Discovery

Discovery

¿Qué es Pandora FMS Discovery?

Discovery Task list

La herramienta Discovery de Pandora FMS permite ver un listado de todas las tareas programadas en el entorno tanto a nivel de consola como a nivel de servidor.

Discovery Applications

Permite monitorizar entornos MySQL®, Oracle® o VMware® desde una nueva consola de administración.

Discovery Cloud

A través de esta utilidad se puede monitorizar su infraestructura en Cloud, desde máquinas virtuales creadas en Amazon Web Services® (EC2) o bases de datos relacionales en AWS RDS a máquinas virtuales corriendo en Azure Computer®.

Discovery Console Tasks

Permite automatizar tanto tareas de consola dentro del sistema Discovery, como programar informes, realizar respaldos de datos o ejecutar guiones (*scripts*) personalizados desde la Consola Pandora FMS.

Discovery Host&Devices

Incluye las herramientas necesarias para descubrir o importar dispositivos.

Discovery Applications

Con Pandora FMS es posible monitorizar aplicaciones de manera remota utilizando *Discovery Applications*.

Discovery Applications: SAP

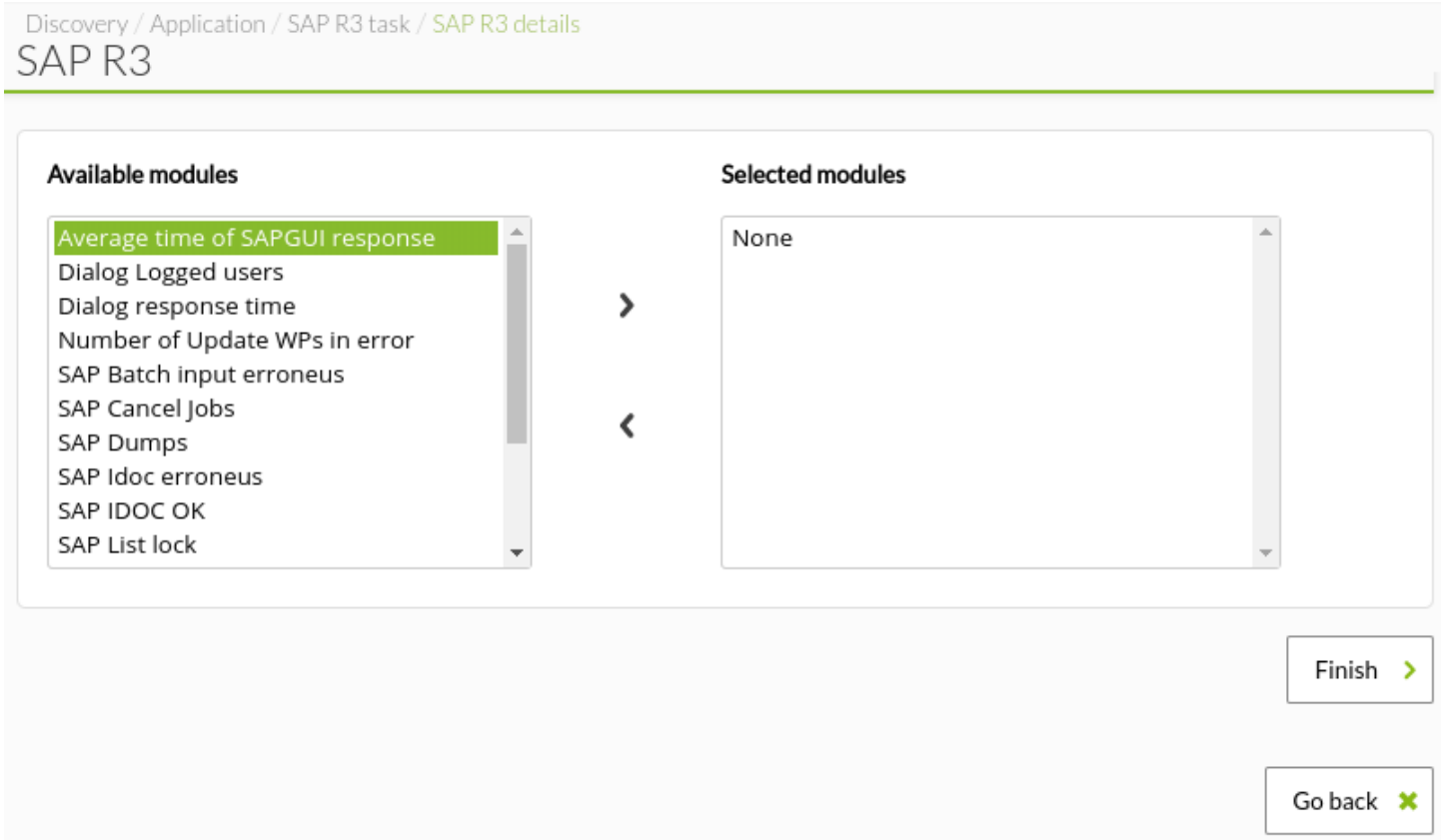
Versión NG 741 o posterior.

El sistema guiará cada paso para configurar SAP según las necesidades que se tengan. Se

podrá definir la misma tarea para monitorizar sistemas con configuraciones similares (versiones 741 a 768).

Si se necesitan monitorizar diferentes configuraciones, se deberá crear una tarea para cada configuración.

Debe seleccionar de la lista la información acerca del sistema SAP que se desee recuperar:



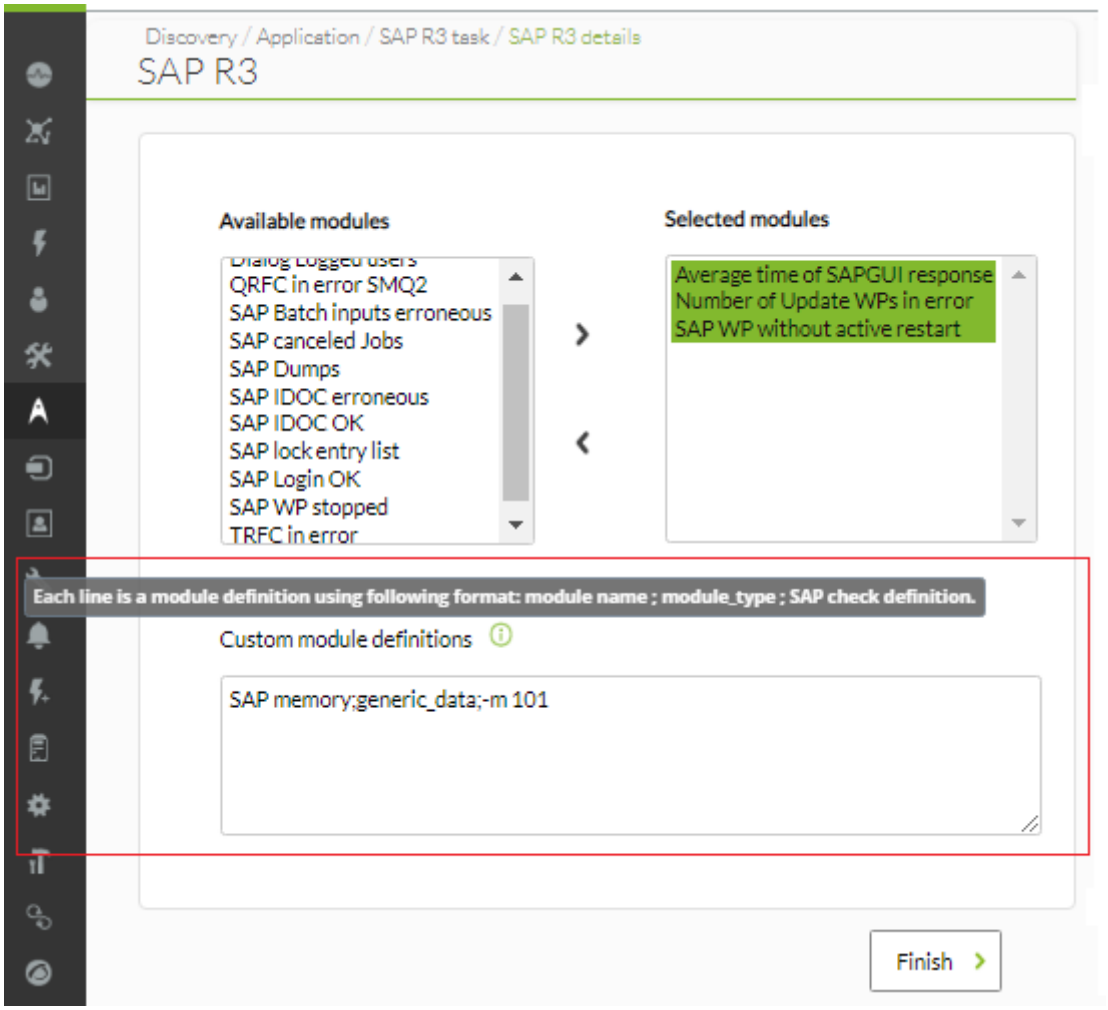
Pandora FMS Discovery se encargará de recolectar la información, almacenándola en agentes representados por los SAP Hostnames que haya definido (versiones 741 a 768) o en SAP Hostname (versión 769 o posterior).

