

Module 5 Lab 1: Inspector

EC2 Dashboard

The screenshot shows the AWS EC2 Dashboard. On the left is a navigation menu with sections like INSTANCES, IMAGES, and ELASTIC BLOCK STORE. The main area displays a 'Resources' section with a table of EC2 resources in the US East (N. Virginia) Region. The table lists various resources and their counts: Running instances (0), Elastic IPs (0), Dedicated Hosts (0), Snapshots (0), Volumes (0), Load balancers (0), Key pairs (3), Security groups (5), and Placement groups (0). Below the table is a 'Launch instance' button. To the right of the resources section is an 'Account attributes' section with links for Supported platforms, Default VPC, Settings, EBS encryption, Zones, and Console experiments. At the bottom right is an 'Explore AWS' section with links for HPC on AWS and Scale your HPC workloads on AWS.

The first step in using Inspector is defining an EC2 instance for testing.

EC2 Quick Start - Choose AMI

The screenshot shows the 'Step 1: Choose an Amazon Machine Image (AMI)' screen in the AWS EC2 Quick Start wizard. It includes a progress bar at the top with steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review. Below the progress bar is a search bar with the text '2016.09.1.20161221'. The main area displays a list of AMIs for Amazon Linux AMI 2016.09.1.20161221-x86_64-ebs. The selected AMI is 'amzn-ami-hvm-2016.09.1.20161221-x86_64-ebs - ami-4de4f15a'. The interface includes a search bar, a list of AMIs with their IDs and descriptions, and a 'Select' button for each.

The AMI selected for this lab falls in the free tier.

EC2 Quick Start - Choose Instance Type

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

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.

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 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 <small>Free tier eligible</small>	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 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
<input type="checkbox"/>	General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

A t2.mico instance type is selected.

EC2 Quick Start - Configure Instance Details

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

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances 1 Launch into Auto Scaling Group

Purchasing option ☐ Request Spot Instances

Network vpc-c64509bc (default) Create new VPC

Subnet No preference (default subnet in any Availability Zone) Create new subnet

Auto-assign Public IP Use subnet setting (Enable)

Placement group ☐ Add instance to placement group

Capacity Reservation Open Create new Capacity Reservation

IAM role None Create new IAM role

Shutdown behavior Stop

Stop - Hibernate behavior ☐ Enable hibernation as an additional stop behavior

Enable termination protection ☐ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.

Cancel Previous Review and Launch Next: Add Storage

Default options selected for all settings.

EC2 Quick Start - Add Storage

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

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ	Encryption ⓘ
Root	/dev/xvda	snap-0dd883af573a28d50	8	Magnetic (standard)	N/A	N/A	<input checked="" type="checkbox"/>	Not Encrypted ▾

Add New Volume

General Purpose (SSD) volumes provide the ability to burst to 3000 IOPS per volume, independent of volume size, to meet the performance needs of most applications and also deliver a consistent baseline of 3 IOPS/GiB. Set my root volume to General Purpose (SSD).
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Cancel Previous Review and Launch Next: Add Tags

Default storage size selected.

EC2 Quick Start - Add Tags

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

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.

Key (128 characters maximum)	Value (256 characters maximum)	Instances ⓘ	Volumes ⓘ
------------------------------	--------------------------------	-------------	-----------

This resource currently has no tags

Choose the Add tag button or [click to add a Name tag](#).
Make sure your [IAM policy](#) includes permissions to create tags.

Add Tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

No tags defined at this point.

EC2 Quick Start - Configure Security Group

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

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.

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

An InspectorDemoSG security group is defined.

Boot from General Purpose (SSD)

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

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.

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Boot from General Purpose (SSD)

General Purpose (SSD) volumes provide the ability to burst to 3000 IOPS per volume, independent of volume size, to meet the performance needs of most applications and also deliver a consistent baseline of 3 IOPS/GiB.

- ☒ Make General Purpose (SSD) the default boot volume for all instance launches from the console going forward (recommended).
- ☐ Make General Purpose (SSD) the boot volume for this instance.
- ☐ Continue with Magnetic as the boot volume for this instance.

Free tier eligible customers can get up to 30GB of General Purpose (SSD) storage.

Amazon is asking how to boot the volume.

