Discovery

Discovery

We are working on the translation of the Pandora FMS documentation. Sorry for any inconvenience.

Discovery

What is Pandora FMS Discovery?

Discovery Task list

The Pandora FMS Discovery tool allows you to see a list of all the tasks scheduled in the environment, both at the console level and at the server level.

Discovery Applications {{:wiki:icono-modulo-enterprise.png?nolink&23x23 |Enterprise Version}}

It allows monitoring MySQL®, Oracle® or VMware® environments from a new administration console.

Discovery Cloud {{:wiki:icono-modulo-enterprise.png?nolink&23x23 |Enterprise Version}}

Through this utility you can monitor your infrastructure in the Cloud, from virtual machines created in Amazon Web Services® (EC2) or relational databases in AWS RDS to virtual machines running on Azure Computer®.

Discovery Console Tasks {{:wiki:enterprise-module-icon.png?nolink&23x23 |Enterprise Version} }

It allows automating both console tasks within the Discovery system, such as scheduling reports, performing data backups or executing custom scripts from the Pandora FMS Console.

Discovery Host&Devices

It includes the necessary tools to discover or import devices.

Discovery Applications

EWith Pandora FMS it is It is possible to monitor applications remotely using Discovery Applications.

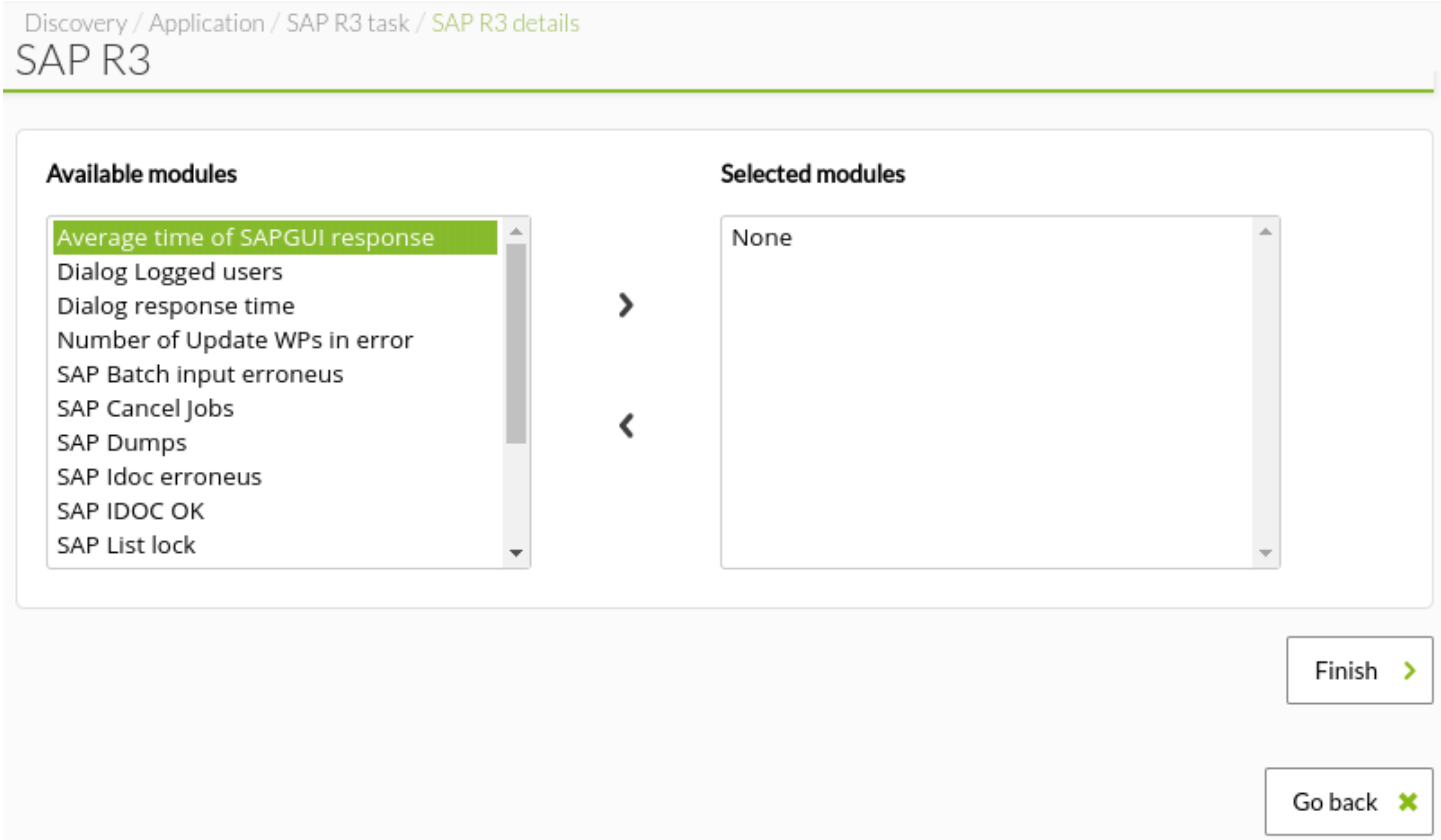
Discovery Applications: SAP

Version NG 741 or later.

The system will guide each Step to configure SAP according to the needs that you have. The same task can be defined to monitor systems with similar configurations (versions 741 to 768).

If different configurations need to be monitored, a task must be created for each configuration.

You must select from the list the information about the SAP system that you want to retrieve:



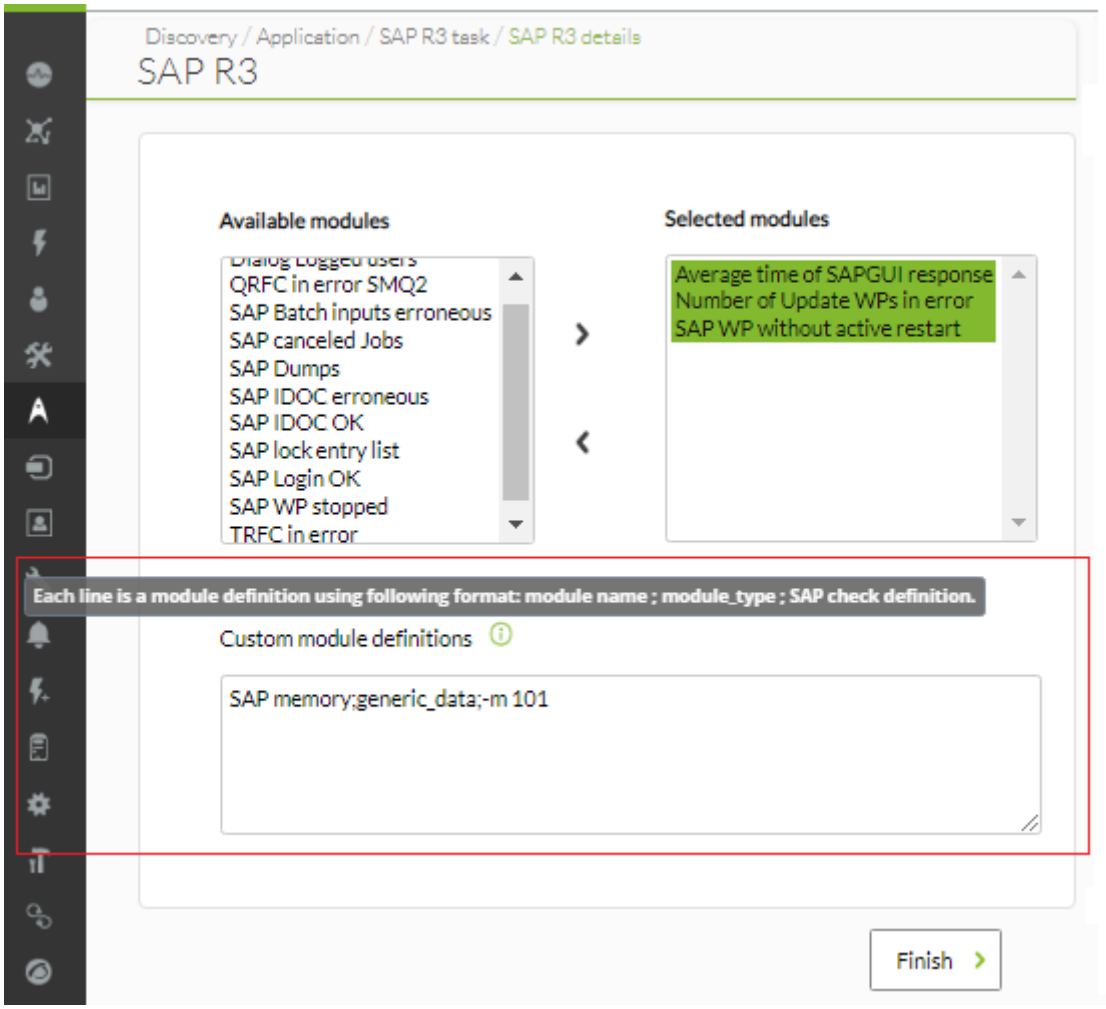
Pandora FMS Discovery will be in charge of collecting the information, storing it in agents represented by the SAP Hostnames that you have defined (versions 741 to 768) or in SAP Hostname (version 769 or later).

