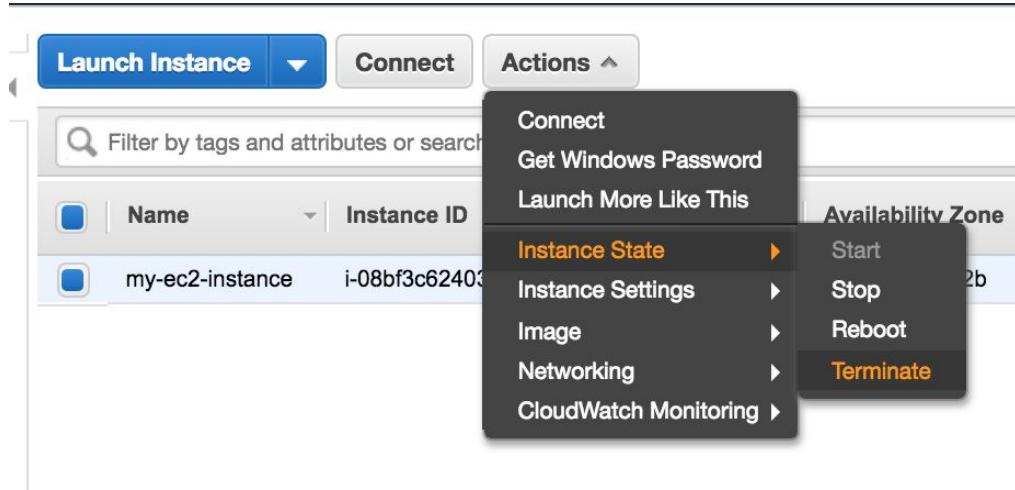
The screenshot shows the AWS CloudWatch Metrics interface. At the top, there are three tabs: "All metrics" (which is selected), "Graphed metrics", and "Graph options". Below the tabs, the breadcrumb navigation shows "All > EC2 > Per-Instance Metrics". There is a search bar with the placeholder "Search for any metric, dimension or resource id". The main area displays "16 Metrics" under the heading "Per-Instance Metrics".

- Have a browse around the available metrics. Over time you will be able to see these metrics graphed here.

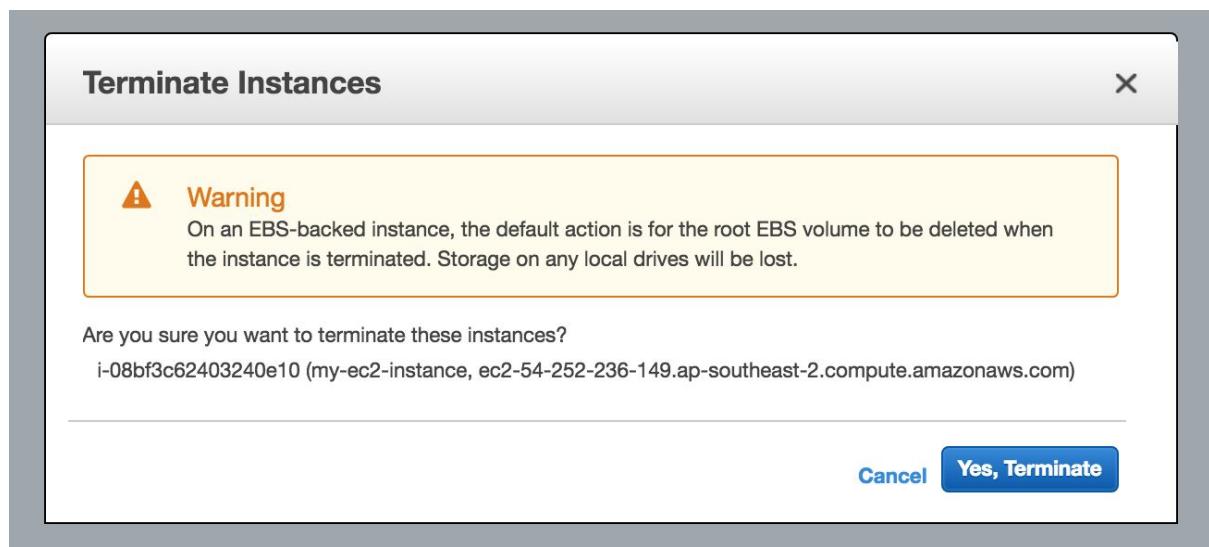


- Now let's clean up. We don't need this server anymore:

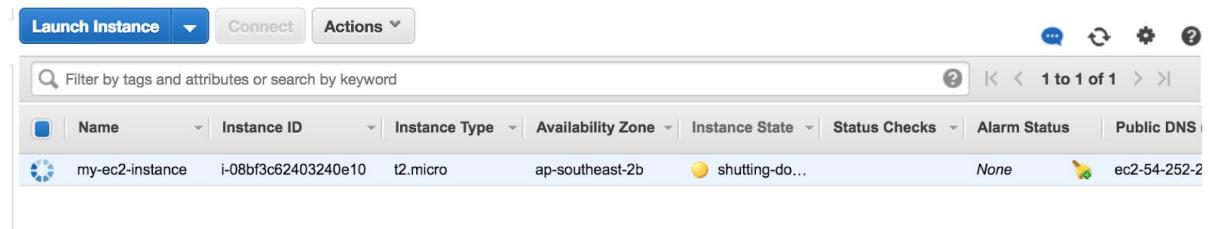
- Change your region back to Sydney.
- Back in the EC2 console page, with the instance selected, select "Actions", "Instance State", "Terminate"



- Review the warning to make sure you are terminating the right instance, if so, select "Yes, Terminate"



- Note the Key Pair is still in the account (along with some other stuff), but that's ok we will use it later.



- Return to the "EC2 Dashboard", you should have 0 (Zero) running instances.

## Resources



You are using the following Amazon EC2 resources in the Asia Pacific (Sydney) region:

0 Running Instances	0 Elastic IPs
0 Dedicated Hosts	0 Snapshots
0 Volumes	0 Load Balancers
1 Key Pairs	2 Security Groups
0 Placement Groups	

Learn more about the latest in AWS Compute from AWS re:Invent 2017 by viewing the [EC2 Videos](#).



## Create Instance

**END**

# Session 2 - CloudFormation

In this session we will get introduced to AWS CloudFormation.

Take the following steps, one at a time. There is plenty of time to complete the session and ask any questions along the way.

## Steps

### - Lets create a CloudFormation template

- Open your favorite text editor (e.g. VSCode) and create a new YAML file.
- File new
- Save as "my-template.yaml"

## Build a CloudFormation Template

### - Now let's build the template

### - First we add the template version:

```
AWSTemplateFormatVersion: 2010-09-09
```

### - In this simple template we are only going to use the 'Resources' section:

#### - In the Resources section we will add an entry for each resource we are going to create. In this case that is one EC2 Instance

- (As we build the YAML file, look to ensure the tab (spaces) are correct)

```
Resources:
```

```
  myInstance:  
    Type: "AWS::EC2::Instance"
```

- The "myInstance" element is used to refer to our instance elsewhere in the template. That's not of much use in this template, but will be useful in more complex templates later.

- Notice that we have used an AWS specific Type of "AWS::EC2::Instance". This is where we set that we are creating an EC2 Instance

- Lets configure the instance with some properties. Create the following lines, read for some values:

Properties:

ImageId:

InstanceType:

KeyName:

- Let's find the Image Id. When we created the image 'by hand' this was listed during Step 1.

- While we are creating this template, open a browser tab, in the EC2 Dashboard, and select "Launch instance"

- In "Step 1" look at the OS/Images, scroll to "Microsoft Windows Server 2016 Base"

The screenshot shows the 'Launch a database using RDS' button at the top. Below it, the 'Windows' section displays the 'Microsoft Windows Server 2016 Base - ami-48d6122a' AMI. It includes details like 'Microsoft Windows 2016 Datacenter edition. [English]', 'Root device type: ebs', 'Virtualization type: hvm', and a note that it is 'Free tier eligible'. Another AMI, 'Deep Learning AMI (Ubuntu) Version 4.0 - ami-e7c23985', is also visible below.

- See the Amazon Machine Image ID (ami-xxxxxx) written next to the AMI name.
- Make a note of this value.

- Let's find the InstanceType.
- Select the AMI in the wizard to see "Step 2"

Filter by: All instance types ▾ Current generation ▾ Show/Hide Columns			
Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB me			
	Family	Type	vCPUs ⓘ
<input type="checkbox"/>	General purpose	t2.nano	1
<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1
<input type="checkbox"/>	General purpose	t2.small	1
<input type="checkbox"/>	General purpose	t2.medium	2
<input type="checkbox"/>	General purpose	t2.large	2
<input type="checkbox"/>	General purpose	t2.udl--	4

- In "Step 2" look at the Type we used. It was "t2.micro"
- Make a note of this value.

- Finally lets find the name of a Key Pair we can use.
- We created a Key Pair in the first session today. Let's find its name.
- Cancel the "Launch Instance" wizard.
- On the left hand side, scroll down to "Key Pairs"



- You should have one Key pair name in here. Make a note of this value. It should be the same name as the PEM file your downloaded in Session 1 (that's another way to find the name)
- Back in the CloudFormation template, enter the values we found into the relevant lines:

Properties:

```
  ImageId: ami-82a458e0
  InstanceType: t2.micro
  KeyName: my-key-pair
```

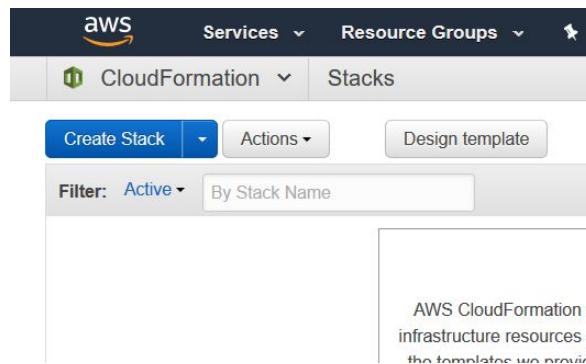
- The complete file should now look like something like this:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  myInstance:
    Type: "AWS::EC2::Instance"
    Properties:
      ImageId: ami-82a458e0
      InstanceType: t2.micro
      KeyName: my-key-pair
```

- Save your YAML CloudFormation template somewhere on your computer.

## Build a CloudFormation Stack

- Let's use the template to create a CloudFormation Stack
- Log into the AWS console
- Set the region to Sydney (stay in this region today, check from time to time)
- Navigate to CloudFormation



- Select "Create Stack"
- From the next screen, select "Upload a template to Amazon S3" and click "Browse" and select the CloudFormation template you created earlier in this session.

**Choose a template** A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. [Learn more](#).

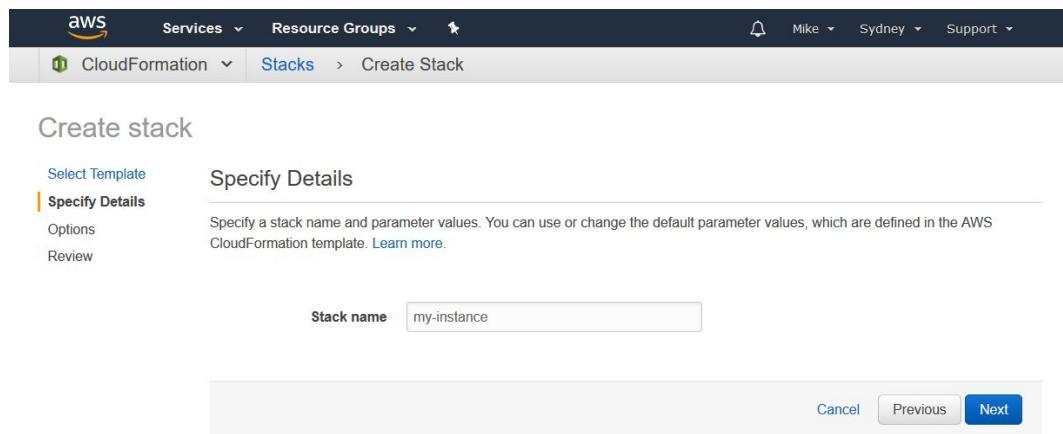
Select a sample template  
 Upload a template to Amazon S3  
 Specify an Amazon S3 template URL

[Browse...](#) No file selected.

- Select "Next"

- If you are shown a validation error at this point, check that your YAML file looks like the example above. Are the spaces correct?

- Enter a name for your CloudFormation Stack. Enter "my-instance".



- Select "Next"

- The next screen provides some more advanced options for your stack. For now, scroll to the bottom of this page and select "Next"

- The next page shows a 'Review' or summary page. Scroll to the bottom of this page and select "Create"

The screenshot shows the AWS CloudFormation Stacks page. At the top, there are navigation links for Services, Resource Groups, and a user profile for Mike in Sydney. Below the header, the 'CloudFormation' service is selected, and the 'Stacks' tab is active. A 'Create Stack' button is available, along with 'Actions' and 'Design template' options. A filter bar allows filtering by 'Active' status or 'By Stack Name'. The main table displays one stack entry:

Stack Name	Created Time	Status	Description
my-instance	2018-02-25 11:08:51 UTC+1000	CREATE_IN_PROGRESS...	

Below the table, an 'Events' section provides detailed logs for the stack creation process:

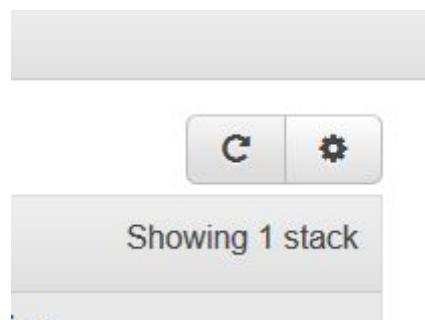
Date	Status	Type	Logical ID	Status Reason
2018-02-25	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	my-instance	User Initiated
	00			

At the bottom of the page, there are links for Feedback, English (US), and legal notices: © 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved., Privacy Policy, and Terms of Use.

- You should now be taken to the CloudFormation stacks page. You can watch your stack being created.

- With your stack selected:

- Click the refresh button (within the page, NOT the main browser refresh button) from time to time, this will update all the information about the stack build.



- Review the "Events" tab, this shows you the steps being taken by the Cloudformation build engine.

Overview	Outputs	Resources	Events	Template	Parameters	Tags	Stack Policy	Change Sets	Rollback Triggers			
Filter by: Status ▾ Search events												
2018-02-25	Status	Type	Logical ID	Status Reason								
▶ 11:09:30 UTC+1000	CREATE_COMPLETE	AWS::CloudFormation::Stack	my-instance									
▶ 11:09:28 UTC+1000	CREATE_COMPLETE	AWS::EC2::Instance	myInstance									
▶ 11:08:55 UTC+1000	CREATE_IN_PROGRESS	AWS::EC2::Instance	myInstance	Resource creation Initiated								
▶ 11:08:54 UTC+1000	CREATE_IN_PROGRESS	AWS::EC2::Instance	myInstance									
▶ 11:08:51 UTC+1000	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	my-instance	User Initiated								

- If there are any errors during the build, they will be shown here.
- Review the "Resources" tab, this shows the resources built in this stack. In this case you should see just one EC2 Instance.

Overview	Outputs	Resources	Events	Template	Parameters	Tags	Stack Policy	Change Sets	Rollback Triggers			
Logical ID	Physical ID	Type	Status	Status	Status	Status						
myInstance	i-0ecd6f05e7e49f4d9	AWS::EC2::Instance	CREATE_COMPLETE	CREATE_COMPLETE	CREATE_COMPLETE	CREATE_COMPLETE						

- When the stack has built, with no errors, you should see the status as "CREATE\_COMPLETE"

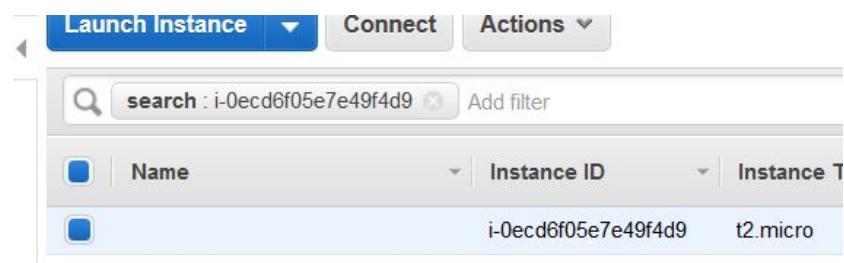
- Not seeing "CREATE\_COMPLETE"? If the build has failed, see if you can see why from the "Events" tab. If you need help please ask :)

- With your stack selected, from the "Resources" tab click the "Physical ID" of the instance that the strack created.

Outputs	Resources	Events	Template
Physical ID			
	i-0ecd6f05e7e49f4d9		

- This will take you to the EC2 Instance list. Note the list of instances is now filtered to just the instance you created (which is your only instance)

- See that the Instance does not have a Name tag. Let's fix that... not in the console, but in the CloudFormation template.



## Update a CloudFormation Stack

- Back in your text editor, with your CloudFormation YAML file loaded, add a Name tag to your instance. Under KeyName, and on the same level as KeyName, add:

```
Tags:  
-  
  Key: Name  
  Value: my-ec2-instance
```

- Again make sure the spacing is correct, your template should now look something like this:

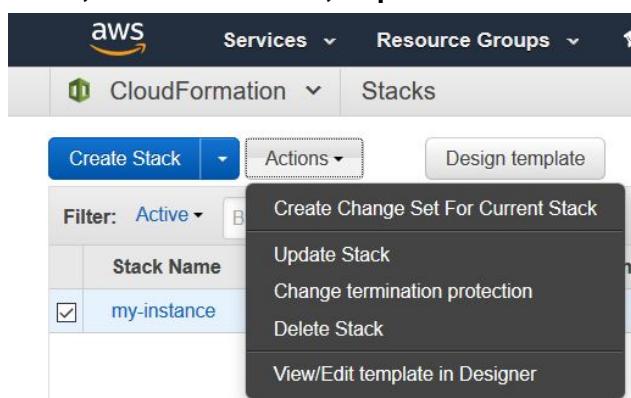
```
AWSTemplateFormatVersion: 2010-09-09  
Resources:  
  myInstance:  
    Type: "AWS::EC2::Instance"  
    Properties:  
      ImageId: ami-82a458e0  
      InstanceType: t2.micro  
      KeyName: mykey  
    Tags:  
    -  
      Key: Name  
      Value: my-ec2-instance
```

- Save your updated template.

- Now, let's update the stack so the changes take effect.

- Navigate to CloudFormation

- With your stack selected, select "Actions", "Update Stack"



- From the next screen, select "Upload a template to Amazon S3" and click "Browse" and select your updated CloudFormation template.

Choose a template A template is a JSON/YAML-formatted text file that describes your stack's resources.

Use current template

Upload a template to Amazon S3

test.yaml

Specify an Amazon S3 template URL

- Select "Next"

- If you are shown a validation error at this point, check that your YAML file looks like the example above. Are the spaces correct?

- There should be nothing to change on the next screen, select "Next"

Update my-instance stack

Select Template       Specify Details

Specify parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. [Learn more.](#)

Options      Review

Stack name

- The next screen provides some more advanced options for your stack. For now, scroll to the bottom of this page and select "Next"

- The next page shows a 'Review' or summary page.

- Notice the "Preview your changes" section, this gives you a very high level summary of what will change in the stack.

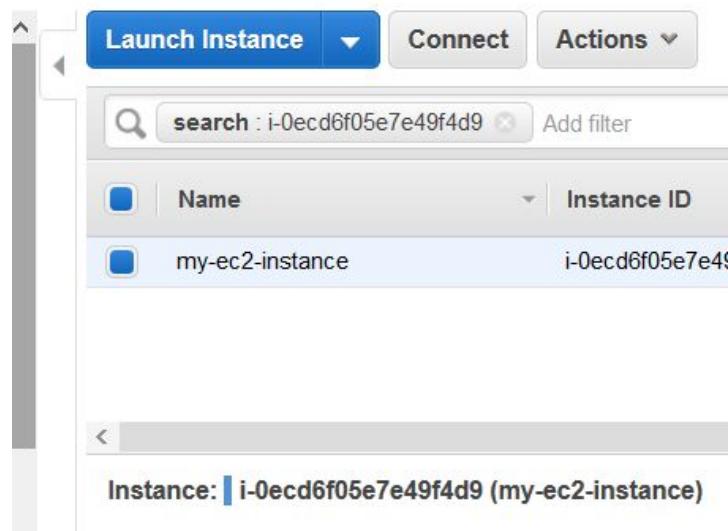
#### Preview your changes

Based on your input, CloudFormation will change the following resources. For more information, choose [View change set details](#).

Action	Logical ID	Physical ID	Resource type	Replacement
Modify	myInstance	i-0ecd6f05e7e49f4d9	AWS::EC2::Instance	False

- Notice that while the EC2 Instance will be updated, it will not get replaced, so the instance will remain running.

- Select "Update"
- As before watch CloudFormation do its work, refresh, and review the "Events" tab.
- When the stack status shows as "UPDATE\_COMPLETE", follow the link from the "Resources" tab to the instance view.
- Notice that the instance is now Named.



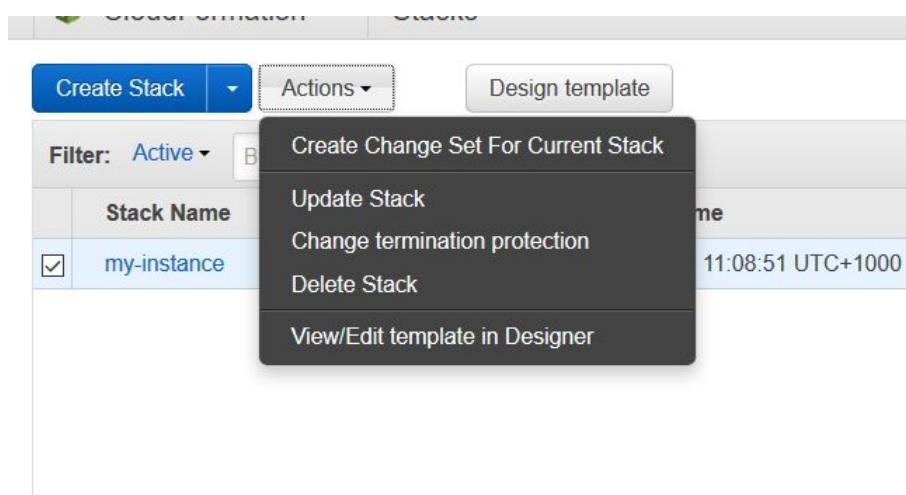
- If you have time you can connect to the server via RDP if you wish. When you're finished...
- We don't need this server anymore, let's clean up.

## Delete a CloudFormation Stack

- Cleaning up the CloudFormation stack is super easy, and super clean. The instance and all related configurations (but not the Key Pair as this wasn't created in the stack) are gone in one action:

- Navigate to CloudFormation

- With your stack selected, select "Actions", "Delete Stack"



- Review the warning and, if you are ready select "Yes, Delete"

- Monitor as the stack is deleted.

- Want to build the server again, name tag and all? Just build a new stack with your saved template!

## Extra Challenge

While we wait for everyone to complete this session....

- Can you make a change to the CloudFormation template to create 2 servers?
- Are the servers created one after each other, or do they build at the same time?

**END**

# Session 3 - Virtual Private Cloud

In this session we will get introduced to AWS VPC.

Take the following steps, one at a time. There is plenty of time to complete the session and ask any questions along the way.

## Steps

- Log into the AWS console
- Set the region to Sydney (stay in this region today, check from time to time)
- The nice thing about CloudFormation templates is that they can be easily shared around. In the resource file for this session you should find 'vpc-network.yaml'
- Take a look at the file, we've added comments along the way to explain how it works. Notice that this template uses 'Parameters' to pass values in to the stack as it builds.

This template creates a VPC with four subnets. Two of these subnets are 'Public' in that they have access to and from the Internet. Two of the subnets are 'Private' in that they have no access to the Internet.

- Navigate to CloudFormation
- Select "Create Stack"
- From the next screen, select "Upload a template to Amazon S3" and click "Browse" and select the CloudFormation template 'vpc-network.yaml'.

Choose a template A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. [Learn more](#).

Select a sample template  Upload a template to Amazon S3  Specify an Amazon S3 template URL

No file selected.

- Select "Next"
- This time as well as a stack name, you have the opportunity to alter some of the values that the stack will use.

## Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. [Learn more.](#)

Stack name

**Parameters**

subnetPrivateCidr1	10.0.4.0/24	Enter a valid CIDR for the first private subnet
subnetPrivateCidr2	10.0.5.0/24	Enter a valid CIDR for the second public subnet
subnetPublicCidr1	10.0.0.0/24	Enter a valid CIDR for the first public subnet
subnetPublicCidr2	10.0.1.0/24	Enter a valid CIDR for the second public subnet
vpcCidr	10.0.0.0/16	Enter a valid CIDR for the VPC

- Enter a 'Stack name' and leave the other Parameters as default. Select 'Next'.
- Scroll to the bottom of the next page and select 'Next' and then select 'Create'.

Create Stack Actions Design template

Filter: Active ▾ By Stack Name Showing 1 stack

Stack Name	Created Time	Status	Description
<input checked="" type="checkbox"/> my-network	2018-03-21 14:37:34 UTC+1000	CREATE_IN_PROGRESS...	This template creates an ...

- As before watch CloudFormation do its work, refresh, and review the "Events" tab.
- Navigate to VPC
- Take a look at the VPC you created.

Search VPCs and their properties

<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR
<input type="checkbox"/>	demo-vpc	vpc-c1f244a6	available	10.0.0.0/16
<input type="checkbox"/>		vpc-17754273	available	172.31.0.0/16

- Notice that this is not the only VPC in your account. You should also see an (unnamed) 'default' VPC.
- We have now created a VPC with four subnets, two are public (in that it can route to and from the Internet) and two subnets are private.

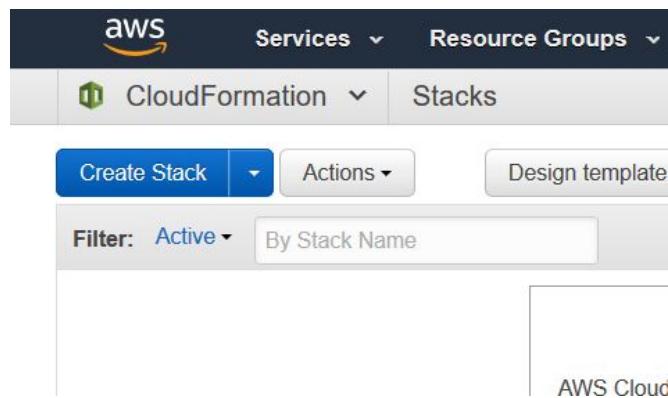
## Testing the Virtual Private Cloud (VPC)

- Now let's create a couple of EC2 Instances to test with.

- First we will create an EC2 instance in a public subnet.

- Navigate to CloudFormation

- Select "Create Stack"



- Select "Upload a template to Amazon S3" and "Browse"...

- In the resources provided for this workshop, in the folder "Session 3" select the template: "ec2-instance-for-subnet.yaml"

**Choose a template** A template is a JSON/YAML-formatted text file that describes your stack's resources.

Select a sample template  Upload a template to Amazon S3  Specify an Amazon S3 template URL

**Upload a template to Amazon S3**

ec2-instance-for-subnet.yaml

- Select "Next"

- This template has been created to prompt you for parameters before the stack is built.

- Enter a name for the stack "my-public-instance-stack" (this is not the name that will be given to the instance)
- The Key parameter is now a dropdown box. Select a key that you have on your machine.
- Enter a server name "my-demo-server-public"
- In the subnet dropdown menu you will have a few options. Select the subnet that has "(subnet-public-1)"
- Before moving on, make a note of the subnet ID and its corresponding name. We will need this information later. (e.g. subnet-public-1 : subnet-beb4bd9de9893478983)

### Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. [Learn more](#).

Stack name

### Parameters

key  Enter a valid EC2 Key

serverName  Enter the name for the server. (This is not a hostname)

subnet  Select a subnet for this instance.

[Cancel](#) [Previous](#) [Next](#)

- Select "Next"
- Leave all the settings on the next screen.
- Scroll to the bottom and select "Next"
- Scroll to the bottom of the Review page and select "Create"
- We won't wait for this stack to create, let's create another EC2 Instance in the private subnet.
- Select "Create Stack" and follow the same process, but this time:
- Enter a name for the stack "my-private-instance-stack"

- Enter a server name "my-demo-server-private"

- Select the subnet with "(subnet-private-1)"

### Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. [Learn more](#).

Stack name

### Parameters

key  Enter a valid EC2 Key

serverName  Enter the name for the server. (This is not a hostname)

subnet  Select a subnet for this instance.

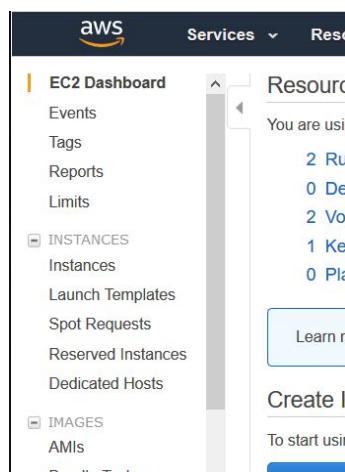
[Cancel](#) [Previous](#) [Next](#)

- Select “Next”, “Next”, then “Create”

- By now, our public EC2 Instance may have built. Let's connect into the server.

- Navigate to EC2

- Select "Instances" on the left hand side.



- By now, you should see two running EC2 instances, if you need to expand the Name column.

The screenshot shows the AWS EC2 Dashboard. On the left sidebar, under 'INSTANCES', 'Instances' is selected. The main area displays a table of instances:

Name	Instance ID	Instance Type	Availability Zone	Instance State
my-demo-server-public	i-0b0329ab389cde695	t2.micro	ap-southeast-2a	running
my-demo-server-private	i-0d4be6f2bf914a872	t2.micro	ap-southeast-2a	running
my-ec2-instance	i-0ecd6f05e7e49f4d9	t2.micro	ap-southeast-2a	terminated

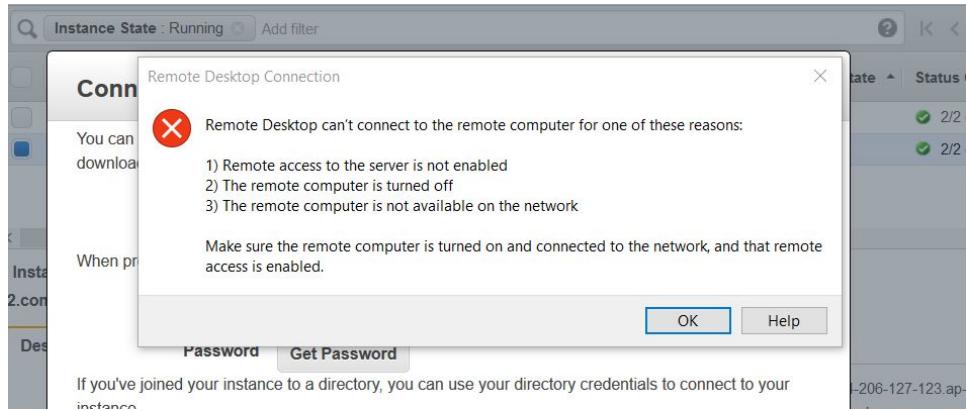
- Connect with RDP into the public server:

- Select the public instance, "Actions" and "Get Windows Password"
- Password not available yet? Hold on a minute, and try again.



- Try to connect to the public instance via your RDP client...

- Its not working!!



- In our VPC we have **Security Groups** that control the traffic that can reach our Instances.

- Both of our instances are in the 'default' security group.

- Let's create a rule in the default security group to allow access to our Instances via RDP.

- From the EC2 list select either of the instances, look at the details section in the lower half of the screen.

- In the "Description" tab, find the "Security groups" and click on "default"

Instance ID	i-0c3729f391f788b4e
Instance state	running
Instance type	t2.micro
Elastic IPs	
Availability zone	ap-southeast-2a
Security groups	default, view inbound rules
Scheduled events	No scheduled events
AMI ID	Windows_Server-2016-English-Full-Base-2018.01.12 (ami-82a458e0)
Platform	windows
IAM role	-
Key pair name	my-key-pair

- On the following screen in the lower half, you will see the details of the security group.
- Select the "Inbound" tab.

The screenshot shows the AWS Security Groups console. At the top, there are tabs for 'Create Security Group' and 'Actions'. Below that is a search bar with 'Group ID: sg-7764b30e' and a 'Add filter' button. The main table has columns for Name, Group ID, Group Name, VPC ID, and Description. One row is selected with values: Name 'sg-7764b30e', Group Name 'default', VPC ID 'vpc-7b5d871c', and Description 'default VPC security group'. Below the table, it says 'Security Group: sg-7764b30e'. At the bottom, there are tabs for 'Description', 'Inbound' (which is highlighted in orange), 'Outbound', and 'Tags'. An 'Edit' button is visible above the rule table.

Name	Group ID	Group Name	VPC ID	Description
sg-7764b30e		default	vpc-7b5d871c	default VPC security group

**Inbound Rules:**

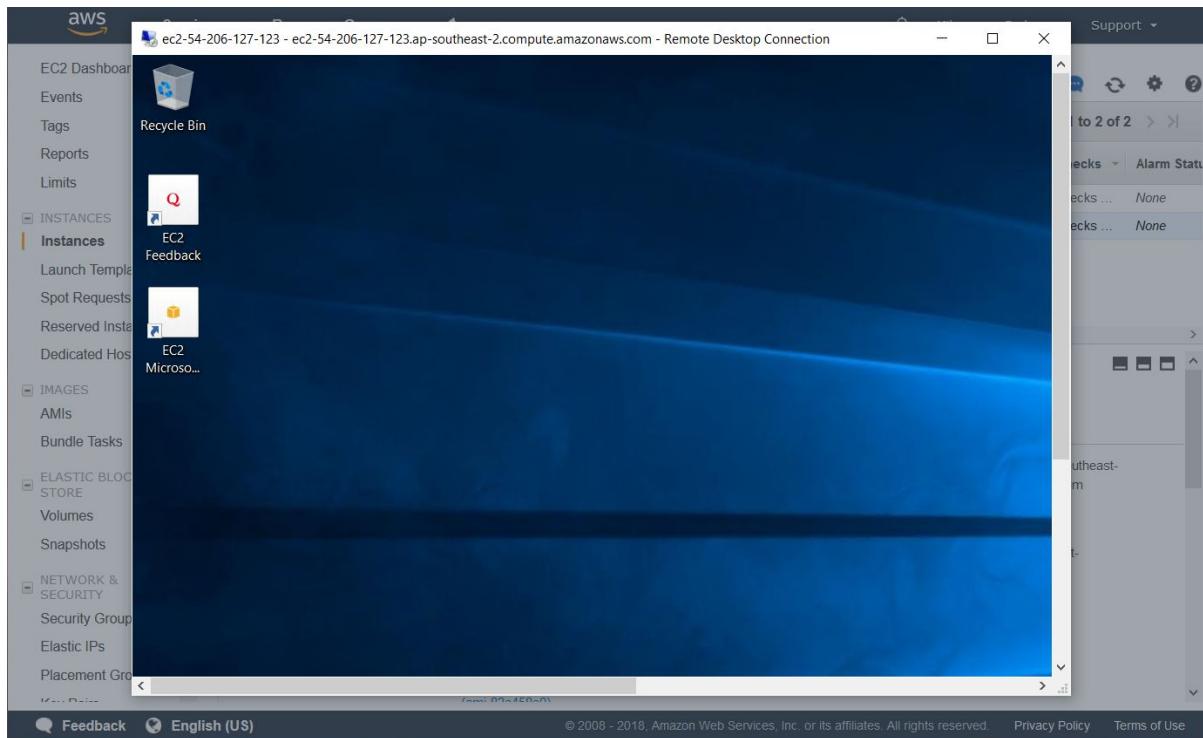
Type	Protocol	Port Range	Source	Description
All traffic	All	All	sg-7764b30e (default)	

- Notice that currently, "All traffic" is allowed inbound to our instances, but the source is this (the same) security group.
- This means that the instances can RDP to each other, but we can't RDP from outside the network.
- Select "Edit", then "Add Rule"

The screenshot shows the 'Edit inbound rules' dialog box. It has fields for Type (set to All traffic), Protocol (All), Port Range (0 - 65535), Source (Custom, sg-7764b30e), and Description (e.g. SSH for Admin Desktop). Below this, another row is being edited with Type (RDP), Protocol (TCP), Port Range (3389), Source (My IP, [REDACTED]/32), and Description (e.g. SSH for Admin Desktop). There is an 'Add Rule' button at the bottom left and 'Cancel' and 'Save' buttons at the bottom right. A note at the bottom states: 'NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.'

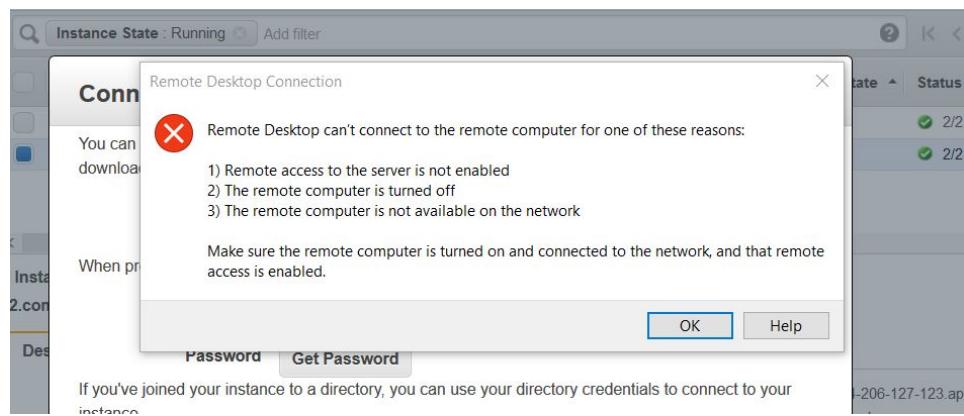
- On the new rule, for Type select "RDP", and for Source select "My IP"
- By selecting "My IP" we restrict RDP access from the outside world to only machines using your Internet connection.

- Now, try again to RDP to your public instance.



- Yay, it works.

- OK, minimise the RDP session to the public instance. Let's see if we can RDP to the private instance:



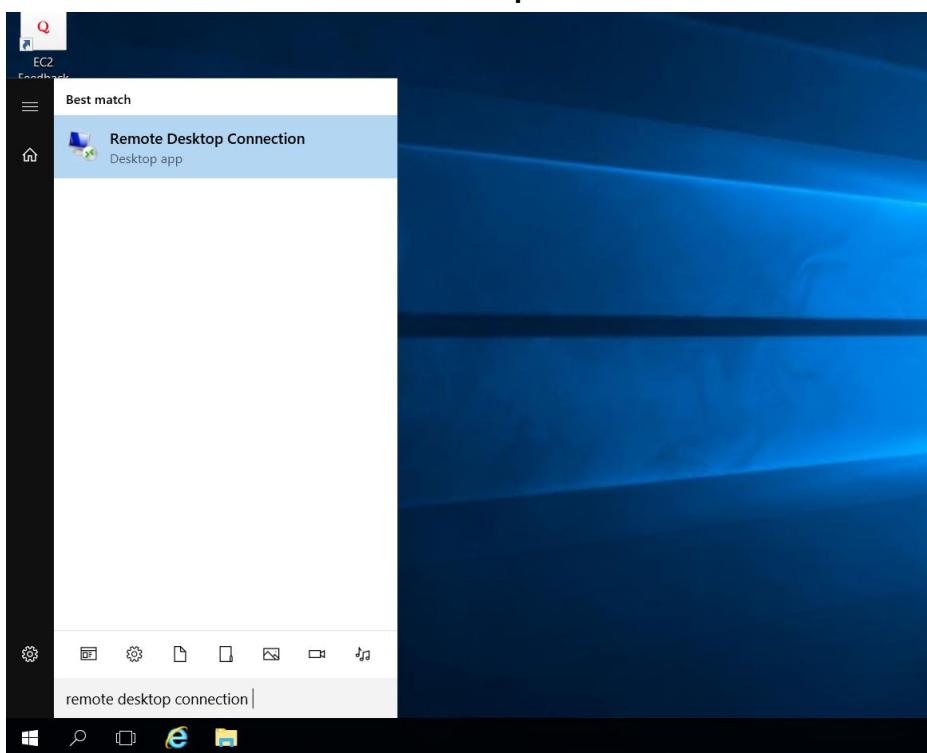
- Of course, it doesn't work. That's because, even though the instance has been allocated a public IP address, its not 'visible' to the Internet through the VPC.

- But we can still get there:

- From the EC2 Instance list, select the private server, and in the details in the bottom half of the screen find "Private IPs".

Public DNS (IPv4)	ec2-13-211-29-84.ap-southeast-2.compute.amazonaws.com
IPv4 Public IP	13.211.29.84
IPv6 IPs	-
Private DNS	ip-10-0-1-7.ap-southeast-2.compute.internal
Private IPs	10.0.1.7
Secondary private IPs	
VPC ID	vpc-7b5d871c
Subnet ID	subnet-942949f3

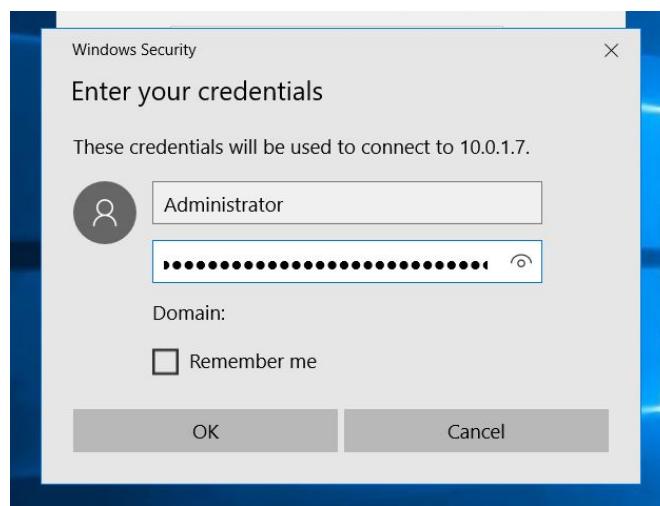