EC2 Quick Start - Review Instance Launch

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

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, **InspectorDemoSG**, 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](#)

AMI Details



amzn-ami-hvm-2016.09.1.20161221-x86_64-ebs - ami-4de4f15a

Amazon Linux AMI 2016.09.1.20161221 x86_64 HVM EBS

Root Device Type: ebs Virtualization type: hvm

[Edit AMI](#)

Instance Type

[Edit 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

[Edit security groups](#)

Security group name	InspectorDemoSG			
Description	InspectorDemoSG			
Type ^①	Protocol ^①	Port Range ^①	Source ^①	Description ^①
SSH	TCP	22	0.0.0.0/0	

Instance Details

[Edit instance details](#)

Storage

[Edit storage](#)

Tags

[Edit tags](#)

[Cancel](#) [Previous](#) [Launch](#)

Review before instance launch.

Key Pair Creation

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

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, **InspectorDemoSG**, 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](#)

AMI Details

amzn-ami-hvm-2016.09.1.20161221-x86_64-ebs - ami-4de4f15a

Amazon Linux AMI 2016.09.1.20161221 x86_64 HVM EBS

Root Device Type: ebs Virtualization type: hvm

[Edit AMI](#)

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Inst
t2.micro	Variable	1	1	EBS

[Edit instance type](#)

Security Groups

Security group name	InspectorDemoSG			
Description	InspectorDemoSG			
Type	Protocol	Port Range	Source	Description
SSH	TCP	22		

[Edit security groups](#)

Instance Details

[Edit instance details](#)

Storage

[Edit storage](#)

[Cancel](#) [Previous](#) [Launch](#)

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

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.

Create a new key pair

Key pair name

InspectorDemoKP

[Download Key Pair](#)



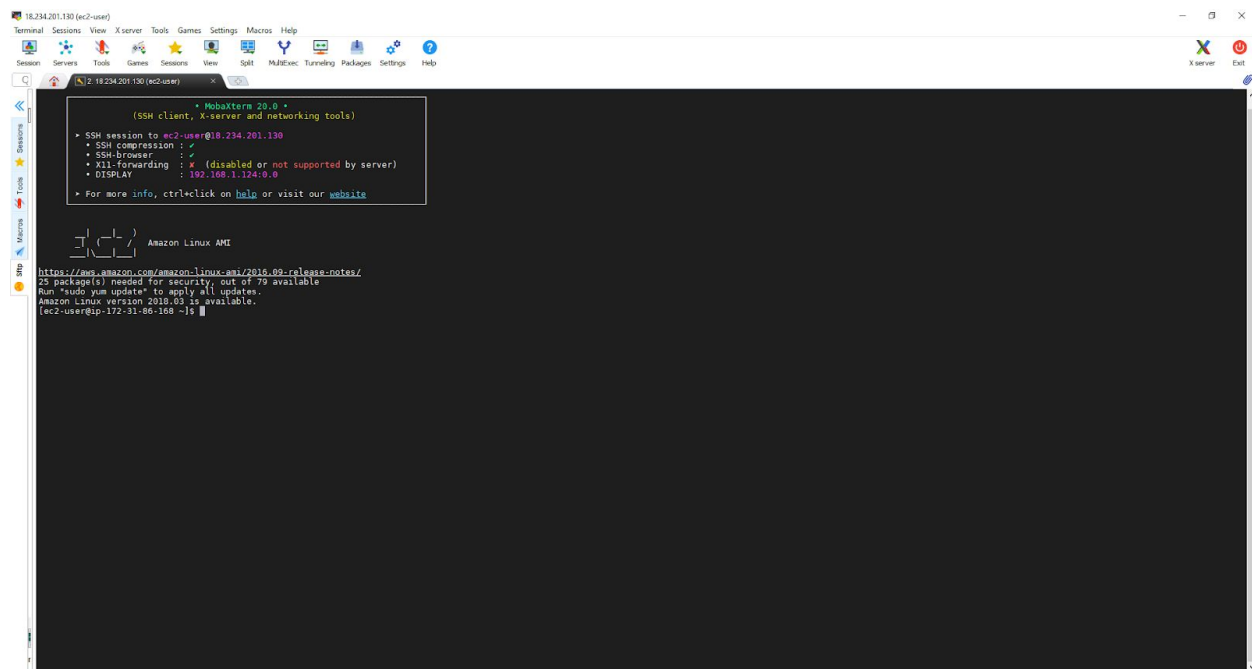
You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

[Cancel](#)

[Launch Instances](#)