If you install Pandora FMS from packages, or your system is older than NG741, you must deploy the official SAP plugin on the Pandora FMS server and configure it manually according to the Manual installation of the Discovery connector for SAP section.

Custom SAPs

Version NG 747 or later.

Apart from the Modules available (Available modules) in Pandora FMS, you can add a large number of additional Modules using the Custom module definitions section.



Each line to be added must use the following format, using the semicolon as a field separator:

```
<module name>;<module type>;<sap check definition>
```

An example to know the information of the SAP system:

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

You can add as many custom modules as needed, the process continues in the same way described in the previous section.

Discovery Applications: VMware

It must be taken into account that if the Pandora FMS server has the `autocreate_group` token active, priority will be given to the group corresponding to the indicated ID, instead of applying the wizard configuration.

Once the basic configuration of VMware is complete, the following must be specified:

- Max threads: Number of threads that the VMware monitoring script will use to speed up data collection.
- Event mode: (Only for VCenter) enables event-based monitoring of VMware VCenter. This working mode is exclusive and independent of standard monitoring.
- Extra settings: Any advanced settings that are necessary to customize the monitoring should be included here, in text mode.VMware no.

Discovery Applications: MS SQL

Pandora FMS allows you to monitor Microsoft SQL Server® databases. For this it is necessary to have installed the Microsoft® Open Database Connectivity (ODBC).

Configuring a Discovery Applications MS SQL Task

To create a task Monitoring for a Microsoft SQL Server® database must be accessed through Discovery (Discovery → Applications → Microsoft SQL Server).

Once the Microsoft SQL Server® task has been chosen, the instances must be defined (Instance):

```
IP\Instance
```

To define a port (Port):

```
IP:Port\Instance
```

Modules available by default

The user and credential used to monitor must have the necessary permissions on the databases to be connected to perform the corresponding operations.

Name	Description
`MSSQL connection`	Checks if there is a connection to the MS SQL server.
`queries: delete`	Number of delete queries executed since last check.

Name	Description
queries: insert	Number of insert queries executed since last check.
queries: update	Number of update queries executed since the last check.
queries: select	Number of read queries executed since last check.
restart detection	Checks since when the database service has been running continuously.
session usage	Percentage of open sessions with respect to the maximum available. Show current and maximum value in Module description.

Discovery Cloud

Discovery Cloud allows monitoring Amazon Web Services®, Google Cloud Platform® and Microsoft Azure® accounts in a single tool.

Management of all accounts is managed through the Credential Store located at Profiles → Manage agent groups → Credential Store, or through Management → Configuration → Credential store.

Discovery Cloud: Amazon Web Services (AWS)

To monitor an infrastructure in Amazon Web Services, the different pages of the wizard must be followed step by step.

