



Envío de métricas de instancias EC2 Linux a CloudWatch.

Guía de Procedimiento

Septiembre, 2021.

Contenido

Contenido	2
Objetivo	3
Introducción	3
¿Qué es el agente de CloudWatch?.....	3
El agente de CloudWatch le permite hacer lo siguiente:	3
Sistemas Operativos compatibles para utilizar el agente de CloudWatch.....	3
Proceso de configuración para obtener métricas de desempeño para instancias EC2. ..	4
1) Crear el rol de IAM para utilizar el agente de CloudWatch.....	4
2) Asociar el rol a una instancia para utilizar el agente de CloudWatch.....	9
Configuración del agente de CloudWatch por SSM para instancias Linux.....	10
1) Crear el rol o usuario de IAM para utilizar el agente de CloudWatch.....	10
2) Asociar el rol a una instancia.....	10
3) Conectarse a la instancia e instalar el paquete del agente.	10
4) Modificar el archivo de configuración y seleccionar las métricas.	13
5) Iniciar el agente en los servidores.	18
Configuración manual del agente de CloudWatch para instancias Linux.....	22
1) Crear el rol o usuario de IAM para utilizar el agente de CloudWatch.....	22
2) Asociar el rol a una instancia.....	22
3) Conectarse a la instancia e instalar el paquete del agente.	22
4) Modificar el archivo de configuración y seleccionar metricas.....	25
5) Instalar e iniciar el agente en los servidores.....	26
Agente de CloudHealth	28
Sistemas operativos de servidor compatibles con el agente.	28
1) Instalar y configurara el agente de CloudHealth.....	28
2) Desinstalar y reinstalar el agente de CloudHealth.....	30
Referencias.....	31

Objetivo

El objetivo de este documento es guiarlos en el proceso de configuración del ambiente para obtener métricas de EC2 en CloudWatch. Esto nos permitirá definir alarmas y hacer un análisis de ahorro sobre los recursos, que utilizamos.

Introducción

AWS tiene un servicio de monitoreo administrado, llamado CloudWatch, que nos muestra métricas sobre el desempeño de los sistemas. Para las instancias EC2 existe un agente que nos permite obtener diferentes métricas internas de los servidores y enviarlas al servicio de CloudWatch.

¿Qué es el agente de CloudWatch?

El agente de CloudWatch nos permite recopilar métricas a nivel de sistema y registros de las instancias en lugar de utilizar el AWS Systems Manager Agente (SSM Agent) para estas tareas. El agente de CloudWatch le permite reunir más métricas que el estándar en instancias EC2.

El agente de CloudWatch le permite hacer lo siguiente:

- Recopilar métricas internas de nivel de sistema de instancias Amazon EC2 en distintos sistemas operativos. Las métricas adicionales que se pueden recopilar se indican en [Métricas collected por el CloudWatch agent](#).
- Recupere métricas personalizadas de sus aplicaciones o servicios mediante los protocolos collectd y StatsD. **StatsD** se admite tanto en los servidores Linux como en los servidores Windows Server. **collectd** solo se admite en servidores Linux.

Sistemas Operativos compatibles para utilizar el agente de CloudWatch.

Compatible con la arquitectura x86-64	Compatible con la arquitectura ARM64
<ul style="list-style-type: none">• Amazon Linux versión 2014.03.02 o posterior y Amazon Linux 2• Ubuntu Server 20.04, 18.04, 16.04 y 14.04• CentOS 8.0, 7.6, 7.2 y 7.0• Red Hat Enterprise Linux (RHEL) versiones 8, 7.7, 7.6, 7.5, 7.4, 7.2 y 7.0• Debian versión 10 y versión 8.0• SUSE Linux (SLES) versión 15 y 12.• Oracle Linux versiones 7.8, 7.6 y 7.5• macOS, incluidas las instancias EC2 Mac1• Versiones de 64 bits de Windows Server 2019, Windows Server 2016 y Windows Server 2012.	<ul style="list-style-type: none">• Amazon Linux 2• Ubuntu Server versiones 20.04 y 18.04• Red Hat Enterprise Linux (RHEL) versión 7.6• SUSE Linux Enterprise Server 15.

Proceso de configuración para obtener métricas de desempeño para instancias EC2.

Para utilizar el agente de CloudWatch y poder visualizar las métricas de las instancias **Linux**, debemos seguir el siguiente flujo:

1. **Crear** el rol de IAM con los permisos necesarios para que las instancias puedan enviar las métricas al servicio de CloudWatch.
2. **Asociar** el rol de IAM en la instancia EC2.
3. **Conectarse** a la instancia e **instalar** el paquete del agente.
4. **Modificar** el archivo de configuración del agente de CloudWatch y especificar las métricas que se desea recopilar.
5. **Iniciar** el agente en sus servidores.

1) Crear el rol de IAM para utilizar el agente de CloudWatch.

Antes de instalar el agente de CloudWatch en tu servidor Linux debemos asegurarnos de que nuestras instancias estén administradas por **AWS System Manager**, para ellos debemos crear un rol que proporcionará permisos para leer información de la instancia , escribirla en CloudWatch y que el agente de CloudWatch se comunique con AWS Systems Manager.

1.1 Para crear el rol debemos acceder desde la consola de AWS y seleccionar el servicio “IAM”.

The screenshot shows the AWS Management Console homepage. The top navigation bar includes the AWS logo, Services dropdown, Resource Groups dropdown, a bell icon, AWS Training, Ohio, and Support. The main title is "AWS Management Console". On the left, there's a sidebar titled "AWS services" with a search bar for "Find Services" and a "Recently visited services" section where "IAM" is highlighted with a red box. Below that is a "All services" section listing various AWS services like Compute, EC2, Lightsail, ECR, ECS, EKS, Lambda, Batch, Management & Governance, AWS Organizations, CloudWatch, AWS Auto Scaling, CloudFormation, CloudTrail, Config, AWS Cost Management, AWS Cost Explorer, AWS Budgets, AWS Marketplace, Subscriptions, and Mobile. To the right, there are three boxes: "Access resources on the go" (with a mobile phone icon), "Explore AWS" (with sections for Global Summits, AWS Marketplace, and Amazon SageMaker), and a "Visit AWS around the world at a Summit" section.

1.2 Navegar en el panel del lado izquierdo y seleccionar “Roles”.

The screenshot shows the AWS Identity and Access Management (IAM) dashboard. On the left, there is a sidebar with the following options: Dashboard, Groups, Users, Roles (which is highlighted with a red box), Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area is titled "Welcome to Identity and Access Management". It displays "IAM users sign-in link: https://46676.signin.aws.amazon.com/console" and "Customize". Below this, there's a section for "IAM Resources" showing "Users: 0", "Groups: 0", "Customer Managed Policies: 0", "Roles: 3", and "Identity Providers: 0". Under "Security Status", there are five items with dropdown arrows: "Delete your root access keys" (checked), "Activate MFA on your root account", "Create individual IAM users", "Use groups to assign permissions", and "Apply an IAM password policy". A progress bar indicates "1 out of 5 complete".

1.3 Seleccionar en “Crear Rol”.

The screenshot shows the "Roles (148)" list page. The left sidebar includes "Identity and Access Management (IAM)", "Dashboard", and "Access management" (with "User groups", "Users", and "Roles" listed). The main table lists three roles: "AmazonEC2RunCommandRoleForManagedInstances" (Trusted entities: AWS Service: ssm) and "AutomationServiceRole" (Trusted entities: AWS Service: ssm, and 2 more, Last activity: 6 days ago). At the top right of the table are "Info", "Delete", and "Create role" buttons. A red box highlights the "Create role" button. The bottom of the table has navigation links from 1 to 8 and a settings gear icon.

- 1.4 Seleccionar “**Servicio de AWS**”, y en el caso de uso selecciona “**EC2**” (para que permita a las instancias comunicarse con otros servicios de AWS en su nombre). Seleccione “Siguiente: Permisos”.

Create role

Select type of trusted entity

- AWS service** EC2, Lambda and others
- Another AWS account Belonging to you or 3rd party
- Web identity Cognito or any OpenID provider
- SAML 2.0 federation Your corporate directory

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

Choose a use case

Common use cases

- EC2** Allows EC2 instances to call AWS services on your behalf.
- Lambda Allows Lambda functions to call AWS services on your behalf.

