



Envío de métricas de instancias EC2 Windows 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 Windows.	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.	18
5) Iniciar el agente en los servidores.	22
Configuración manual del agente de Cloudwatch para instancias Windows.	25
1) Crear el rol o usuario de IAM para utilizar el agente de CloudWatch.....	25
2) Asociar el rol a una instancia.....	25
3) Conectarse a la instancia e instalar el paquete del agente.	25
4) Modificar el archivo de configuración y seleccionar las métricas.	28
5) Iniciar el agente en los servidores.	30
Lista de Métricas disponibles para configurar el agente de CloudWatch.	32
Agente de CloudHealth	33
Sistemas operativos de servidor compatibles con el agente.	33
1) Instalar y configurara el agente de CloudHealth.....	33
2) Desinstalar y reinstalar el agente de CloudHealth.....	35
Referencias.	36

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 ManagerAgente (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 [Métricascollected por el CloudWatchagent](#).
- 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 **Windows**, 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 Windows 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 y escribirlo 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. At the top, there's a navigation bar with the AWS logo, 'Services' dropdown, 'Resource Groups' dropdown, and other account-related links. Below the navigation is the main header 'AWS Management Console'. On the left, there's a sidebar titled 'AWS services' with a search bar and a 'Find Services' section. Under 'Recently visited services', 'EC2' and 'IAM' are listed; 'IAM' is highlighted with a red box. Under 'All services', several categories like Compute, Management & Governance, AWS Cost Management, and others are listed. To the right, there are two large boxes: 'Access resources on the go' (describing the AWS Mobile App) and 'Explore AWS' (describing AWS Global Summits, Marketplace, and SageMaker).

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

Welcome to Identity and Access Management

IAM users sign-in link: <https://146676.signin.aws.amazon.com/console>

IAM Resources

Users: 0	Roles: 3
Groups: 0	Identity Providers: 0
Customer Managed Policies: 0	

Security Status

1 out of 5 complete.
<input checked="" type="checkbox"/> Delete your root access keys
<input type="checkbox"/> Activate MFA on your root account
<input type="checkbox"/> Create individual IAM users
<input type="checkbox"/> Use groups to assign permissions
<input type="checkbox"/> Apply an IAM password policy

1.3 Seleccionar en “Crear Rol”.

Identity and Access Management (IAM)

Access management

Roles

Roles (148) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Role name	Trusted entities	Last activity
AmazonEC2RunCommandRoleForManagedInstances	AWS Service: ssm	-
AutomationServiceRole	AWS Service: ssm, and 2 more.	6 days ago

Create role

- 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

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

Another AWS account Belonging to you or 3rd party

Web identity Cognito or any OpenID provider

SAML 2.0 federation Your corporate directory

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

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

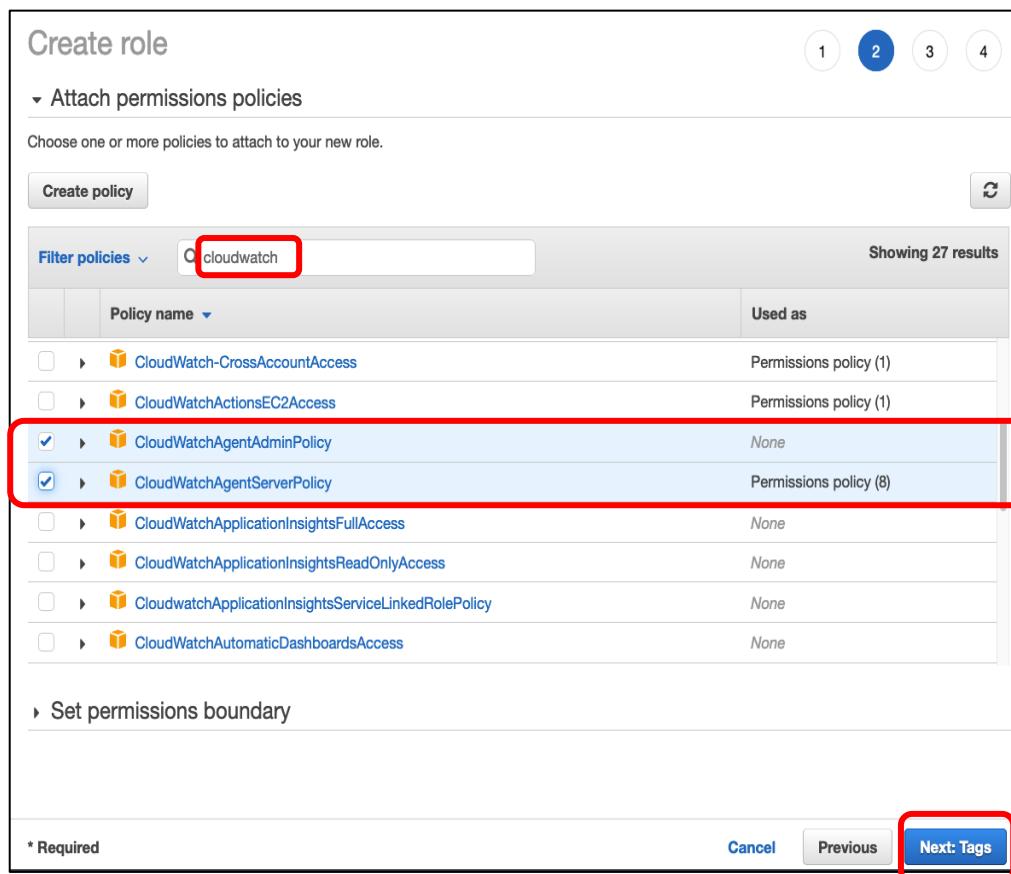
Set permissions boundary

* Required

Cancel Previous **Next: Tags**

1.6 Ahora instalaremos las políticas que permita que el agente de CloudWatch escriba las métricas en CloudWatch y para que el agente de CloudWatch se comunique con Amazon EC2 y AWS Systems Manager. Un rol permite que el agente de CloudWatch **se instale en un servidor y envíe métricas a CloudWatch**. El otro rol es necesario para almacenar la configuración del agente de CloudWatch “**Parameter Store**” de Systems Manager.

En el filtro de políticas eliminar la palabra SSM y coloque “cloudwatch”, seleccionar las políticas **CloudWatchAgentServerPolicy** y **CloudWatchAgentAdminPolicy**. Seleccionar “Siguiente: etiquetas”.



Notas.

- I. Para 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

Permissions boundary Permissions boundary is not set

The new role will receive the following tag

Key	Value
env	PDR

* Required

Cancel Previous Create role

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 options like EC2 Dashboard, Events, Tags, Limits, Instances (selected), Instances (New), and Instance Types. The main area shows a table with three instances: 'o-test', 'o-priv', and 'Webserver-CWagent'. A red box highlights the checkbox next to 'Webserver-CWagent'. On the right, there's an 'Actions' dropdown menu with several options: Connect, View details, Manage instance state, Instance settings, Networking, Security (highlighted with a red box), Image and templates, and Monitor and troubleshoot. The 'Modify IAM role' option is also highlighted with a red box in this menu.