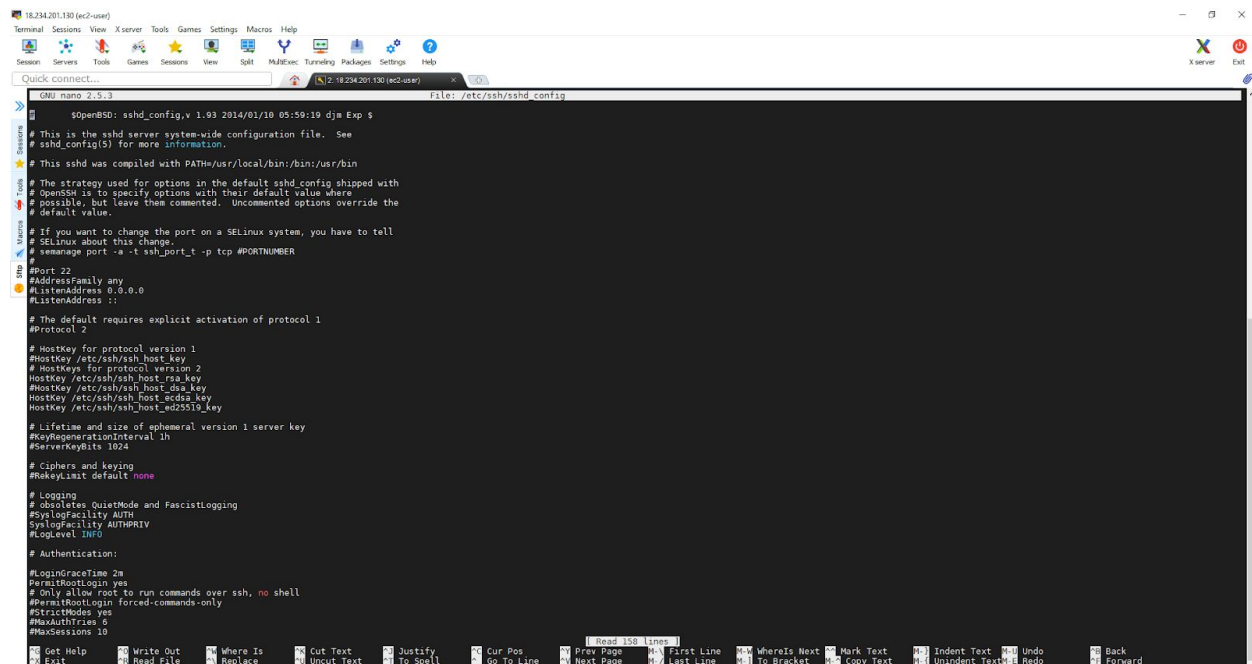
The keypair is required for the EC2 instance remote login.

MobaXterm



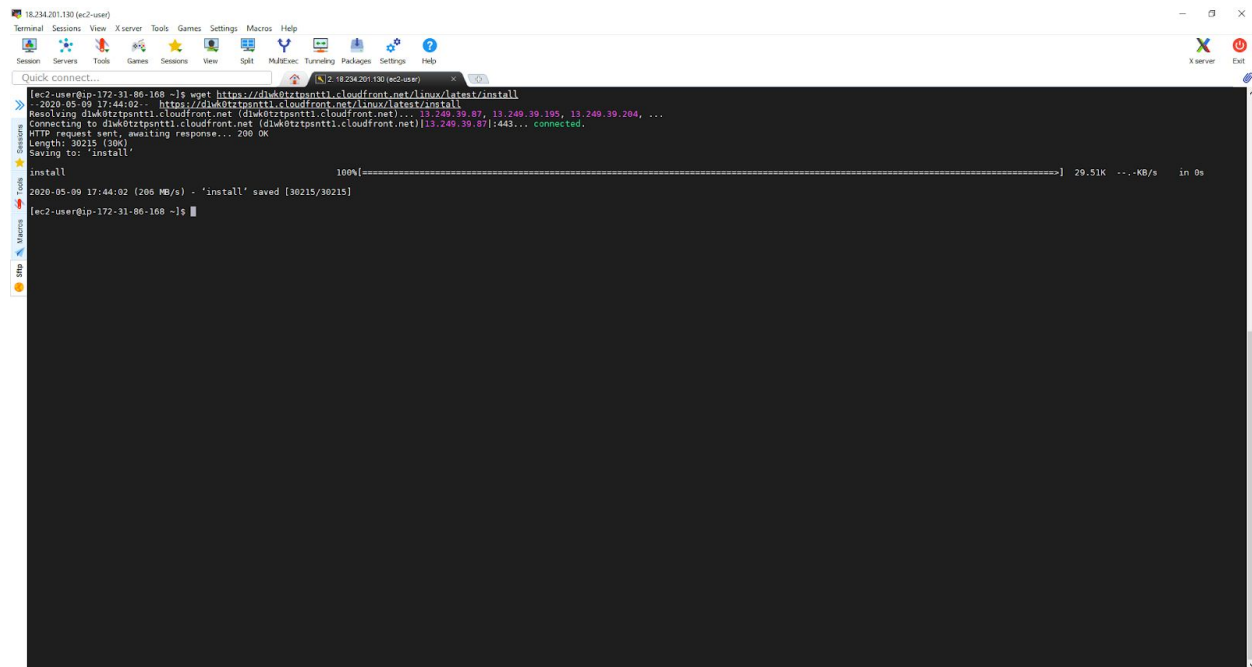
Using the IP4 address of the EC2 instance and the Key Pair, a successful SSH remote login has been established in MobaXterm.