Or select a service to view its use cases

API Gateway	CodeBuild	EMR Containers	IoT SiteWise	RDS
AWS Backup	CodeDeploy	ElastiCache	IoT Things Graph	Redshift
AWS Chatbot	CodeGuru	Elastic Beanstalk	KMS	Rekognition
AWS Marketplace	CodeStar Notifications	Elastic Container Registry	Kinesis	RoboMaker
AWS Support	Comprehend	Elastic Container Service	Lake Formation	S3
Amplify	Config	Elastic Transcoder	Lambda	SMS
AppStream 2.0	Connect	ElasticLoadBalancing	Lex	SNS

* Required

Cancel **Next: Permissions**

- 1.5 Ahora debemos seleccionar el permiso adecuado, en este caso necesitamos agregar el permiso de System Manager (SSM) para que nos permita administrar nuestras instancias. Colocar “SSM” en el filtro de políticas, seleccionar **AmazonSSMManagedInstanceCore** (es la versión actualizada del rol **Amazon EC2RoleforSSM**).

Create role

Attach permissions policies

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

Create policy

Filter policies ▾ Q SSM Showing 20 results

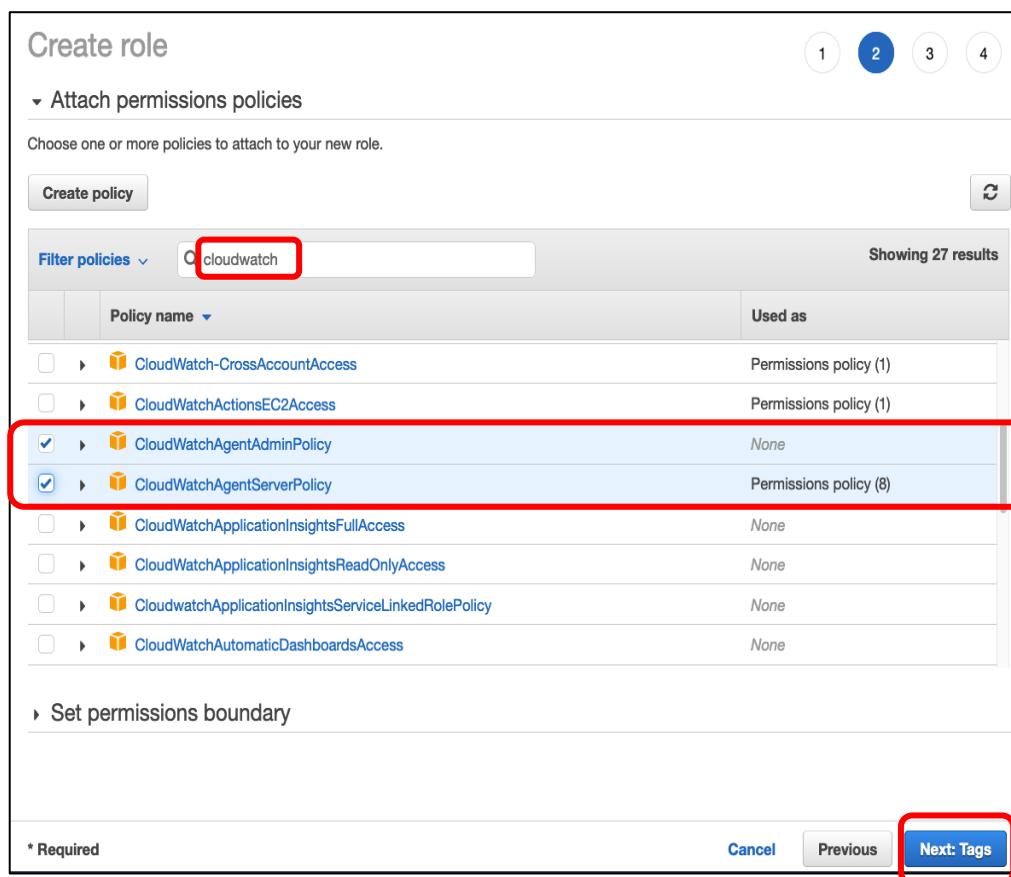
Policy name ▾	Used as
<input checked="" type="checkbox"/> AmazonEC2RoleforSSM	Permissions policy (18)
<input type="checkbox"/> AmazonSSMAutomationApproverAccess	None
<input type="checkbox"/> AmazonSSMAutomationRole	Permissions policy (4)
<input type="checkbox"/> AmazonSSMDirectoryServiceAccess	Permissions policy (2)
<input type="checkbox"/> AmazonSSMFullAccess	Permissions policy (6)
<input type="checkbox"/> AmazonSSMMaintenanceWindowRole	Permissions policy (4)
<input type="checkbox"/> AmazonSSMManagedInstanceCore	Permissions policy (9)
<input type="checkbox"/> AmazonSSMPatchAssociation	None

Set permissions boundary

* Required Cancel Previous **Next: Tags**

1.6 Ahora agregaremos al rol las siguientes Políticas: **CloudWatchAgentServerPolicy** permite que el agente de CloudWatch **se instale en un servidor y envíe métricas a CloudWatch**. **CloudWatchAgentAdminPolicy** es necesaria para almacenar la configuración del agente de CloudWatch “**Parameter Store**” de Systems Manager.

En el filtro de políticas del rol eliminar la palabra SSM y coloque “cloudwatch”, seleccionar “Siguiente: etiquetas” .



Notas.

- I. Al utilizar estas políticas para escribir el archivo de configuración del agente en el “Parameter Store” o para descargarlo del “Parameter Store”, el archivo de configuración del agente debe tener un nombre que empiece por “**AmazonCloudWatch-** ”.
- II. “Parameter Store” permite que varios servidores usen una configuración del agente de CloudWatch.

1.7 Agregar etiquetas (opcionales) a las políticas. Seleccionar Siguiente: Revisión.

Create role

Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. [Learn more](#)

Key	Value (optional)	Remove
Env	PRD	x
Project	Einstein	x

Add new key

You can add 48 more tags.

Cancel Previous **Next: Review**

1.8 Asignar un nombre al rol, confirmar que tenga las políticas deseadas, Seleccionar crear rol.

Create role

Review

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

Role name* **EC2CloudWatchRole**

Use alphanumeric and '+-=_,@-_.' characters. Maximum 64 characters.

Role description Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+-=_,@-_.' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies **AmazonEC2RoleforSSM**, **CloudWatchAgentAdminPolicy**, **CloudWatchAgentServerPolicy**

2) Asociar el rol a una instancia para utilizar el agente de CloudWatch.

Puedes asociar el rol a instancias existentes o bien crear una instancia nueva .

2.1 Asociar el rol a instancias existentes:

- Seleccionar la instancia >> Acciones >> Seguridad >> Modificar el rol IAM.
- Seleccionar el rol que tiene las políticas y permisos que permitan interactuar con el agente de CloudWatch.

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with 'Instances' selected. In the main area, there's a table titled 'Instances (1/3)' with one row. The row has a checkbox checked (highlighted by a red box), the name 'Webserver-CWagent', and an empty 'Instance ID' field. To the right of the table is a 'Actions' dropdown menu with several options: 'Connect', 'View details', 'Manage instance state', 'Instance settings', 'Networking', 'Security' (highlighted by a red box), 'Get Windows password', 'Image and templates', and 'Monitor and troubleshoot'. The 'Modify IAM role' option is also highlighted by a red box.

Nota. El agente de Cloudwatch permite a la instancia enviar métricas a Cloudwatch a través de Systems Manager, por lo que debemos confirmar que la instancia tenga instalado el agente de Systems Manager. Para validar si tu instancia ya tiene preinstalado el agente SSM consulta el siguiente link: <https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-install-ssm-agent.html>

En caso necesario instalar el agente de SSM siguiendo la documentación, seleccionando el sistema operativo que requieras (Amazon Linux 2, CentOS, Debian Server, Oracle Linux, Red Hat,etc.).

Linux:<https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-manual-agent-install.html>

Configuración del agente de CloudWatch por SSM para instancias Linux.

1) Crear el rol o usuario de IAM para utilizar el agente de CloudWatch.

Seguir los pasos indicados en paso 1, página 4.

2) Asociar el rol a una instancia.

Seguir los pasos indicados en el paso 2, página 9.

3) Conectarse a la instancia e instalar el paquete del agente.

A continuación, encontrará la sección para instalar el agente de CloudWatch por **Systems Manager** para Linux.