- Make a note of this address.
- Also take a moment to discover the password for this server.
- Go back to the RDP session with your 'public' instance.
- From the 'Start' menu select "Remote Desktop Connection"



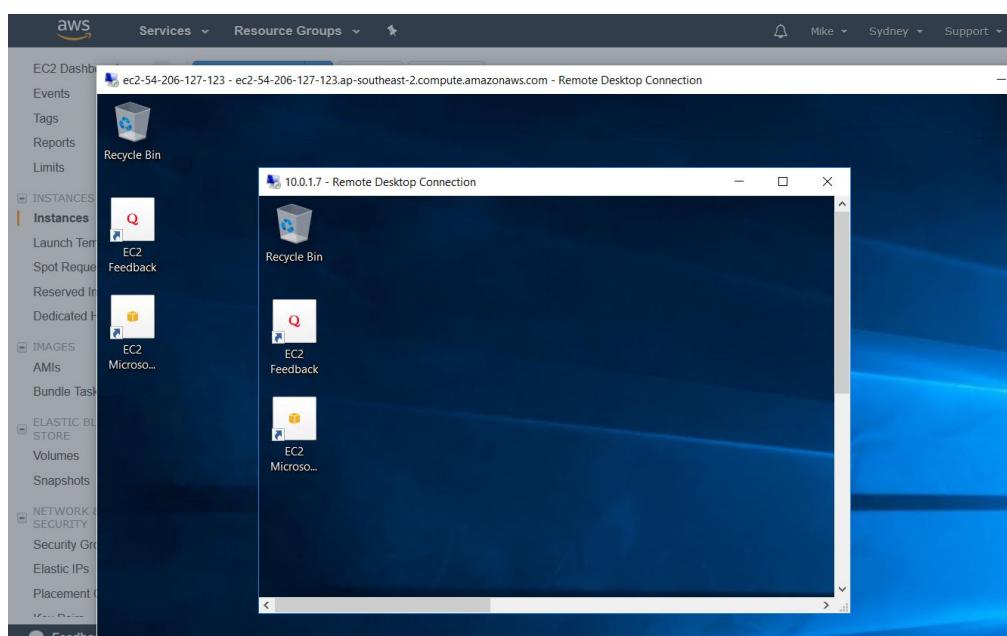
- Enter in to the "Computer" field the Private IP address of the private server that you noted down just before.



- Select "Connect"



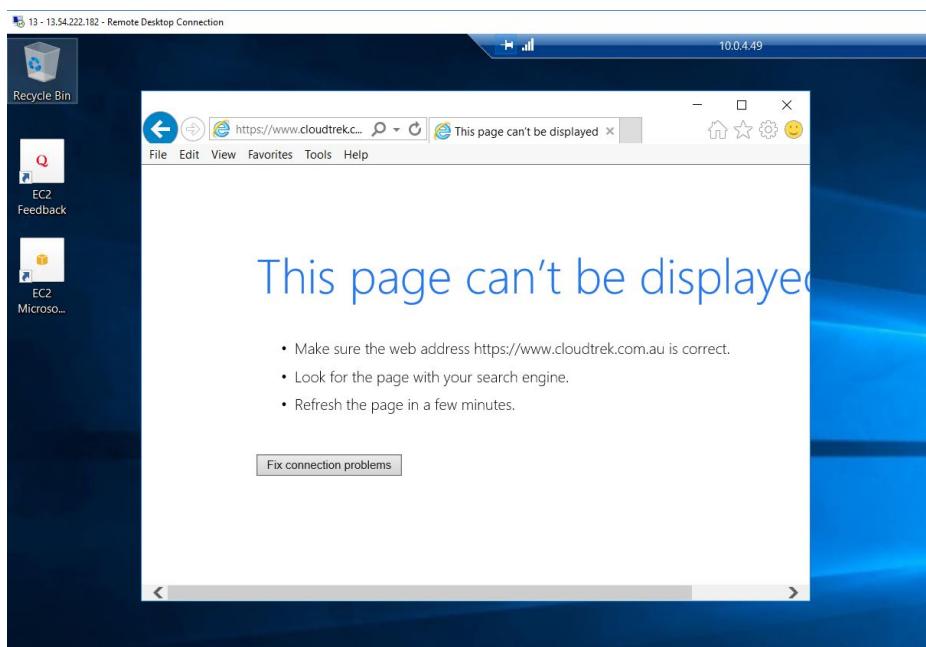
- In the credentials box, enter the User name "Administrator" and the password for the private server.



- Yay, it works.
- You have created a private server, in a private network, that is accessible via what we call a bastion host.

Before we finish...

- Let's look at Internet FROM connectivity for our EC2 Instances. It's often the case that servers need to connect to the Internet to download patches etc.
- From the RDP session with the public server, open up Internet Explorer and navigate to <http://wikipedia.com> (or any website).
- As this is a default 'super paranoid' server configuration, there will be a slew of warning messages, but you should end up looking at a webpage.
- If you do the same from the Private server... It does not work!



- Let's fix this. Let's allow our private server to have access to reach out to the Internet, keeping it in its private subnet so that nobody can connect to it from the outside world directly.
- Leave your RDP sessions open....
- Navigate to VPC in the AWS console.

The screenshot shows the AWS VPC Dashboard. On the left, there's a sidebar with options like 'Virtual Private Cloud', 'Your VPCs', and 'Subnets'. The main area is titled 'Resources' with a 'Start VPC Wizard' and 'Launch EC2 Instances' button. It displays a note about launching instances in the Asia Pacific (Sydney) region and lists VPC resources: 1 VPC, 1 Internet Gateway, 0 Egress-only Internet Gateways, and 3 Subnets.

- From the menu on the left select 'NAT Gateways' then 'Create NAT Gateway'.

The screenshot shows the 'Create NAT Gateway' page. At the top, there's a 'Services' and 'Resource Groups' navigation bar. Below it, there's a search bar and an 'Actions' dropdown menu. The main area has a large blue 'Create NAT Gateway' button.

- For 'Subnet' choose the subnet ID that correspond to 'subnet-public-1' in demo-vpc. You should have this information noted down from earlier. If not, you will have to go to VPC -> Subnet and copy down the subnet-public-1 subnet ID.

The screenshot shows the 'Create NAT Gateway' page with a 'Subnet' dropdown. The dropdown contains a search bar and a list of subnets. One subnet, 'subnet-0c9eef27de3668699', is highlighted in orange. The list includes:

Subnet ID	VPC
subnet-3951675e	vpc-23baf644
subnet-0d55f455	vpc-23baf644
subnet-0c9eef27de3668699	vpc-0aae0d75e9e5ab1a8   demo-vpc
subnet-6b95b522	vpc-23baf644
subnet-01d40461452049b9d	vpc-0aae0d75e9e5ab1a8   demo-vpc
subnet-058a0686a179f1902	vpc-0aae0d75e9e5ab1a8   demo-vpc
subnet-07a4f1b5a17a39fa2	vpc-0aae0d75e9e5ab1a8   demo-vpc

- For 'Elastic IP Allocation ID' click on Create New EIP to fill in the box.

## Create NAT Gateway

Create a NAT gateway and assign it an Elastic IP address. [Learn more.](#)

Subnet*	subnet-f1512796		
Elastic IP Allocation ID*	eipalloc-351b180f		
<a href="#">Create New EIP</a>			
<small>* Required</small>			
<a href="#">Cancel</a> <a href="#">Create a NAT Gateway</a>			

### - Select ‘Create a NAT Gateway’

NAT Gateways > Create NAT Gateway

Create NAT Gateway

Your NAT gateway has been created.

Note: In order to use your NAT gateway, ensure that you [edit your route tables](#) to include a route with the following NAT gateway. [Find out more.](#)

NAT Gateway ID nat-0daed058153071711

[Edit route tables](#) [Close](#)

### - Select ‘Edit route tables’

### - Look for the entry in this table for a ‘Main’ table for the ‘demo-vpc’

Search Route Tables and their X

« « 1 to 3 of 3 Route Tables » »

Name	Route Table ID	Explicitly Associated With	Main	VPC
public-route-table	rtb-28f4de4f	2 Subnets	No	vpc-c1f244a6   demo-vpc
	rtb-a8e432cf	0 Subnets	Yes	vpc-17754273
<input checked="" type="checkbox"/>	rtb-55f1db32	0 Subnets	Yes	vpc-c1f244a6   demo-vpc

rtb-55f1db32

Summary Routes Subnet Associations Route Propagation Tags

Route Table ID: rtb-55f1db32  
Explicitly Associated With: 0 Subnets

Main: yes  
VPC: vpc-c1f244a6 | demo-vpc

### - Select the ‘Routes’ tab, then ‘Edit’, then ‘Add another route’

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
0.0.0.0/0		No		×

**Add another route**

igw-32b8d156 | demo-igw  
nat-0daed058153071711

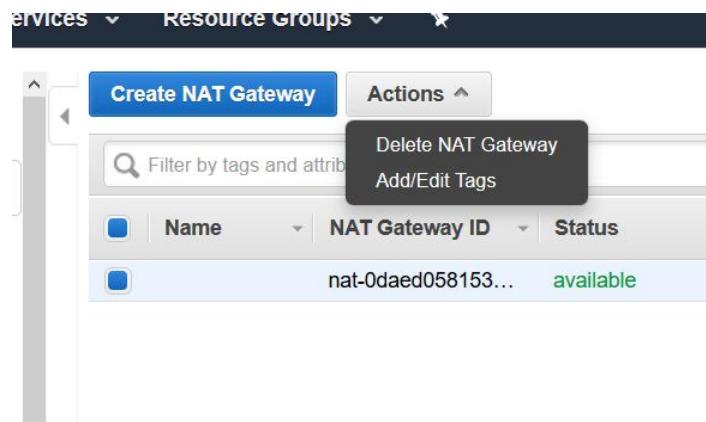
- In 'Destination' enter '0.0.0.0/0' and under 'Target' start to type 'nat..' and select the ID of the NAT gateway.
- Select 'Save'
- Go back to the RDP session on your Private server (inside the session to your public server. Try the web page again... it works!
- Note, you still can't RDP directly to the Private server.
- Once you're done experimenting with this environment it's time to clean up.

# Deleting your Resources

- Navigate to VPC

- Select 'Nat Gateways' from the left hand menu. If the gateway list is empty, you may have to click the 'refresh' button.

- With the Gateway selected, use the action menu and select 'Delete NAT Gateway' and then confirm again 'Delete NAT Gateway'.



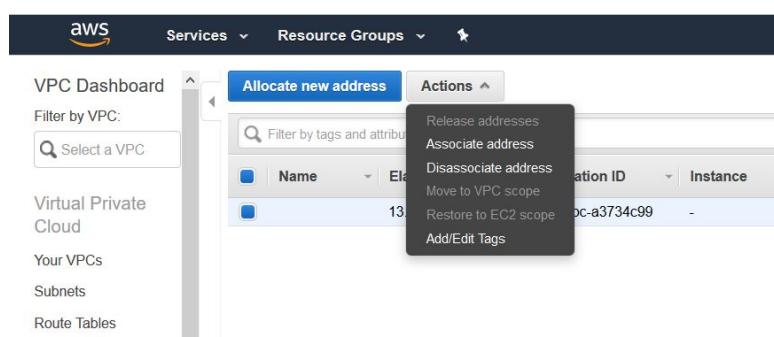
- Navigate back to CloudFormation

- Delete the Server stacks by selecting the stack, and selecting "Actions", "Delete Stack", then "Yes, Delete"

- Wait for these stacks to fully delete before doing the same to the network stack.

- One last thing, select "Elastic IPs" from the menu on the left.

- Select the Elastic IP entry, and select "Actions", "Release addresses", then "Release"



## Extra Challenge

While we wait for everyone to complete this session....

- At the end of this session the Private server had access to the Internet.
- What are some of the reasons that this server needed access to the Internet?
  - Hint 'AWS'
- Are there other methods for this server to get access to the Internet? Ways that are more controlled?

**END**

# Session 4 - Bootstrapping

In this session we will get introduced to the concept of “Bootstrapping”.

Take the following steps, one at a time. There is plenty of time to complete the session and ask any questions along the way.

## Steps

- In this session we are going to get a Windows server to do a “real job”. But we're not going to configure it by hand.
- Log into the AWS console
- Set the region to Sydney (stay in this region today, check from time to time)
- Navigate to EC2
- First let's use the AWS console to build a web server:

## Bootstrap an Instance with the Console

- Select "Launch Instance"
- Select "Microsoft Windows Server 2016 Base"
- This time, as we will be getting the server to do some work, and we don't want to wait too long, let's select a bigger instance type:
- Select "t2.large"

Currently selected: t2.large (Variable ECUs, 2 vCPUs, 2.3 GHz, Intel Broadwell E5-2686v4, 8 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

- Select "Next: Configure Instance Details"

- Take a look at the different settings options here.
- We will leave all the default values, but we will scroll down and expand the "Advanced Details":
- Here we see the "User data" entry.

▼ Advanced Details

User data <span style="font-size: small;">(i)</span>	<input checked="" type="radio"/> As text <input type="radio"/> As file <input type="checkbox"/> Input is already base64 encoded
<small>(Optional)</small> <div style="border: 1px solid #ccc; height: 100px; width: 100%;"></div>	

- Text we add to "User data" will be passed to the Instance as it boots, and if its script, will be executed by an Administrator user automatically.
- In the resources for this session you will find user-data.txt
- Open up this file in a text editor and take a look. You will see that its some Powershell script that copies an ASPX web page, enables the IIS Web Role, and starts a website.
- Copy the text (completely) and paste it into the "User data" section of the EC2 console.

▼ Advanced Details

User data <span style="font-size: small;">(i)</span>	<input checked="" type="radio"/> As text <input type="radio"/> As file <input type="checkbox"/> Input is already base64 encoded
<pre>new-site -name test -port 80 -physicalpath c:\inetpub\test ApplicationPool ".NET v4.5" -force remove-website -name "Default Web Site" start-website -name test &lt;/powershell&gt;</pre>	

- Select "Next: Add Storage"

- We won't make any changes here, but see how we could change the size and number of disks that the server has.

Volume Type <span style="font-size: small;">(i)</span>	Device <span style="font-size: small;">(i)</span>	Snapshot <span style="font-size: small;">(i)</span>	Size (GiB) <span style="font-size: small;">(i)</span>	Volume Type <span style="font-size: small;">(i)</span>	IOPS <span style="font-size: small;">(i)</span>	Throughput (MB/s) <span style="font-size: small;">(i)</span>	Delete on Termination <span style="font-size: small;">(i)</span>	Encrypted <span style="font-size: small;">(i)</span>
Root	/dev/sda1	snap-049c714bc2eed31ff	30	General Purpose SSD (GP2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted
<a href="#">Add New Volume</a>								

- Select "Next: Add Tags"
- We want the server configuration to be named

- Select "Add Tag"

- Enter "Name" for the key (note ensure the N is capital)
- Enter "my-web-server" for the value.

#### Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

The screenshot shows a form for adding a tag. It has two input fields: 'Key' (127 characters maximum) and 'Value' (255 characters maximum). Below these is a table with one row. The 'Name' column contains 'my-web-server' and the 'Value' column also contains 'my-web-server'. There is a checked checkbox next to the value. At the bottom left is a button labeled 'Add another tag'.

Key	(127 characters maximum)	Value	(255 characters maximum)
Name	my-web-server		<input checked="" type="checkbox"/>

Add another tag (Up to 50 tags maximum)

- Select "Next: Configure Security Group"

- Let's change the name of the Security Group so we can find it in the future, change the name to "web-server-group"
- Using descriptions is always a good idea in AWS, add a description so that when you look at this in the future you understand what it is

- Now we are going to allow connection on port 80 (HTTP) from the outside world

- Select "Add Rule"

- In the Type dropdown select "HTTP"

- In the "Source" dropdown select "Anywhere"

#### Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

The screenshot shows the 'Configure Security Group' interface. It starts with a radio button for 'Assign a security group':  Create a new security group and  Select an existing security group. Below this is a table for defining a new rule. The 'Security group name' is 'web-server-group' and the 'Description' is 'Mike told me to write a description in here...'. The table has columns for Type, Protocol, Port Range, Source, and Description. There are two rows of rules. The first row is for SSH (Custom TCP) on port 3389 to 0.0.0.0/0 with a description 'e.g. SSH for Admin Desktop'. The second row is for HTTP (TCP) on port 80 to 0.0.0.0/0 with a description 'e.g. SSH for Admin Desktop'. Both rows have an 'x' icon to delete them. At the bottom is a 'Save Rule' button.

Type <small>i</small>	Protocol <small>i</small>	Port Range <small>i</small>	Source <small>i</small>	Description <small>i</small>
Custom TCP	TCP	3389	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

Add Rule

- Select: "Review and Launch"

- Review the details of the instance, and if all looks ok select "Launch"

### Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

**⚠ Improve your instances' security. Your security group, web-server-group, is open to the world.**  
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

**⚠ Your instance configuration is not eligible for the free usage tier**  
To launch an instance that's eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. Learn more about [free usage tier](#) eligibility and usage restrictions.

[Don't show me this again](#) [Edit AMI](#)

**AMI Details**

	Microsoft Windows Server 2016 Base - ami-48d6122a
Free tier eligible	Microsoft Windows 2016 Datacenter edition. [English]
	Root Device Type: ebs Virtualization type: hvm

If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the [License Mobility Form](#). Don't show me this again

**Instance Type**

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance

[Edit instance type](#) [Cancel](#) [Previous](#) **Launch**

- Select the Key Pair that you created earlier today

- You will need to acknowledge that DO have the Key Pair

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair

Select a key pair

my-key-pair

I acknowledge that I have access to the selected private key file (my-key-pair.pem), and that without this file, I won't be able to log into my instance.

[Cancel](#) **Launch Instances**

- Select: "Launch Instances"

- Scroll to the bottom of the screen and select "View Instances"

## Bootstrap an Instance with CloudFormation

- Wow that was a lot of steps to create a server, there must be a better way?
- Well there are a few, but let's do the same thing again with CloudFormation.
- This time we have created the template for you, let's review it, you will find it in this sessions resources called "web-server-instance.yaml"