MobaXterm - sshd_config



“PermitRootLogin forced-commands-only” has been commented out. “PermitRootLogin yes” has been uncommented out.

MobaXterm - Inspector Agent Download



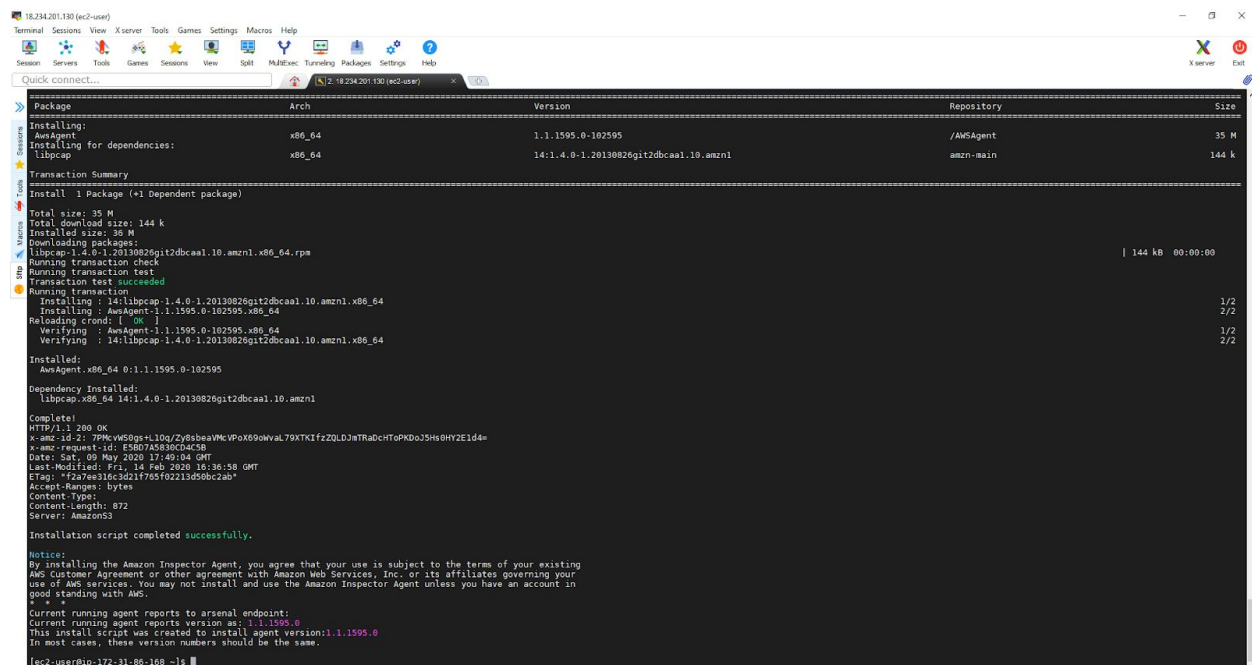
```
18.234.201.130 (ec2-user)
Terminal Sessions View X server Tools Games Settings Macros Help
Quick connect...
[ec2-user@ip-172-31-86-168 ~]$ wget https://dlw0ztzpsntt1.cloudfront.net/linux/latest/install
--2020-05-09 17:44:02-- https://dlw0ztzpsntt1.cloudfront.net/linux/latest/install
Resolving dlw0ztzpsntt1.cloudfront.net (dlw0ztzpsntt1.cloudfront.net)... 13.249.39.87, 13.249.39.195, 13.249.39.204, ...
Connecting to dlw0ztzpsntt1.cloudfront.net (dlw0ztzpsntt1.cloudfront.net)[13.249.39.87]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 30215 (30k)
Saving to: 'install'

install                                     100%[=====] 29.51K  ---KB/s  in 0s
2020-05-09 17:44:02 (205 MB/s) - 'install' saved [30215/30215]

[ec2-user@ip-172-31-86-168 ~]$
```