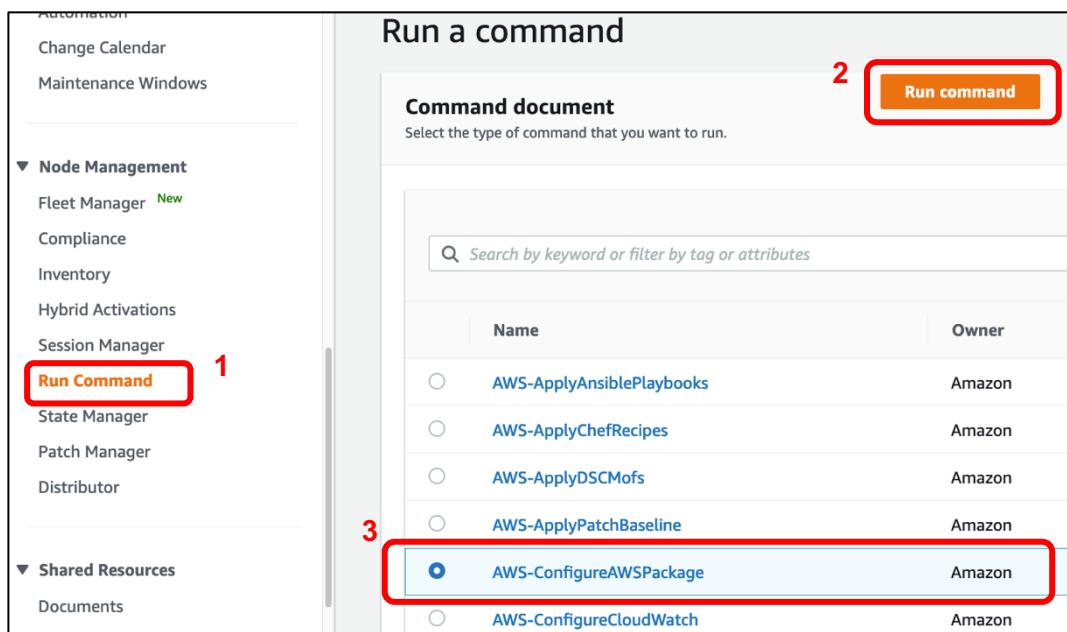
Nota. Utilizar Systems Manager para correr el comando, nos facilita instalar el agente de Cloudwatch en una o mas instancias a la vez, facilitando el proceso en lugar de instalar manualmente el agente en cada una de las instancias que se deseen.

3.1 Ingresar desde la consola de AWS al servicio de *Systems Manager*, seleccionar “**Fleet manager**” y confirmamos que la instancia este corriendo. En versiones anteriores de la interfaz grafica de la consola de AWS lo encontraras como “Managed Instances”.

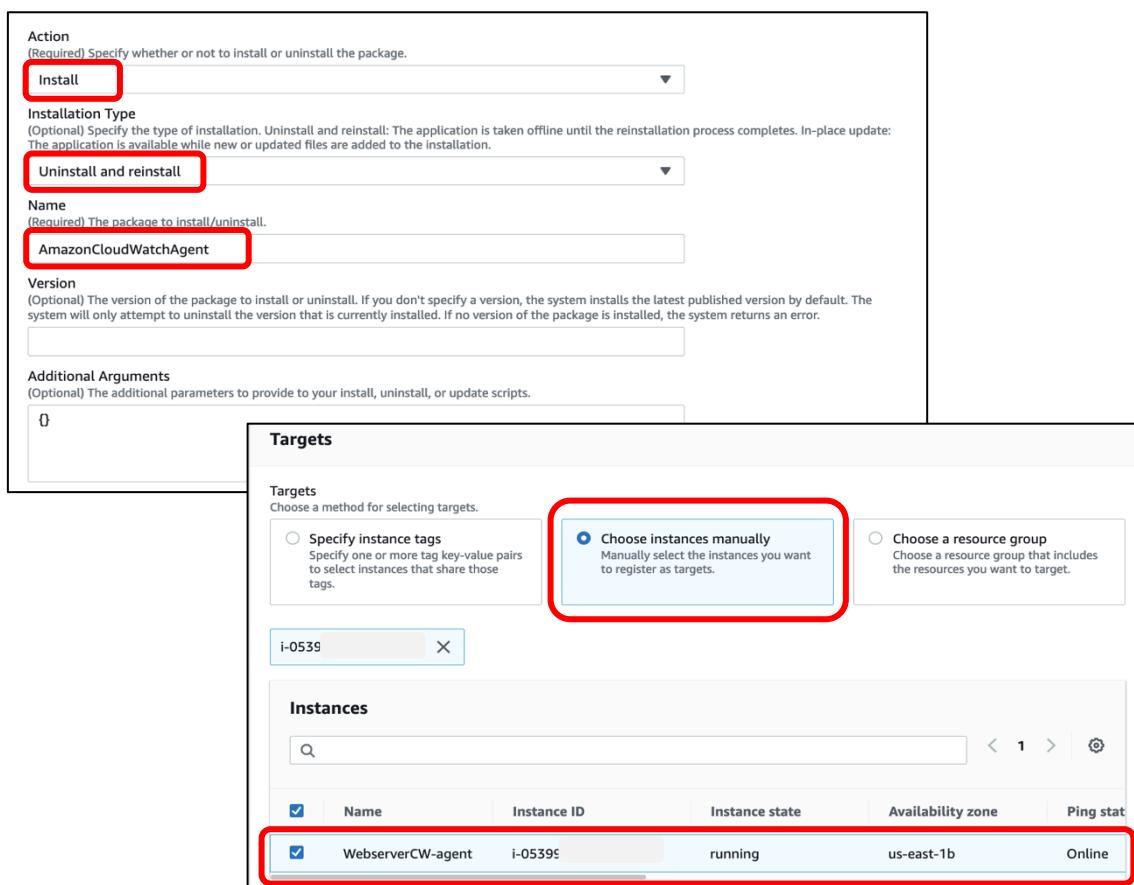
The screenshot shows the AWS Systems Manager Fleet Manager interface. On the left, there's a navigation sidebar with sections for Change Management (Change Manager, Automation, Change Calendar, Maintenance Windows) and Node Management (Fleet Manager, Compliance, Inventory, Hybrid Activations, Session Manager, Run Command, State Manager, Patch Manager, Distributor). The 'Fleet Manager' link is highlighted with a red box. The main panel title is 'Fleet Manager'. Below it, there are two tabs: 'Managed instances' (which is selected and highlighted in orange) and 'Advanced instances'. A search bar is present above the instance list. The instance list table has columns for Instance ID, Instance state, Instance name, and SSM Agent p. One instance is listed: 'i-0539' with 'Running' status, 'WebserverC...' as the name, and 'Online' as the SSM Agent status. The entire table row for this instance is also highlighted with a red box.

Ahora utilizaremos el “Run command” para **instalar** el agente en la instancia por **SSM**.

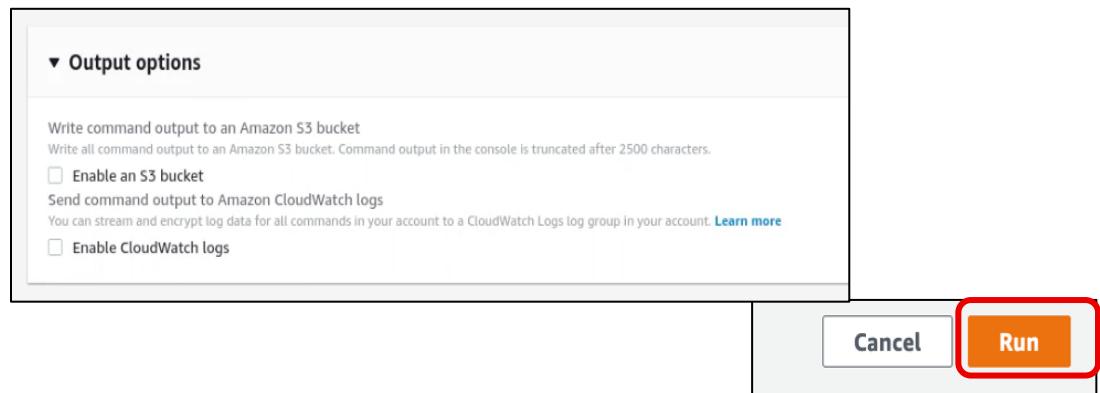
3.1 Seleccionar “Run Command” y elegir **AWS-ConfigureAWSPackage**.



3.2 Desplegar hacia abajo, colocar el nombre **AmazonCloudWatchAgent**, seleccionar la instancia o varias instancias donde queramos instalar el agente de CloudWatch y seleccionar “Run”.



En caso que requieras que escriba en un bucket S3 o Habilitar los logs de Cloudwatch puedes seleccionarlo sino desmarcar la casilla (considerar que podrán generar un costo adicional).



Nota. Puedes seleccionar todas las instancias que deseas instalar el agente de cloudwatch en una sola acción.

3.12 Una vez que se ejecuto el “Run command” se mostrará que el agente se instaló de manera “**exitosa**” y podremos observarlo desde la vista de “output”.