Si instala Pandora FMS desde paquetes, o su sistema es anterior a NG741 deberá desplegar el *plugin* oficial de SAP en el servidor de Pandora FMS y configurarlo manualmente según la sección Instalación manual del conector de Discovery para SAP.

SAP personalizados

Versión NG 747 o posterior.

Aparte de los Módulos disponibles (Available modules) en Pandora FMS, puede agregar una gran cantidad de Módulos adicionales mediante la sección de definiciones de Módulos personalizados (Custom module definitions).



Cada línea a agregar debe usar el siguiente formato, usando el punto y coma como separador de campos:

```
<nombre de módulo>;<tipo de módulo>;<definición de chequeo sap>
```

Un ejemplo para conocer la información del sistema SAP:

```
SAP info;generic_data_string;-m 120
```

Se pueden agregar tantos módulos personalizados como se necesiten, el proceso continúa de la misma manera descrita en la sección anterior.

Discovery Applications: VMware

Se debe tener en cuenta que si el servidor de Pandora FMS tiene activo el token `autocreate_group`, se dará

prioridad al grupo correspondiente al ID indicado, en vez de aplicar la configuración del asistente.

Una vez completada la configuración básica de VMware, se ha de especificar lo siguiente:

- Max threads: Número de hilos que utilizará el *script* de monitorización VMware para agilizar la obtención de datos.
- Event mode: (Solo para VCenter) habilita la monitorización basada en eventos del VMware VCenter. Este modo de trabajo es exclusivo e independiente de la monitorización estándar.
- Extra settings: Se deben incluir aquí, en modo texto, cualquier configuración avanzada que sea necesaria para personalizar la monitorización de VMware.

Discovery Applications: MS SQL

Pandora FMS permite monitorizar bases de datos de Microsoft SQL Server®. Para ello es necesario tener instalado el Open Database Connectivity (ODBC) de Microsoft®.

Configurar una tarea de Discovery Applications MS SQL

Para crear una tarea de monitorización para una base de datos Microsoft SQL Server® se debe acceder a través de Discovery (Discovery → Applications → Microsoft SQL Server).

Una vez elegida la tarea de Microsoft SQL Server®, se han de definir las instancias (*Instance*):

```
IP\Instance
```

Para definir un puerto (*Port*):

```
IP:Port\Instance
```

Módulos disponibles por defecto

El usuario y credencial utilizado para monitorizar debe tener los permisos necesarios sobre las bases de datos a conectar para realizar las operaciones correspondientes.

Nombre	Descripción
`MSSQL connection`	Comprueba si existe conexión al servidor MS SQL.
`queries: delete`	Cantidad de consultas de borrado ejecutadas desde la última comprobación.
`queries: insert`	Cantidad de consultas de inserción ejecutadas desde la última comprobación.
`queries: update`	Cantidad de consultas de actualización ejecutadas desde la última comprobación.
`queries: select`	Cantidad de consultas de lectura ejecutadas desde la última comprobación.
`restart detection`	Comprueba desde cuándo se ejecuta el servicio de base de datos de manera ininterrumpida.

Nombre	Descripción
`session usage`	Porcentaje de sesiones abiertas respecto al máximo disponible. Muestra el valor actual y el máximo en la descripción del Módulo.

Discovery Cloud

Discovery Cloud permite monitorizar cuentas de Amazon Web Services®, Google Cloud Platform® así como de Microsoft Azure® en una única herramienta.

La gestión de todas las cuentas se administra por medio de la Credential Store ubicada en Profiles → Manage agent groups → Credential Store, o bien por medio de Management → Configuration → Credential store.

Discovery Cloud: Amazon Web Services (AWS)

Para monitorizar una infraestructura en Amazon Web Services se deberán seguir paso a paso las diferentes páginas del asistente.

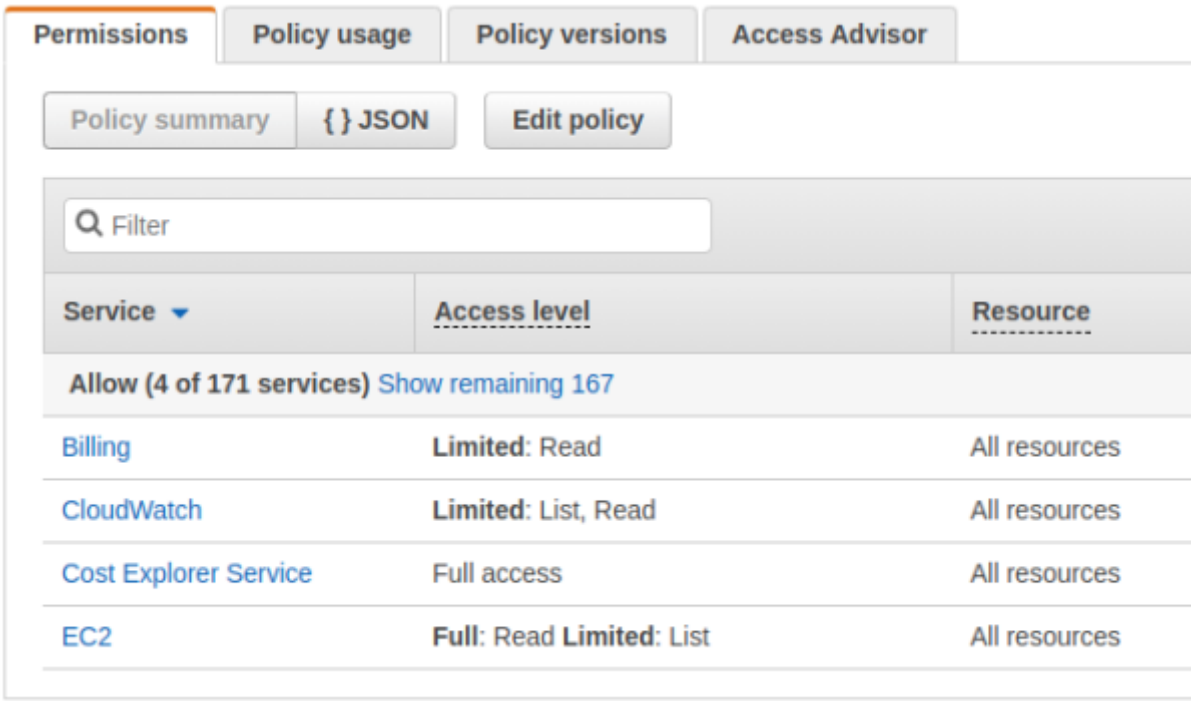
Validación de credenciales AWS

Al acceder al menú de Amazon Web Services® se solicitará seleccionar una cuenta AWS; si existe alguna registrada de versiones anteriores se mostrará como imported_aws_account.

Para añadir mas cuentas se utiliza la opción Manage Accounts, ubicado junto al desplegable de AWS Account. Luego en la sección Credential store de Profiles → Manage agent groups se almacenan todas las cuentas de Amazon Web Services® previamente creadas.

Por cada cuenta que hay en el almacén de credenciales solo se podrá realizar una tarea en el Discovery Amazon EC2.

Se debe ir a AWS y crear las cuentas de consulta con los siguientes permisos:



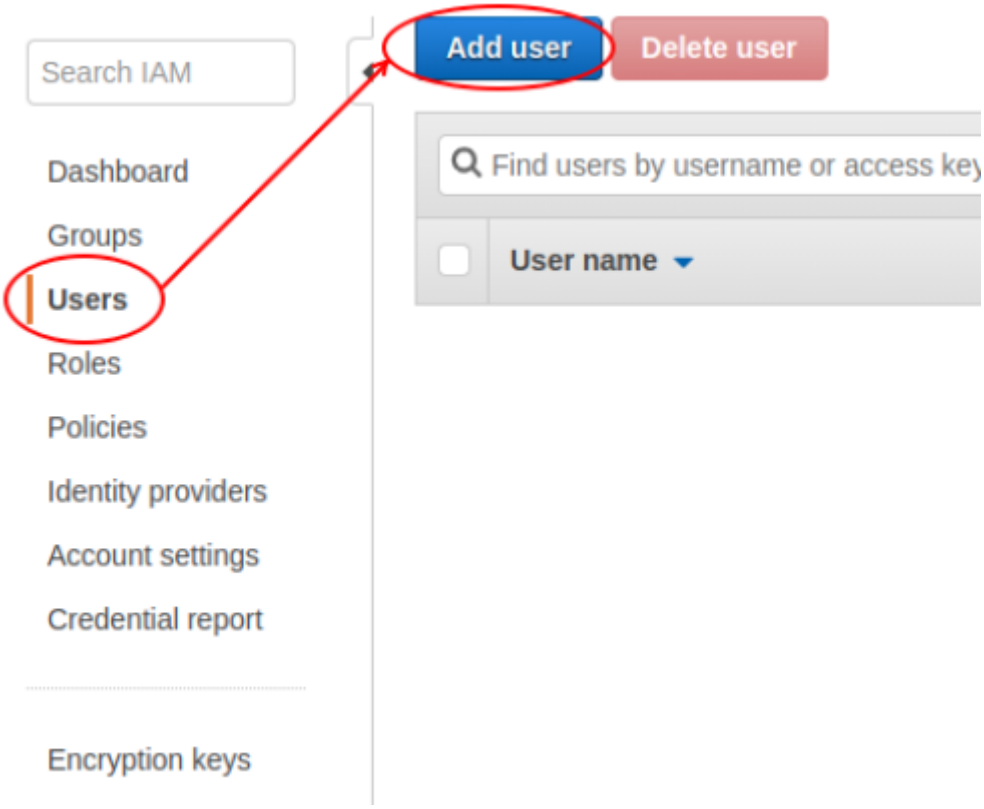
Resumen de la política en JSON:

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Sid": "VisualEditor0",
           "Effect": "Allow",
           "Action": [
               "ec2:DescribeInstances",
               "ec2:DescribeVolumesModifications",
               "ec2:GetHostReservationPurchasePreview",
               "ec2:DescribeSnapshots",
               "aws-portal:ViewUsage",
               "ec2:DescribePlacementGroups",
               "ec2:GetConsoleScreenshot",
               "ec2:DescribeHostReservationOfferings",
               "ec2:DescribeInternetGateways",
               "ec2:GetLaunchTemplateData",
               "ec2:DescribeVolumeStatus",
               "ec2:DescribeScheduledInstanceAvailability",
               "ec2:DescribeSpotDatafeedSubscription",
               "ec2:DescribeVolumes",
               "ec2:DescribeFpgaImageAttribute",
               "ec2:DescribeExportTasks",
               "ec2:DescribeAccountAttributes",
               "aws-portal:ViewBilling",
               "ec2:DescribeNetworkInterfacePermissions",
               "ec2:DescribeReservedInstances",
               "ec2:DescribeKeyPairs",
               "ec2:DescribeNetworkAcls",
               "ec2:DescribeRouteTables",
               "ec2:DescribeReservedInstancesListings",
               "ec2:DescribeEgressOnlyInternetGateways",
```

```
                "ec2:DescribeSpotFleetRequestHistory",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeSnapshotAttribute",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeIdFormat",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribePrefixLists",
                "cloudwatch:GetMetricStatistics",
                "ec2:GetReservedInstancesExchangeQuote",
                "ec2:DescribeVolumeAttribute",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeImportSnapshotTasks",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:GetPasswordData",
                "ec2:DescribeScheduledInstances",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeReservedInstancesModifications",
                "ec2:DescribeElasticGpus",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpnGateways",
                "ec2:DescribeMovingAddresses",
                "ec2:DescribeAddresses",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeRegions",
                "ec2:DescribeFlowLogs",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeVpcEndpointServices",
                "ce:GetCostAndUsage",
                "ec2:DescribeSpotInstanceRequests",
                "cloudwatch:ListMetrics",
                "ec2:DescribeVpcAttribute",
                "ec2:GetConsoleOutput",
                "ec2:DescribeSpotPriceHistory",
                "ce:GetReservationUtilization",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ce:GetDimensionValues",
                "ec2:DescribeVpcEndpointConnections",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeHostReservations",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeTags",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeBundleTasks",
                "ec2:DescribeIdentityIdFormat",
                "ec2:DescribeImportImageTasks",
```

```
                "ec2:DescribeClassicLinkInstances",
                "ec2:DescribeNatGateways",
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeVpcEndpointConnectionNotifications",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSpotFleetRequests",
                "ec2:DescribeHosts",
                "ec2:DescribeImages",
                "ec2:DescribeFpgaImages",
                "ec2:DescribeSpotFleetInstances",
                "ec2:DescribeSecurityGroupReferences",
                "ec2:DescribeVpcs",
                "ec2:DescribeConversionTasks",
                "ec2:DescribeStaleSecurityGroups",
                "ce:GetTags"
            ],
            "Resource": "*"
        }
    ]
}
```

Se debe asignar la política anterior a un usuario nuevo.



Al regresar a la configuración en Pandora FMS, se podrá usar la cuenta registrada para vincular y acceder a la monitorización de AWS.

Si no se dispone de pandora-cm-api en la instalación, se puede obtener del siguiente enlace: Pandora Cloud

Monitoring API .

Discovery Cloud AWS

Una vez validadas las credenciales debe acceder al menú Discovery Cloud → Amazon Web Services. Por cada cuenta que se añada a la Credential store se podrá monitorizar el entorno EC2 albergado en esa cuenta.

Discovery Cloud AWS EC2

Dentro de la monitorización de EC2 están disponibles:

- Monitorización de costes.
- Resumen de recursos registrados en AWS EC2.
- Monitorización de instancias específicas.
- Monitorización de volúmenes y direcciones IP elásticas.

Para iniciar el proceso de monitorización se solicitan una serie de datos básicos para la tarea como el nombre, Discovery Server que la ejecutará, grupo e intervalo.

La monitorización de costes de Amazon Web Services implica pagos extra según explican en Amazon cost management pricing .

Se puede monitorizar tanto el coste global como los costes independientes por región.

Para recolectar información general del estado de reservas en todas las regiones se ha de activar la opción Scan and general monitoring en el paso denominado Recon.

Monitorización de instancias específicas AWS EC2

Se pueden monitorizar instancias específicas para obtener lecturas de:

- `CPUUtilization`: Uso promedio de CPU.
- `DiskReadBytes`: Bytes de lectura (disco).
- `DiskWriteBytes`: Bytes de escritura (disco).
- `DiskReadOps`: Operaciones de lectura (disco).
- `DiskWriteOps`: Operaciones de escritura (disco).
- `NetworkPacketsIn`: Paquetes de entrada (red).
- `NetworkPacketsOut`: Paquetes de salida (red).

Los agentes que representan las instancias específicas tendrán como padre el agente que representa la región en la que se alojan. El *token* update_parent debe estar configurado al valor de

1 en el servidor de Pandora FMS para mantener las relaciones padre-hijo actualizadas.

Discovery Cloud Extras AWS EC2

En este último paso se puede indicar el monitorizar los volúmenes que utilizan las instancias reservadas. Aparecerán dos módulos extra en los agentes de región:

- Total de volumen reservado (GB).
- Total de volúmenes registrados (número).

También se puede elegir activar el *token* Elastic IP Addresses para informar del número de IP elásticas registradas en la cuenta AWS EC2.

En el Discovery Task list siempre se podrá consultar el progreso de la ejecución.

Discovery Cloud AWS RDS

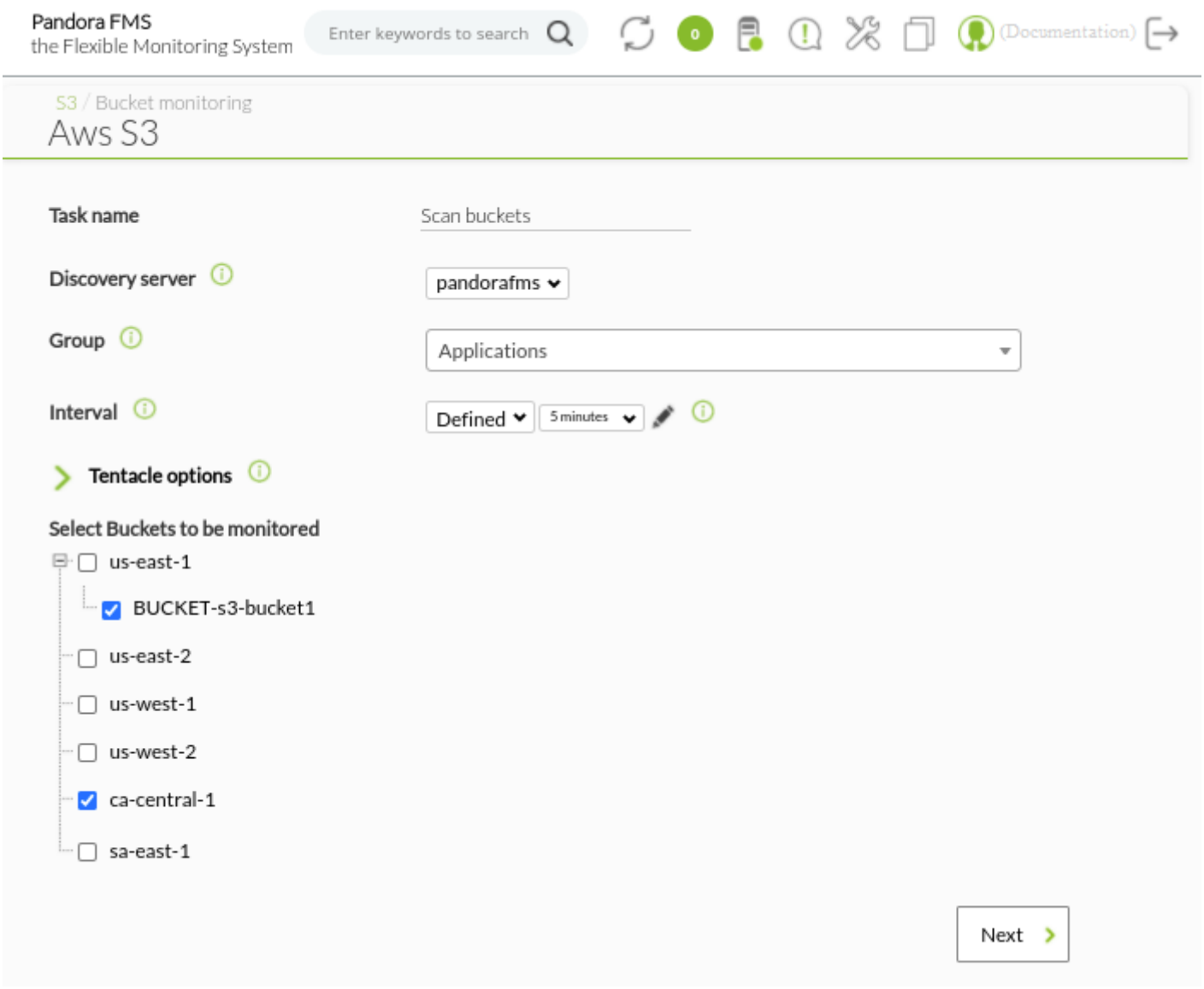
El servicio RDS provee un servidor de base de datos y permite crear la instancia relacionada a dicha base de datos. Ofrece la posibilidad de conectar sus instancias por medio de clientes como SSMS, MySQL workbench o mediante JDBC u ODBC DB APIs.

La integración con AWS RDS sólo soporta Oracle, MySQL y MariaDB.

Discovery Cloud S3 Buckets

El servicio S3 Buckets provee un almacenamiento de ficheros llamados objetos, tales como aplicaciones empresariales, *data lakes*, sitios web, análisis de *big data*, aplicaciones móviles, procesos de copia de seguridad y restauración, operaciones de archivado, entre muchas otras.

Con las credenciales registradas se accede a la creación de una tarea de reconocimiento y se seleccionan los objetos a monitorizar, ya sea uno a uno y/o por regiones.



Pulse el botón Next para avanzar al próximo paso: seleccione el monitorizar tamaño del Bucket y/o su número de elementos, guarde haciendo clic en Finish. Los Agentes que obtendrá serán AWS global y las regiones monitorizadas; los Módulos nuevos serán:

```
bucket.size <bucket-id> (region)
bucket.items <bucket-id> (region)
```

En el caso de monitorización por regiones, un *bucket* que haya sido descubierto y monitorizado, y después haya sido borrado, dejará todos sus Módulos correspondientes en estado desconocido Unknown .

Discovery Cloud. Vista general

Discovery Cloud incluye una vista general que permite revisar los puntos claves de la infraestructura en Amazon Web Services. Pandora FMS mostrará diferentes mapas en función de

las cuentas existentes.

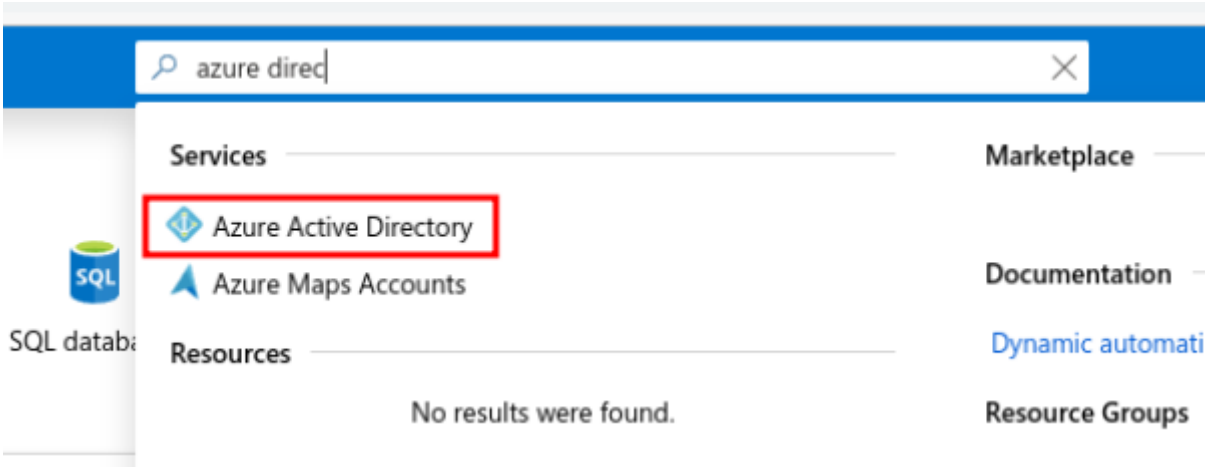
- Coste actual.
- Coste en el periodo previo.
- Gráfica de evolución de costes (6 meses).
- Gráfica de evolución de reservas/instancias (1 mes).
- Mapa de regiones con el número de instancias por región.

Discovery Cloud: Microsoft Azure

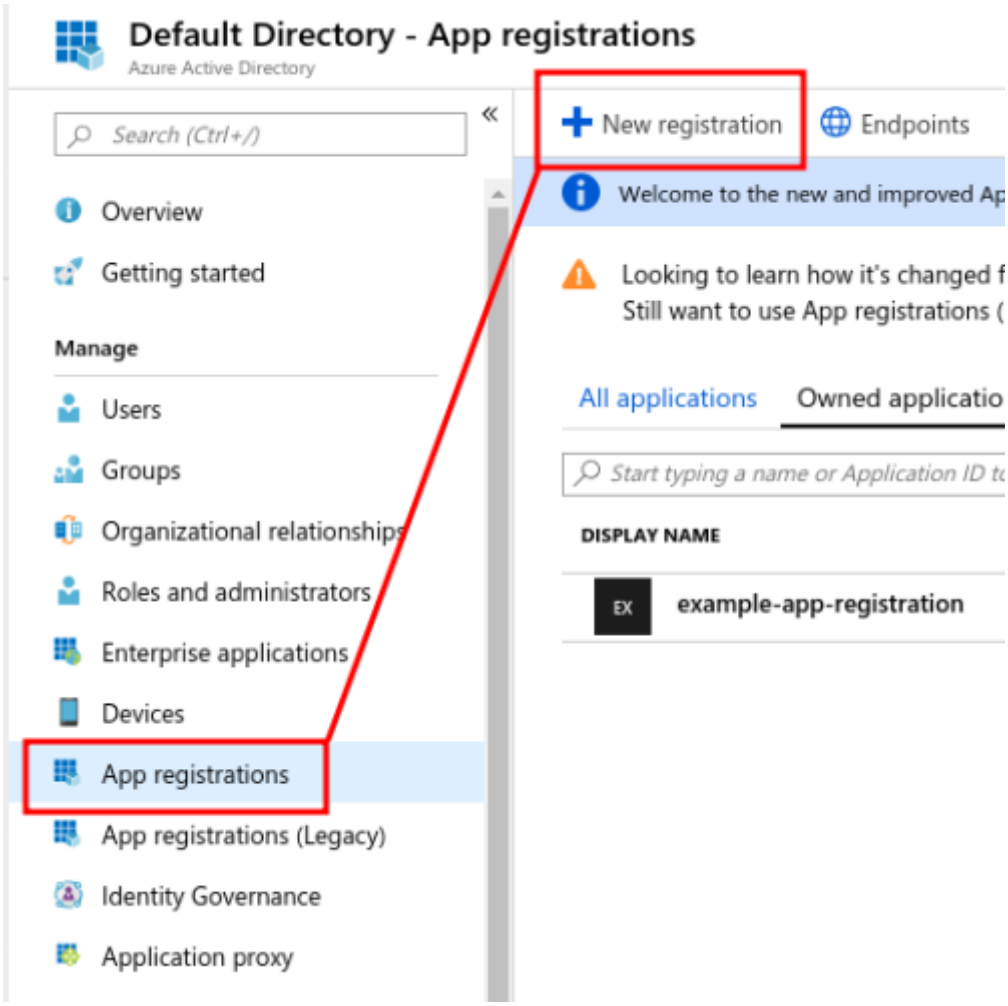
Para monitorizar una infraestructura en Microsoft Azure® cumpla paso a paso las siguientes instrucciones.

¿Cómo dar de alta un usuario para usar la API de Azure?

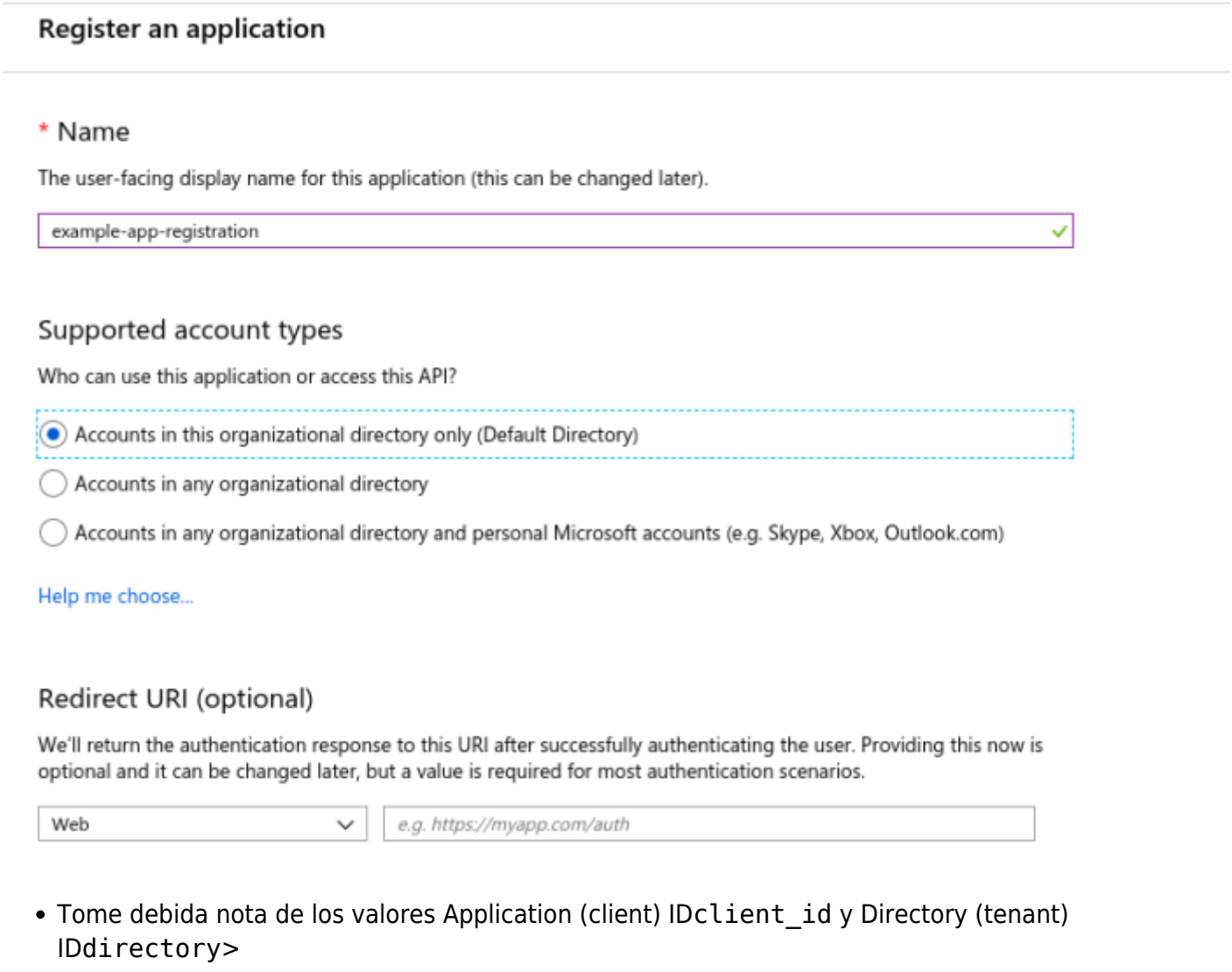
- Se ha de acceder al portal de Microsoft Azure®.
- Se abre el servicio Azure Active Directory:



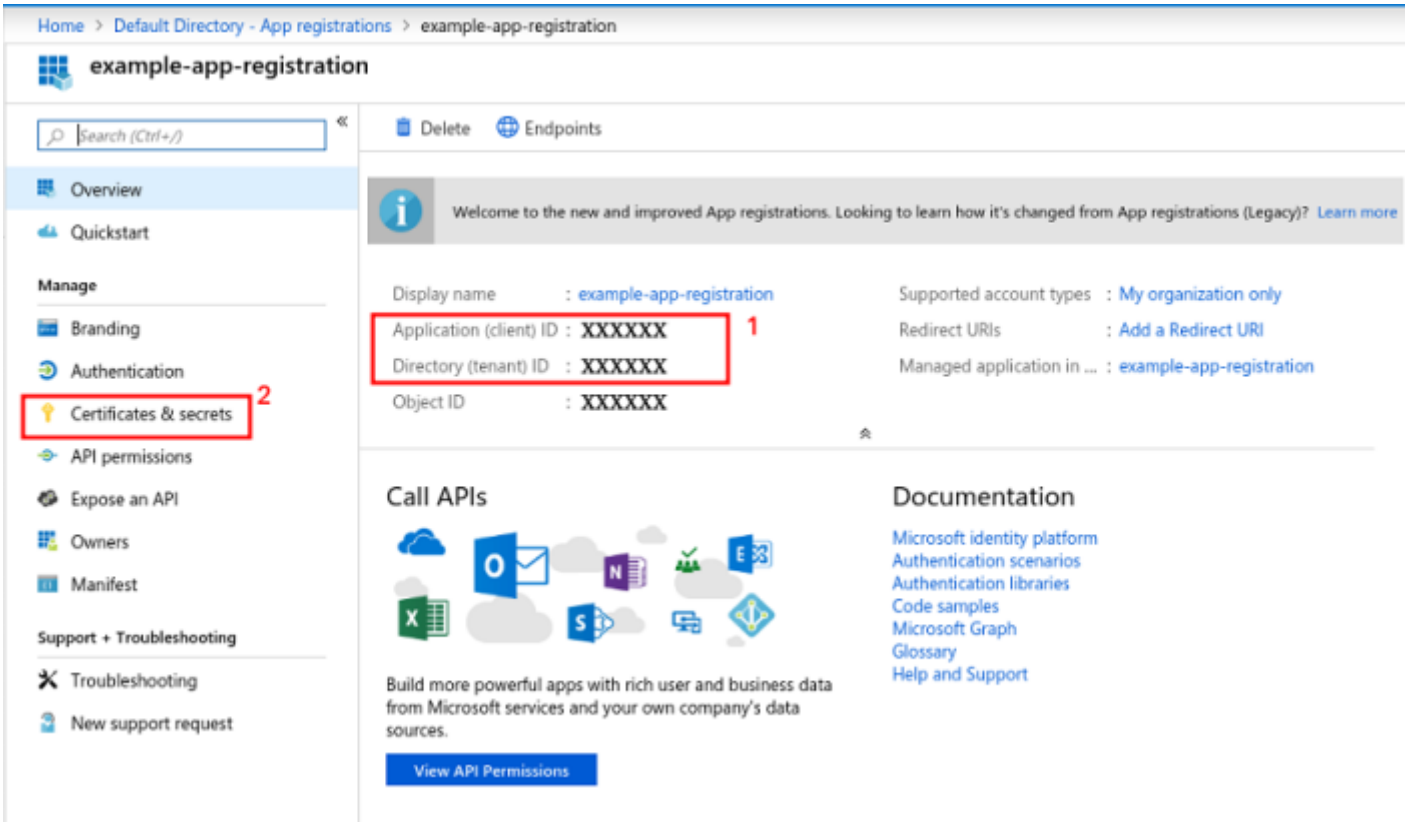
- App registrations → New registration:



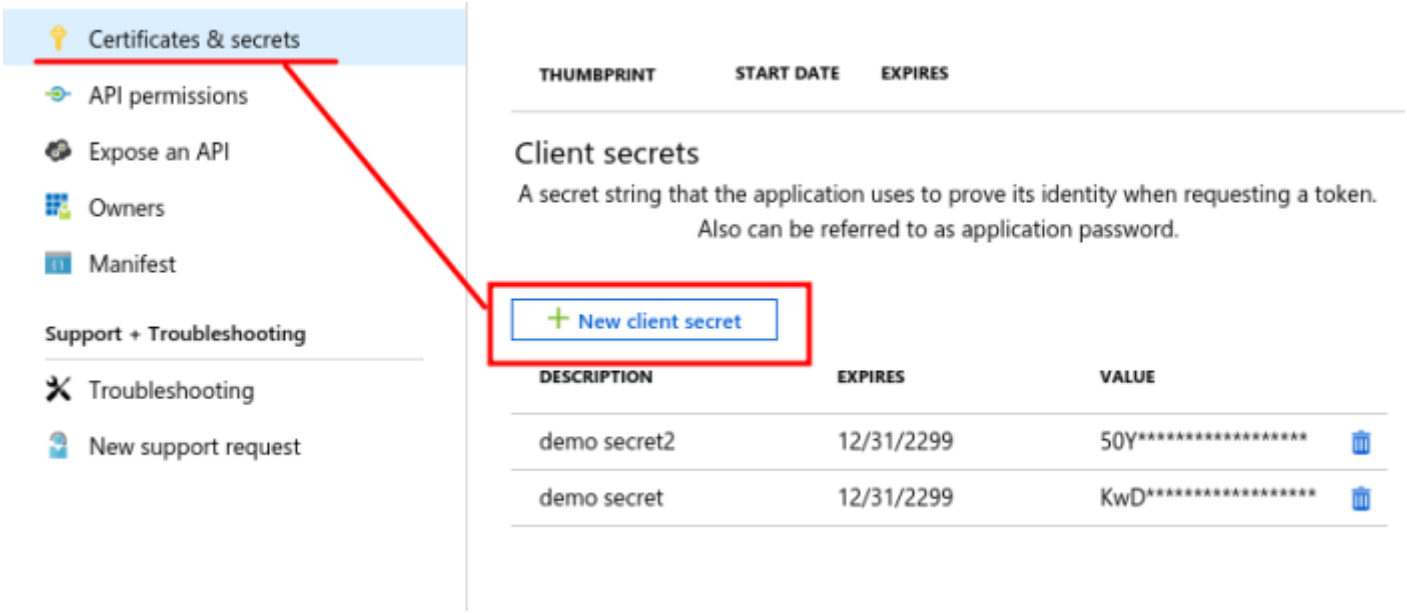
- Introduzca los siguientes datos:



- Tome debida nota de los valores Application (client) ID`client_id` y Directory (tenant) ID`directory>`



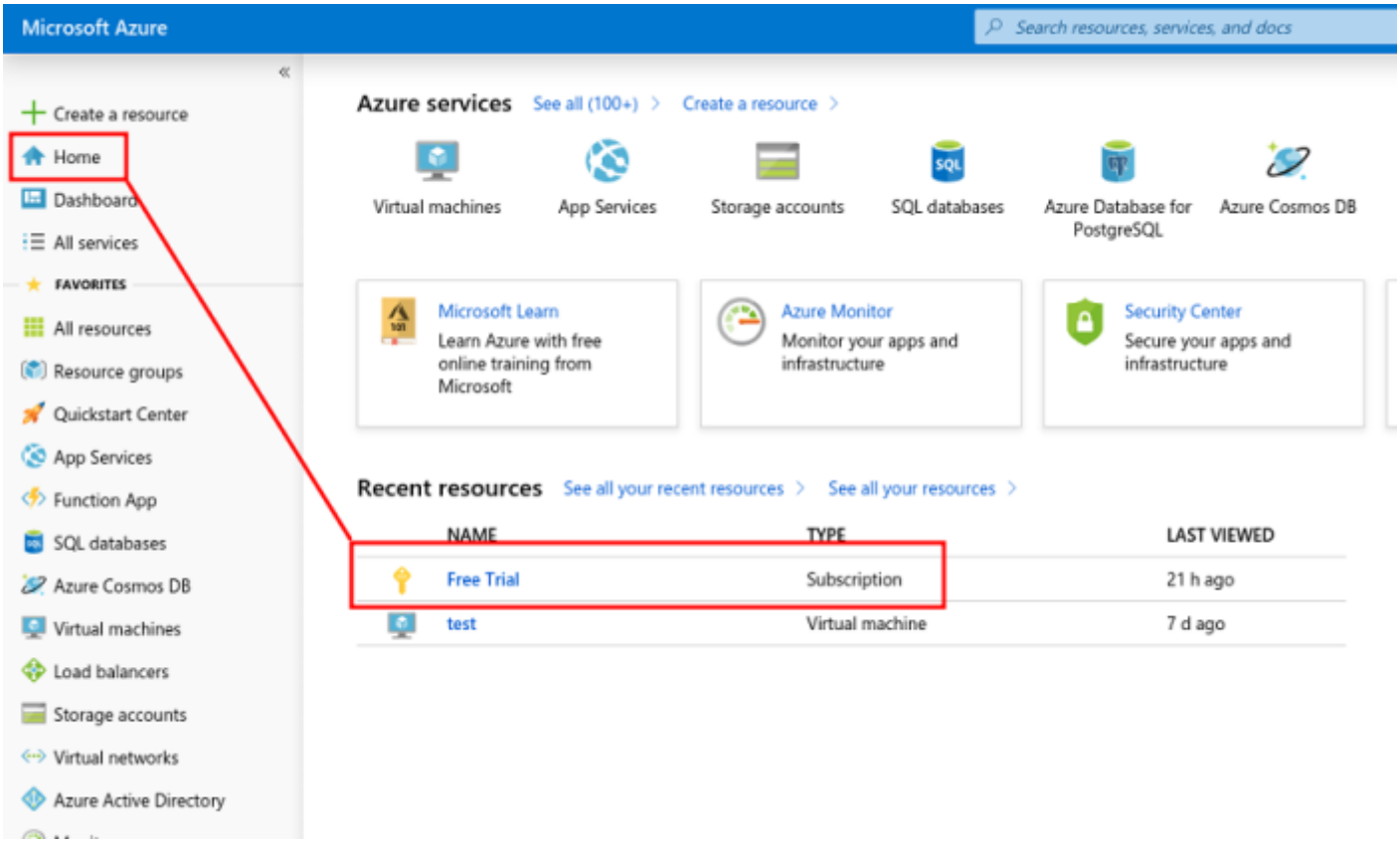
- En certificates & secrets se agrega uno nuevo:



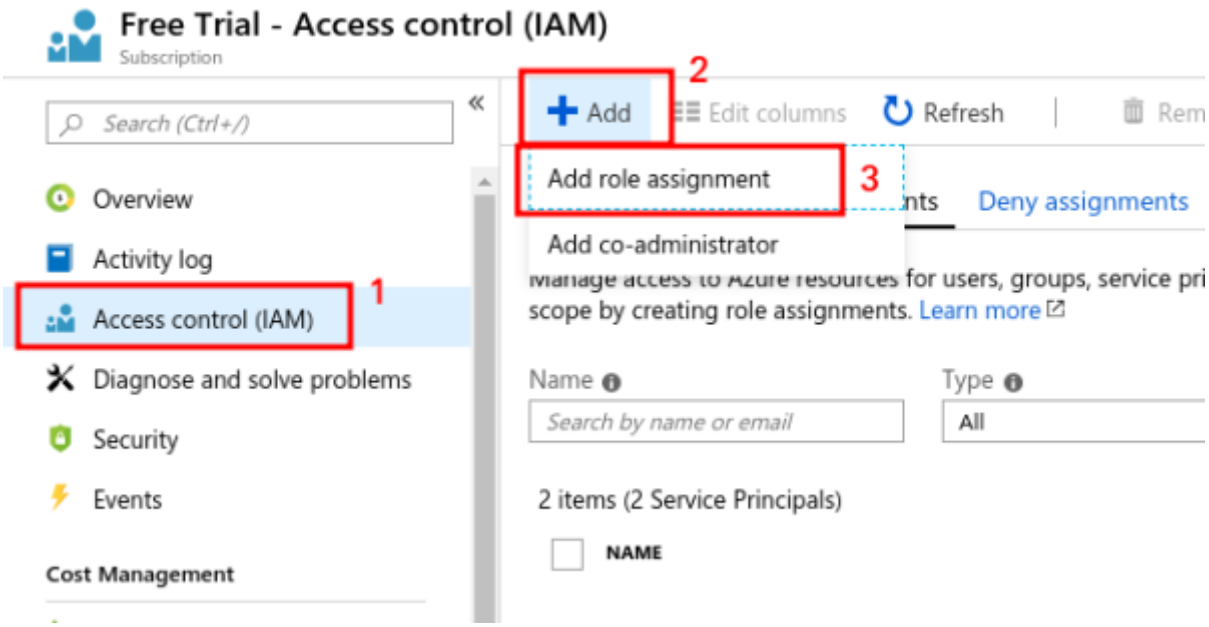
Será necesario apuntar la clave que se muestra, es el `application_secret`.

Asignación de permisos

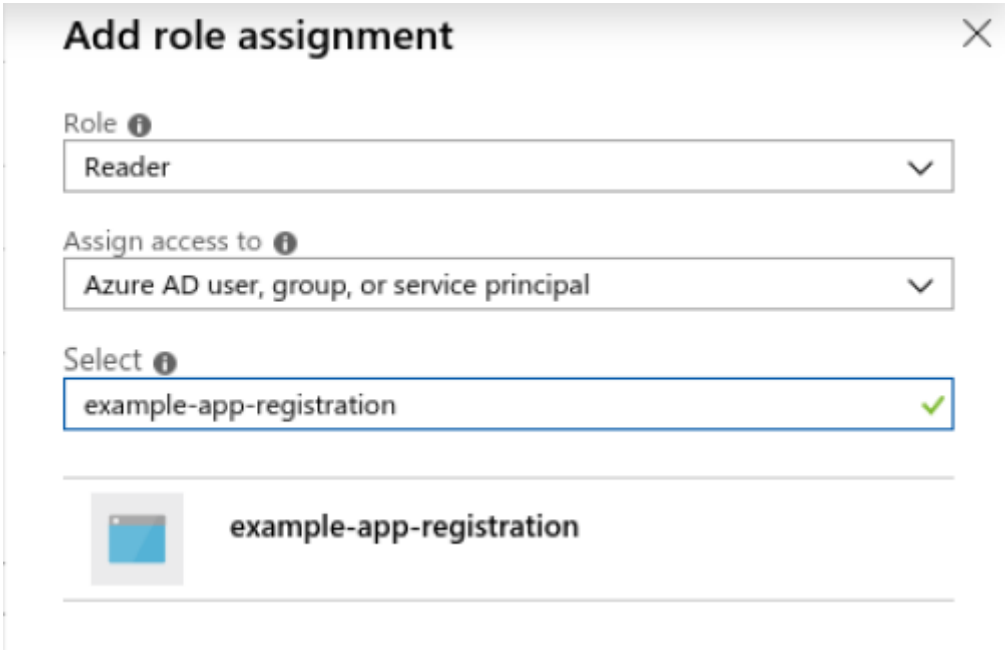
Se debe asignar un rol a la cuenta con la que vaya a operar la *app*, para ello se accede a Home → Suscription:



Se selecciona Access control (IAM):



Se agregará una nueva asignación de rol, se coloca Reader para la *app* creada:



Guarde los cambios pulsando *Save* .

A partir de ese momento podrá conectar con el servicio y hacer solicitudes a través de pandora-cm-api.

Configurar la tarea en Pandora FMS

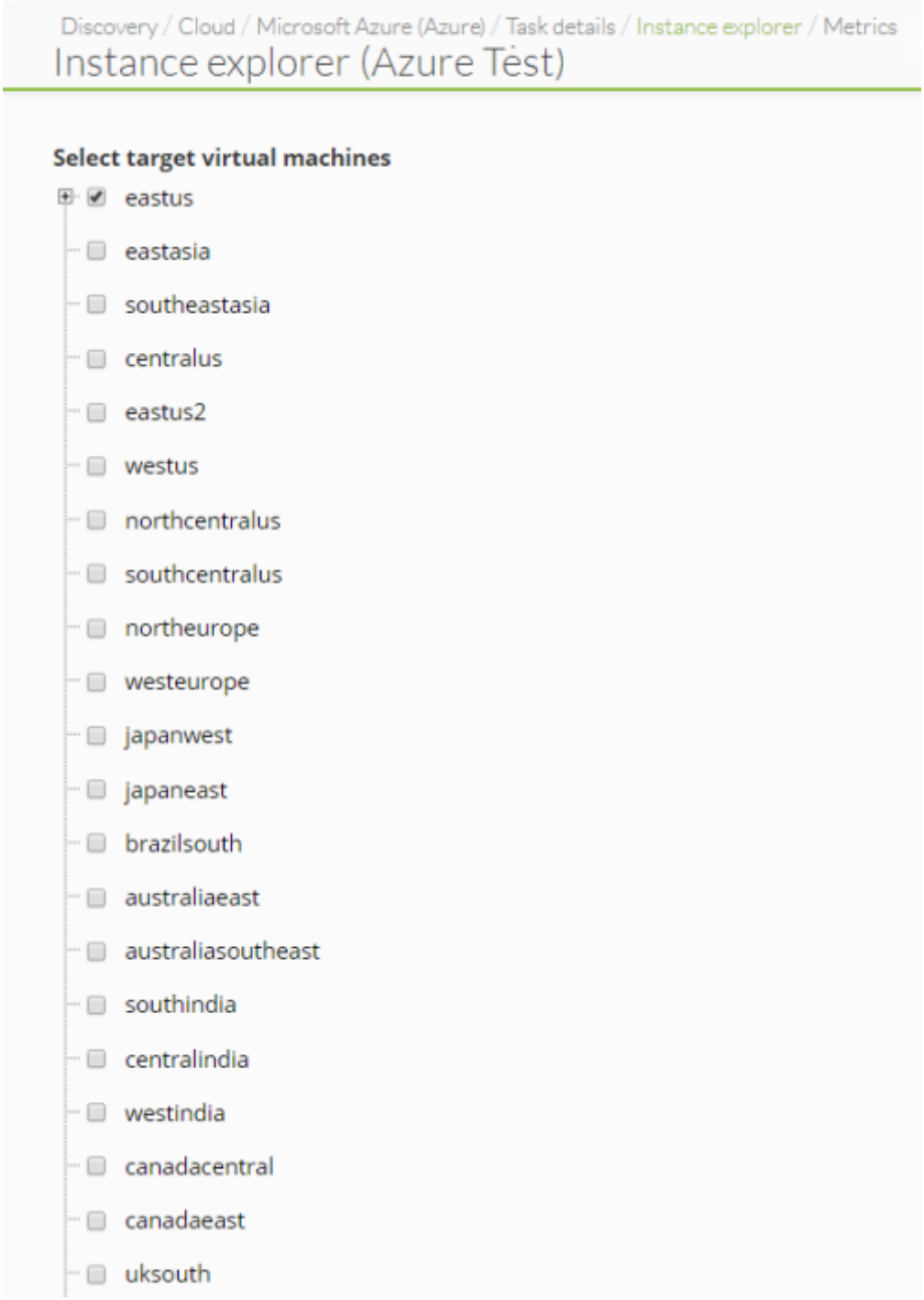
Pandora FMS permite la gestión de varias cuentas de Microsoft Azure®. Se pueden añadir tantas cuentas como sea necesario a través de la opción Manage Accounts que se encuentra junto al

desplegable de Account.

Esto permite acceder a la sección Credential store ubicada en Profiles → Manage agent groups y que hará las veces de almacén de todas las cuentas de Microsoft Azure® previamente creadas y registradas.

Se ha de configurar una nueva tarea:

- Se agrega una nueva clave a la Credential store .
- Se accede a Discovery → Cloud → Azure y valida la cuenta de Azure.
- A partir de este punto se necesita definir nombre, servidor que ejecutará la tarea, grupo al e intervalo de ejecución.
- Una vez definidos los datos de la tarea, se seleccionan las regiones de la cuenta creada de Azure que serán monitorizadas. Cada región permitirá a su vez seleccionar las instancias deseadas.



- El último paso será seleccionar las métricas a obtener de los agentes que Pandora FMS creará por cada instancia que encuentre en Microsoft Azure®. Una vez configurada esta sección, se podrá lanzar la tarea y Pandora FMS creará de forma automática los agentes en función de las instancias solicitadas en los pasos previos.

Complementos en Pandora FMS

- " Pandora Azure Storage ".

Discovery Cloud: Google Cloud Platform (GCP)

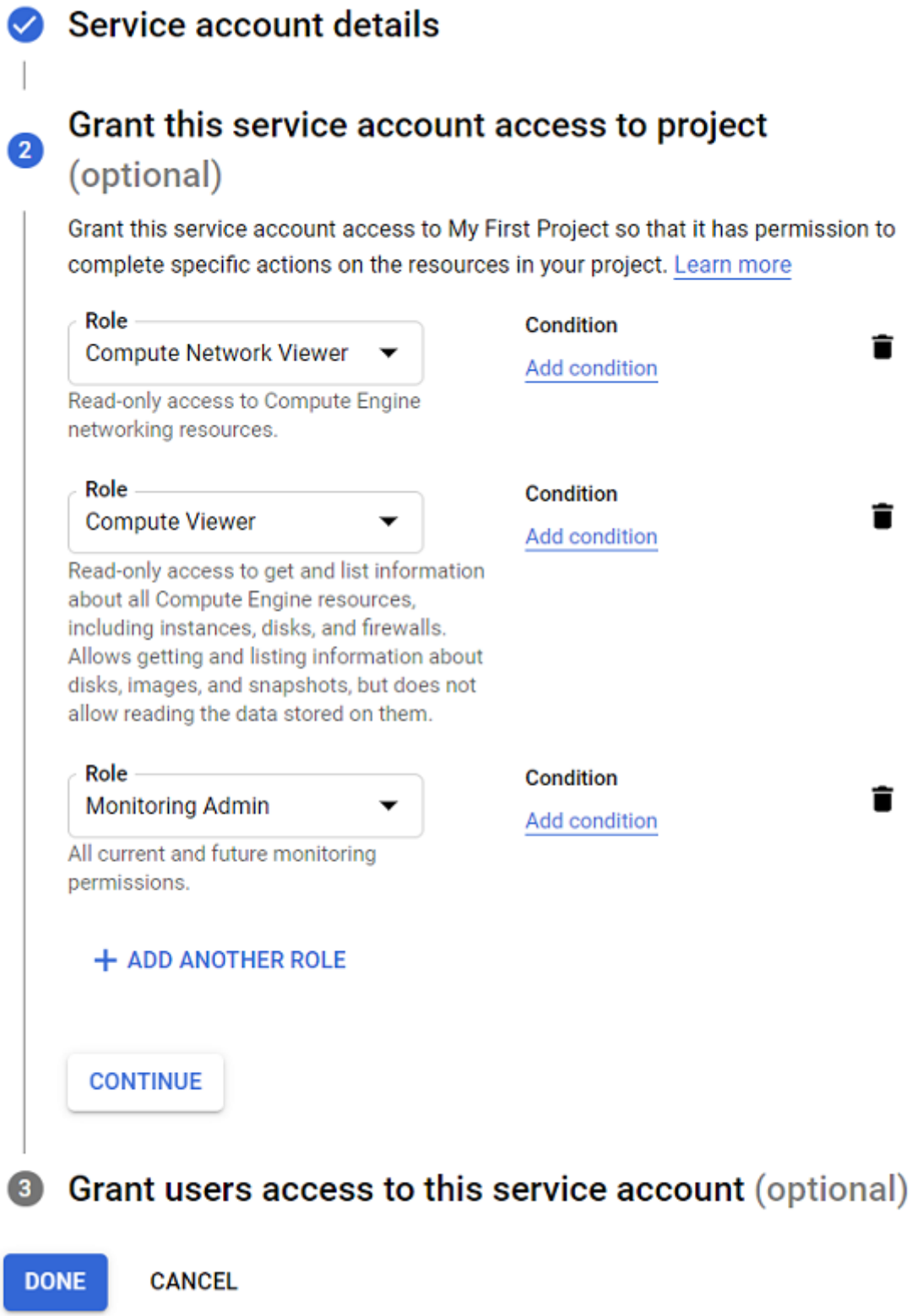
Esta funcionalidad esta disponible a partir de la versión

750 de Pandora FMS.

Validación de credenciales Google Cloud Platform (GCP)

Para acceder a la consola de Google Cloud se ha de registrar la clave JSON.

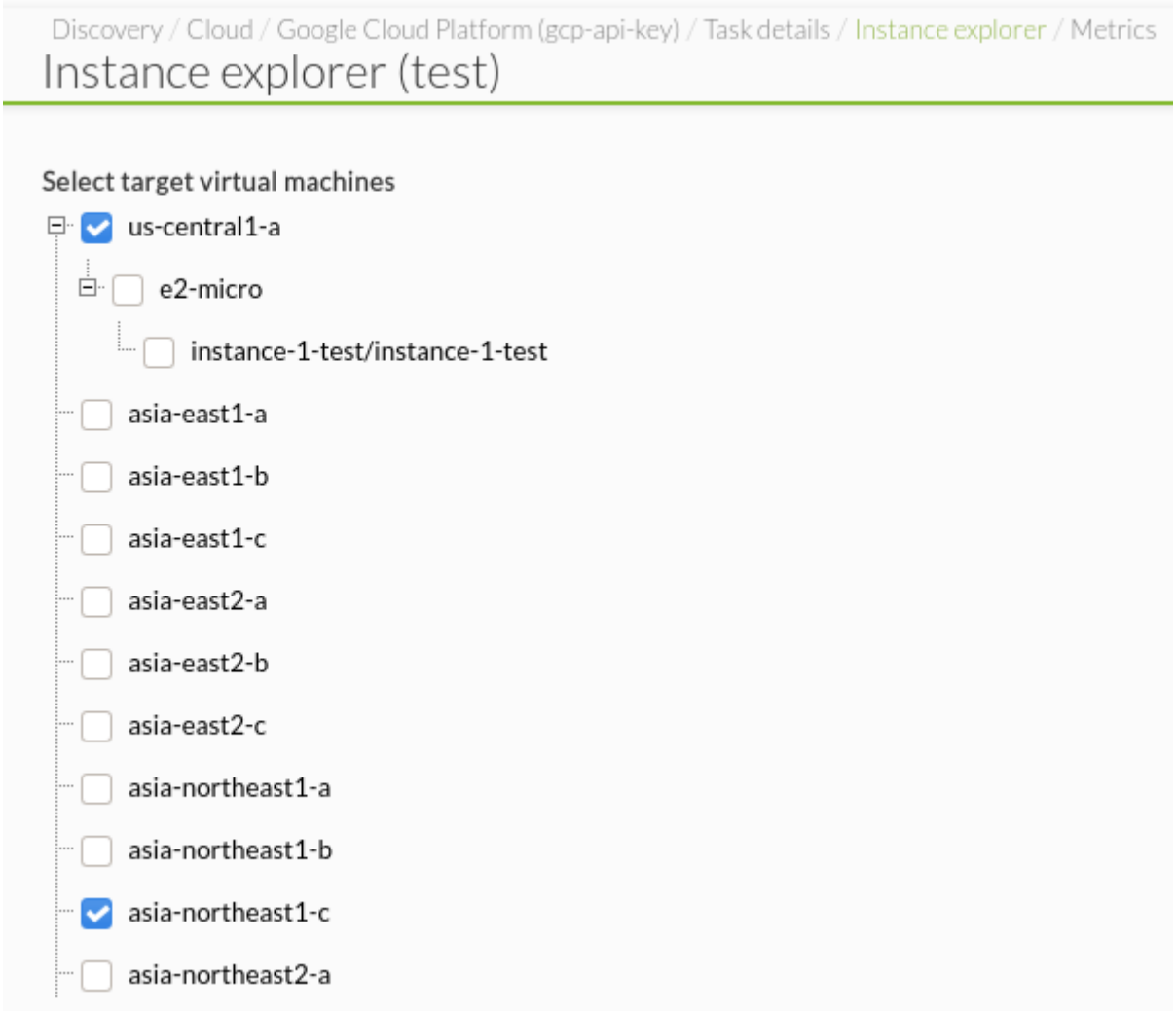