A download of the Linux Inspector agent to the EC2 instance.

MobaXterm - Bash Script Install

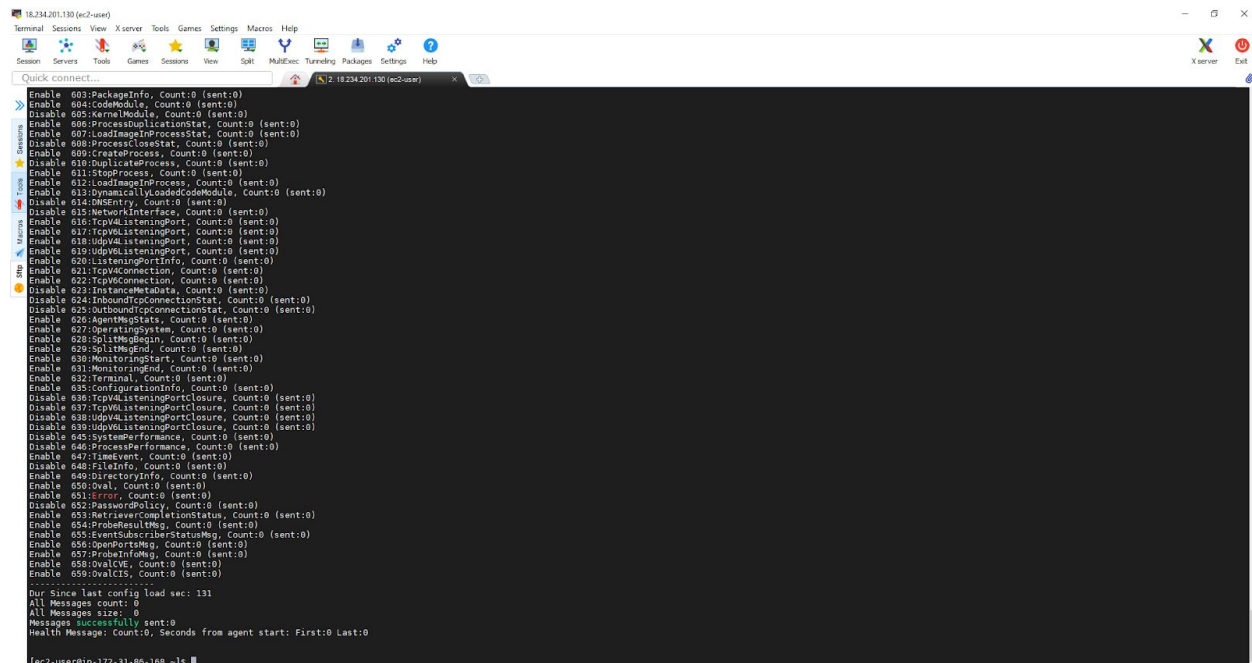


```
18.234.201.130 (ec2-user)
Terminal Sessions View X server Tools Games Settings Macros Help
Quick connect...
Package Arch Version Repository Size
Installing:
AwsAgent x86_64 1.1.1595.0-102595 /AWSAgent 35 M
Installing for dependencies:
libpcap x86_64 14:1.4.0-1.20130826git2dbcaal.10.amzn1 amzn-main 144 k
Transaction Summary
Install 1 Package (+1 Dependent package)
Total size: 35 M
Total download size: 144 k
Installed size: 36 M
Downloading packages:
libpcap-1.4.0-1.20130826git2dbcaal.10.amzn1.x86_64.rpm | 144 kB 00:00:00
Running transaction check
Transaction test succeeded
Running transaction
Installing : 14:libpcap-1.4.0-1.20130826git2dbcaal.10.amzn1.x86_64
Installing : AwsAgent-1.1.1595.0-102595.x86_64 1/2
Reloading crond: [ OK ] 2/2
Verifying : AwsAgent-1.1.1595.0-102595.x86_64 1/2
Verifying : 14:libpcap-1.4.0-1.20130826git2dbcaal.10.amzn1.x86_64 2/2
Installed:
AwsAgent.x86_64 0:1.1.1595.0-102595
Dependency Installed:
libpcap.x86_64 14:1.4.0-1.20130826git2dbcaal.10.amzn1
Complete!
HTTP/1.1: 200 OK
x-amz-id-2: 7PMcVW5GgsL10Q/Zy6sbaeVMcVPoX90Wval79XTKIfZ2LOJ3tRAdChITpKQdJSH6BHY2E1d4=
x-amz-request-id: ES607830BC04C68
Date: Sat, 09 May 2020 17:49:04 GMT
Last-Modified: Fri, 14 Feb 2020 16:36:58 GMT
ETag: "f2a7ee316cd21f7d5f0221d50bc2ab"
Accept-Ranges: bytes
Content-Type:
Content-Length: 872
Server: AmazonS3
Installation script completed successfully.
Notice:
By installing the Amazon Inspector Agent, you agree that your use is subject to the terms of your existing
AWS Customer Agreement or other agreement with Amazon Web Services, Inc. or its affiliates governing your
use of AWS services. You may not install and use the Amazon Inspector Agent unless you have an account in
good standing with AWS.
Current running agent reports to arsenal endpoint:
Current running agent reports version as: 1.1.1595.0
This install script was created to install agent version: 1.1.1595.0
In most cases, these version numbers should be the same.

[ec2-user@ip-172-31-86-168 ~]$
```