Command ID: 91a49843-69ee-4514-8432-e41171fc1254					
Cancel command Rerun Copy to new					
Command status					
Overall status ✓ Success	Detailed status ✓ Success	# targets 1	# completed 1	# error 0	# delivery timed out 0
Targets and outputs					
View output					
<input type="text"/> Search Previous 1 Next					
Instance ID	Instance name	Status	Detailed Status	Start time	Finish time
i-05		✓ Success	✓ Success	Wed, 25 Aug 2021 06:25:41 GMT	Wed, 25 Aug 2021 06:25:42 GMT

Status Success	Detailed status Success	Response code 0
Step name configurePackage	Start time Wed, 25 Aug 2021 06:25:42 GMT	Finish time Wed, 25 Aug 2021 06:25:57 GMT
▼ Output		
The command output displays a maximum of 48,000 characters. You can view the complete command output in either Amazon S3 or CloudWatch Logs, if you specify an S3 bucket or a logs group when you run the command.		
<pre>Initiating arn:aws:ssm:::package/AmazonCloudWatchAgent 1.247349.0b251399 install Plugin aws:runPowerShellScript ResultStatus Success install output: Running install.ps1 Successfully installed arn:aws:ssm:::package/AmazonCloudWatchAgent 1.247349.0b251399</pre>		
<div style="text-align: right;"> Copy Download </div>		

4) Modificar el archivo de configuración y seleccionar las métricas.

4.1 Conectarse a la instancia mediante SSM.

Instances (1/1) [Info](#)

Filter instances

Name	Instance ID	Instance state	Instance type
Webserver-CWagent	i-06a5	Running	t2.micro

Instance: i-06a5 (Webserver-CWagent)

Actions ▾ [Launch instances](#)

- [Connect](#) 1
- [View details](#)
- [Manage instance state](#)
- [Instance settings](#)
- [Networking](#)
- [Security](#)
- [Image and templates](#)
- [Monitor and troubleshoot](#)

Connect to instance [Info](#)

Connect to your instance i-06a509e9b7570f317 (CWA Dan) using any of these options

EC2 Instance Connect 2 Session Manager SSH client EC2 Serial Console

Session Manager usage:

- Connect to your instance without SSH keys or a bastion host.
- Sessions are secured using an AWS Key Management Service key.
- You can log session commands and details in an Amazon S3 bucket or CloudWatch Logs log group.
- Configure sessions on the Session Manager [Preferences](#) page.

Cancel 3 Connect

4.2 Modificar el archivo de configuración y seleccionar métricas.

Antes de ejecutar el agente de CloudWatch en cualquier servidor, debe crear un **archivo de configuración** del agente, que es un archivo JSON, que especifica las métricas y los registros que el agente debe recopilar. Puede crearlo utilizando el asistente de configuración (Wizard) o escribiéndolo usted mismo desde cero.

Para utilizar el asistente de configuración (Wizard) ejecutar el siguiente comando:
`sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard`

```
sh-4.2$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard
=====
= Welcome to the AWS CloudWatch Agent Configuration Manager =
=====

On which OS are you planning to use the agent?
1. linux
2. windows
3. darwin
default choice: [1]:
1
Trying to fetch the default region based on ec2 metadata...
Are you using EC2 or On-Premises hosts?
1. EC2
2. On-Premises
default choice: [1]:
1
Which user are you planning to run the agent?
1. root
2. cwagent
3. others
default choice: [1]: → Puede utilizar el usuario root o
alguno que tenga creado que
desea utilizar para esta función.

Do you want to turn on StatsD daemon?
1. yes
2. no
default choice: [1]:

Which port do you want StatsD daemon to listen to?
default choice: [8125]

What is the collect interval for StatsD daemon?
1. 10s
2. 30s
3. 60s
default choice: [1]:

What is the aggregation interval for metrics collected by StatsD daemon?
1. Do not aggregate
2. 10s
3. 30s
4. 60s
default choice: [4]:

Do you want to monitor metrics from CollectD?
1. yes
2. no
default choice: [1]:

Do you want to monitor any host metrics? e.g. CPU, memory, etc.
1. yes
2. no
default choice: [1]:

Do you want to monitor cpu metrics per core? Additional CloudWatch charges may apply.
1. yes
2. no
default choice: [1]:
```

```

Do you want to monitor any host metrics? e.g. CPU, memory, etc.
1. yes
2. no
default choice: [1]: → Si se habilita generaría un costo adicional.

Do you want to monitor cpu metrics per core? Additional CloudWatch charges may apply.
1. yes
2. no
default choice: [1]: →

Do you want to add ec2 dimensions (ImageId, InstanceId, InstanceType, AutoScalingGroupName) into all of your metrics i
1. yes
2. no
default choice: [1]: →

Would you like to collect your metrics at high resolution (sub-minute resolution)? This enables sub-minute resolution
1. 1s
2. 10s
3. 30s
4. 60s
default choice: [4]: →

Which default metrics config do you want?
1. Basic
2. Standard
3. Advanced
4. None
default choice: [1]: → Dependrá el tipo de métricas que se desea instalar. Puedes consultar la siguiente tabla para definir tus métricas.
3

```

Nota. En la siguiente tabla se muestra la lista de Métricas disponibles para configurar el agente de CloudWatch.

Amazon EC2 instances running Linux

Detail level	Metrics included
Basic	Mem: mem_used_percent Disk: disk_used_percent The disk metrics such as <code>disk_used_percent</code> have a dimension for <code>Partition</code> , which means that the number of custom metrics generated is dependent on the number of partitions associated with your instance. The number of disk partitions you have depends on which AMI you are using and the number of Amazon EBS volumes you attach to the server.
Standard	CPU: cpu_usage_idle, cpu_usage_iowait, cpu_usage_user, cpu_usage_system Disk: disk_used_percent, disk_inodes_free Diskio: diskio_io_time Mem: mem_used_percent Swap: swap_used_percent

Advanced	CPU: cpu_usage_idle, cpu_usage_iowait, cpu_usage_user, cpu_usage_system Disk: disk_used_percent, disk_inodes_free Diskio: diskio_io_time, diskio_write_bytes, diskio_read_bytes, diskio_writes, diskio_reads Mem: mem_used_percent Netstat: netstat_tcp_established, netstat_tcp_time_wait Swap: swap_used_percent
-----------------	---

Listas de Métricas disponibles para la configuración (Linux EC2 y Linux On- Premise):
<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/create-cloudwatch-agent-configuration-file-wizard.html>

4.3 Validar el documento de configuración del agente de Cloudwatch.

Una vez que seleccionaste el tipo de Métricas que deseas configurar, obtendrás un archivo Json como el que se muestra en la siguiente imagen, para tu revisión y aprobación.

```
Current config as follows:
{
  "agent": {
    "metrics collection interval": 60,
    "run as user": "root"
  },
  "metrics": {
    "append dimensions": {
      "AutoScalingGroupName": "${aws:AutoScalingGroupName}",
      "ImageId": "${aws:ImageId}",
      "InstanceId": "${aws:InstanceId}",
      "InstanceType": "${aws:InstanceType}"
    },
    "metrics collected": {
      "collectd": {
        "metrics aggregation interval": 60
      },
      "cpu": {
        "measurement": [
          "cpu usage idle",
          "cpu usage iowait",
          "cpu usage user",
          "cpu usage system"
        ],
        "metrics collection interval": 60,
        "resources": [
          "*"
        ],
        "totalcpu": false
      },
      "disk": {
        "measurement": [
          "used percent",
          "inodes free"
        ],
        "metrics collection interval": 60,
        "resources": [
          "*"
        ]
      },
      "diskio": {
        "measurement": [
          "io time",
          "write bytes",
          "read bytes",
          "writes",
          "reads"
        ],
        "metrics collection interval": 60,
        "resources": [
          "*"
        ]
      }
    }
  }
}
```

```

Are you satisfied with the above config? Note: it can be manually customized after the wizard completes to add additional items.
1. yes
2. no
default choice: [1]: [1]

Do you have any existing CloudWatch Log Agent (http://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AgentReference.html) configuration file?
1. yes
2. no
default choice: [2]: [2]

Do you want to monitor any log files?
1. yes
2. no
default choice: [1]: [1]

```

Dependerá si cuentas con un agente de Logs de Cloudwatch y si deseas monitorear los archivos de logs de lo contrario seleccionar que no.

4.4 Almacenar el archivo de configuración en “Parameter Store”.

```

Please check the above content of the config.
The config file is also located at /opt/aws/amazon-cloudwatch-agent/bin/config.json. /opt/aws/amazon-cloudwatch-agent/bin/config.json →
Edit it manually if needed.

Do you want to store the config in the SSM parameter store?
1. yes
2. no
default choice: [1]: [1]

What parameter store name do you want to use to store your config? (Use 'AmazonCloudWatch-' prefix if you use our managed AWS policy)
default choice: [AmazonCloudWatch-linux] AmazonCloudWatch-demo

Trying to fetch the default region based on ec2 metadata...
Which region do you want to store the config in the parameter store?
default choice: [us-east-1]

Which AWS credential should be used to send json config to parameter store?
1. ASIAULEHRFSP44Y6UCJA(From SDK)
2. Other
default choice: [1]: [1]

Successfully put config to parameter store AmazonCloudWatch-demo.
Program exits now.