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-win.html>

En caso necesario instalar el agente de SSM seguiendo la documentación dependiendo el sistema operativo que se utilice.

Windows: <https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-install-win.html>

Configuración del agente de Cloudwatch por SSM para instancias Windows.

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

Seguir los pasos indicados en la sección de Windows (paso 1, página 4).

2) Asociar el rol a una instancia.

Seguir los pasos indicados en la sección de Windows (paso 2, página 9).

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

En este ejemplo se utilizará el método de conexión con cliente RDP por lo que es importante tener instalado una aplicación de conexión remota como “Microsoft Remote Desktop”.

Para poder conectarnos a la instancia, primero debemos obtener el password, para ello:

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

The screenshot shows the AWS Management Console interface. In the top navigation bar, there is a search bar with the text "EC2" entered. Below the search bar, a dropdown menu is open, showing "EC2" highlighted with a red box. Other options like "ECS" are also visible.

3.2 Seleccionar la instancia con la que deseamos trabajar y seleccionar “Conectar”.

The screenshot shows the AWS EC2 Instances page. On the left sidebar, under the "Instances" section, the "Instances" tab is selected. In the main content area, there is a table titled "Instances (1/3)". The first row of the table has a checkbox checked and is highlighted with a red box. The column header for this row is "Name". The name "Webservice-CWagent" is also highlighted with a red box. To the right of the table, there is a "Connect" button, which is also highlighted with a red box.

3.3 Seleccionar conexión por Cliente RDP y seleccionar “Obtener Password”

The screenshot shows the AWS EC2 Instances page for an instance named 'i-0'. The 'Connect to instance' section is displayed, with the 'RDP client' tab selected. The page provides instructions for connecting using a remote desktop client or by downloading an RDP shortcut file. It also lists the Public DNS and User name for the instance. A red box highlights the 'Get password' button, which is used to retrieve the initial Windows administrator password.

EC2 > Instances > i-0 > Connect to instance

Connect to instance Info

Connect to your instance i-0f18a95a64a41ecc (Webserver-CWagent) using any of these options

Session Manager | **RDP client** | EC2 Serial Console

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

[Download remote desktop file](#)

When prompted, connect to your instance using the following details:

Public DNS User name
ec2-[REDACTED].compute-1.amazonaws.com Administrator

Password [Get password](#)

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

3.4 Cargar el archivo de la llave (.pem) con la que se creo la instancia y seleccionar “Decrypt Password”.

The screenshot shows the 'Get Windows password' page. It displays the key pair associated with the instance ('testdan') and a 'Browse' button to select a key pair file. A red box highlights the 'Browse' button. Below it, a file named 'testdan.pem' (1.7KB) is listed. The page also contains a large text area with a long RSA private key, and a red box highlights the 'Decrypt Password' button at the bottom right.

Get Windows password Info

Retrieve and decrypt the initial Windows administrator password for this instance.

To decrypt the password, you will need your key pair for this instance.

Key pair associated with this instance
testdan

Browse to your key pair:
[Browse](#)

testdan.pem
1.7KB

Or copy and paste the contents of the key pair below:

```
JtXXTlxxMkvrkueTj4N1bMxQBpnTJspoSkEctlm6uglqDwT1zm1yweDzAndjm
7nYf30zKXVbgBsAiC88t0x04hVmG687JvnB2GPAs8jYsn9PZaijcgMbgeQEf66nQ
pmiYqsyBi59NBYLZTA911sCgYBRX2RB7daF0CkzA605kr2W07MCYXA6CeFcrJX
29zOxx74zuX2kpYGdVl7nSutWwecm2m/3OsQRgPyMBBE+zCYRkeMstfXmkDUUs
xkuPp5qOrZGZnjBM82NCtsOqCc+M/VLsbFrzaKbrrFg1Ysf0/JEj0ggXpeOU31g
ZsthHwKBgAootZuYRfhaV8TYJJMNCrpPVsmRniPgfyqcwBPPs2GOOGASvkY0lxdf
4VO5RnAPNUhzllJcCmayo/tBLKjOzpIVZWd2hhRhGjCFQxr6/QQsgLBdgj5CPSe
FcK9NAXiEw5ZWL2boDi55Gw0FzetqYCRCHjCYGvV6ujLkvgpgN+9T
-----END RSA PRIVATE KEY-----
```

[Cancel](#) **Decrypt Password**

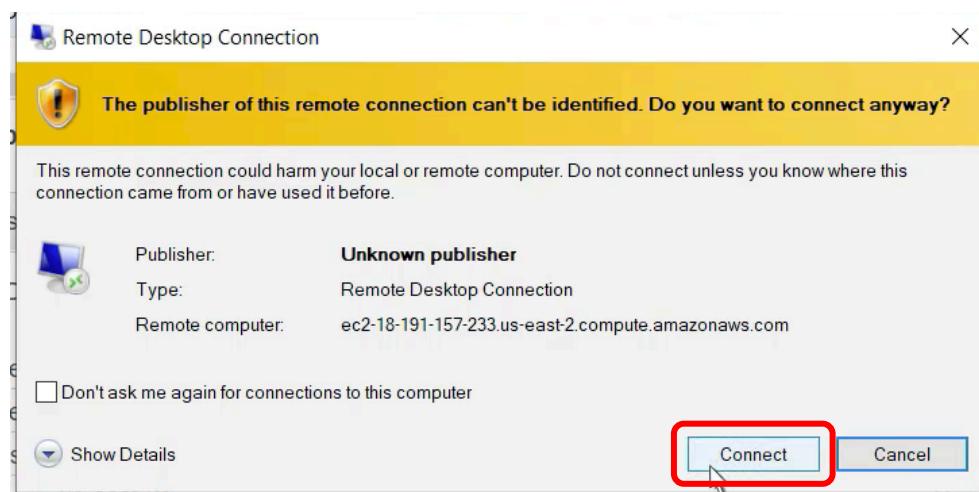
3.5 Copiar el Password que se generó.

The screenshot shows the 'Connect to instance' page for an EC2 instance. The 'RDP client' tab is selected. A red box highlights the 'Password' field, which contains the generated password: '3H=tOD@Ga);qt*t9quR@2@YMPNCn@d7C'.