```
AWSTemplateFormatVersion: 2010-09-09
```

Description: This template creates an EC2 web server instance and allows you to select the subnet it will use. To keep it simple it only works in Sydney (ap-southeast-2).

Parameters:

serverName:

Type: String

Default: my-demo-server

Description: Enter the name for the server. (This is not a hostname)

subnet:

Type: AWS::EC2::Subnet::Id

Description: Select a subnet for this instance.

key:

Type: AWS::EC2::KeyPair::KeyName

Description: Enter a valid EC2 Key

Resources:

instance:

Type: "AWS::EC2::Instance"

Properties:

ImageId: ami-82a458e0

InstanceType: t2.large

KeyName: !Ref key

NetworkInterfaces:

- DeviceIndex: 0

SubnetId: !Ref subnet

AssociatePublicIpAddress: true

```
UserData:  
Fn::Base64: !Sub |  
    <powershell>  
        mkdir c:\inetpub\test  
        curl https://s3-ap-southeast-2.amazonaws.com/test-aspx/default.aspx  
        -OutFile C:\inetpub\test\default.aspx  
        add-windowsfeature web-webserver -includeallsubfeature -logpath  
        $env:temp\webserver_addrole.log  
        new-website -name test -port 80 -physicalpath c:\inetpub\test  
        -ApplicationPool ".NET v4.5" -force  
        remove-website -name "Default Web Site"  
        start-website -name test  
    </powershell>  
Tags:  
-  
    Key: Name  
    Value: !Ref serverName
```

- In the template you will see a "Description", "Parameters", and "Resources" sections.
- Parameters are the inputs you're prompted for when you launch the template.
- Resources are the service instances that will be created in the stack.
- Notice that the EC2 Instance has UserData in the template, the same user data that you pasted into the console earlier.
- Go ahead and create a stack from this template. If you need a hand follow these steps:
  - Navigate to CloudFormation
  - Select "Create Stack"
  - Select "Upload a template to Amazon S3"
  - Select "Browse..." and select the template file from your computer
  - Select "Next"

## Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. [Learn more](#).

Stack name

## Parameters

key  Enter a valid EC2 Key

serverName  Enter the name for the server. (This is not a hostname)

subnet  Select a subnet for this instance.

[Cancel](#) [Previous](#) [Next](#)

- Enter "my-web-server-stack" for the "Stack name"
- Select your "Key Pair" for the "key"
- Enter a "serverName", let's call this one "my-cfn-web-server"
- For "subnet" choose any subnet in the "172." range.
- Select "Next"
- Scroll down and select "Next"
- Select "Create"
- Now lets navigate back to EC2 and see how our other build is going
- By now we should see 2 EC2 Instances building.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks
my-cfn-web-server	i-0b778c2ac0f7faf4f	t2.large	ap-southeast-2c	running	Initializing
my-web-server	i-0bef1c39711796603	t2.large	ap-southeast-2a	running	2/2 checks ...

- It can take a few mins for the servers to build. This is mainly them enabling the Web Role and setting up the website.

- While the CloudFormation template was excellent, it didn't enable port 80 for the Security Group. Let's fix this:

- Navigate to VPC

- Select 'Security Group' from the menu on the left hand side.

- Locate and select the security group with the description 'default VPC security group'.

- Select the 'Inbound Rules' tab, and select 'Edit'



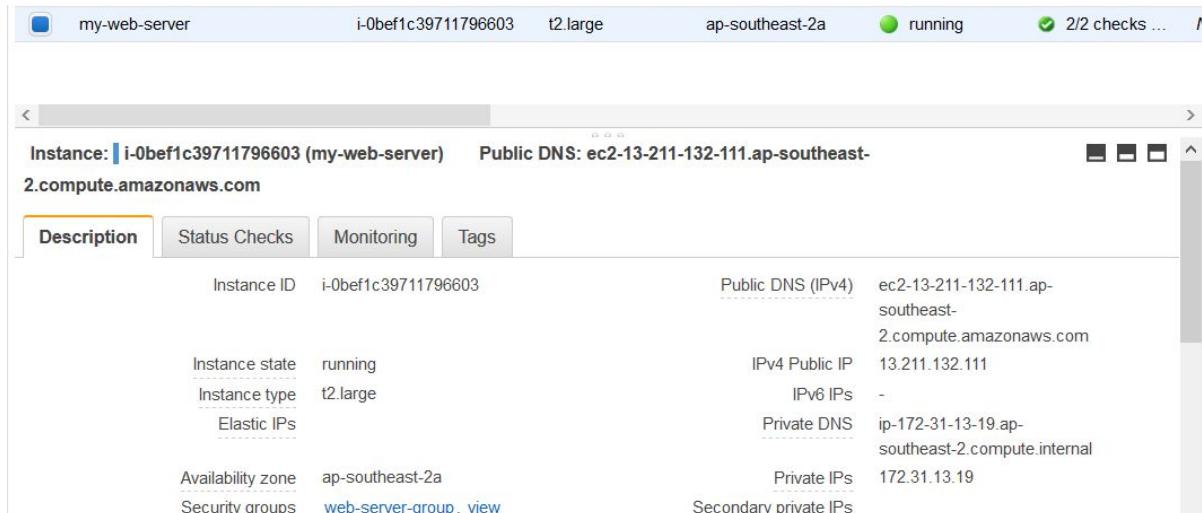
- In the new entry, select 'HTTP' for 'Type', and add '0.0.0.0/0' to the 'Source'

- Select 'Save'

- Ok, let's take a look at our handy work!

- Select the first server we created "my-web-server"

- In the details towards the bottom of the page find and copy the "Public DNS" value for the server.



- Enter this value into a new tab of your web browser.

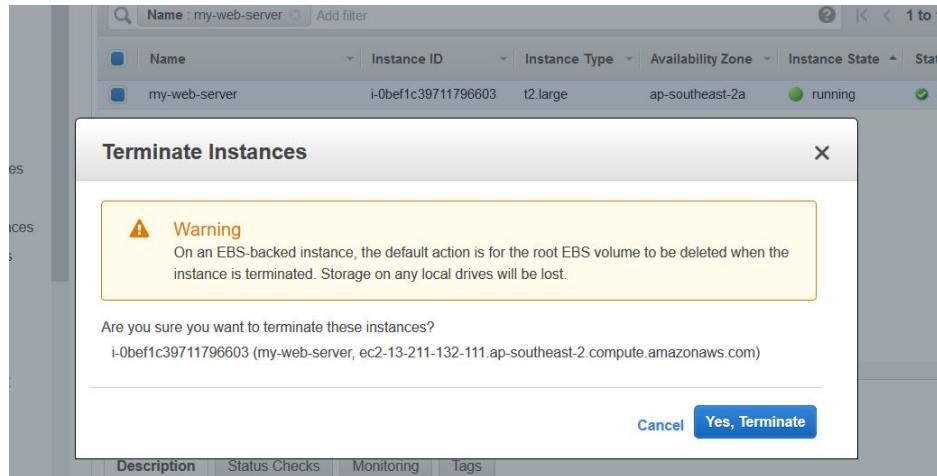
- Do you see a webpage?

- No need to RDP into the server, the job is done.
- In a few minutes, do the same with your Cloudformation server.
- You should see a webpage there too.
- Discuss: How could we get this build to be even faster?

## Cleanup the Resources

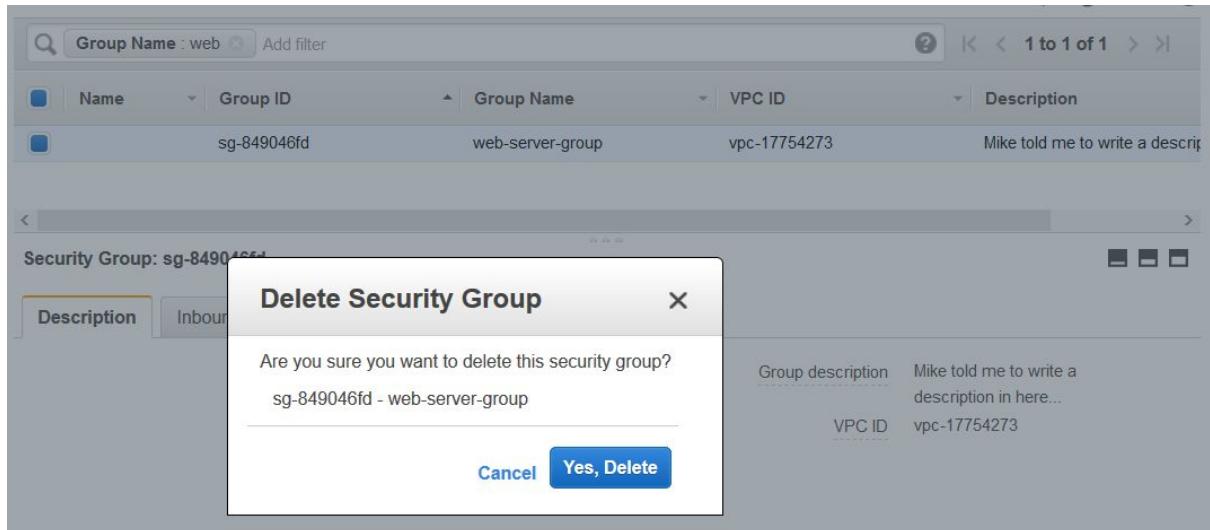
- We don't need these servers anymore. Let's clean up:

- Navigate to EC2
- Select the instance called "my-web-server"
- Select "Actions", "Instance State", "Terminate" and "Yes, Terminate"



- From the menu on the left hand side, select "Security Groups"

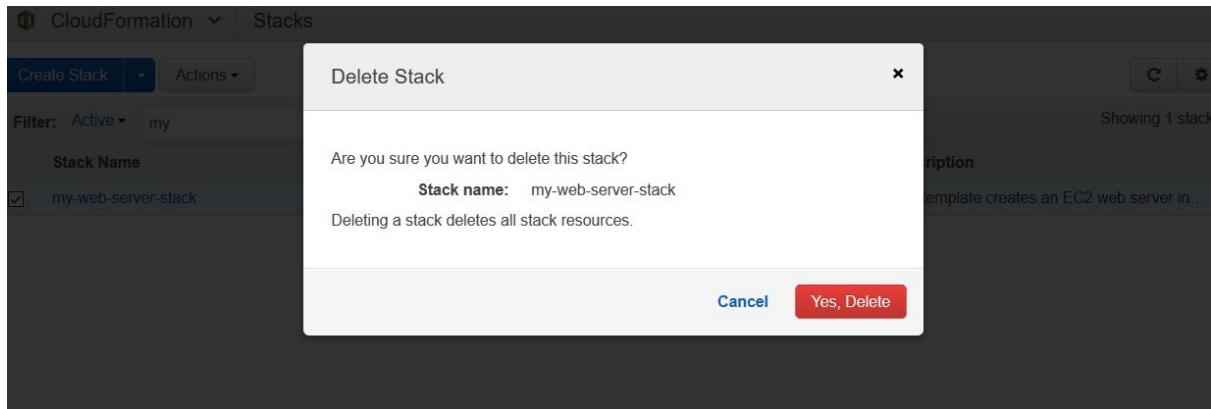
- Look for a Security Group with the GROUP NAME (note this is not the "Name" column) of "web-server-group", select "Actions", "Delete Security Group", and "Yes, Delete".



- Cleaning up the CloudFormation server/stack is much easier

- Navigate to CloudFormation

- Select your web server stack, then "Actions", "Delete Stack", "Yes, Delete"



## Extra Challenge

While we wait for everyone to complete this session....

- What other things could you do during a boot-strap?
- Could you pass in credentials to do tasks such as domain join?

**END**

# Session 5 - AWS Systems Manager

In this session we will get introduced to AWS Systems Manager (SSM).

Take the following steps, one at a time. There is plenty of time to complete the session and ask any questions along the way.

## Steps

- First we're going to set up a (small) fleet of servers to manage.
- Navigate to CloudFormation
- Select "Create Stack"
- Select "Upload a template to Amazon S3" and "Browse..."
- With the resources for this session find "three-server-instances.yaml"
- Select "Next"
- For the stack name enter "my-instance-fleet"

### Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. [Learn more](#).

Stack name

Cancel Previous **Next**

- Select "Next"
- Scroll to the bottom and select "Next"

## Capabilities

**i** The following resource(s) require capabilities: [AWS::IAM::Role]

This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions.

[Learn more.](#)

I acknowledge that AWS CloudFormation might create IAM resources.

[Quick Create Stack](#) (Create stacks similar to this one, with most details auto-populated)

[Cancel](#) [Previous](#) [Create](#)

- As this template will adjust the security of your account you will now need to check the box for "I acknowledge that AWS CloudFormation might create IAM resources."

- Select "Create"

- Wait a minute or two while the instances build. You can watch them build from the "Events" tab in the CloudFormation stack page, and from the Instance list in the EC2 page.

CloudFormation Stacks																																							
Stack Name		Created Time	Status	Description																																			
<input checked="" type="checkbox"/>	my-instance-fleet	2018-02-25 13:09:14 UTC+1000	CREATE_IN_PROGRESS...	This template creates three EC2 instances managed b...																																			
Events																																							
Filter by: Status ▾ Search events																																							
<table border="1"> <thead> <tr> <th>Time</th> <th>Status</th> <th>Type</th> <th>Logical ID</th> <th>Status Reason</th> </tr> </thead> <tbody> <tr> <td>2018-02-25 13:09:47 UTC+1000</td> <td>CREATE_IN_PROGRESS</td> <td>AWS::IAM::InstanceProfile</td> <td>serverRoleInstanceProfile</td> <td>Resource creation Initiated</td> </tr> <tr> <td>2018-02-25 13:09:46 UTC+1000</td> <td>CREATE_IN_PROGRESS</td> <td>AWS::IAM::InstanceProfile</td> <td>serverRoleInstanceProfile</td> <td></td> </tr> <tr> <td>2018-02-25 13:09:44 UTC+1000</td> <td>CREATE_COMPLETE</td> <td>AWS::IAM::Role</td> <td>serverRole</td> <td></td> </tr> <tr> <td>2018-02-25 13:09:18 UTC+1000</td> <td>CREATE_IN_PROGRESS</td> <td>AWS::IAM::Role</td> <td>serverRole</td> <td>Resource creation Initiated</td> </tr> <tr> <td>2018-02-25 13:09:17 UTC+1000</td> <td>CREATE_IN_PROGRESS</td> <td>AWS::IAM::Role</td> <td>serverRole</td> <td></td> </tr> <tr> <td>2018-02-25 13:09:14 UTC+1000</td> <td>CREATE_IN_PROGRESS</td> <td>AWS::CloudFormation::Stack</td> <td>my-instance-fleet</td> <td>User Initiated</td> </tr> </tbody> </table>					Time	Status	Type	Logical ID	Status Reason	2018-02-25 13:09:47 UTC+1000	CREATE_IN_PROGRESS	AWS::IAM::InstanceProfile	serverRoleInstanceProfile	Resource creation Initiated	2018-02-25 13:09:46 UTC+1000	CREATE_IN_PROGRESS	AWS::IAM::InstanceProfile	serverRoleInstanceProfile		2018-02-25 13:09:44 UTC+1000	CREATE_COMPLETE	AWS::IAM::Role	serverRole		2018-02-25 13:09:18 UTC+1000	CREATE_IN_PROGRESS	AWS::IAM::Role	serverRole	Resource creation Initiated	2018-02-25 13:09:17 UTC+1000	CREATE_IN_PROGRESS	AWS::IAM::Role	serverRole		2018-02-25 13:09:14 UTC+1000	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	my-instance-fleet	User Initiated
Time	Status	Type	Logical ID	Status Reason																																			
2018-02-25 13:09:47 UTC+1000	CREATE_IN_PROGRESS	AWS::IAM::InstanceProfile	serverRoleInstanceProfile	Resource creation Initiated																																			
2018-02-25 13:09:46 UTC+1000	CREATE_IN_PROGRESS	AWS::IAM::InstanceProfile	serverRoleInstanceProfile																																				
2018-02-25 13:09:44 UTC+1000	CREATE_COMPLETE	AWS::IAM::Role	serverRole																																				
2018-02-25 13:09:18 UTC+1000	CREATE_IN_PROGRESS	AWS::IAM::Role	serverRole	Resource creation Initiated																																			
2018-02-25 13:09:17 UTC+1000	CREATE_IN_PROGRESS	AWS::IAM::Role	serverRole																																				
2018-02-25 13:09:14 UTC+1000	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	my-instance-fleet	User Initiated																																			

- The stack can take longer than you might expect to create the "AWS::IAM::InstanceProfile", but things should speed along after that step is complete.

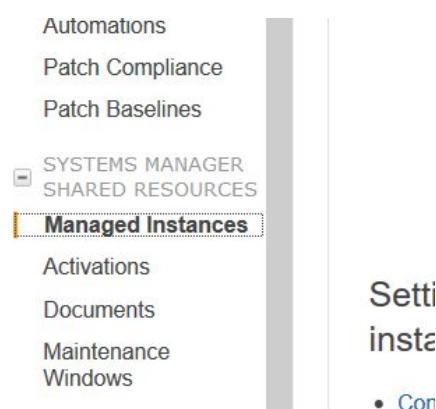
- Still waiting? Have a look at the template you are building. In some ways its more complex than other templates we've built.

...

- Now the instances are built, let's check to make sure that SSM can 'see' them.

- Navigate to EC2

- From the menu on the left hand side, scroll down and select "Managed Instances" under the heading "SYSTEMS MANAGER SHARED RESOURCES".



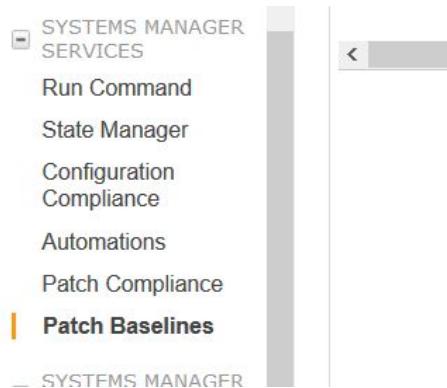
- If there is nothing listed yet, the SSM service might not have discovered the Instances yet. Wait a moment.
- When we created the Instances (via CloudFormation) we gave them the security rights to communicate with SSM. We are now waiting for the SSM agent on the server to poll the services.
- Refresh the page (maybe a few times) until you see all three servers listed.

The screenshot shows the AWS Systems Manager Managed Instances list. The left sidebar has 'SYSTEMS MANAGER SERVICES' and 'SYSTEMS MANAGER SHARED RESOURCES' sections, with 'Managed Instances' selected. The main area has tabs for 'Run a command', 'Create Association', 'Setup Inventory', 'Resource Data Syncs', and 'Actions'. Below is a table with columns: Name, Instance ID, Ping status, Platform Type, and Platform Name. Three instances are listed: 'server-one', 'server-three', and 'server-two', all marked as 'Online' and 'Windows'. At the bottom, there is a note 'Select a managed instance above'.

	Name	Instance ID	Ping status	Platform Type	Platform Name
<input type="checkbox"/>	server-one	i-028394d3cc8a67f57	Online	Windows	Microsoft Windows Server 2016 Datacenter
<input type="checkbox"/>	server-three	i-07ff680f019f9d63f	Online	Windows	Microsoft Windows Server 2016 Datacenter
<input type="checkbox"/>	server-two	i-0bf2a0cc458e61fd3	Online	Windows	Microsoft Windows Server 2016 Datacenter

## SSM - Check server patch status

- First let's check the patch status of our Instances against the default Patch Baseline.
- To see the default baseline select "Patch Baselines" from the menu on the left hand side.



- You will see several Default Baselines provided by AWS. Select the one with the name "AWS-DefaultPatchBaseline" as this applies to Windows.

The screenshot shows the AWS Systems Manager Patch Baselines management interface. The left sidebar is identical to the previous one, showing options like Run Command, State Manager, Configuration Compliance, Automations, Patch Compliance, and Patch Baselines. The 'Patch Baselines' option is also highlighted with an orange bar.

The main area displays a table of patch baselines:

Baseline ID	Baseline Name	Baseline Description	Operating System
pb-031ce0a726ee6ae26	AWS-SuseDefaultPatchBaseline	Default Patch Baseline for Suse Provided by A...	SUSE
pb-03df220ec156a717d	<b>AWS-DefaultPatchBaseline</b>	Default Patch Baseline Provided by AWS.	Windows
pb-043db686aff4f8d26	AWS-UbuntuDefaultPatchBaseline	Default Patch Baseline for Ubuntu Provided by...	Ubuntu
pb-0866fa6eac4913cdb	AWS-RedHatDefaultPatchBaseline	Default Patch Baseline for Redhat Enterprise ...	RedhatEnterpriseLi...
pb-0a19328b328e41f91	AWS-AmazonLinuxDefaultPatchBaseline	Default Patch Baseline for Amazon Linux Prov...	AmazonLinux

Below the table, a section titled "Patch Baseline: pb-03df220ec156a717d" is shown. It includes tabs for "Description", "Approval Rules" (which is selected), and "Patch Exceptions". Under "Approval Rules", there is a table:

Product	Classification	Severity	Auto Approval Delay	Compliance Level
*	CriticalUpdates, SecurityUpdates	Critical, Important	Wait 7 days before approving	Unspecified

At the bottom of the interface, there are links for Feedback, English (US), Copyright notice (© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.), Privacy Policy, and Terms of Use.

- In the lower section of the screen select "Approval Rules"

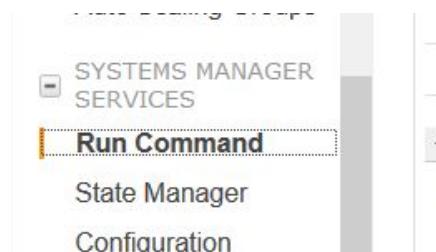
- You can see that this Baseline defines all patches with:
  - Classification of "CriticalUpdates, SecurityUpdates"
  - Severity of Critical, Important
  - Older than 7 days

Product	Classification	Severity	Auto Approval Delay	Compliance Level
*	CriticalUpdates, SecurityUpdates	Critical, Important	Wait 7 days before approving	Unspecified

- Let's check our servers against this baseline.

- Normally we would do this using a "Maintenance Window", or "State Manager" that checks periodically, but today we will run a one off check using "Run Command"

- Select "Run Command" from the menu on the left hand side.



- Select "Run a command"

- Under "Command document" select "AWS-RunPatchBaseline". This is a prewritten document to check any type of instance against a Patch Baseline.

<input type="radio"/>	AWS-InstallApplication	Amazon	Windows
<input type="radio"/>	AWS-JoinDirectoryServiceDomain	Amazon	Windows
<input checked="" type="radio"/>	AWS-RunPatchBaseline	Amazon	Windows,Linux
<input type="radio"/>	AWS-InstallSpecificWindowsUpdates	Amazon	Windows
<input type="radio"/>	AWS-RunShellScript	Amazon	Linux

- Scroll down and select "Manually Selecting Instances"

Select Targets by\*

Manually Selecting Instances  
 Specifying a Tag

i-028394d3cc8a67f57  i-07ff680f019f9d63f  i-0bf2a0cc458e61fd3

Select instances ▾

Name	Instance ID	Instance State	Availability Zone	Ping Status	Last Ping Date	Agent Version
server-one	i-028394d3cc8a67f57	running	ap-southeast-2a	Online	February 25, 2018	2.2.93.0
server-three	i-07ff680f019f9d63f	running	ap-southeast-2a	Online	February 25, 2018	2.2.93.0
server-two	i-0bf2a0cc458e61fd3	running	ap-southeast-2a	Online	February 25, 2018	2.2.93.0

Where are my instances?

- Select "Select instances" and select all of your three instances.

Execute on  Targets concurrently

Stop after  errors

Operation\*

Timeout (seconds)

Advanced Options

AWS Command Line Interface command

Cancel  Run

- Scroll to the bottom and select "Run"

- Ensure on the next page that there are entries under "Instance IDs"
- Select "View result"

The screenshot shows a success message: "Success" with a green checkmark. It states: "We are running your command against the instances listed below." Below this, it lists "Instance IDs" and "Command ID". A blue "View result" button is at the bottom right.

Instance IDs	i-028394d3cc8a67f57, i-07ff680f019f9d63f, i-0bf2a0cc458e61fd3
Command ID	5d4fda43-82a8-45bc-8f46-08848572317f

[View result](#)

- You should see a list of commands "In Progress", the list has a refresh button on it so you can watch the progress.

The screenshot shows a table of commands. The columns are: Command ID, Instance ID, Document name, and Status. All three entries have a yellow "In Progress" status icon. A "Run a command" button and an "Actions" dropdown are visible at the top left.

Command ID	Instance ID	Document name	Status
a6fafafa84-fdc3-4a1b...	i-07ff680f019f9d63f	AWS-RunPatchBaseline	<span style="color: yellow;">In Progress</span>
a6fafafa84-fdc3-4a1b...	i-028394d3cc8a67f57	AWS-RunPatchBaseline	<span style="color: yellow;">In Progress</span>
5d4fda43-82a8-45b...	i-0bf2a0cc458e61fd3	AWS-RunPatchBaseline	<span style="color: yellow;">In Progress</span>

- When any of the commands are complete, shown as "Success" you can view the output.
- Select the command from the list, in the lower section of the screen select the "Output" tab.

The screenshot shows the "Output" tab selected. It displays two rows of data: "PatchLinux" and "PatchWindows", both with a "Success" status and a response code of 0. The "Output" column contains a "View Output" link. Navigation buttons like back, forward, and search are visible at the top of the table.

Plugin name	Status	Response code	Start Time	Finish Time	Output
PatchLinux	<span style="color: green;">Success</span>	0	February 25, 2018 at 1:26:56 PM...	February 25, 2018 at 1:26:56 PM...	<a href="#">View Output</a>
PatchWindows	<span style="color: green;">Success</span>	0	February 25, 2018 at 1:22:38 PM...	February 25, 2018 at 1:26:56 PM...	<a href="#">View Output</a>

- In the output list you should see two entries. The command/document that we ran operates on both Windows and Linux OS's. There should be one output per OS type, and only any useful information in the Windowseat man output.

- You will (probably) see that "Scan found no missing updates."

[Commands](#) > Output

## Output for PatchWindows