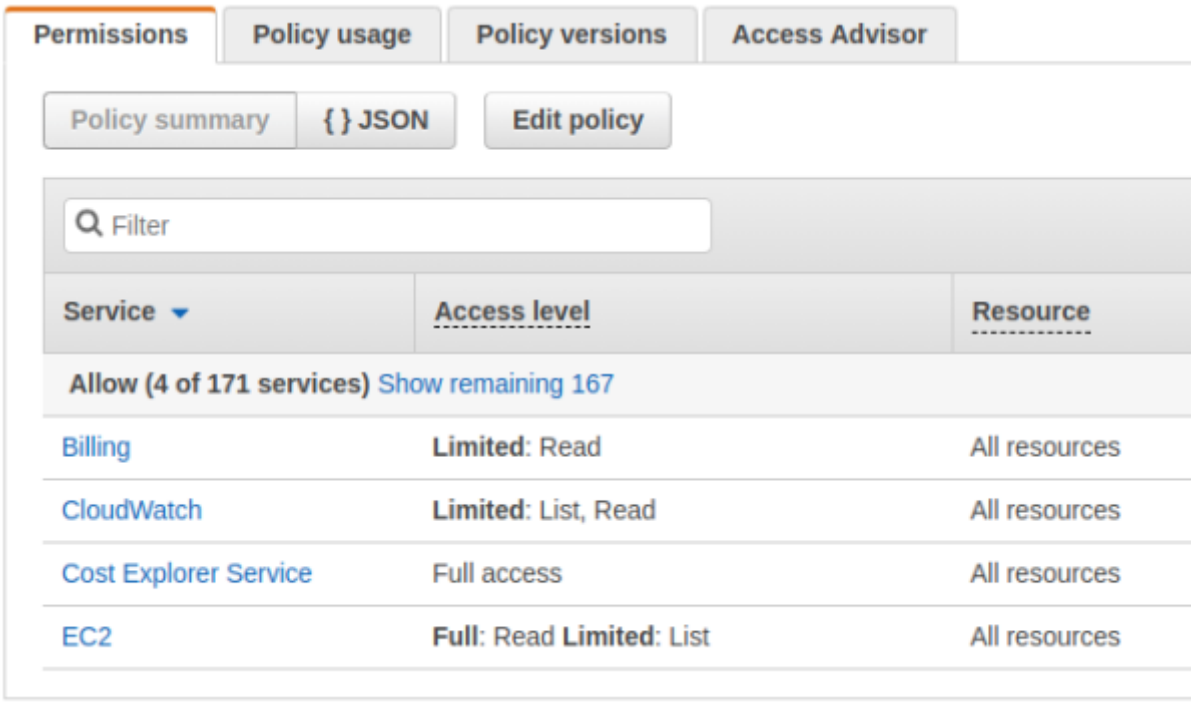
AWS Credential Validation

When accessing the Amazon Web Services® menu, you will be asked to select an AWS account; if there are any registered from previous versions it will be shown as imported_aws_account.

To add more accounts, use the Manage Accounts option, located next to the AWS Account dropdown. Then, in the Credential store section of Profiles → Manage agent groups, all previously created Amazon Web Services® accounts are stored.

For each account in the credential store, only one task can
be performed in Amazon EC2 Discovery.

You need to go to AWS and create the query accounts with the following permissions:



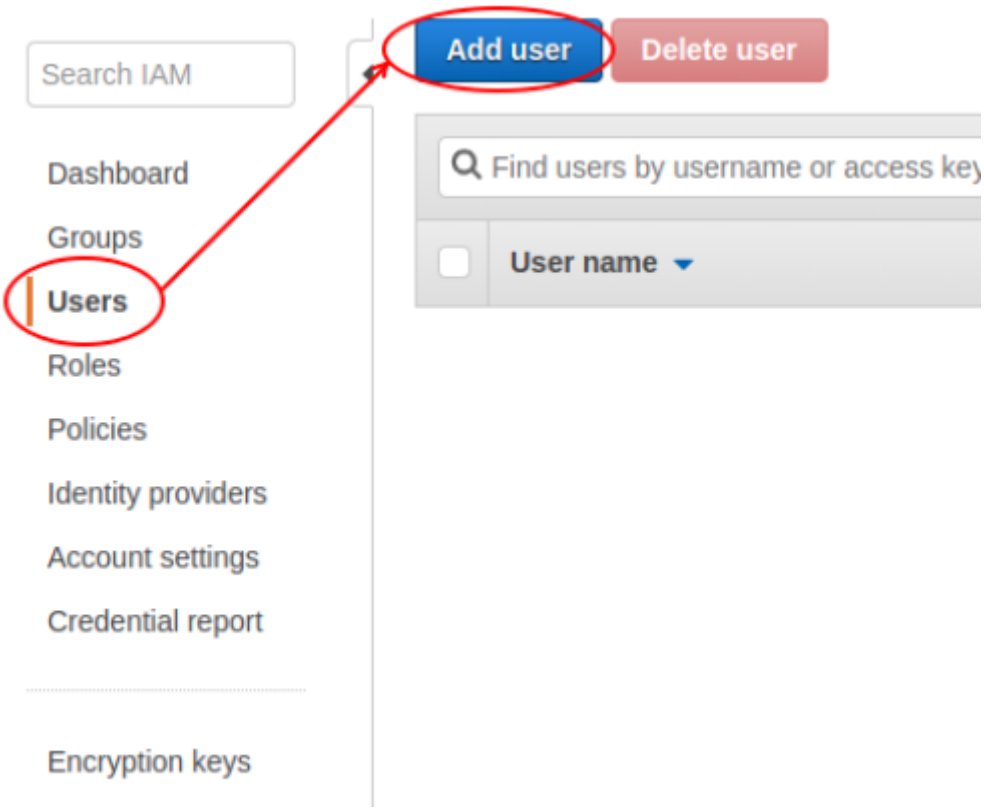
Policy summary in JSON:

```
{
    "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": "*"
        }
    ]
}
```

The old policy must be assigned to a new user.