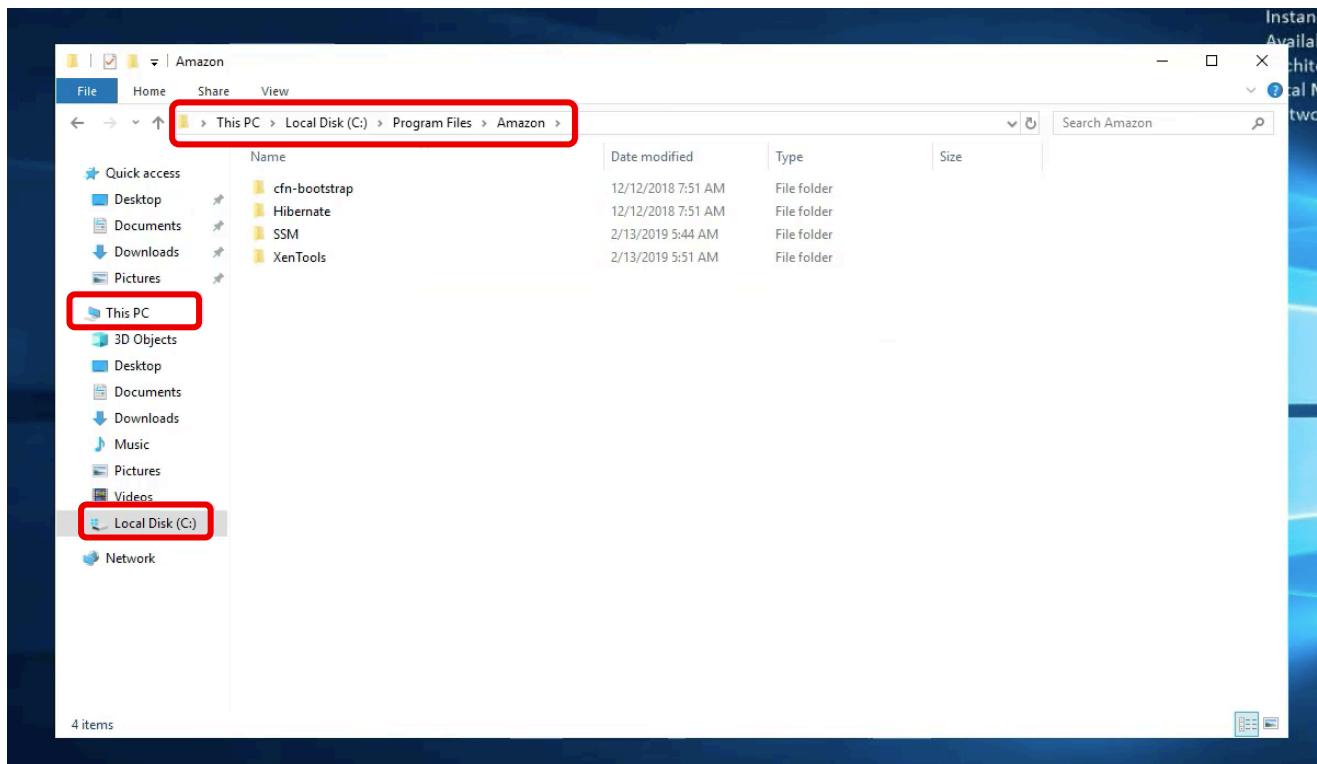
3.6 Ahora ya podremos conectarnos por “**Remote Desktop**”, para ello descargamos el archivo de “remote desktop”.

The screenshot shows the 'Connect to instance' page for an EC2 instance. The 'RDP client' tab is selected. A red box highlights the 'Download remote desktop file' button.

3.7 Abrir el archivo descargado “RDS shortcut file” para conectarte a la instancia con el “password” previamente obtenido.



3.8 Al conectarnos se abrirá la ventana de Windows (a través de la aplicación de Microsoft Remote) de la instancia que creamos, a través de la aplicación de conexión Remoto. Para ubicar la localización donde se instalara el agente de CloudWatch seleccionamos: >> This PC >> Local Disk >> Program Files >> Amazon.



Nota. La carpeta de “Amazon” Incluye drivers en la instancia, pero el agente de CloudWatch aún no está instalado, para ello debemos ir al servicio de [Systems Manager](#).

3.9 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 like Change Management and Node Management. Under Node Management, the 'Fleet Manager' option is selected and highlighted with a red box. The main pane is titled 'Fleet Manager' and has tabs for 'Managed instances' (which is selected) and 'Settings'. Below this, the 'Managed instances' section shows one instance: 'i-0539' which is 'Running' and 'Online'. There are buttons for creating a new fleet ('C') and deleting ('D').

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

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

The screenshot shows the 'Run a command' interface. On the left, the 'Run Command' option in the Node Management section is highlighted with a red box and labeled '1'. The main pane is titled 'Run a command' and shows a 'Command document' section with a search bar and a table of available commands. A specific command, 'AWS-ConfigureAWSPackage', is selected and highlighted with a red box and labeled '3'. A large red box highlights the 'Run command' button at the top right of the table, labeled '2'.

Name	Owner
AWS-ApplyAnsiblePlaybooks	Amazon
AWS-ApplyChefRecipes	Amazon
AWS-ApplyDSCMofs	Amazon
AWS-ApplyPatchBaseline	Amazon
AWS-ConfigureAWSPackage	Amazon
AWS-ConfigureCloudWatch	Amazon

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

Action
(Required) Specify whether or not to install or uninstall the package.
Install

Installation Type
(Optional) Specify the type of installation. Uninstall and reinstall: The application is taken offline until the reinstallation process completes. In-place update: The application is available while new or updated files are added to the installation.
Uninstall and reinstall

Name
(Required) The package to install/uninstall.
AmazonCloudWatchAgent

Version
(Optional) The version of the package to install or uninstall. If you don't specify a version, the system installs the latest published version by default. The system will only attempt to uninstall the version that is currently installed. If no version of the package is installed, the system returns an error.

Additional Arguments
(Optional) The additional parameters to provide to your install, uninstall, or update scripts.
0

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 group
Choose a resource group that includes the resources you want to target.

i-0539 X

Instances

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Availability zone	Ping stat
<input checked="" type="checkbox"/>	WebserverCW-agent	i-0539e	running	us-east-1b	Online

En caso que requieras que escriba en un bucket S3 puedes seleccionarlo sino desmarcar la casilla.

Output options

Write command output to an Amazon S3 bucket
Write all command output to an Amazon S3 bucket. Command output in the console is truncated after 2500 characters.

Enable an S3 bucket

Send command output to Amazon CloudWatch logs
You can stream and encrypt log data for all commands in your account to a CloudWatch Logs log group in your account. [Learn more](#)

Enable CloudWatch logs

Run

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 instalo 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	Detailed status	# targets	# completed	# error	# delivery timed out
Success	Success	1	1	0	0

Targets and outputs

[View output](#)