```
Patch Summary for i-0bf2a0cc458e61fd3
PatchGroup      :
BaselineId      : pb-03df220ec156a717d
SnapshotId      : d4b95834-a53f-4a19-b1ef-cbb7d75f3426
OwnerInformation :
OperationType   : Scan
OperationStartTime: 2018-02-25T03:22:44.2777320Z
OperationEndTime : 2018-02-25T03:26:53.8367563Z
InstalledCount   : 0
InstalledOtherCount: 10
FailedCount      : 0
MissingCount     : 0
NotApplicableCount: 2390

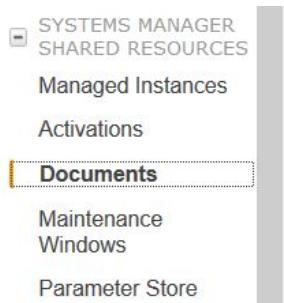
EC2AMAZ-95VG6Q9 - PatchBaselineOperations Assessment Results -
2018-02-25T03:26:56.461

Scan found no missing updates.
```

**- Great.**

## SSM - Run our own command/document

- Now let's create our own document, and run a bigger command.
- Navigate to EC2, scroll down the left hand menu and select "Documents"



- Select "Create Document"
- Enter "myWebServerInstall" into the "Name"
- Make sure that "Document Type" is set to "Command"

Create Document

Specify the following parameters to create a document

Name*	<input type="text" value="myWebServerInstall"/>	<a href="#">i</a>
Document Type	<input type="text" value="Command"/>	<a href="#">i</a>

- In the resources for this session you will find a file called "ssm-document.json". Open this in a text editor and copy all of the content to the clipboard.
- Under "Content" delete the curly braces "{}" and paste in the contents of your clipboard.

Content\*