- Se accede a la configuración de seguridad en GCP IAM. La cuenta de acceso a registrar será una cuenta de servicio con los siguientes privilegios:



- Se accede en Pandora FMS enCredential Store ubicada en Profiles → Manage agent groups → Credential Store con el botón Add key.
- En el desplegable Producto se escoge Google y se añade la clave JSON de la cuenta GCP (el campo usuario se rellenará automáticamente).
- Luego se accede a Discovery → Cloud → Google Cloud Platform y se valida la cuenta de GCP al definir una tarea de Discovery GCP.

Configurar la tarea en Pandora FMS

Para definir la tarea, se especifica un nombre, el servidor Discovery encargado de ella junto con el grupo e intervalo de monitorización. Una vez definidos los datos de la tarea, se ha de seleccionar las regiones de la cuenta GCP que serán monitorizadas. Cada región permitirá a su vez seleccionar las instancias deseadas.



Al seleccionar una zona automáticamente se monitorizarán nuevas instancias detectadas dentro de esa zona. Al seleccionar una instancia esta se monitorizará de manera explícita aunque su zona no esté monitorizada.

El último paso es seleccionar las métricas a obtener de los agentes que Pandora FMS creará por cada instancia que encuentre en Google Cloud Platform®:

- Scan and general monitoring.
- CPU performance summary.
- IOPS performance summary.
- Disk performance summary.
- Network performance summary.

Un agente *genérico* llamado Google o GCP en el que aparecerán todos los módulos relacionados con la monitorización de google.

Aquellas instancias que desaparezcan de una zona que se monitoriza de forma constante aparecerán en estado crítico o *removed* y todos los demás módulos en desconocido. En caso de que toda la instancia pase a desconocido puede utilizar el modo auto-disable.

Posteriormente también podrá consultar un mapa desde la lista de tareas de GCP.

Discovery Console Tasks