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

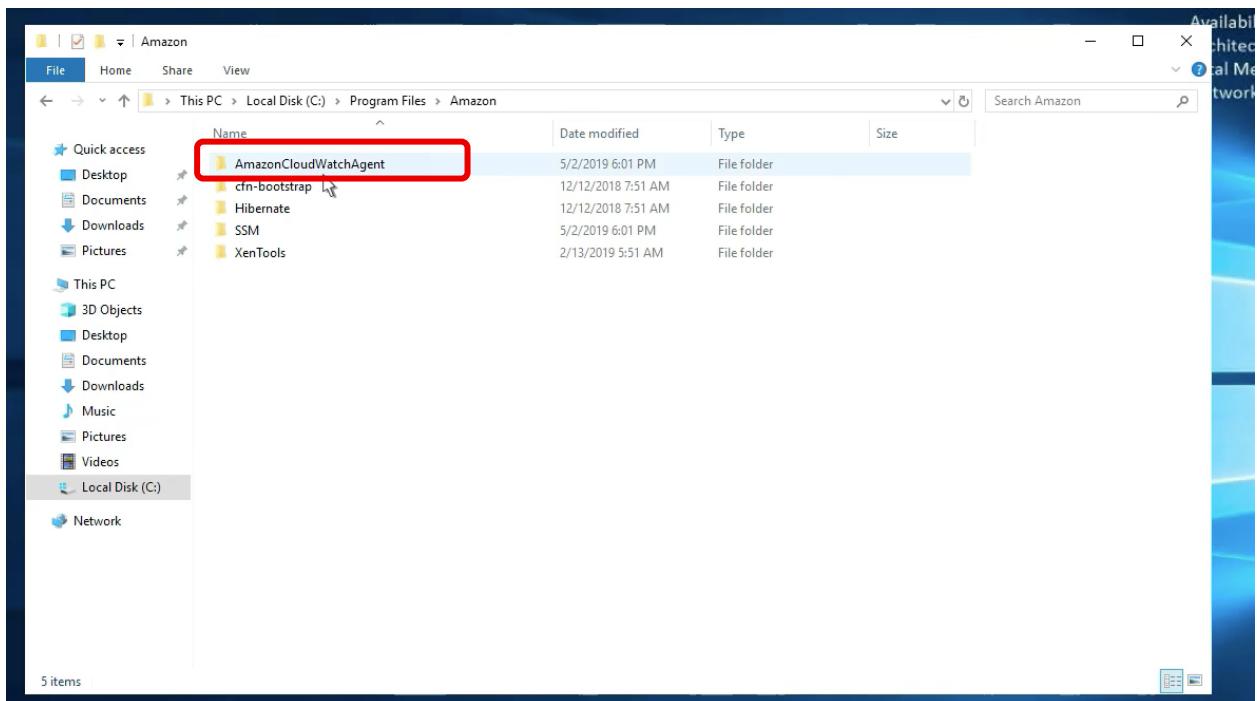
▼ Output

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.

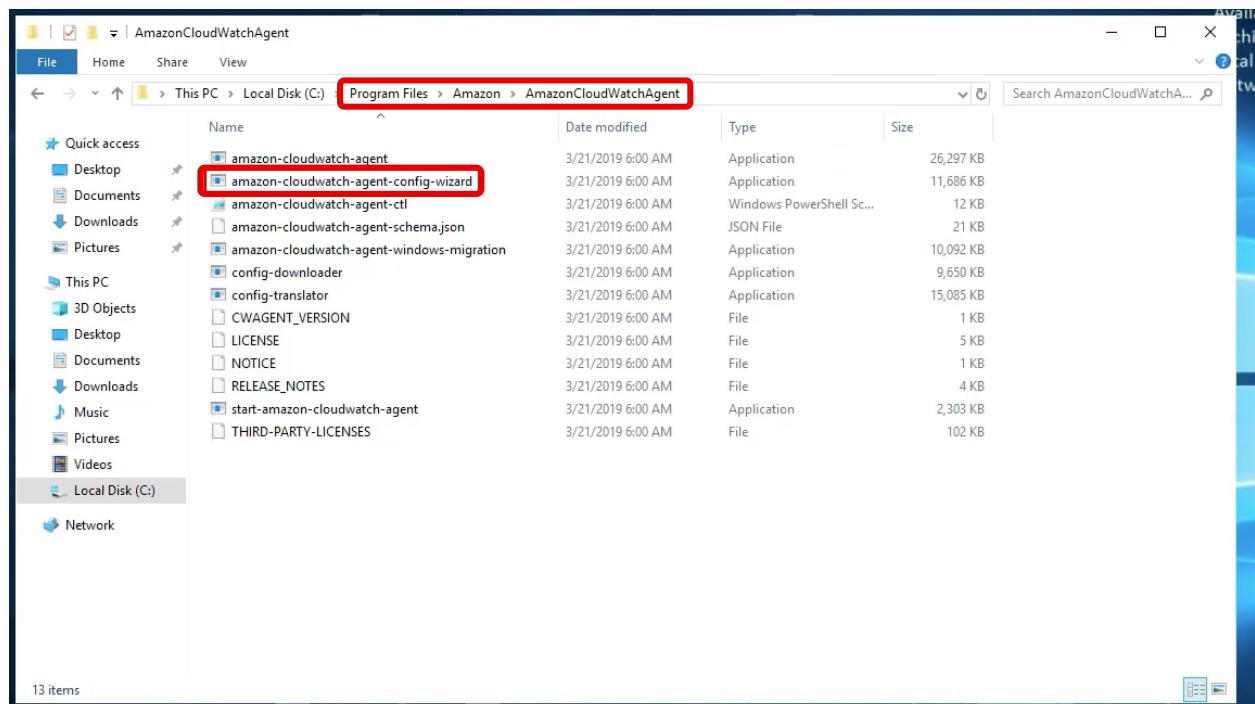
```
Initiating arn:aws:ssm:::package/AmazonCloudWatchAgent 1.247349.0b251399 install
Plugin aws:runPowerShellScript ResultStatus Success
install output: Running install.ps1
Successfully installed
arn:aws:ssm:::package/AmazonCloudWatchAgent 1.247349.0b251399
```

[Copy](#) [Download](#)

3.13 Podrás validar que se instaló el agente desde tu ventana de “Remote Desktop” donde se observará ahora el folder del agente de CloudWatch.



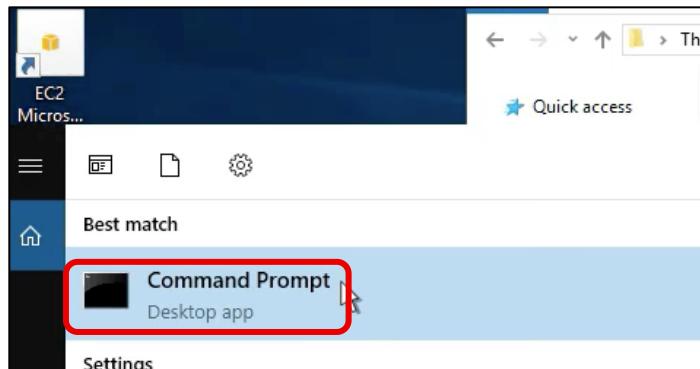
3.14 “Run command” instaló un asistente de configuración que se podrá utilizar para crear el “archivo de configuración” para la configuración del agente.



4) Modificar el archivo de configuración y seleccionar las 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.

4.1 Para utilizar el “Asistente de configuración” dirigirse al folder del agente de CloudWatch desde el Command Prompt o Power Shell (Click derecho correr como administrador).