```

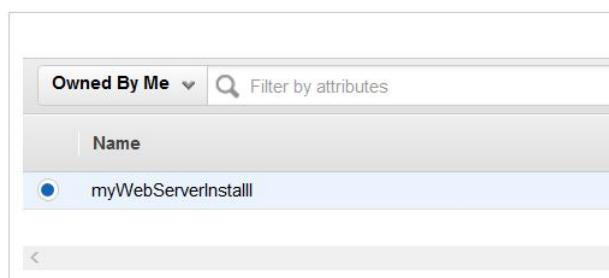
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
  "name": "SetupWebsite",
  "inputs": {
    "timeoutSeconds": 300,
    "runCommand": [
      "mkdir c:\\inetpub\\test",
      "",
      "curl https://s3-ap-southeast-2.amazonaws.com/test-aspx/def",
      "",
      "add-windowsfeature web-webserver -includeallsubfeature -lo",
      "",
      "new-website -name test -port 80 -physicalpath c:\\inetpub\\",
      "",
      "remove-website -name \"Default Web Site\"",
      "",
      "start-website -name test"
    ]
  }
}
  
```

- There will be some time in a moment to review the document.
- Scroll down and select "Create Document", then "Close"

## Create Document



- Let's run this document as a command against our fleet.
- Select "Run Command" from the menu on the left hand side.
- Select "Run a command"
- Under "Command document" change the dropdown filter to "Owned By Me"



- Select your document "myWebServerInstall"
- Again select "Manually Selecting Instances" and select all your instances from "Select instances"



- Again select "3" and "1" for "Execute on" and "Stop after"
- Scroll down and select "Run", ensure the instances are listed, and select "View result"

## Run a command

 Success

We are running your command against the instances listed below.

Instance IDs i-028394d3cc8a67f57, i-07ff680f019f9d63f, i-0bf2a0cc458e61fd3

Command ID 6b919209-98c9-4251-b294-8aeab9a8b405

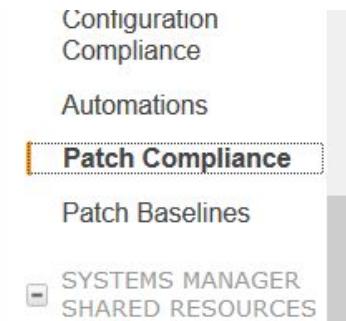
[View result](#)

- This might take a couple of minutes.

....

- Let's go and take another look at the result of the patch baseline we did.

- From the menu on the left hand side select "Patch Compliance"



- This page will show a report on the patch compliance of our managed fleet.

- In the "Select instances" dropdown, select all our instances

## Patch Compliance

Patch compliance reporting allows you to view compliance information across a number of different axis. Select the report type below to see a summary of the information that you are interested in.

The screenshot shows the AWS Patch Compliance dashboard. At the top, there is a "Report Type" dropdown set to "Instances". Below it, a "Select instances" section contains three instance IDs: i-028394d3cc8a67f57, i-07ff680f019f9d63f, and i-0bf2a0cc458e61fd3. A "Select instances" button is also present. Below these, a table displays instance details:

Name	Instance ID	Patch Status	Availability Zone	Ping Status	Last Ping Date
server-one	i-028394d3cc8...	running	ap-southeast-2a	Online	February 25, 2...
server-three	i-07ff680f019f9...	running	ap-southeast-2a	Online	February 25, 2...

- The dashboard should update with a review of the current patch status.

## Compliance Summary



- This is a useful tool, especially if you are running "AWS-RunPatchBaseline" on a regular basis.

- To catch up on the status of our web server installs, select "Run Command" again from the left hand menu.

- When the commands are showing as "Success"

The screenshot shows the AWS Lambda Run Command interface. At the top, there are two buttons: "Run a command" (highlighted in blue) and "Actions". Below is a search bar labeled "Filter by attributes". A table lists three run commands:

	Command ID	Instance ID	Document name	Status
<input type="checkbox"/>	fc1e9ce7-f56a-4431...	i-0bf2a0cc458e61fd3	myWebServerInstall	<span style="color: green;">Success</span>
<input type="checkbox"/>	fc1e9ce7-f56a-4431...	i-07ff680f019f9d63f	myWebServerInstall	<span style="color: green;">Success</span>
<input type="checkbox"/>	33addfe3-be11-48e...	i-028394d3cc8a67f57	myWebServerInstall	<span style="color: green;">Success</span>

- Navigate to EC2, Instances

The screenshot shows the AWS EC2 Instances dashboard. On the left sidebar, under the "INSTANCES" section, "Instances" is selected. The main area displays a table of running instances:

Name	Instance ID	Instance Type	Availability Zone	Instance State
server-one	i-028394d3cc8a67f57	t2.large	ap-southeast-2a	<span style="color: green;">running</span>
server-three	i-07ff680f019f9d63f	t2.large	ap-southeast-2a	<span style="color: green;">running</span>
server-two	i-0bf2a0cc458e61fd3	t2.large	ap-southeast-2a	<span style="color: green;">running</span>

- Locate the "Public DNS" for the instances and test the website from the details section at the bottom of the screen.

The screenshot shows the AWS EC2 Instance details page for instance i-028394d3cc8a67f57 (server-one). At the top, it shows the instance ID and Public DNS. Below is a table with instance details:

Description	Status Checks	Monitoring	Tags
Instance ID: i-028394d3cc8a67f57 (server-one)	Public DNS: ec2-54-252-132-55.ap-southeast-2.compute.amazonaws.com		
Instance ID: i-028394d3cc8a67f57	Public DNS (IPv4): ec2-54-252-132-55.ap-southeast-2.compute.amazonaws.com		
Instance state: running	IPv4 Public IP: 54.252.132.55		
Instance type: t2.large	IPv6 IPs: -		
Elastic IPs	Private DNS: ip-172-31-14-230.ap-southeast-2.compute.internal		

- You may have to wait a few moments after the command is complete before the website appears.

- Issue: Sometimes the run commands don't show in the list. Try creating them again.

- Open a new tab in your browser and navigate to the Public DNS name of one of the instances:

The screenshot shows a web browser window with the URL `ec2-54-252-132-55.ap-southeast-2.compute.amazonaws.com`. The page title is "TrekDay Basecamp" and the subtitle is "AWS Essentials for Windows Admins". A section titled "Here is some information about this server:" contains a table of metadata. The table has two columns: "metaData" and "value". The data is as follows:

metaData	value
instance-id	i-028394d3cc8a67f57
local-hostname	ip-172-31-14-230.ap-southeast-2.compute.internal
local-ipv4	172.31.14.230
public-hostname	ec2-54-252-132-55.ap-southeast-2.compute.amazonaws.com
public-ipv4	54.252.132.55

- It's our website again.

- Fancy logging into the Instance via RDP? Well you can't we didn't use a Key Pair, this server is 100% not a pet.

- No need to clean up, leave the server fleet there, we'll be using it in the next session.

## Extra Challenge

While we wait for everyone to complete this session....

- Let's talk about how we can use SSM to get logging data from the EC2 Instance into CloudWatch Logs

**END**

# Session 6 - Security

In this session we will get introduced to Amazon Inspector.

Take the following steps, one at a time. There is plenty of time to complete the session and ask any questions along the way.

## Steps

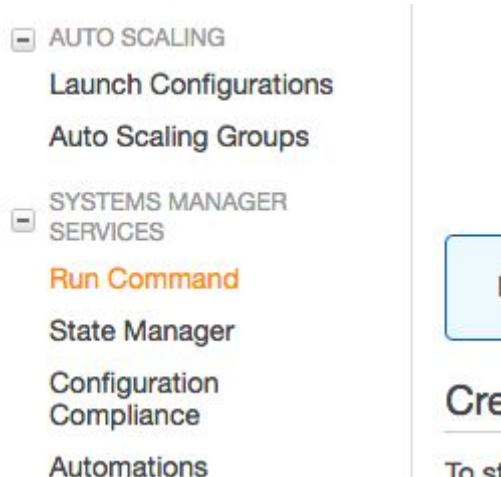
- Do you still have your small fleet of servers?
- If you deleted the stack after the SSM session, now would be a good time to recreate it!
- We're going to start this session off, back in SSM.

## Run an SSM Command

- Navigate to EC2



- From the menu on the left hand side select "Run Command"



- We're going to install the "AWS Inspector" agent on our fleet.

**- Select "Run a command"**

## Welcome to EC2 Systems Manager

Use EC2 Systems Manager to easily configure and manage your on-premises machines configured for Systems Manager.

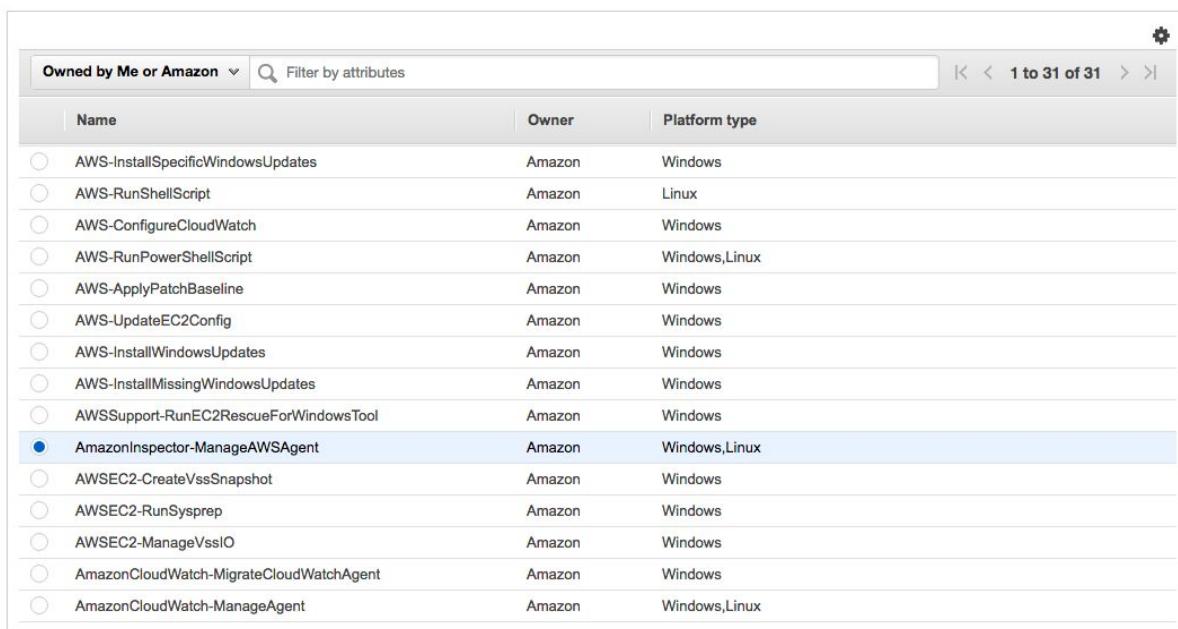
Run Command automates common administrative tasks by running Linux shell scripts or Windows PowerShell commands.

Before you can run a command, you must configure your targets and setting up permissions as described in the Help topic for running commands on VMs with Systems Manager using the activation process.

[Run a command](#)

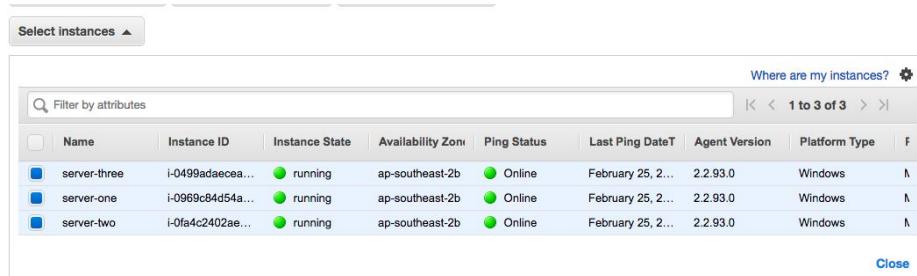
[More about Run Command](#)

**- Select "AmazonInspector-ManageAWSAgent"**



Name	Owner	Platform type
AWS-InstallSpecificWindowsUpdates	Amazon	Windows
AWS-RunShellScript	Amazon	Linux
AWS-ConfigureCloudWatch	Amazon	Windows
AWS-RunPowerShellScript	Amazon	Windows,Linux
AWS-ApplyPatchBaseline	Amazon	Windows
AWS-UpdateEC2Config	Amazon	Windows
AWS-InstallWindowsUpdates	Amazon	Windows
AWS-InstallMissingWindowsUpdates	Amazon	Windows
AWS-Support-RunEC2RescueForWindowsTool	Amazon	Windows
AmazonInspector-ManageAWSAgent	Amazon	Windows,Linux
AWSEC2-CreateVssSnapshot	Amazon	Windows
AWSEC2-RunSysprep	Amazon	Windows
AWSEC2-ManageVssIO	Amazon	Windows
AmazonCloudWatch-MigrateCloudWatchAgent	Amazon	Windows
AmazonCloudWatch-ManageAgent	Amazon	Windows,Linux

**- From the "Select instances" dropdown, select all your instances**



Select instances ▾	Where are my instances? ⚙								
	Name	Instance ID	Instance State	Availability Zone	Ping Status	Last Ping DateT	Agent Version	Platform Type	F
<input checked="" type="checkbox"/>	server-three	i-0499adaecea...	● running	ap-southeast-2b	● Online	February 25, 2...	2.2.93.0	Windows	
<input checked="" type="checkbox"/>	server-one	i-0969cd4d54a...	● running	ap-southeast-2b	● Online	February 25, 2...	2.2.93.0	Windows	
<input checked="" type="checkbox"/>	server-two	i-0fa4c2402ae...	● running	ap-southeast-2b	● Online	February 25, 2...	2.2.93.0	Windows	