```

La configuración quedará guardada en esa dirección.

Si se cuentan con credenciales se pueden utilizar, de lo contrario seleccionar la credencial que se genera por default.

Notas.

- El nombre del parameter store debe llevar la siguiente nomenclatura “AmazonCloudWatch-XXX”
- Al decidir almacenar el archivo de configuración en el “Systems Manager Parameter Store” permite configurar tantos servidores o instancias como se requiera con la misma configuración del agente de CloudWatch.

4.5 Una vez que ya no se requiere transmitir el archivo de configuración hacia el “Parameter Store” se recomienda eliminar, del rol, la política **CloudWatchAgentAdminPolicy** por buenas prácticas de seguridad. Para eliminar la política:

>> Ingresar a IAM >> Seleccionar el rol >> Editar >> Eliminar la política.

4.6 Validar la configuración del agente (Config File) en Parameter Store.

Desde la consola de AWS >> Systems Manager >> Parameter Store >> Filtar por el nombre de archivo de configuración que seleccionamos.

The screenshot shows the AWS Systems Manager Parameter Store. On the left sidebar, under 'Operations Management', 'Parameter Store' is highlighted with a red box. In the main 'My parameters' section, there is a search bar and a filter bar with the text 'Name: contains: AmazonCloudWatch-demo'. Below these, a table lists parameters, with one row for 'AmazonCloudWatch-demo' selected and highlighted with a red box. The table includes columns for Name, Tier, and Type (Standard).

5) Iniciar el agente en los servidores.

5.1 Seleccionar Actions >> Run Command >> Seleccionar AmazonCloudWatch-ManageAgent.

The screenshot shows the AWS Systems Manager Run Command interface. On the left sidebar, under 'Actions', 'Run Command' is highlighted with a red box. In the main 'Run a command' section, there is a 'Command document' section with a search bar and a filter bar. A radio button next to 'AmazonCloudWatch-ManageAgent' is selected and highlighted with a red box. Below this, there is a 'Description' field.

5.2 En “Optional Configuration Location” colocar el nombre del archivo de configuración que se creo en el “Parameter Store” >> Seleccionar la instancia de forma manual >> Seleccionar “Run”.

Command parameters

Action
The action CloudWatch Agent should take.

Mode
Controls platform-specific default behavior such as whether to include EC2 Metadata in metrics.

Optional Configuration Source
Only for 'configure' related actions. Use 'ssm' to apply a ssm parameter as config. Use 'default' to apply default config for amazon-cloudwatch-agent. Use 'all' with 'configure (remove)' to clean all configs for amazon-cloudwatch-agent.

Optional Configuration Location
Only for 'configure' related actions. Only needed when Optional Configuration Source is set to 'ssm'. The value should be a ssm parameter name.

Optional Open Telemetry Collector Configuration Source
Only for 'configure' related actions. Use 'ssm' to apply a ssm parameter as config. Use 'default' to apply default config for amazon-cloudwatch-agent. Use 'all' with 'configure (remove)' to clean all configs for amazon-cloudwatch-agent. It does not support MacOS instance.

Optional Open Telemetry Collector Configuration Location
Only for 'configure' related actions. Only needed when Optional Configuration Source is set to 'ssm'. The value should be a ssm parameter name. It does not support MacOS instance.

Optional Restart
Only for 'configure' related actions. If 'yes', restarts the agent to use the new configuration. Otherwise the new config will only apply on the next agent restart.

Targets

Targets
Choose a method for selecting targets.

Specify instance tags
Specify one or more tag key-value pairs to select instances that share those tags.

Choose instances manually
Manually select the instances you want to register as targets.

Choose a resource
Choose a resource group

Run command

5.3 Es probable que al momento de ejecutar el comando, nos arroje el siguiente error:

Command ID: 26d5e1b9-f202-463a-acb2-4596285925d8			
Command status			
Overall status ✖ Failed	Detailed status ✖ Failed	# targets 1	# completed 1
Targets and outputs			
<input type="text" value="Q"/>	Instance ID	Instance name	Status
<input type="radio"/> i-06a	ip-10-0-1-154.ec2.internal	✖ Failed	✖ Failed

Esto nos indica que la carpeta **collectd** no se encuentra ya que es un archivo que debe crearse en caso de marchar error. Es un error esperado que está documentado y deberá remediarlo de la siguiente manera:

Correr en la terminal de la instancia el siguiente comando:

```
sudo su
```

```
mkdir -p /usr/share/collectd/; touch /usr/share/collectd/types.db
```

Ahora nos regresamos al comando que fallo en Systems Manager y seleccionamos “Rerun”.

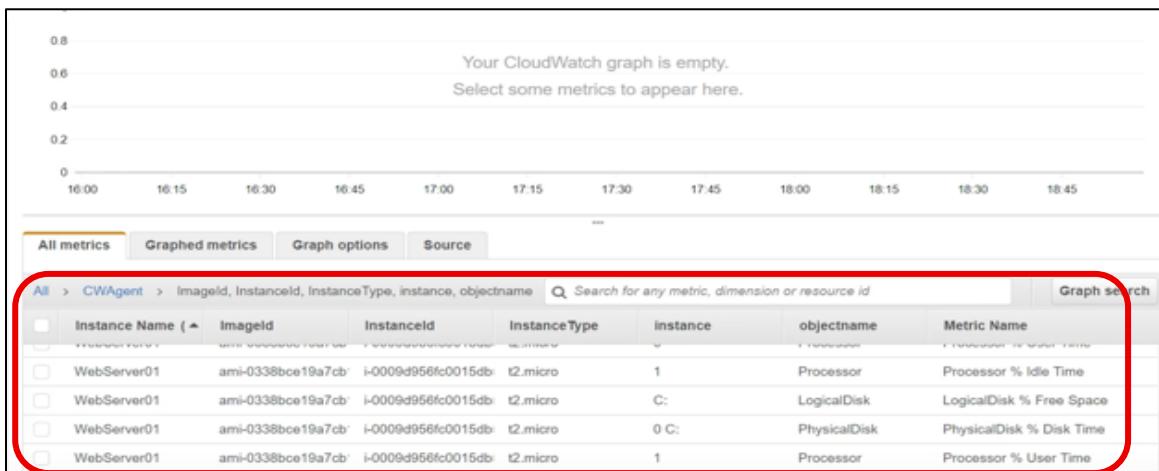
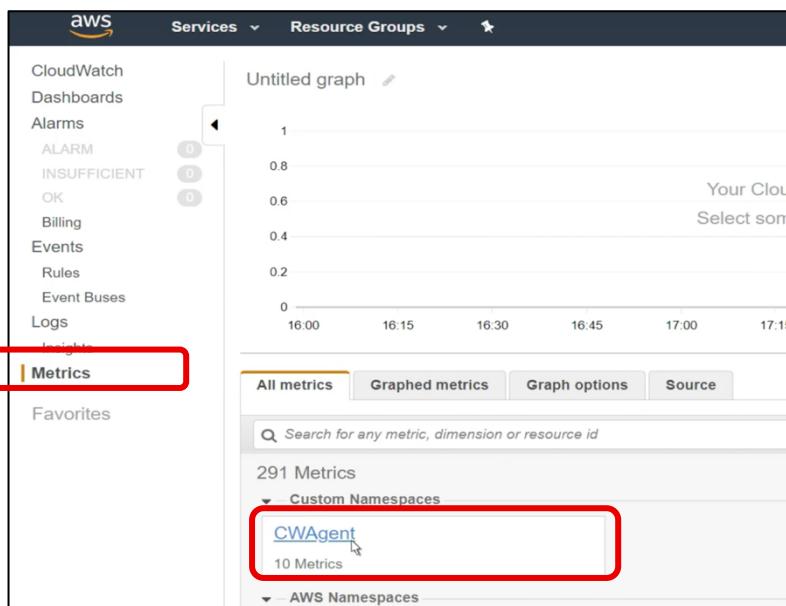
The screenshot shows the AWS Systems Manager interface for a failed command. The top navigation bar includes 'AWS Systems Manager > Run Command > Command ID: 26d5e1b9-f202-463a-acb2-4596285925d8'. Below this, the 'Command status' section shows an overall status of 'Failed' and a detailed status of 'Failed'. The 'Targets and outputs' section lists one instance (i-06a509e9b7570f317) with a status of 'Failed' and a detailed status of 'Failed'. A red box highlights the 'Rerun' button at the top right of the command details.