4.2 Para utilizar el “asistente de configuración” ejecutar el siguiente comando:

```
cd "C:\Program Files\Amazon\AmazonCloudWatchAgent"
```

```
amazon-cloudwatch-agent-config-wizard.exe
```

```
Microsoft Windows [Version 10.0.17763.2183]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd "C:\Program Files\Amazon\AmazonCloudWatchAgent"
C:\Program Files\Amazon\AmazonCloudWatchAgent>amazon-cloudwatch-agent-config-wizard.exe
=====
= 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: [2]: [2]

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]

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

1
Which port do you want StatsD daemon to listen to?
default choice: [8125]: [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 have any existing CloudWatch Log Agent configuration file to import for migration?  
1. yes  
2. no  
default choice: [2]:  
2  
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 add ec2 dimensions (ImageId, InstanceId, InstanceType, AutoScalingGroupName) into all of your metrics if the info is available?  
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 for all metrics, but you can customize for specific metrics in the output json file.  
1. 1s  
2. 10s  
3. 30s  
4. 60s  
default choice: [4]:  
4  
Which default metrics config do you want?  
1. Basic  
2. Standard  
3. Advanced  
4. None  
default choice: [1]:  
3
```

Si se habilita generaría un costo adicional.

Dependerá el tipo de métricas que se desea instalar. Puedes consultar la siguiente tabla para definir tus métricas.

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:
{
  "metrics": {
    "append_dimensions": {
      "AutoScalingGroupName": "${aws:AutoScalingGroupName}",
      "ImageId": "${aws:ImageId}",
      "InstanceId": "${aws:InstanceId}",
      "InstanceType": "${aws:InstanceType}"
    },
    "metrics_collected": {
      "LogicalDisk": {
        "measurement": [
          "% Free Space"
        ],
        "metrics_collection_interval": 60,
        "resources": [
          "*"
        ]
      },
      "Memory": {
        "measurement": [
          "% Committed Bytes In Use"
        ],
        "metrics_collection_interval": 60
      },
      "Paging File": {
        "measurement": [
          "% Usage"
        ],
        "metrics_collection_interval": 60,
        "resources": [
          "*"
        ]
      },
      "PhysicalDisk": {
        "measurement": [
          "% Disk Time",
          "Disk Write Bytes/sec",
          "Disk Read Bytes/sec",
          "Disk Writes/sec",
          "Disk Reads/sec"
        ],
        "metrics_collection_interval": 60,
        "resources": [
          "*"
        ]
      },
      "Processor": {
        "measurement": [
          "% User Time",
          "% System Time"
        ],
        "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 want to monitor any customized log files?
1. yes
2. no
default choice: [1]:
2
Do you want to monitor any Windows event log?
1. yes
2. no
default choice: [1]:
2
Saved config file to config.json successfully.
Current config as follows:
{
    "metrics": {
        "append_dimensions": {
            "AutoScalingGroupName": "${aws:AutoScalingGroupName}",
            "ImageId": "${aws:ImageId}",
            "InstanceId": "${aws:InstanceId}",
            "InstanceType": "${aws:InstanceType}"
        },
}

```

Dependerá 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 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-windows]
AmazonCloudWatch-demoagent
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. ASIAULEHRFSPYD67U2EN(From SDK)
2. Other
default choice: [1]:

```

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 interface. On the left, there's a sidebar with various management options like Quick Setup, Operations Management (Explorer, OpsCenter, CloudWatch Dashboard, PHD, Incident Manager), Application Management (Application Manager, AppConfig), and Parameter Store. The Parameter Store option is highlighted with a red box. The main pane shows a search bar with the filter 'Name: contains: AmazonCloudWatch-demoagent'. Below the search bar is a table with one result: 'AmazonCloudWatch-demoagent' under the 'Name' column, with 'Standard' under 'Tier'.

5) Iniciar el agente en los servidores.

5.1 Ahora aplicaremos la configuración en las instancias para comenzar a colectar datos en CloudWatch para ellos nos vamos de nuevo a “**Fleet Manager**”. Confirmarmos que la instancia este corriendo.

The screenshot shows the AWS Systems Manager Fleet Manager interface. The left sidebar has 'Fleet Manager' selected. The main pane shows a table titled 'Managed instances' with one entry: 'i-0539'. The instance is listed as 'Running' and 'Online'. There's a 'Run command' button at the top right of the main pane.

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

AWS Systems Manager X

- Resource Groups
 - Find Resources
 - Saved Resource Groups
- Insights
 - Built-In Insights
 - Dashboard by CloudWatch
 - Inventory
 - Compliance
- Actions
 - Automation
 - Run Command**
 - Session Manager
 - Patch Manager
 - Maintenance Windows
 - Distributor

AWS Systems Manager > Run Command > Run a command

Run a command

Command document

Select the type of command that you want to run.

Document name prefix : Equals : AmazonCloudWatch

Name
<input checked="" type="radio"/> AmazonCloudWatch-ManageAgent
<input type="radio"/> AmazonCloudWatch-MigrateCloudWatchAgent

Description

5.3 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 config.

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 config.

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

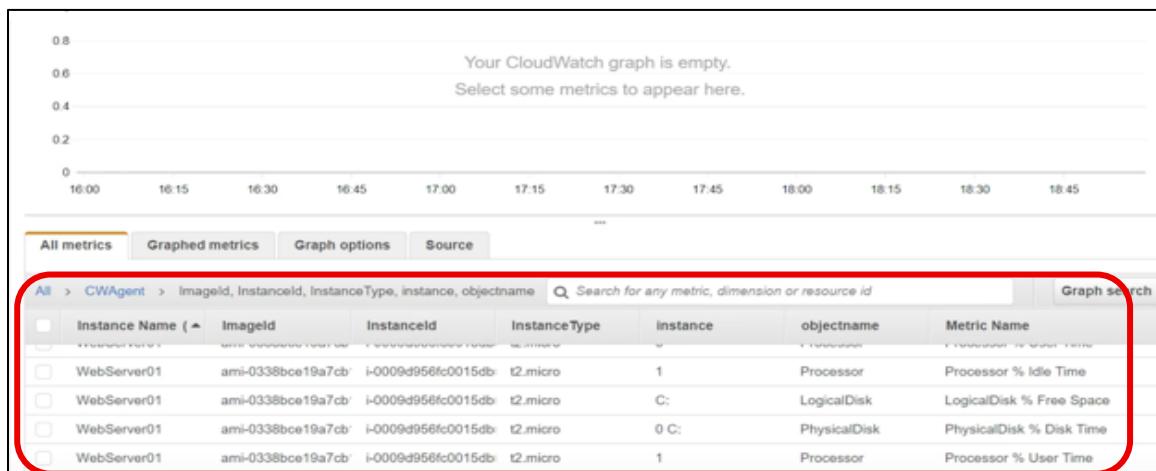
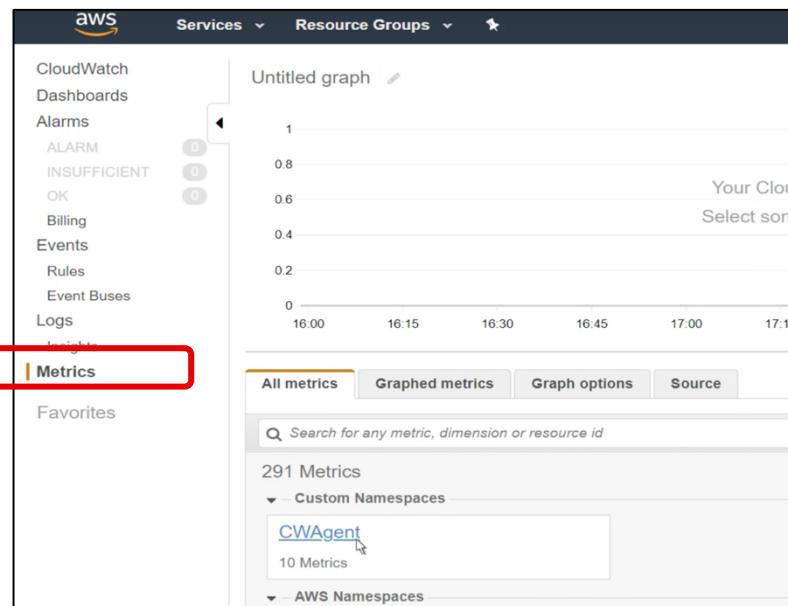
Targets
Choose a method for selecting targets.