- Enter "3" and "1" for "Execute on" and "Stop after"

- For "Operation" ensure that "Install" is selected

Execute on: 3 Targets concurrently

Stop after: 1 errors

Operation\*: Install

- Scroll down and select "Run", then "View result"

### Run a command

✓ Success  
We are running your command against the instances listed below.

Instance IDs: i-0fa4c2402aeae6e33, i-0969c84d54a607bb2, i-0499adaecea7df3b6

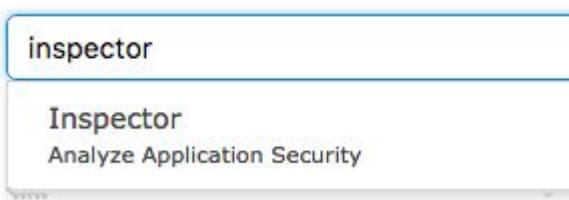
Command ID: 2aa166b7-c6d8-4388-91b4-2fbe551027dc

[View result](#)

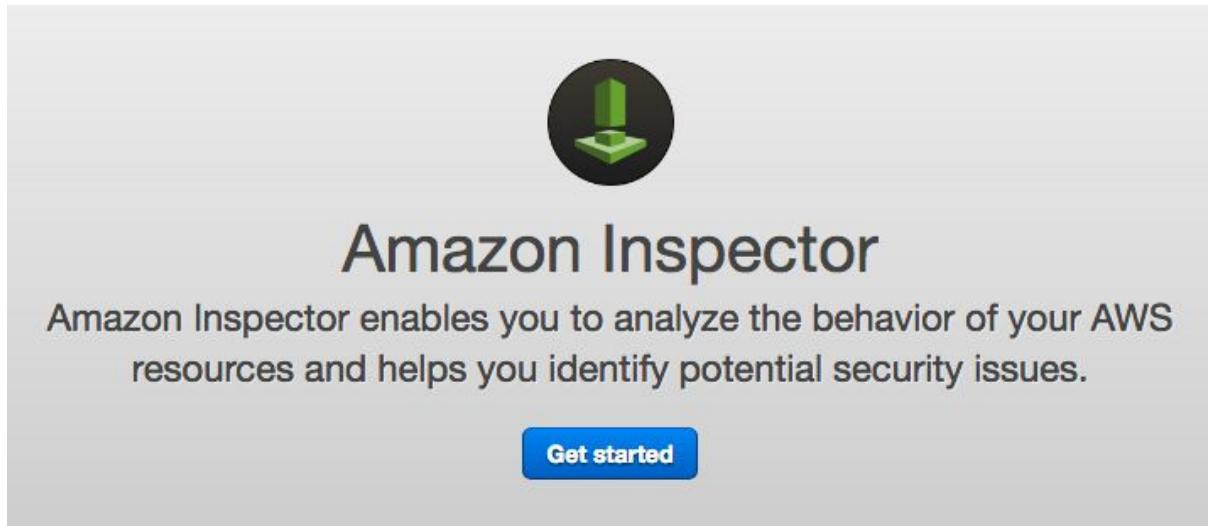
- When the command is a "Success" the Amazon Inspector Agent is installed on the instance.

Run a command	Actions				
<input type="checkbox"/> Filter by attributes					
Command ID	Instance ID	Document name	Status	Requested date	C
2aa166b7-c6d8-438...	i-0fa4c2402aeae6e33	AmazonInspector-M...	<span style="color: green;">●</span> Success	February 25, 2018 ...	-
2aa166b7-c6d8-438...	i-0969c84d54a607bb2	AmazonInspector-M...	<span style="color: green;">●</span> Success	February 25, 2018 ...	-
2aa166b7-c6d8-438...	i-0499adaecea7df3b6	AmazonInspector-M...	<span style="color: green;">●</span> Success	February 25, 2018 ...	-

- Navigate to "Amazon Inspector"



- Select "Get Started"



- You should now see the "Get started with Amazon Inspector" page

- Notice that an IAM role will be created for us called "AWSServiceRoleForAmazonInspector", AWS creates this on our behalf.

- Select "Next"

- Under "Define an assessment target"

- Enter a name for the assessment "**WindowsDevAssessment**"

- Under Tags, select Key "**Environment**" and Value "**dev**"

- Select "Next"

- Under "Define an assessment template"

- Enter a name of "**SecurityScan**"

- Expand the "Rules packages" dropdown and review the types of packages that can be run.

- For now select "**Common Vulnerabilities and Exposures-1.1**"

- For "Duration" select "**1 Hour (Recommended)**"

- Select "Next" and "Create"

## Define an assessment template

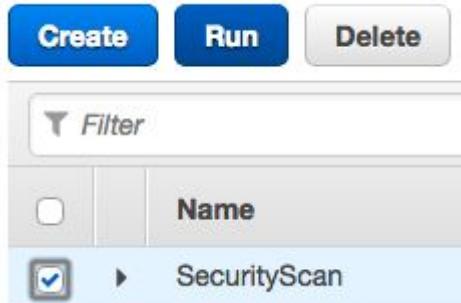
An assessment template allows you to specify various properties for an assessment run, including rules packages, duration, SNS notifications, and labels. [Learn more.](#)

Name*	SecurityScan
Rules packages*	Common Vulnerabilities and Exposures-1.1
	Select an Inspector rules package
Amazon Inspector runs assessments for the assessment target against selected rules package(s). Learn more.	
Duration*	1 Hour (Recommended)
The default Amazon Inspector assessment template duration is 1 hour. You can modify the duration, but longer assessment templates with longer durations can deliver fuller sets of findings.	

- Now that we have defined an assessment, let's run it

- Select "SecurityScan" from the list

- Select "Run"



- Notice that the "Last run" column shows "Collecting data"

	Name	Duration	Target name	Last run	All runs
<input type="checkbox"/>	▶ SecurityScan	1 Hour	WindowsDevAssessment	Collecting data	1

- If you navigate around while the run is collecting data, and want to check on the progress navigate to "Assessment runs" on the left hand side and expand the row entry to see the "Status"

Assessment runs		Run	Cancel	Delete	Last updated on February 25, 2018 1:46:41 PM (0m ago)		
<b>Findings</b>							
	Start time	Status	Template name	Findings	Findings by severity	Reports	
<input checked="" type="checkbox"/>	Today at 1:45 PM (...)	Collecting data	SecurityScan	0			

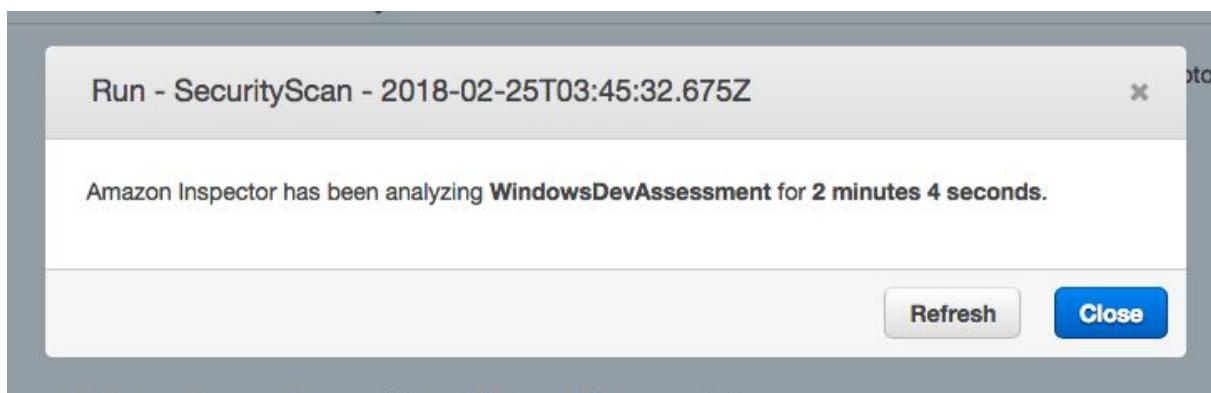
- Click "Show status" for a detailed report on the scan progress.

The screenshot shows the AWS Inspector interface for a security scan named 'SecurityScan'. The top bar displays the date and time as 'Today at 1:45 PM ...' and the status as 'Collecting data'. The scan ID is '0-KIAAN2hC/template/0-n71otoBi/run/0-IY2x1oir'. Below this, the 'Assessment - Run - SecurityScan - 2018-02-25T03:45:32.675Z' section provides detailed information:

- ARN: arn:aws:inspector:ap-southeast-2:226649799576:target/0-KIAAN2hC/template/0-n71otoBi/run/0-IY2x1oir
- Start: Today at 1:45 PM (GMT+10) (a minute ago)
- Target name: WindowsDevAssessment
- Template name: SecurityScan
- Rules packages: Common Vulnerabilities and Exposures-1.1
- Duration: 1 Hour (Recommended)
- Status: Collecting data
- Findings: 0

At the bottom, there are two buttons: 'Show AWS agents' and 'Show status'.

- The scan will take some time, so lets come back to this later today.



END

## Session 7 - Serverless

In this session we will get introduced to the concept of “Serverless” event driven architectures.

Take the following steps, one at a time. There is plenty of time to complete the session and ask any questions along the way.

### Creating S3 Buckets

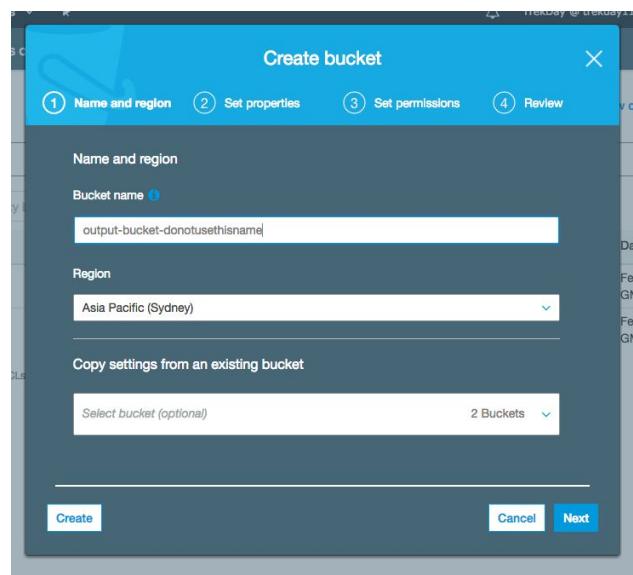
- For this workflow we will need a couple of S3 buckets

- Open the AWS console, make sure you are in Sydney, and navigate to S3

The screenshot shows the AWS services search interface. A search bar at the top contains the text 's3'. Below the search bar, a list of services is displayed, with 'S3' being the first item. The description 'Scalable Storage in the Cloud' is shown below 'S3'. There are other service names listed below it, though they are partially cut off.

- Select Create bucket

- Enter a bucket name (this must be globally unique) don't use the same name as in the screenshot, and don't use the same as your neighbour!



- Tip: Enter the name "input-bucket-" then add some pseudo random characters by mashing the keyboard.

- The S3 console page is global, so you need to select a region to create the bucket. **Make sure this is Sydney**.

- Select "Create"

- Repeat this step and create a "output-bucket-xxxxxxxx"

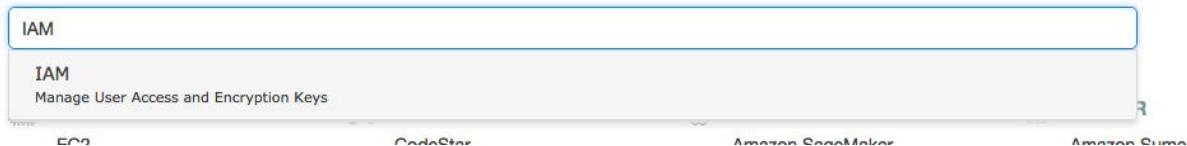
- Make a note of the bucket names.

	input-bucket-donotusethisname	Not public *	Asia Pacific (Sydney)	Feb 25, 2018 11:46:33 AM GMT+1000
	output-bucket-donotusethisname	Not public *	Asia Pacific (Sydney)	Feb 25, 2018 11:46:50 AM GMT+1000

## Creating an IAM Role

- Before we create our Lambda function, we need to create a security profile (called an IAM Role) that will give the function all the necessary permissions it needs to run.

- Navigate to IAM (Identity and Access Management)



- Select "Roles"

- Dashboard
- Groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings
- Credential report

- Select "Create role"

A screenshot of the 'Create role' wizard. At the top, there are two buttons: 'Create role' (in blue) and 'Delete role'. Below that is a search bar with the placeholder 'Search'. The main area has a table with two columns: 'Role name' and 'Description'. The 'Role name' column contains a dropdown menu with the option 'AWS Service'. The 'Description' column is empty.

- Ensure that "AWS Service" is selected, then select "Lambda", and "Next: Permissions"

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role

API Gateway	Data Pipeline	ElasticLoadBalancing	MediaConvert	Service Catalog
Auto Scaling	DeepLens	Glue	OpsWorks	Step Functions
Batch	Directory Service	Greengrass	RDS	Storage Gateway
CloudFormation	DynamoDB	GuardDuty	Redshift	
CloudHSM	EC2	Inspector	Rekognition	
CloudWatch Events	EMR	IoT	S3	
CodeBuild	ElastiCache	Kinesis	SMS	
CodeDeploy	Elastic Beanstalk	Lambda	SNS	
Config	Elastic Container Service	Lex	SWF	
DMS	Elastic Transcoder	Machine Learning	SageMaker	

\* Required      [Cancel](#)      [Next: Permissions](#)

- In the policy type search box, type "Lambda", and scroll to "AWSLambdaExecute"
- SELECT THE CHECKBOX next to the policy name (if you select the policy name itself, you will be sent elsewhere!)

Attach permissions policies

Choose one or more policies to attach to your new role.

[Create policy](#) [Refresh](#)

Policy name	Attachments	Description
<input type="checkbox"/> AWSLambdaENIManagementAccess	0	Provides minimum permissions for a Lambda function to ma...
<input checked="" type="checkbox"/> AWSLambdaExecute	0	Provides Put, Get access to S3 and full access to CloudWat...

- Select "Next Review"
- Enter a name for your role "my-lambda-role"
- Select "Create role"

Create role

1 Trust    2 Permissions    3 Review

**Review**

Provide the required information below and review this role before you create it.

**Role name\*** my-lambda-role  
 Maximum 64 characters. Use alphanumeric and '+-=,@-\_.' characters.

**Role description** Allows Lambda functions to call AWS services on your behalf.  
 Maximum 1000 characters. Use alphanumeric and '+-=,@-\_.' characters.

**Trusted entities** AWS service: lambda.amazonaws.com

**Policies** AWSLambdaExecute

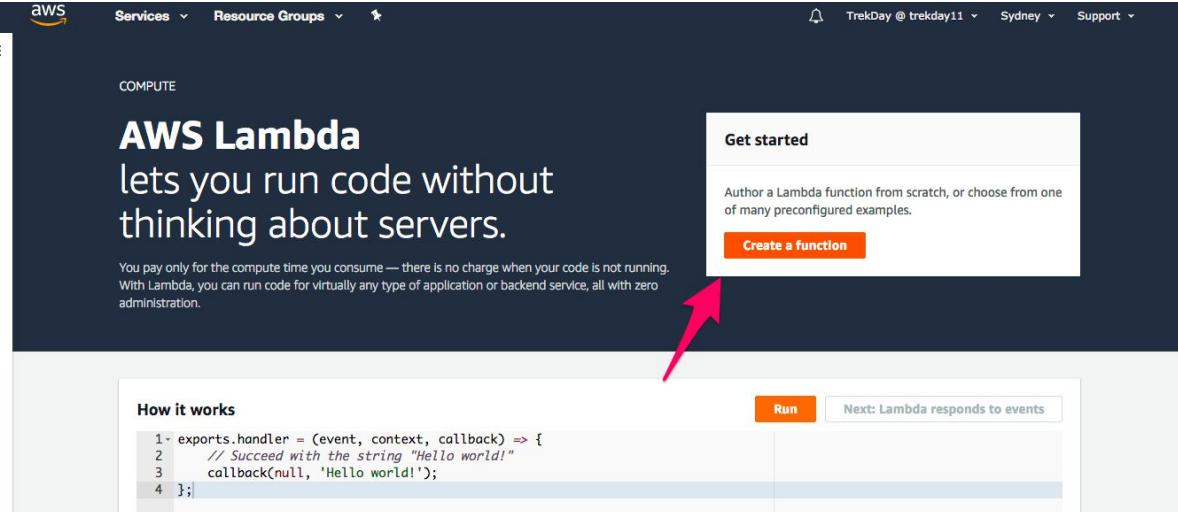
\* Required    Cancel    Previous    **Create role**

## Create a Lambda Function

- Now lets create our Lambda function

- Navigate to Lambda

- Select "Create function"



The screenshot shows the AWS Lambda 'Get started' page. The main heading is 'AWS Lambda lets you run code without thinking about servers.' Below it, a sub-section titled 'How it works' contains a snippet of code:

```

1- exports.handler = (event, context, callback) => {
2-   // Succeed with the string "Hello world!"
3-   callback(null, 'Hello world!');
4- };

```

On the right side, there is a 'Run' button and a link 'Next: Lambda responds to events'. At the top right of the main area, there is a 'Create a function' button, which is highlighted with a red arrow pointing towards it.

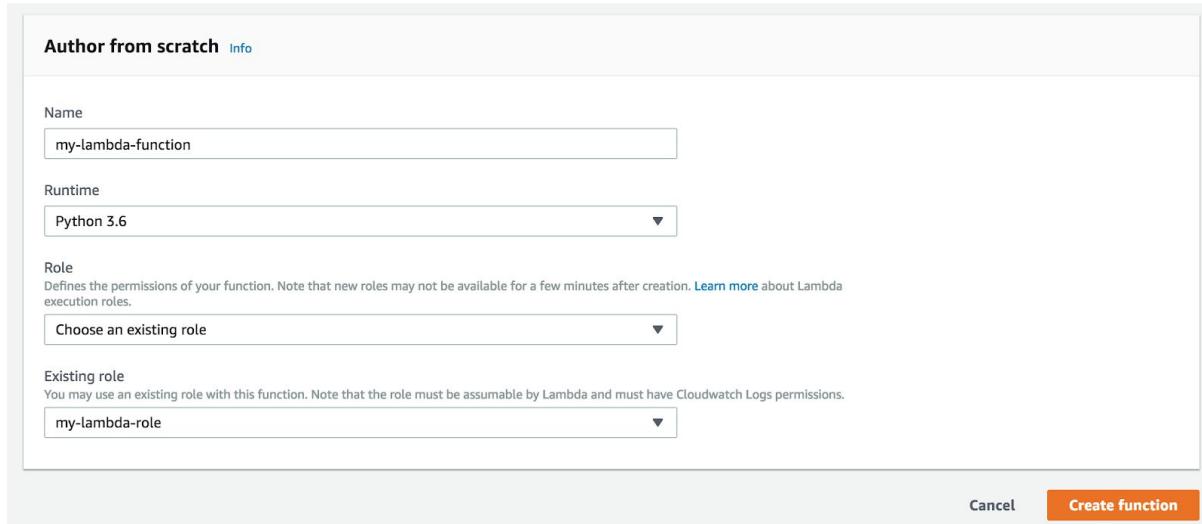
- Make sure that "Author from scratch" is selected

- Enter a function name: "my-lambda-function"

- In the Runtime selection, select "Python 3.6" (*Notice the other runtimes you could use when writing your own functions.*)

- In Role, select "Choose an existing role" and then select in the "Existing role" selection to find "my-lambda-role"

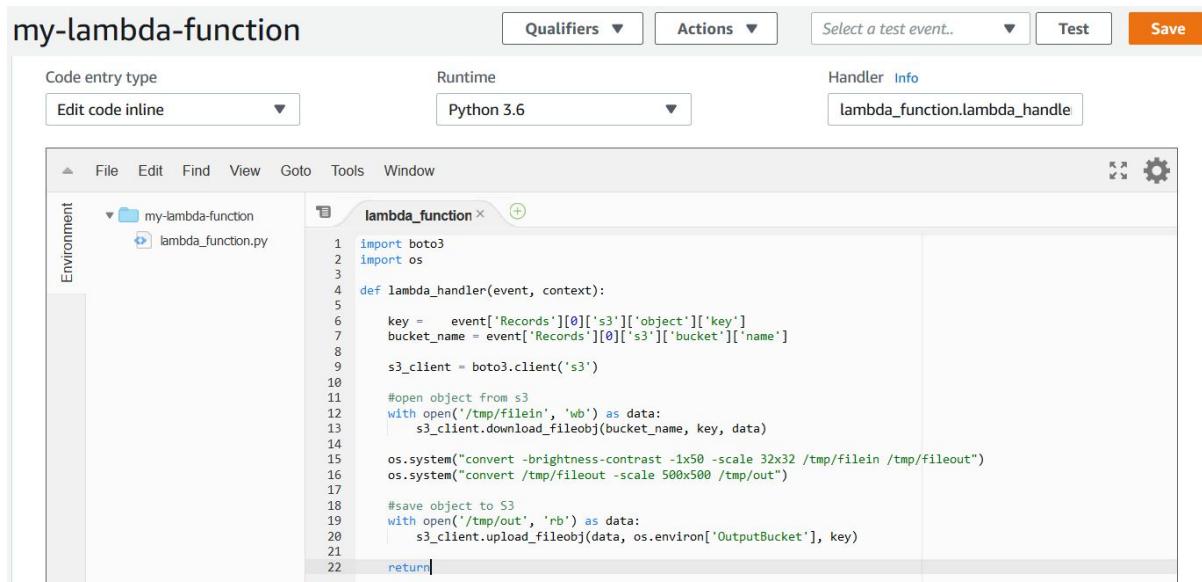
- Select "Create function"



- You will now be taken to the main Lambda function page.

- Scroll down and find the code editor.

- From the resources with the session, locate 'lambda\_handler.py' open up the file in a text editor. It's a pretty simple script. Copy and paste it into the Lambda code editor, replacing all the code that was there



- In the "Environment variables" section enter the "Key" of "OutputBucket" and the name of YOUR output bucket "output-bucket-xxxxxx"

Environment variables
You can define Environment Variables as key-value pairs that are accessible from your function code. These are useful to store configuration settings without the need to change function code. <a href="#">Learn more</a> .
<input type="text" value="OutputBucket"/> <input type="text" value="output-bucket-donotusethisname"/> <input type="button" value="Remove"/>
<input type="text" value="Key"/> <input type="text" value="Value"/> <input type="button" value="Remove"/>
<a href="#">Encryption configuration</a>

- In the "Basic settings" section move the "Memory" slider up to "1024 MB" and the "Timeout" to "30" seconds.

**my-lambda-function**

[Qualifiers](#) [Actions](#) [Select a test event...](#) [Test](#) **Save**

<b>Execution role</b> <p>Defines the permissions of your function. Note that new roles may not be available for a few minutes after creation. <a href="#">Learn more</a> about Lambda execution roles.</p> <p><input type="button" value="Choose an existing role"/></p> <p><b>Existing role*</b> You may use an existing role with this function. Note that the role must be assumable by Lambda and must have Cloudwatch Logs permissions.</p> <p><input type="button" value="my-lambda-role"/></p>	<b>Basic settings</b> <p>Description <input type="text"/></p> <p><b>Memory (MB)</b> <small>Info</small> Your function is allocated CPU proportional to the memory configured. <input type="range" value="1024"/> 1024 MB</p> <p><b>Timeout</b> <small>Info</small> 0 min <input type="text" value="30"/> sec</p>
<b>Network</b> <p>VPC <small>Info</small> Select a VPC that your function will access.</p> <p><input type="button" value="No VPC"/></p>	<b>Debugging and error handling</b> <p>DLQ Resource <small>Info</small> Choose the AWS service to send event payload to after exceeding maximum retries.</p> <p><input type="button" value="None"/></p>

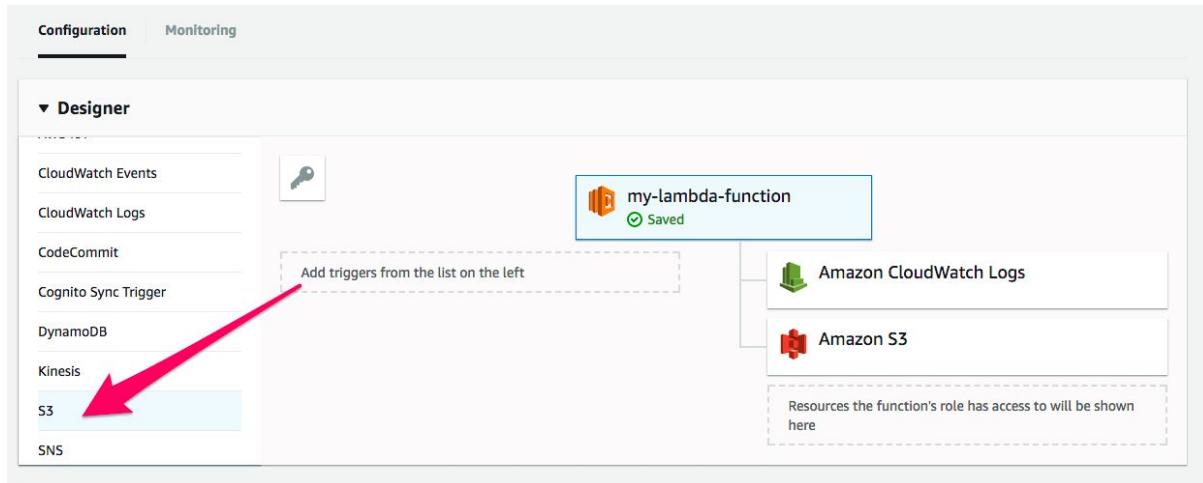
[Feedback](#) [English \(US\)](#)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

- Select "Save"

## Adding A Trigger

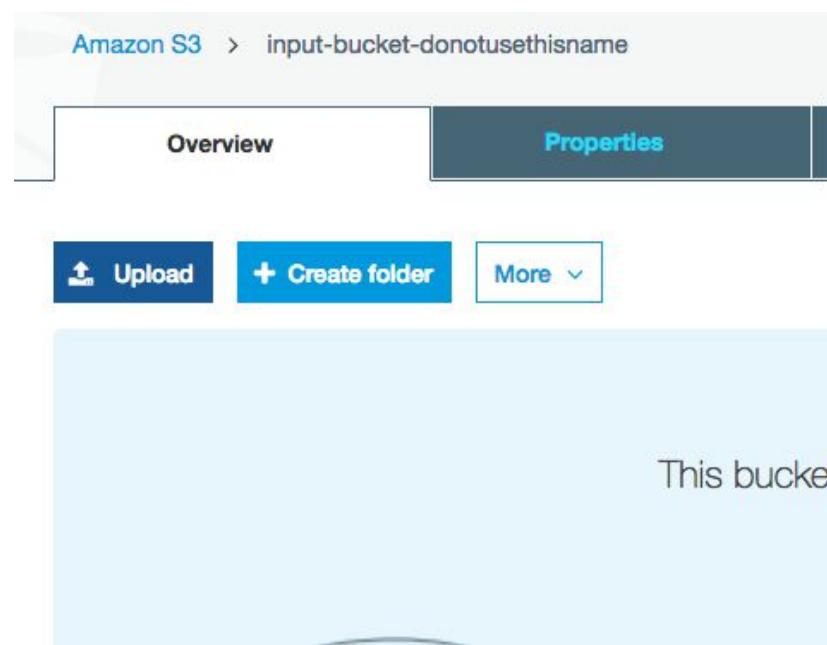
- Scroll back up to the top of the page. In the "Designer" section, scroll under "Add triggers" until you see "S3" and select it.



- You should now see a section called "Configure triggers"
- In the "Bucket" selection, find and select YOUR input bucket "input-bucket-xxxxxx"
- Under "Event type" select "Object Created (All)"
- Ensure the "Enable trigger" checkbox is ticked and select "Add" (in the bottom right)

The screenshot shows the configuration page for the 'my-lambda-function' trigger. The title bar says 'my-lambda-function'. Above the configuration area are buttons for 'Qualifiers ▾', 'Actions ▾', 'Select a test event.. ▾', 'Test', and 'Save'. The main configuration area starts with a note: 'Please select the S3 bucket that serves as the event source. The bucket must be in the same region as the function.' Below this is a dropdown menu set to 'input-bucket-donotusethisname'. The next section is 'Event type', with a note: 'Select the events that you want to have trigger the Lambda function. You can optionally set up a prefix or suffix for an event. However, for each bucket, individual events cannot have multiple configurations with overlapping prefixes or suffixes that could match the same object key.' A dropdown menu is set to 'Object Created (All)'. Below this are 'Prefix' and 'Suffix' fields, both containing 'e.g. Images/' and 'e.g. jpg' respectively. At the bottom, there is a note: 'Lambda will add the necessary permissions for Amazon S3 to invoke your Lambda function from this trigger. Learn more about the Lambda permissions model.' A 'Enable trigger' section includes a note: 'Enable the trigger now, or create it in a disabled state for testing (recommended)' and a checked checkbox. At the bottom right are 'Cancel' and 'Add' buttons.

- Select "Save"
- Now it's time to test:
- Navigate to S3, and select YOUR 'input-bucket-xxxx'
- Select 'Upload'



- Within the resources for this lesson you will find a test image. Feel free to use a JPG image of your own to upload to the bucket.

Name
ImageGrayscaler.zip
session7.txt
<b>test-image.jpg</b>
▶ VSProject

**Result!**



Greyscale fun! :)

**If you are running into issues...**

- Check that your role has the appropriate rights
- Make sure you are uploading a .JPG file in your input-bucket
- Make sure that you have placed the OutputBucket Key and Value in the Environment Variables and not in Tags

## Extra Challenge

While we wait for everyone to complete this session....

- Let's get AWS to send us an email when the image has been processed!
- We will use SNS

**END**

# Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/au/about](http://www.deloitte.com/au/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

The entity named herein is a legally separate and independent entity. In providing this document, the author only acts in the named capacity and does not act in any other capacity. Nothing in this document, nor any related attachments or communications or services, have any capacity to bind any other entity under the 'Deloitte' network of member firms (including those operating in Australia).

#### About Deloitte

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's approximately 244,000 professionals are committed to becoming the standard of excellence.

#### About Deloitte Australia

In Australia, the member firm is the Australian partnership of Deloitte Touche Tohmatsu. As one of Australia's leading professional services firms, Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 7,000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at [www.deloitte.com.au](http://www.deloitte.com.au).

Liability limited by a scheme approved under Professional Standards Legislation.