De forma análoga a Task List, Console Tasks permite crear nuevas tareas teniendo en cuenta el grupo al que pertenecerá, periodicidad, consola que la ejecuta, etcétera.

Discovery Host&Devices

NetScan

NetScan permite descubrir dispositivos en una red y aplicar diferentes reglas de monitorización. Al crear una tarea se establece de antemano el grupo al cual pertenecerá y debe seleccionar la opción en el reconocimiento:

- Cargar un archivo en formato CSV con los dispositivos concretos a comprobar (en Use CSV file definition: puede seleccionar un fichero).
- O por medio de la red, en Network puede especificar redes o nombres de dominio completos de un *host* específico, separados por comas, por ejemplo: `192.168.50.0/24` o `192.168.60.0/24, hostname.pandorafms.com`. De ser necesario habilite la opción Name resolution para los nombres de dominio.

Los intervalos seleccionados como manuales deberán lanzarse manualmente. Discovery no lanzará una tarea manual automáticamente. Los agentes detectados por NetScan son agentes remotos sin fichero de configuración. No podrá aplicar políticas de monitorización locales ni agregar cambios de configuración en bloque si no despliega un agente en los objetivos.

Algunas opciones de NetScan:

- Auto discover known hardware: El autodescubrimiento de hardware conocido aplica de forma dinámica las plantillas añadidas que se hayan añadido por medio de Private Enterprise Number.
- Modules templates: Intenta aplicar los módulos de las plantillas seleccionadas. Si la ejecución no pasa la prueba, no se agregarán a la lista de monitorización.
- Apply autoconfiguration rules: Aplica las reglas de configuración automática definidas previamente a los agentes detectados. La configuración automática permite aplicar políticas, cambios de grupo y configuración, así como lanzar eventos personalizados o ejecutar *scripts* en acciones.