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 re...
Choose a resc...

5.4 Seleccionar el servicio de CloudWatch y podremos observar la información recolectada. CloudWatch nos permite colectar y rastrear métricas de diferentes servicios de AWS y aplicaciones.



Aquí encontrarás 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 Windows.

En este manual se mostrará como realizar la conexión SSH a una instancia Windows e instalar manualmente el agente de CloudWatch.

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.

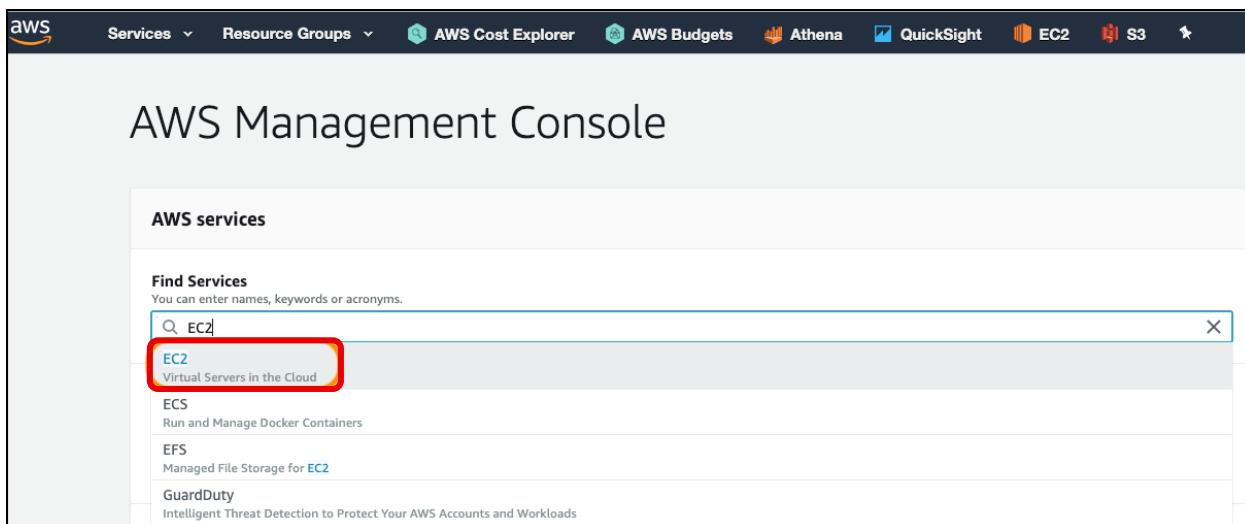
Seguir los pasos indicados en la sección de Windows (paso 1, página 4).

2) Asociar el rol a una instancia.

Seguir los pasos indicados en la sección de Windows (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.



- 3.2 En la barra del lado izquierdo seleccionar “Instancias” y seleccionar la instancia que previamente le asociamos el rol con la política **CloudWatchAgentServerPolicy**.

Name	Environment	Project	Schedule	Instance ID
	DEV	Beta		i-00ec37
		Beta		i-01cfb6
	PRD	Beta		i-020f2c
	PRD	Beta		i-07bcfc
	Dev	Beta		i-099ab
Einstein	PRD	Einstein		i-07ffd0
	PRD	Einstein		i-0cb650
	PRD	Einstein		i-0e196
	PRD	Euler		i-01555
	PRD	Euler		i-041cd
	PRD	Euler		i-08052
	PRD	Euler		i-0d1c9a

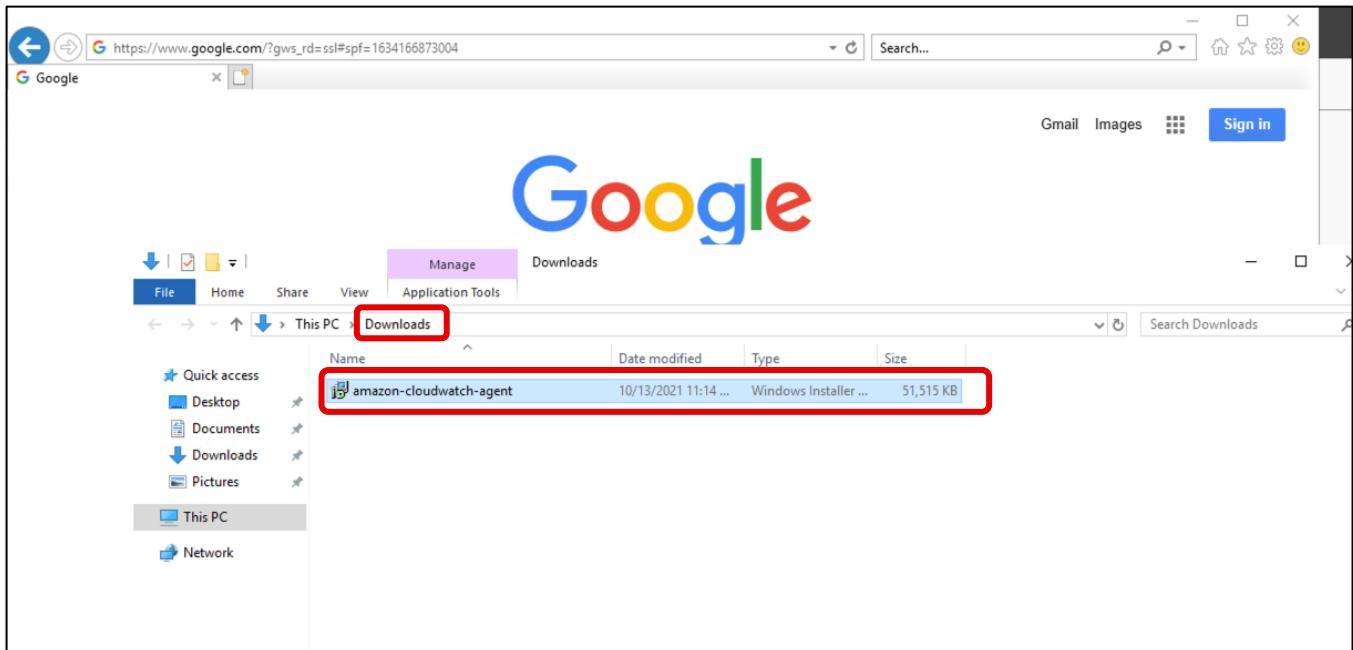
- 3.3 Conectarse a la instancia utilizando SSH y seguir el procedimiento de comandos en la terminal.