The Bash Inspector script has been successfully installed.

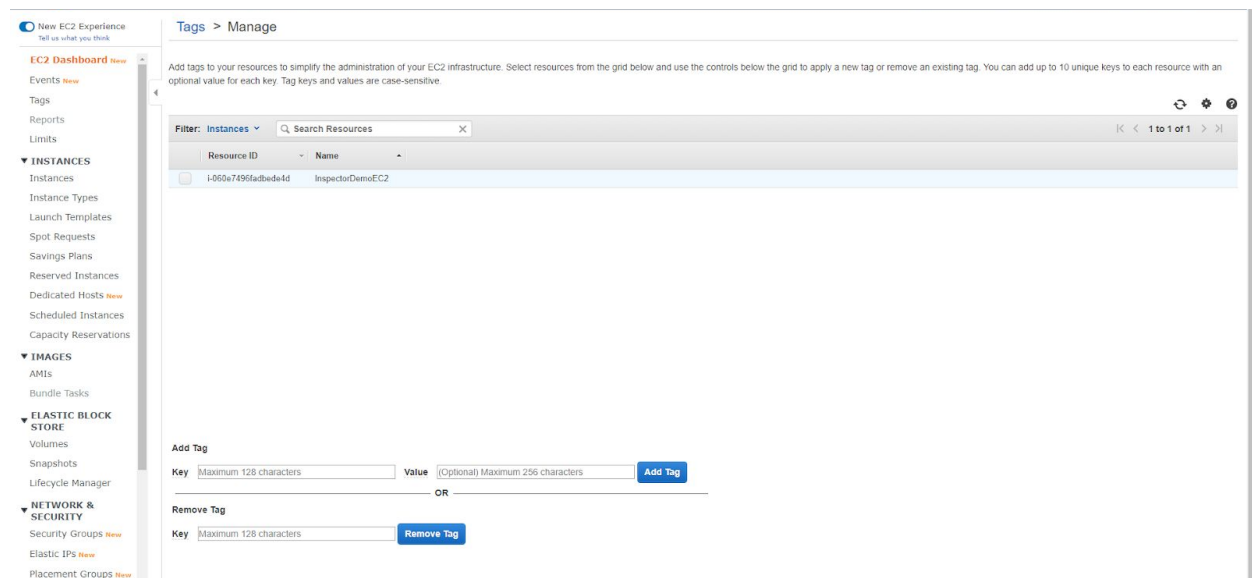
MobaXterm - sudo /opt/aws/awsagent/bin/awsagent status



```
18.234.201.130 (ec2-user)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultExec Tunneling Packages Settings Help
Quick connect...
Enable 603:PackageInfo, Count:0 (sent:0)
Enable 604:CodeModule, Count:0 (sent:0)
Disable 605:KernelModule, Count:0 (sent:0)
Enable 606:ProcessDuplicateLimitStat, Count:0 (sent:0)
Enable 607:LoadImageInProcessStat, Count:0 (sent:0)
Disable 608:ProcessCloseStat, Count:0 (sent:0)
Enable 609:CreateProcess, Count:0 (sent:0)
Disable 610:DuplicateProcess, Count:0 (sent:0)
Enable 611:StopProcess, Count:0 (sent:0)
Enable 612:LoadImageInProcess, Count:0 (sent:0)
Enable 613:DynamicallyLoadedCodeModule, Count:0 (sent:0)
Disable 614:MMEntry, Count:0 (sent:0)
Disable 615:NetworkInterface, Count:0 (sent:0)
Enable 616:TcpV4ListeningPort, Count:0 (sent:0)
Enable 617:TcpV4ListeningPort, Count:0 (sent:0)
Enable 618:UdpV4ListeningPort, Count:0 (sent:0)
Enable 619:UdpV4ListeningPort, Count:0 (sent:0)
Enable 620:ListeningPortInfo, Count:0 (sent:0)
Enable 621:TcpV4Connection, Count:0 (sent:0)
Enable 622:TcpV4Connection, Count:0 (sent:0)
Disable 623:InstanceMetadata, Count:0 (sent:0)
Disable 624:InboundTcpConnectionStat, Count:0 (sent:0)
Disable 625:OutboundTcpConnectionStat, Count:0 (sent:0)
Enable 626:AgentMsgStats, Count:0 (sent:0)
Enable 627:OperatingSystem, Count:0 (sent:0)
