

# Working with EC2 Metadata and User data

---



**Mike Brown**

SENIOR CLOUD INSTRUCTOR

@mgbbleeds



# Overview



**Introduce EC2 instance metadata**

**Introduce EC2 user data**

**Demonstrate working with metadata and user data**



# Introducing EC2 Instance Metadata and User Data

---



# Metadata and User Data

## Metadata

Data about an instance used  
to configure or manage a  
running instance

## User Data

Instructions used to customize  
an EC2 instance configuration  
at launch



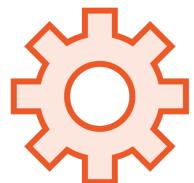
# Metadata Examples



Retrieve the IAM role associated the EC2 instance



Public and private IP addresses



Monitor for scheduled maintenance events



# Two Metadata Versions

## IMDSv1

Uses a request/response method, vulnerable to application misconfigurations

## IMDSv2

Uses a session-orientated method, tokens issued and expire



Metadata makes it easy to  
pass secure often rotated  
credentials to applications.



# Instance Metadata Service Best Practices



**Disable IMDS if it is not needed**



**Do not assign roles to EC2 instance unless they are required**



**Analyze software and use least-privileged roles**



**Consider disabling IMDSv1**



# EC2 User Data

**User data must be base64-encoded**

**You can specify user data at launch**

**You can retrieve user data using  
[http://169.254.169.254/latest/  
user-data](http://169.254.169.254/latest/user-data)**

**User data can be modified if the instance is stopped**



```
#!/bin/bash  
  
yum update -y  
  
service httpd start  
  
chkconfig httpd on
```

## Example Linux User Data

**Bash script used during the launch of an EC2 instance**



```
<powershell>
```

```
Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

```
</powershell>
```

## Example Windows User Data

**PowerShell command used during the launch of an EC2 instance**



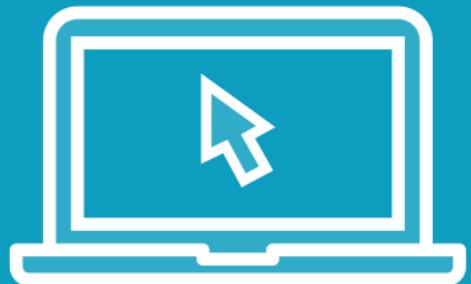
```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m5.medium \
--key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234 \
\
--user-data file://my_script.txt
```

## Example CLI and User Data

**Using the - --user-data property you can specify a script that contains your user data**



Demo



**Deploy an EC2 instance and use user data to configure it**

**Connect to the EC2 instance and display its metadata**

**Working with**

- AWS Console

**To follow along you will need an AWS Account**



# Summary



**Learned how to use user data to configure an EC2 instance at launch**

**Learned the power of EC2 metadata**

**In the next module**

- Discuss CloudWatch logs, alarms and metrics
- Discuss CloudTrail logs in CloudWatch
- Learn how to query logged data