When you return to the configuration in Pandora FMS, you can use the registered account to link and access AWS monitoring.

If pandora-cm-api is not available in the installation, it can be obtained from the following link: Pandora Cloud

Monitoring API .

Discovery Cloud AWS

Once the credentials you must access the menu Discovery Cloud → Amazon Web Services. For each account that is added to the Credential store, the EC2 environment hosted by that account can be monitored.

Discovery Cloud AWS EC2

Within monitoring from EC2 are available:

- Cost monitoring.
- Summary of resources registered in AWS EC2.
- Monitoring of specific instances.
- Monitoring volumes and elastic IP addresses.

To start the monitoring process, a series of basic data is requested for the task, such as the name, Discovery Server that will execute it, group, and interval.

Amazon Web Services cost monitoring involves extra payments as explained in Amazon cost management pricing .

You can monitor tboth the global cost and the independent costs by region.

To collect general information on the status of reservations in all regions, the Scan and general monitoring option must be activated in the step called Recon.

Monitoring specific AWS EC2 instances

Specific instances can be monitored to obtain readings of:

- `CPUUtilization`: Average CPU usage.
- `DiskReadBytes`: Read bytes (disk).
- `DiskWriteBytes`: Write bytes (disk).
- `DiskReadOps`: Read operations (disk).
- `DiskWriteOps`: Write operations (disk).
- `NetworkPacketsIn`: Input packets (network).
- `NetworkPacketsOut`: Outgoing packets (network).

The agents that represent the specific instances will be parented by the agent that represents the region in which they are hosted. The update_parent token must be configured to the value of 1 in

the Pandora FMS server to keep the parent-child relationships updated.

Discovery Cloud Extras AWS EC2

In this last step, you can specify to monitor the volumes used by the reserved instances. Two extra modules will appear in region agents:

- Total reserved volume (GB).
- Total volumes registered (number).

You can also choose to enable the Elastic IP Addresses token to report the number of Elastic IPs registered in the AWS EC2 account.

In the Discovery Task list you can always check the progress of the execution.