Enable 628:SplitMsgBegin, Count:0 (sent:0)
Enable 629:SplitMsgEnd, Count:0 (sent:0)
Enable 630:MonitoringStart, Count:0 (sent:0)
Enable 631:MonitoringEnd, Count:0 (sent:0)
Enable 632:Terminal, Count:0 (sent:0)
Enable 633:ConfigurationInfo, Count:0 (sent:0)
Disable 634:TcpV4ListeningPortClosure, Count:0 (sent:0)
Disable 635:TcpV4ListeningPortClosure, Count:0 (sent:0)
Disable 636:UdpV4ListeningPortClosure, Count:0 (sent:0)
Disable 637:UdpV4ListeningPortClosure, Count:0 (sent:0)
Disable 640:SystemPerformance, Count:0 (sent:0)
Disable 641:ProcessPerformance, Count:0 (sent:0)
Enable 642:FileEvent, Count:0 (sent:0)
Disable 643:FileInfo, Count:0 (sent:0)
Enable 644:DirectoryInfo, Count:0 (sent:0)
Enable 645:Oval, Count:0 (sent:0)
Enable 646:Error, Count:0 (sent:0)
Disable 647:PasswordPolicy, Count:0 (sent:0)
Enable 648:RetrieverCompletionStatus, Count:0 (sent:0)
Enable 649:EventSubscribeStatusMsg, Count:0 (sent:0)
Enable 650:OpenPortsMsg, Count:0 (sent:0)
Enable 651:ProbeInfoMsg, Count:0 (sent:0)
Enable 652:OvalCVE, Count:0 (sent:0)
Enable 653:OvalCIS, Count:0 (sent:0)
Our Since last config load sec: 131
All Messages count: 0
All Messages size: 0
Messages successfully sent: 0
Health Message: Count:0, Seconds from agent start: First:0 Last:0
[ec2-user@ip-172-31-86-168 ~]$
```

Confirmation of AWS Inspector Agent has been installed on the EC2 instance.

EC2 Dashboard - Tags



Inspector requires tags to be defined on the EC2 instance.