Name	Instance ID	Instance state	Instance type
<input checked="" type="checkbox"/> Webservice-CWagent	i-0	Running	t2.micro
<input type="checkbox"/> o-test	i-0	Stopped	t2.medium
<input type="checkbox"/> o-priv	i-0	Stopped	t2.medium

- 3.4 Una vez conectados a la instancia, descargar el siguiente archivo desde el browser:

<https://s3.amazonaws.com/amazoncloudwatch-agent/windows/amd64/latest/amazon-cloudwatch-agent.msi>

3.5 Confirmar que se haya descargado el archivo:



3.6 En la terminal posicionarse en la carpeta donde se descargo el archivo

```
C:\Windows\system32>
C:\Windows\system32>cd C:\Users\racker-dani-09f932d8\Downloads
```

3.7 Ejecutar el siguiente comando para abrir el archivo:

```
msiexec /i amazon-cloudwatch-agent.msi
```

```
C:\Users\racker-dani-09f932d8\Downloads> msiexec /i amazon-cloudwatch-agent.msi
```

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

Antes de ejecutar el agente de CloudWatch en cualquier servidor, debe crear un **archivo de configuración** del agente de CloudWatch, que es un 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.

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

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

```
cd "C:\Program Files\Amazon\AmazonCloudWatchAgent"  
amazon-cloudwatch-agent-config-wizard.exe
```

```
Microsoft Windows [Version 10.0.17763.2183]  
(c) 2018 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>cd "C:\Program Files\Amazon\AmazonCloudWatchAgent"  
  
C:\Program Files\Amazon\AmazonCloudWatchAgent>amazon-cloudwatch-agent-config-wizard.exe  
=====  
= 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: [2]:  
  
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]:  
  
Do you want to turn on StatsD daemon?  
1. yes  
2. no  
default choice: [1]:  
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 have any existing CloudWatch Log Agent configuration file to import for migration?

1. yes
2. no

```
default choice: [2]:
```

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 add ec2 dimensions (ImageId, InstanceId, InstanceType, AutoScalingGroupName) into all of your metrics if the info is available?

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 for all metrics, but you can customize for specific metrics in the output json file.

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]:
```

Si se habilita generaría un costo adicional.

Dependerá el tipo de métricas que se desea instalar. Puedes consultar la siguiente tabla para definir tus métricas.

4.2 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.

```

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

Dependerá si deseas monitorear los archivos de logs de lo contrario seleccionar que no.

```
2
Do you want to monitor any Windows event log?
1. yes
2. no
default choice: [1]:
2
Saved config file to config.json successfully.
```

4.3 Confirmar que el archivo de configuración para el agente se guarde como config.json

```
        "statsd": {  
            "metrics_aggregation_interval": 60,  
            "metrics_collection_interval": 10,  
            "service_address": ":8125"  
        }  
    }  
}  
Please check the above content of the config.  
The config file is also located at 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]:  
2  
Please press Enter to exit...
```

5) Iniciar el agente en los servidores.

5.1 Para iniciar el Agente de CloudWatch:

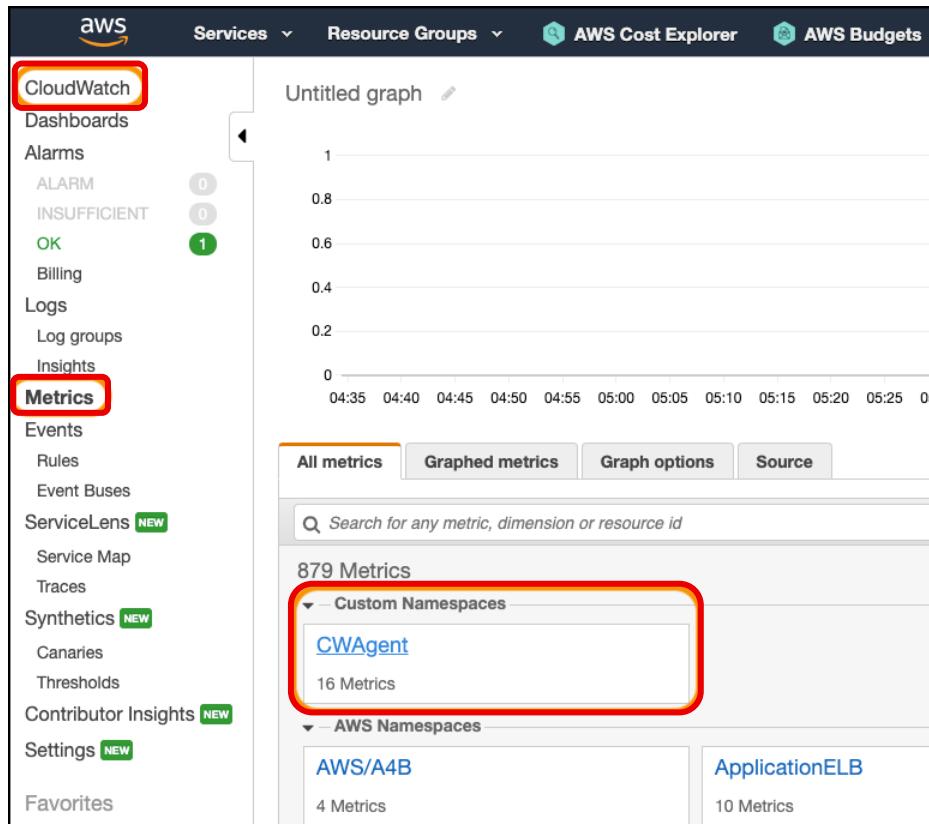
Colocarse en la dirección: cd "C:\Program Files\Amazon\AmazonCloudWatchAgent" ejecutar el siguiente comando:

Ejecutar el comando:

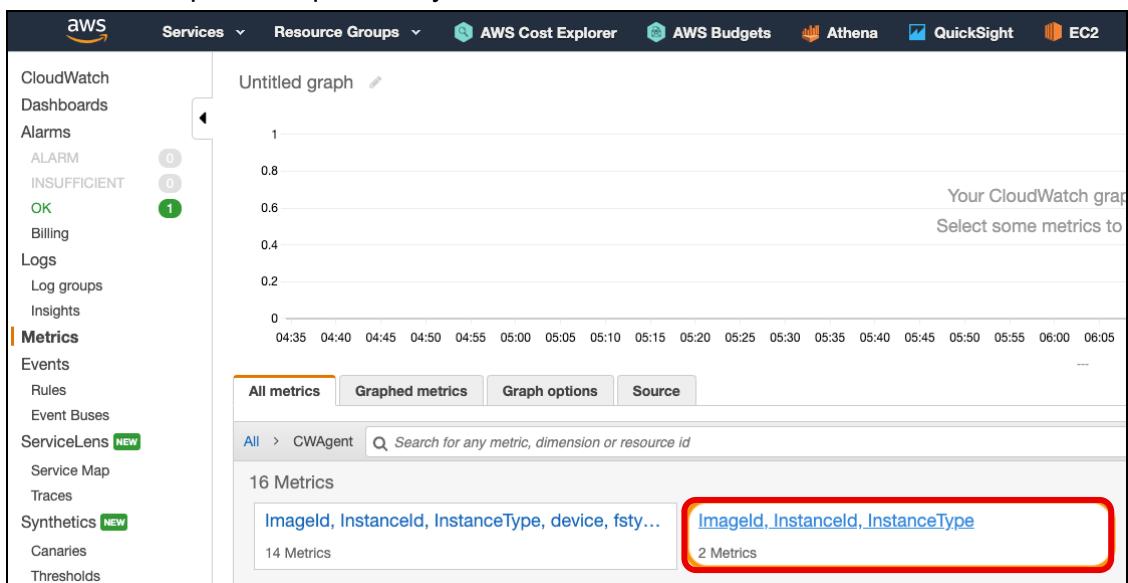
```
& "C:\Program Files\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1" -a fetch-config -m ec2 -s -c file:config.json
```