Discovery Cloud AWS RDS

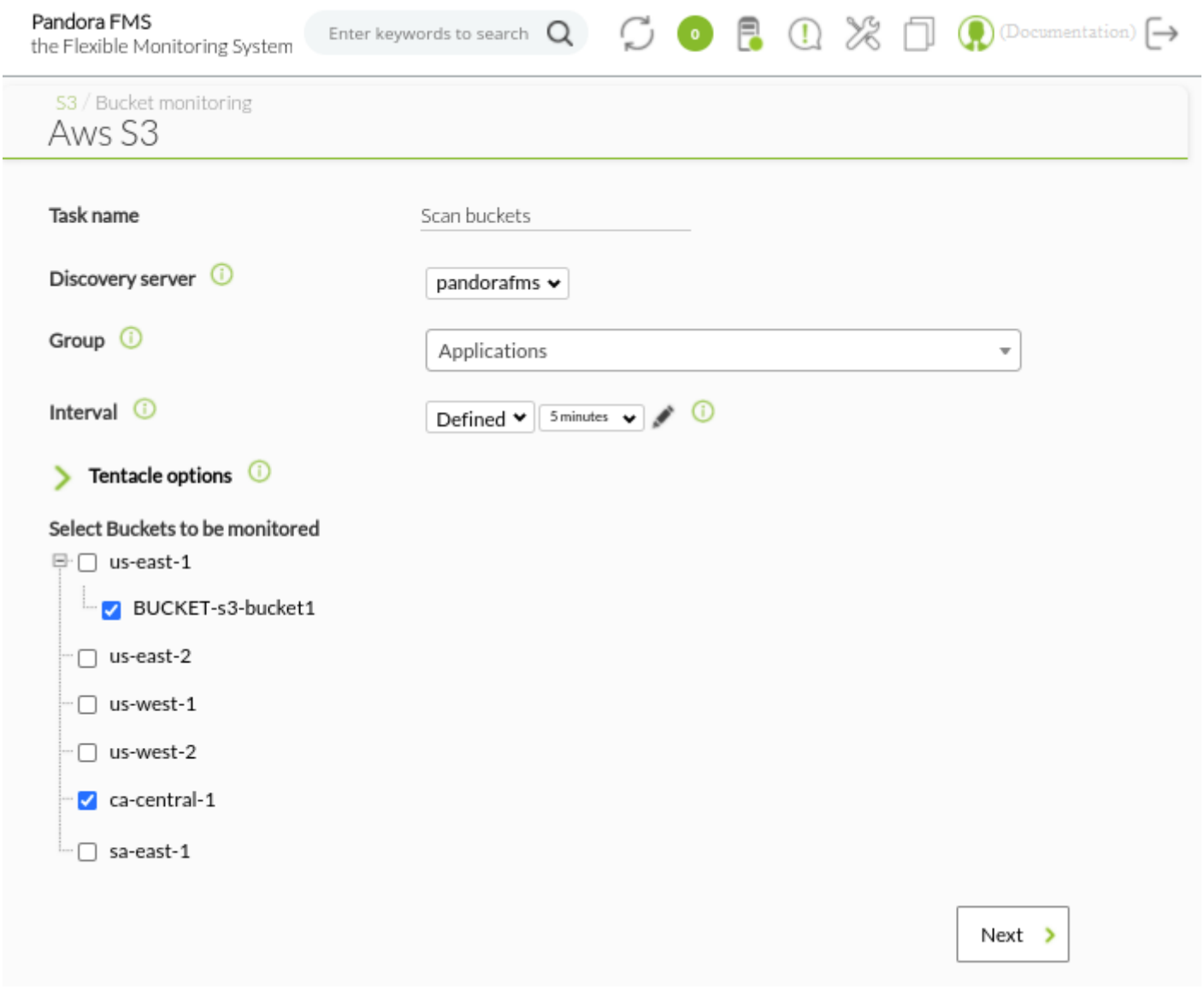
The RDS service provides a database server and allows you to create the instance related to said database. It offers the possibility to connect your instances through clients such as SSMS, MySQL workbench or through JDBC or ODBC DB APIs.

Integration with AWS RDS only supports Oracle, MySQL and MariaDB.

Discovery Cloud S3 Buckets

The S3 Buckets service provides storage for files called objects, such as business applications, data lakes, websites, big data analytics, mobile applications, backup and restore processes, archiving operations, among many others.

With the registered credentials access to the creation of a recognition task and select the objects to monitor, either one by one and/or by regions.



Press the Next button to advance to the next step: select the monitor Bucket size and/or its number of elements, save by clicking Finish. The Agents you will get will be AWS global and monitored regions; the new Modules will be:

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

In the case of region monitoring, a bucket that has been discovered and monitored, and then deleted, will leave all of its corresponding Modules in the Unknown state.

Discovery Cloud. Overview

Discovery Cloud includes a overview that allows you to review the key points of the infrastructure in Amazon Web Services. Pandora FMS will show different maps depending on the existing accounts.

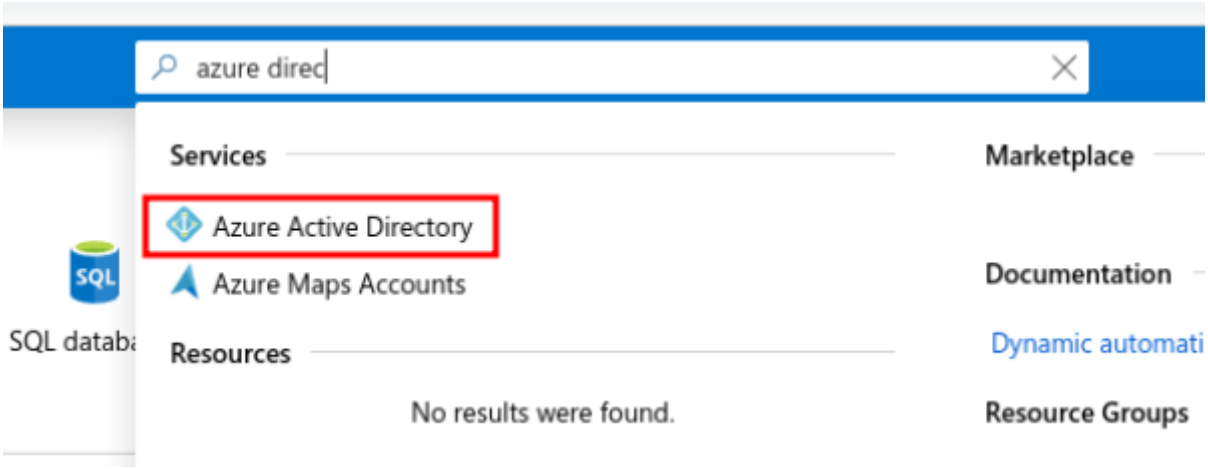
- Current cost.
- Cost in the previous period.
- Cost evolution graph (6 months).
- Graph of evolution of reservations/instances (1 month).
- Map of regions with the number of instances per region.