Y deberá ejecutarse de manera exitosa:

The screenshot shows the AWS Systems Manager interface for a successful command. The top navigation bar includes 'AWS Systems Manager > Run Command > Command ID: 9ec4580f-c8ff-4122-aebb-57331b4036b2'. Below this, the 'Command status' section shows an overall status of 'Success' and a detailed status of 'Success'. The 'Targets and outputs' section lists one instance (i-06a509e9b7570f317) with a status of 'Success' and a detailed status of 'Success'. All metrics in the status sections show a value of 1.

Nota. Cada vez que cambie el archivo de configuración del agente, debe reiniciar el agente para que los cambios surtan efecto.

5.4 Finalmente, al cabo de 5 minutos aproximadamente, podremos validar que se muestran las métricas recolectadas en CloudWatch.



Aquí encontraras todas las métricas que serán capturadas por el agente de CloudWatch incluyendo métricas del procesador, memoria, disco y mas.

Configuración manual del agente de CloudWatch para instancias Linux.

Nota. Este procedimiento seguirá el mismo flujo de instalación mencionado en la página No.4.

1) Crear el rol o usuario de IAM para utilizar el agente de CloudWatch.

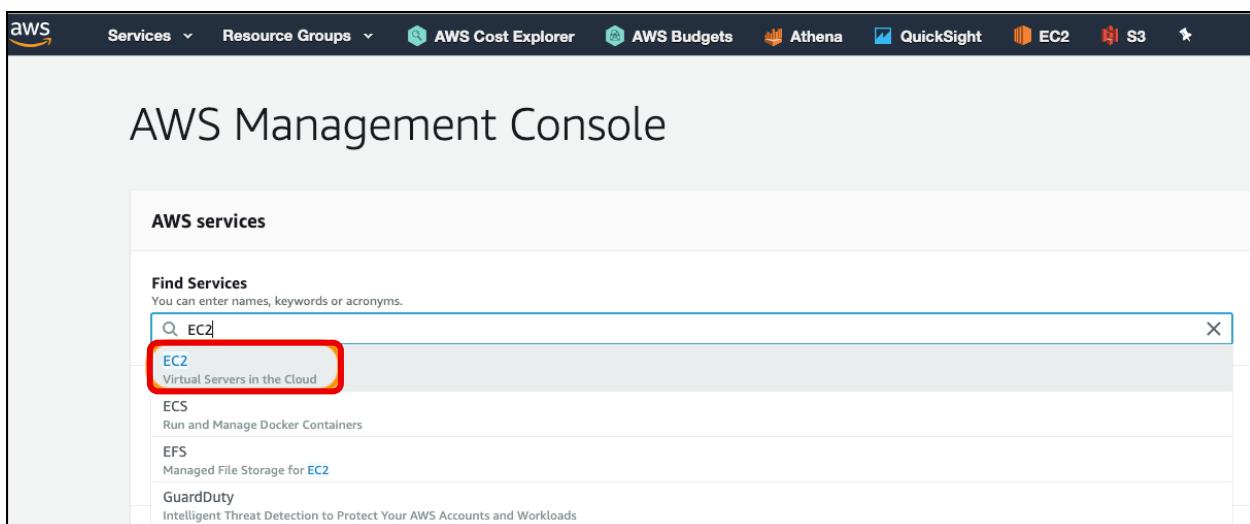
Seguir los pasos indicados en la sección del paso 1, página 4.

2) Asociar el rol a una instancia.

Seguir los pasos indicados en la sección del paso 2, página 9.

3) Conectarse a la instancia e instalar el paquete del agente.

3.1 Desde la consola de AWS, seleccionar el servicio de EC2.



3.1 Conectarse a la instancia, que previamente le asociamos el rol con la política [CloudWatchAgentServerPolicy](#), y seguir el procedimiento de comandos en la terminal. En este ejemplo se mostrará la conexión por SSH.

The screenshot shows the AWS EC2 Instances page. On the left sidebar, under the 'Instances' section, 'Instances' is highlighted with a red box. In the main content area, a table lists three instances. The first instance, 'Webserver-CWagent', has a checked checkbox and is highlighted with a red box. At the top right of the table, there is a 'Connect' button, which is also highlighted with a red box. Below the table, there are three tabs: 'EC2 Instance Connect', 'Session Manager', and 'SSH client'. The 'SSH client' tab is highlighted with a red box. The 'Instance ID' field below shows 'i-01b19842'. A numbered list provides instructions for connecting via SSH:

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is testdan.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
chmod 400 testdan.pem
4. Connect to your instance using its Public DNS:
ec2-34-2.compute-1.amazonaws.com

Below the instructions, there is an 'Example:' section with a command line example:

```
ssh -i "testdan.pem" ec2-user@ec2-34-2.compute-1.amazonaws.com
```

A note in a box states: **Note:** In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

3.4 Una vez conectados a la instancia, la terminal se verá como la siguiente imagen:

The screenshot shows a terminal window with the URL 'console.aws.amazon.com/ec2/v2/connect/ec2-user/i-0e196...' in the address bar. The terminal output shows:

```
Last login: Tue Nov 26 00:25:34 2019 from ec2-18-206-... .amazonaws.com
[ec2-user@ip-172-...] ~]$
```

The terminal prompt shows the user is connected to an Amazon Linux 2 AMI instance.

3.2 Descargar la paquetería del agente de CloudWatch para **Linux** con el siguiente comando:

```
wget https://s3.amazonaws.com/amazoncloudwatch-agent/linux/amd64/latest/AmazonCloudWatchAgent.zip
```

```
[ec2-user@ip-172-1-75-125 ~]$ wget https://s3.amazonaws.com/amazoncloudwatch-agent/linux/amd64/latest/AmazonCloudWatchAgent.zip
--2019-11-26 01:18:08-- https://s3.amazonaws.com/amazoncloudwatch-agent/linux/amd64/latest/AmazonCloudWatchAgent.zip
Resolving s3.amazonaws.com (s3.amazonaws.com)... 52.216.133.237
Connecting to s3.amazonaws.com (s3.amazonaws.com)|52.216.133.237|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 117860791 (112M) [application/zip]
Saving to: 'AmazonCloudWatchAgent.zip'

100%[=====] 2019-11-26 01:18:09 (96.1 MB/s) - 'AmazonCloudWatchAgent.zip' saved [117860791/117860791]

[ec2-user@ip-172-1-75-125 ~]$
```

3.3 Descomprimir e instalar la paquetería del agente.

```
unzip AmazonCloudWatchAgent.zip
```

```
sudo ./install.sh
```

```
[ec2-user@ip-172-1-75-125 ~]$ unzip AmazonCloudWatchAgent.zip
Archive: AmazonCloudWatchAgent.zip
  inflating: amazon-cloudwatch-agent.deb
  inflating: install.sh
  inflating: manifest.json
  inflating: detect-system.sh
  inflating: uninstall.sh
  inflating: amazon-cloudwatch-agent.rpm
[ec2-user@ip-172-1-75-125 ~]$ sudo ./install.sh
create group cwagent, result: 0
create user cwagent, result: 0
[ec2-user@ip-172-1-75-125 ~]$
```

4) Modificar el archivo de configuración y seleccionar metricas.

Antes de ejecutar el agente de CloudWatch en cualquier servidor, debe crear un **archivo de configuración** del agente de CloudWatch (archivo JSON), que especifica las métricas y los registros que el agente debe recopilar, incluidas las métricas personalizadas. Puede crearlo utilizando el asistente de configuración (Wizard) o escribiéndolo usted mismo desde cero.

4.1 Para utilizar el asistente de configuración ejecutar el siguiente comando:

```
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard
```

```
[ec2-user@ip-172- ~]$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard
=====
= Welcome to the AWS CloudWatch Agent Configuration Manager =
=====
On which OS are you planning to use the agent?
1. linux
2. windows
default choice: [1]:
```

En este ejemplo seleccionamos todos los parametros del wizard por default.

4.2 El archivo de configuración del agente de CloudWatch debería tener el siguiente aspecto:

```
{
    "agent": {
        "metrics_collection_interval": 60,
        "run_as_user": "cwagent"
    },
    "metrics": {
        "append_dimensions": {
            "AutoScalingGroupName": "${aws:AutoScalingGroupName}",
            "ImageId": "${aws:ImageId}",
            "InstanceId": "${aws:InstanceId}",
            "InstanceType": "${aws:InstanceType}"
        },
        "metrics_collected": {
            "disk": {
                "measurement": [
                    "used_percent"
                ],
                "metrics_collection_interval": 60,
                "resources": [
                    "*"
                ]
            },
            "mem": {
                "measurement": [
                    "mem_used_percent"
                ],
                "metrics_collection_interval": 60
            }
        }
    }
}
```

5) Iniciar el agente en los servidores.