Amazon Inspector - Assessment Targets

The screenshot shows the 'Assessment Targets' page in the Amazon Inspector console. The left sidebar contains links to 'Dashboard', 'Assessment targets', 'Assessment templates', 'Assessment runs', and 'Findings'. The main content area is titled 'Assessment Targets' and includes a description: 'An assessment target represents a collection of AWS resources that help you accomplish your business goals. Learn more.' Below this are 'Create', 'Edit', and 'Delete' buttons. A table lists the assessment targets, with one entry 'InspectorTarget' selected. The details for 'InspectorTarget' are shown below the table. The 'Name' field is 'InspectorTarget'. The 'All instances' checkbox is checked, with a note: 'Note: The limit on the maximum number of agents that can be included in an assessment run applies. Learn more.' The 'Use Tags' section has a table with one row: 'InspectorTester' with a value of 'YES'. The 'Install Agents' checkbox is checked, with a note: 'To use this option, make sure that your EC2 instances have the SSM Agent installed and an IAM role that allows Run Command. Learn more.' At the bottom, there are 'Save', 'Cancel', and 'Preview' buttons. A footer note says 'Max records per page: 25' and '* refresh browser to reflect change'.

From Amazon Inspector, select the newly created tags.

Service-Linked Role created for Amazon Inspector

This screenshot shows the same 'Assessment Targets' page as before, but with a modal dialog box open in the center. The dialog is titled 'Service-Linked Role created for Amazon Inspector' and contains the following text: 'Amazon Inspector now uses IAM Service-Linked Roles to describe EC2 instances and EC2 tags for your assessment targets. The Service-Linked Role will be created for you now. Learn more.' Below this text, it specifies the 'IAM role' as 'AWSServiceRoleForAmazonInspector' and notes it was 'Created and managed on your behalf'. The dialog has 'Cancel' and 'OK' buttons. The background page is dimmed, showing the 'InspectorTarget' configuration details.

Notice that a IAM Service-Linked Role will be created for the Administrator account.

Amazon Inspector - Assessment Template

Amazon Inspector - Assessment Template

Dashboard
Assessment targets
Assessment templates
Assessment runs
Findings

SUCCESS
Run command successfully issued to install the Amazon Inspector Agent. You can check the agent status by choosing the Preview Target button or by viewing the Systems Manager Run Command console for more details.

Filter: []

Name	Duration	Target name	Last run	All runs
InspectorTemplate	N/A	InspectorTarget		

Assessment Template - InspectorTemplate

Name: InspectorTemplate

Target name: InspectorTarget

Rules packages: Common Vulnerabilities and Exposures-1.1, Security Best Practices-1.0

Duration: 1 Hour (Recommended)

SNS topics: Select a new SNS topic to notify of events

Tags: InspectorTester: YES

Attributes added to findings: Key, Value

Assessment Schedule: Set up recurring assessment runs once every 7 days. The first run starts on create. Learn more

Create and run, Create, Cancel

The template will search for one hour utilizing two packages.

Amazon Inspector - Assessment Runs

Start: Today at 11:14 AM (GMT-7) (x minute ago)

Tags: InspectorTester: YES

Target name: InspectorTarget

Template name: InspectorTemplate

Rules packages: Common Vulnerabilities and Exposures-1.1, Security Best Practices-1.0

Duration: 1 Hour (Recommended)

Status: Collecting data

Findings: 0

Show AWS agents, Show status

Max records per page: 25

The inspection has started.

Amazon Inspector

The screenshot shows the Amazon Inspector dashboard. On the left is a navigation menu with 'Dashboard' selected, and links for 'Assessment targets', 'Assessment templates', 'Assessment runs', and 'Findings'. The main header area includes the 'Amazon Inspector' title, a brief description, a 'Help me create an Assessment' link, and a 'Notable findings' section with '110 Important findings' and '214 Recent findings'. Below this is the 'Assessment status' section, which shows '0 Assessments running', '1 Assessment run completed', and '0 Assessment runs failed'. At the bottom is the 'Account settings' section with a link to 'Manage Amazon Inspector Service-Linked Role'. On the right, the 'Recent Assessment Runs (Last 10)' table is displayed.

Name	Date Run	Status
Run - InspectorTemplate - 2020-05-09T18:14:22.260Z	Today at 11:14 AM (GMT-7)	Analysis complete

The completed assessment found 214 Findings.

Inspector Findings Report

The screenshot shows a PDF document titled 'Amazon Inspector - Assessment Report Findings Report'. The document is generated on 2020-05-09 at 20:02:57 UTC. It specifies the assessment template as 'InspectorTemplate', the start time as 2020-05-09 at 18:14:24 UTC, and the end time as 2020-05-09 at 19:15:57 UTC. The Amazon Web Services logo is at the top. The PDF is displayed in a browser window with the title '0-ooV4VtH-finding-report.pdf' and a page indicator '1 / 113'.

The finding reports is 113 pages.