- SNMP enabled: Para completar la información obtenida de los dispositivos de red descubiertos se debe de habilitar SNMP. Con ello se mejora la detección explorando la información SNMP disponible en los objetivos descubiertos. Al habilitar este *token* aparecerán dos opciones adicionales:
  - Versión SNMP.
  - Versión 766 o posterior: Utilice la opción Skip non-enabled interfaces para evitar consultar las interfaces inhabilitadas.
- WMI enabled: Se puede habilitar el escaneo WMI para MS Microsoft con las credenciales previamente cargadas en el almacén de claves.

Se probarán las diferentes credenciales provistas contra los objetivos detectados que soporten WMI, complementando la monitorización con módulos que informarán sobre el uso de CPU, memoria y disco.

- Parent recursion: Mejora la detección de padres agregando recursión al proceso.
- VLAN enabled: Detecta las VLAN a las que están conectados los diferentes dispositivos.

Despliegue automático de agentes

Consulte el tema "Despliegue automático de agentes".

Custom NetScan

Permite la ejecución de *scripts* personalizados para la ejecución de tareas de reconocimiento de red. Se ha de especificar el grupo al que pertenece y el intervalo de ejecución. Una vez completado el proceso de creación de la tarea será necesario especificar el *script* a ejecutar, así como el fichero de configuración necesario para su ejecución.

Net scan scripts

Esta sección muestra los diferentes *scripts* que se hayan creado para las tareas de reconocimiento personalizadas, se accede mediante el menú Management → Discovery → Host&devices → Manage scan scripts.

Pandora FMS permite añadir *scripts* adicionales para facilitar la monitorización y el reconocimiento de las redes requeridas. Con la creación de *scripts* se permite añadir macros con las cuales se

pueden definir todos los parámetros que sean necesarios para la correcta ejecución del *script*.

Volver al índice de documentación de Pandora FMS