5.1 Para iniciar el Agente de CloudWatch, ejecutar el siguiente comando:

```
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json -s
```

```
[ec2-user@ip-172-16-1-15 ~]$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json -s
/opt/aws/amazon-cloudwatch-agent/bin/config-downloader --output-dir /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d --download-source file:/opt/aws/amazon-cloudwatch-agent/bin/config.json --mode ec2 --config /opt/aws/amazon-cloudwatch-agent/etc/common-config.toml --multi-config default
Successfully fetched the config and saved in /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp
Start configuration validation...
/opt/aws/amazon-cloudwatch-agent/bin/config-translator --input /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json --input-dir /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d --output /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml --mode ec2 --config /opt/aws/amazon-cloudwatch-agent/etc/common-config.toml --multi-config default
2019/11/26 07:29:20 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp ...
Valid Json input schema.
! Detecting runasuser...
No csm configuration found.
No log configuration found.
Configuration validation first phase succeeded
/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -schematest -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml
Configuration validation second phase succeeded
Configuration validation succeeded
Created symlink from /etc/systemd/system/multi-user.target.wants/amazon-cloudwatch-agent.service to /etc/systemd/system/amazon-cloudwatch-agent.service.
Redirecting to /bin/systemctl restart amazon-cloudwatch-agent.service
[ec2-user@ip-172-16-1-15 ~]$
```

5.2 Es muy probable que al momento de ejecutar el comando, nos arroje el siguiente error: [/usr/share/collectd not found](#)

Nos indica que la carpeta [collectd](#) no se encuentra ya que es un archivo que debe crearse en caso de marchar error. Es un error esperado que está documentado y deberá remediarlo de la siguiente manera:

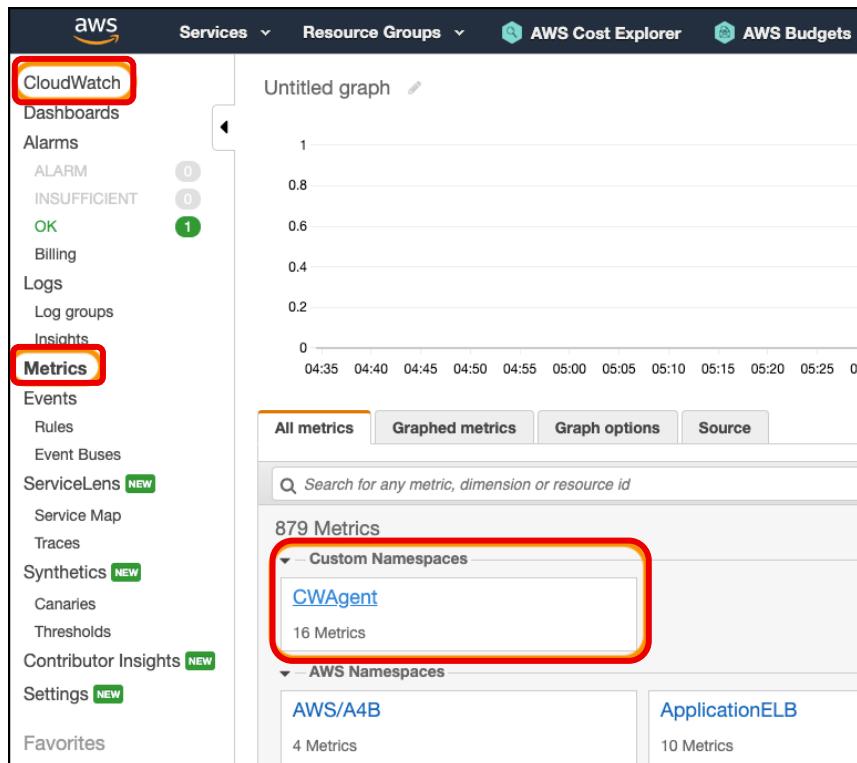
Correr en la consola de la instancia el siguiente comando:

```
sudo su
```

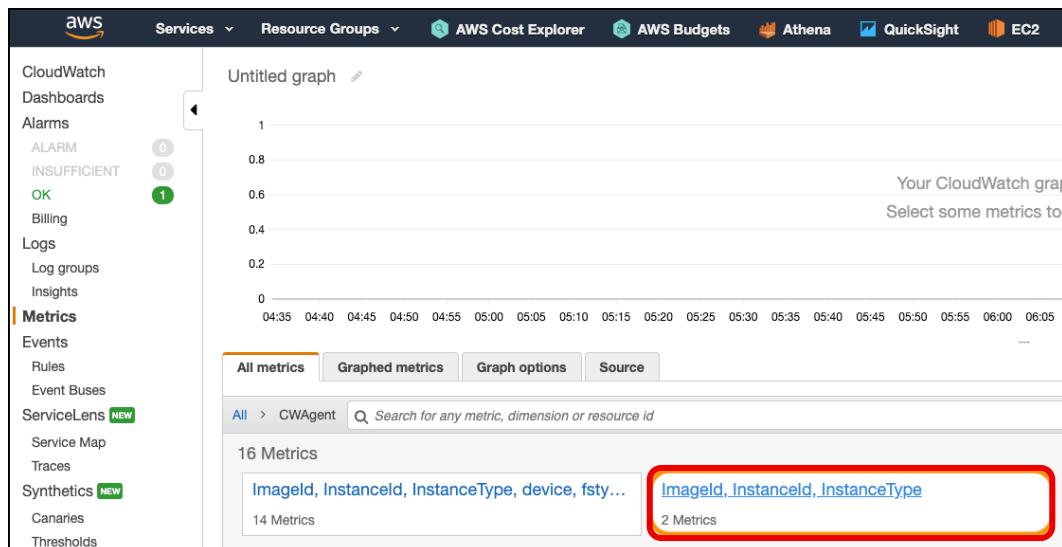
```
mkdir -p /usr/share/collectd/; touch /usr/share/collectd/types.db
```

Nota. Cada vez que cambie el archivo de configuración del agente, debe reiniciar el agente para que los cambios surtan efecto.

5.3 Para validar que se están capturando los datos a través del agente, desde la consola de AWS seleccionamos el Servicio de **CloudWatch**. Ahora podremos ver las diferentes métricas y logs.



5.4 Puedes visualizar en grafica las diferentes métricas y logs dependiendo el intervalo de tiempo en el que se hayan creado.



Finalmente se completo el proceso para enviar métricas de las Instancias EC2 a CloudWatch, instalando de manera manual el Agente de CloudWatch.

Agente de CloudHealth

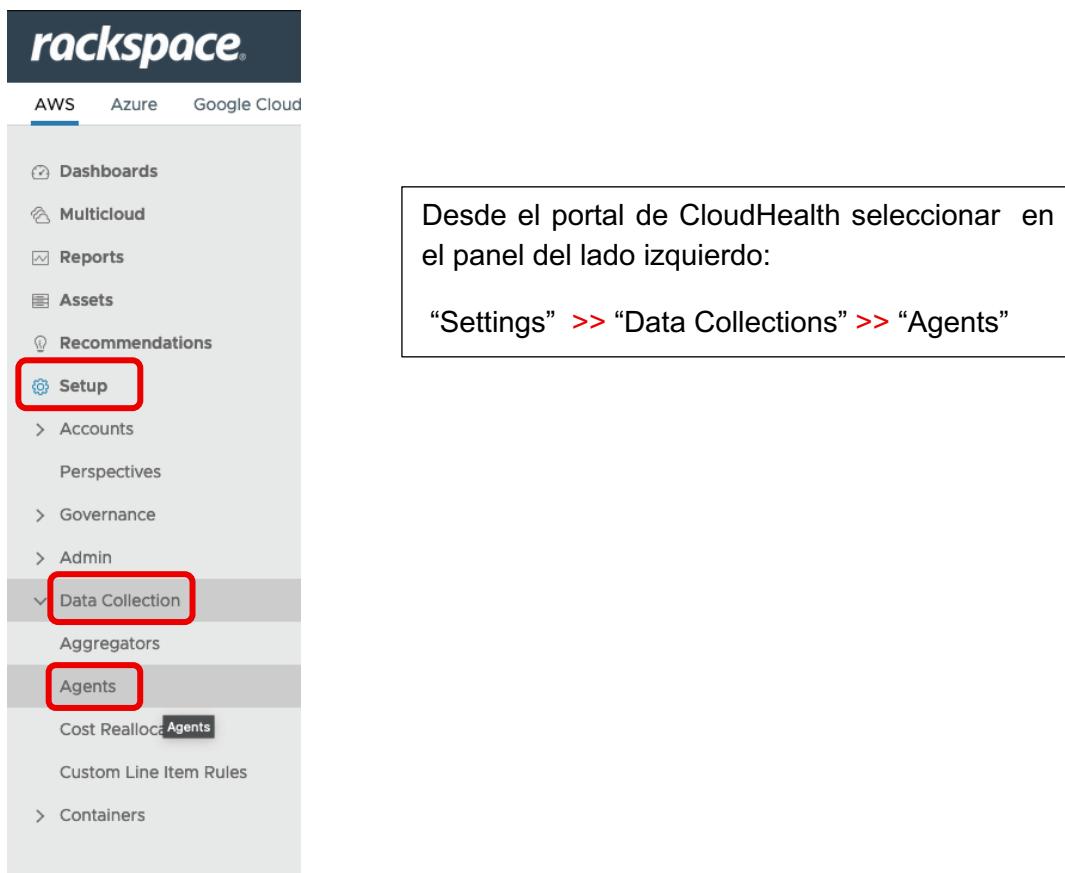
CloudHealth Agent es un servicio de monitoreo ligero para sus recursos en la nube. Puede instalar el Agente en sus instancias en la nube para obtener métricas de CPU, memoria y sistema de archivos del sistema operativo de la instancia. Si tiene Docker, el agente también cataloga los contenedores y las imágenes.