```
PS C:\Windows\system32> cd "C:\Program Files\Amazon\AmazonCloudWatchAgent"  
PS C:\Program Files\Amazon\AmazonCloudWatchAgent> & "C:\Program Files\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1" -a fetch-config -m ec2 -s -c file:config.json  
***** processing amazon-cloudwatch-agent *****  
Successfully fetched the config and saved in C:\ProgramData\Amazon\AmazonCloudWatchAgent\Configs\file_config.json.tmp  
Start configuration validation...  
2021/10/14 00:46:46 Reading json config file path: C:\ProgramData\Amazon\AmazonCloudWatchAgent\Configs\file_config.json.tmp ...  
Valid Json input schema.  
No csm configuration found.  
No log configuration found.  
Configuration validation first phase succeeded  
Configuration validation second phase succeeded  
Configuration validation succeeded  
AmazonCloudWatchAgent has been stopped  
AmazonCloudWatchAgent has been started  
PS C:\Program Files\Amazon\AmazonCloudWatchAgent> |
```

5.2 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.



5.3 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, utilizando el Agente de CloudWatch.

Lista de Métricas disponibles para configurar el agente de CloudWatch.

Instancias de Amazon EC2 que ejecutan Windows Server

DetalleLevel	Métricas excluidas
Básica	Memoria: Memory % Committed Bytes In Use Disco lógico: LogicalDisk % Free Space
Standard	Memoria: Memory % Committed Bytes In Use Paginación: Paging File % Usage Procesador: Processor % Idle Time, Processor % Interrupt Time, Processor % User Time Disco físico: PhysicalDisk % Disk Time Disco lógico: LogicalDisk % Free Space
Advanced (Avanzado)	Memoria: Memory % Committed Bytes In Use Paginación: Paging File % Usage Procesador: Processor % Idle Time, Processor % Interrupt Time, Processor % User Time Disco lógico: LogicalDisk % Free Space Disco físico: PhysicalDisk % Disk Time, PhysicalDisk Disk Write Bytes/sec, PhysicalDisk Disk Read Bytes/sec, PhysicalDisk Disk Writes/sec, PhysicalDisk Disk Reads/sec TCP: TCPv4 Connections Established, TCPv6 Connections Established

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.

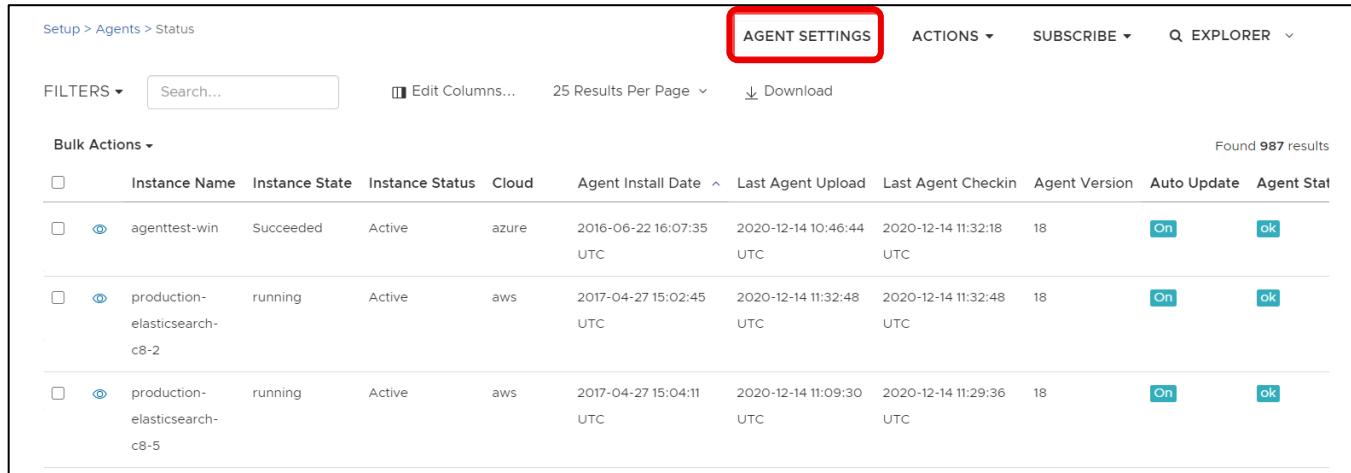
Sistemas operativos de servidor compatibles con el agente.

- 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 configurara el agente de CloudHealth



1.1 Seleccionar “Agent Settings”



The screenshot shows a table of agent instances. The columns include 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:

	Instance Name	Instance State	Instance Status	Cloud	Agent Install Date	Last Agent Upload	Last Agent Checkin	Agent Version	Auto Update	Agent Stat
<input type="checkbox"/>	agenttest-win	Succeeded	Active	azure	2016-06-22 16:07:35 UTC	2020-12-14 10:46:44 UTC	2020-12-14 11:32:18 UTC	18	On	ok
<input type="checkbox"/>	production-elasticsearch-c8-2	running	Active	aws	2017-04-27 15:02:45 UTC	2020-12-14 11:32:48 UTC	2020-12-14 11:32:48 UTC	18	On	ok
<input type="checkbox"/>	production-elasticsearch-c8-5	running	Active	aws	2017-04-27 15:04:11 UTC	2020-12-14 11:09:30 UTC	2020-12-14 11:29:36 UTC	18	On	ok

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



The screenshot shows the 'Configuration' page for the Windows agent. It includes sections for 'HOW TO INSTALL' (with Linux and Windows tabs), 'Proxy setup' options (No proxy setup, Proxy setup, Authenticated proxy setup), and a 'To install:' section with 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 Windows >> “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>