Una vez instalado, el agente toma instantáneas a intervalos específicos e informa métricas a la plataforma CloudHealth cada hora. El agente envía datos desde la instancia al punto final de CloudHealth a través de https. Los datos tienen la forma de un archivo JSON que contiene la E / S de disco agregada, el sistema de archivos y las métricas de memoria.

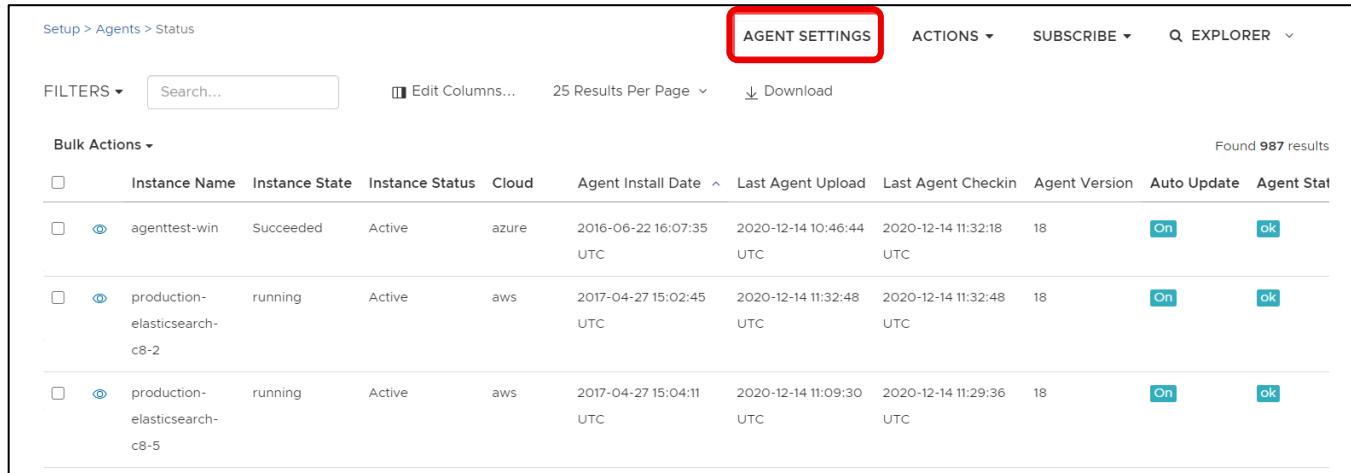
Sistemas operativos de servidor compatibles con el agente.

- Ubuntu 12.04 y superior
- RHEL 6.5 y superior
- Amazon Linux 2014.09 a través de paquetes RPM o DEB
- Windows Server 2008 R2 y superior.

1) Instalar y configurar el agente de CloudHealth



1.1 Seleccionar “Agent Settings”



The screenshot shows the 'Setup > Agents > Status' page. At the top right, there is a red box around the 'AGENT SETTINGS' button. Below it are 'ACTIONS', 'SUBSCRIBE', and 'EXPLORER' dropdowns. There are also 'FILTERS', a search bar, and a 'Edit Columns...' link. The main area displays a table of agent instances with columns: Instance Name, Instance State, Instance Status, Cloud, Agent Install Date, Last Agent Upload, Last Agent Checkin, Agent Version, Auto Update, and Agent Stat. Three instances are listed: 'agenttest-win' (Succeeded, Active, azure), 'production-elasticsearch-c8-2' (running, Active, aws), and 'production-elasticsearch-c8-5' (running, Active, aws). Each row has a checkbox and a 'Details' icon.

1.2 En la pagina de configuración, expandir “How to Install”



The screenshot shows the 'Setup > Agents > Configuration' page. Under 'HOW TO INSTALL', it says 'Installation, launch, and uninstallation. Supports Ubuntu 12.04 and above, RHEL 6.5 and above, Amazon Linux 2014.09 via RPM or DEB packages, and Windows Server 2008 R2 and above.' Below this, there are tabs for 'Linux' (selected) and 'Windows'. Under 'Linux', there are three options: 'No proxy setup' (highlighted with a red box), 'Proxy setup', and 'Authenticated proxy setup'. A 'To install:' section contains a command:

```
wget https://s3.amazonaws.com/remote-collector/agent/v24/install_cht_perfmon.sh -O install_cht_perfmon.sh;
sudo sh install_cht_perfmon.sh 24 4fd106a3-99f0-4102-8cd2-b1fc87373822 aws;
```

1.3 Debajo de Linux >> “No Proxy Setup” >> “To install” ingresar el siguiente comando:

https://s3.amazonaws.com/remote-collector/agent/v24/install_cht_perfmon.sh -O install_cht_perfmon.sh; sudo sh install_cht_perfmon.sh 24 <api-key> <cloud-name>

1.4 Configurar los ajustes del Agente para especificar qué métricas se desea recopilar y qué intervalos de muestreo usar.

The screenshot shows the 'Agent Settings' page with two main sections: 'MONITORS' and 'SETTINGS'. In the 'MONITORS' section, three metrics are listed with 'ON' toggle switches: 'CPU Usage', 'File System Utilization', and 'Memory Usage'. Each switch has a tooltip explaining its function. In the 'SETTINGS' section, various sampling intervals are configured: 'Global Sampling Interval' (10 seconds), 'CPU Sampling Interval' (10 seconds), 'File System Sampling Interval' (20 seconds), 'Memory Sampling Interval' (10 seconds), 'Update Check Interval' (5 minutes), and 'Auto Update' (ON). A 'Save Agent Settings' button is at the bottom.

MONITORS	
CPU Usage	<input checked="" type="button"/> ON
File System Utilization	<input checked="" type="button"/> ON
Memory Usage	<input checked="" type="button"/> ON

SETTINGS	
Global Sampling Interval	10
CPU Sampling Interval	10
File System Sampling Interval	20
Memory Sampling Interval	10
Update Check Interval	5
Auto Update	<input checked="" type="button"/> ON

Save Agent Settings

2) Desinstalar y reinstalar el agente de CloudHealth.

En caso de tener algún fallo en la instalación del agente de CloudHealth puede desinstalar y reinstalarlo manualmente utilizando los siguientes comandos:

1. Desinstalar el agente:

```
 wget -O - https://s3.amazonaws.com/remote-collector/agent/v24/uninstall_cht_perfmon.sh | sudo sh;
 sudo rm -rf cht_agent_install/; sudo rm -rf install_cht_perfmon.sh
```

2. Reinstalar el Agente:

```
 wget https://s3.amazonaws.com/remote-collector/agent/v24/install_cht_perfmon.sh -O
 install_cht_perfmon.sh; sudo sh install_cht_perfmon.sh 24 <api_key> <cloud_name>;
```

Referencias.

CloudWatch, documentación oficial:

https://docs.aws.amazon.com/es_es/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html

AWS Well Architected Labs:

https://www.wellarchitectedlabs.com/cost/200_labs/200_aws_resource_optimization/4_memory_plugin/

With SSM Installation

<https://www.youtube.com/watch?v=vAnlhIwE5hY>

Download and configure the CloudWatch agent using the command line:

https://docs.aws.amazon.com/es_es/AmazonCloudWatch/latest/monitoring/download-cloudwatch-agent-commandline.html

Create IAM roles and users for use with CloudWatch agent

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/create-iam-roles-for-cloudwatch-agent-commandline.html>

Installing and running the CloudWatch agent on your servers

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/install-CloudWatch-Agent-commandline-fleet.html>

Create the CloudWatch agent configuration file with the wizard

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/create-cloudwatch-agent-configuration-file-wizard.html>

Agente de CloudHealth

<https://help.cloudhealthtech.com/integrations/integrate-with-cht-agent/>