Discovery Cloud: Microsoft Azure

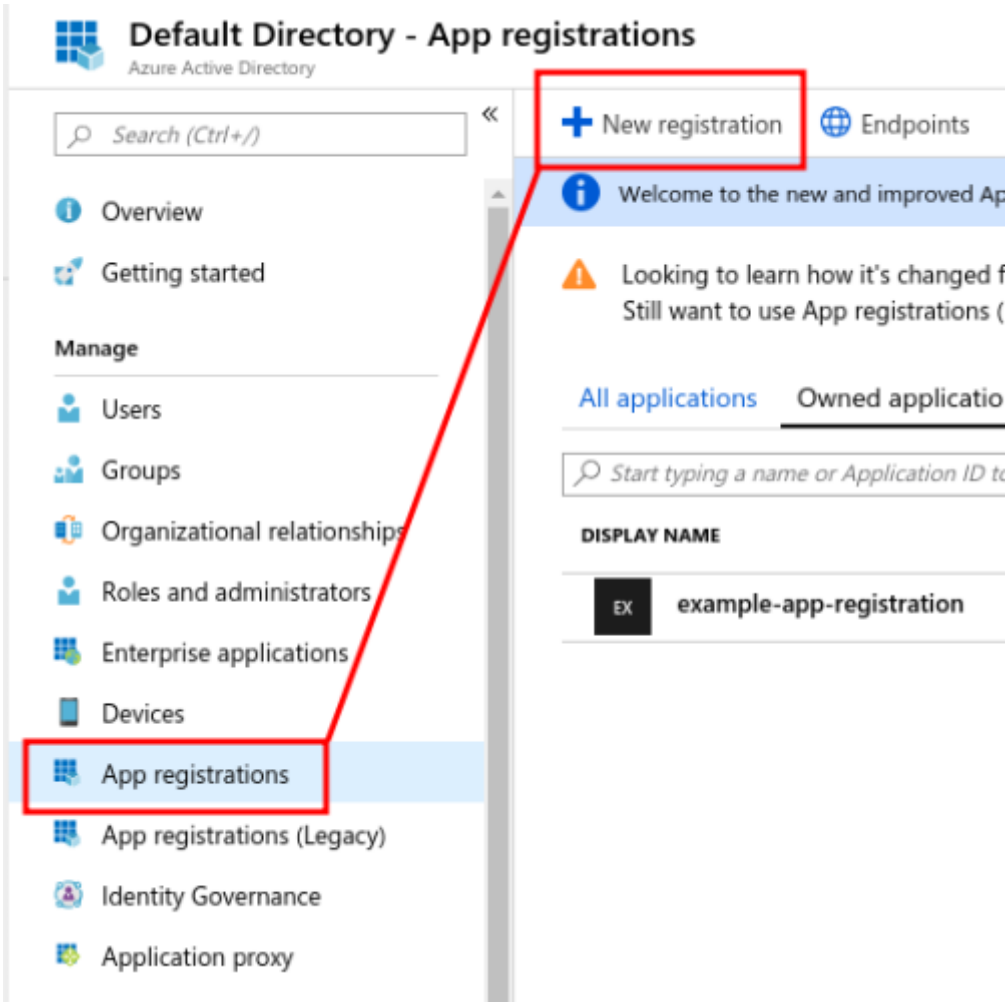
To monitor an infrastructure in Microsoft Azure® follow the instructions below step by step.

How to register a user to use the Azure API?

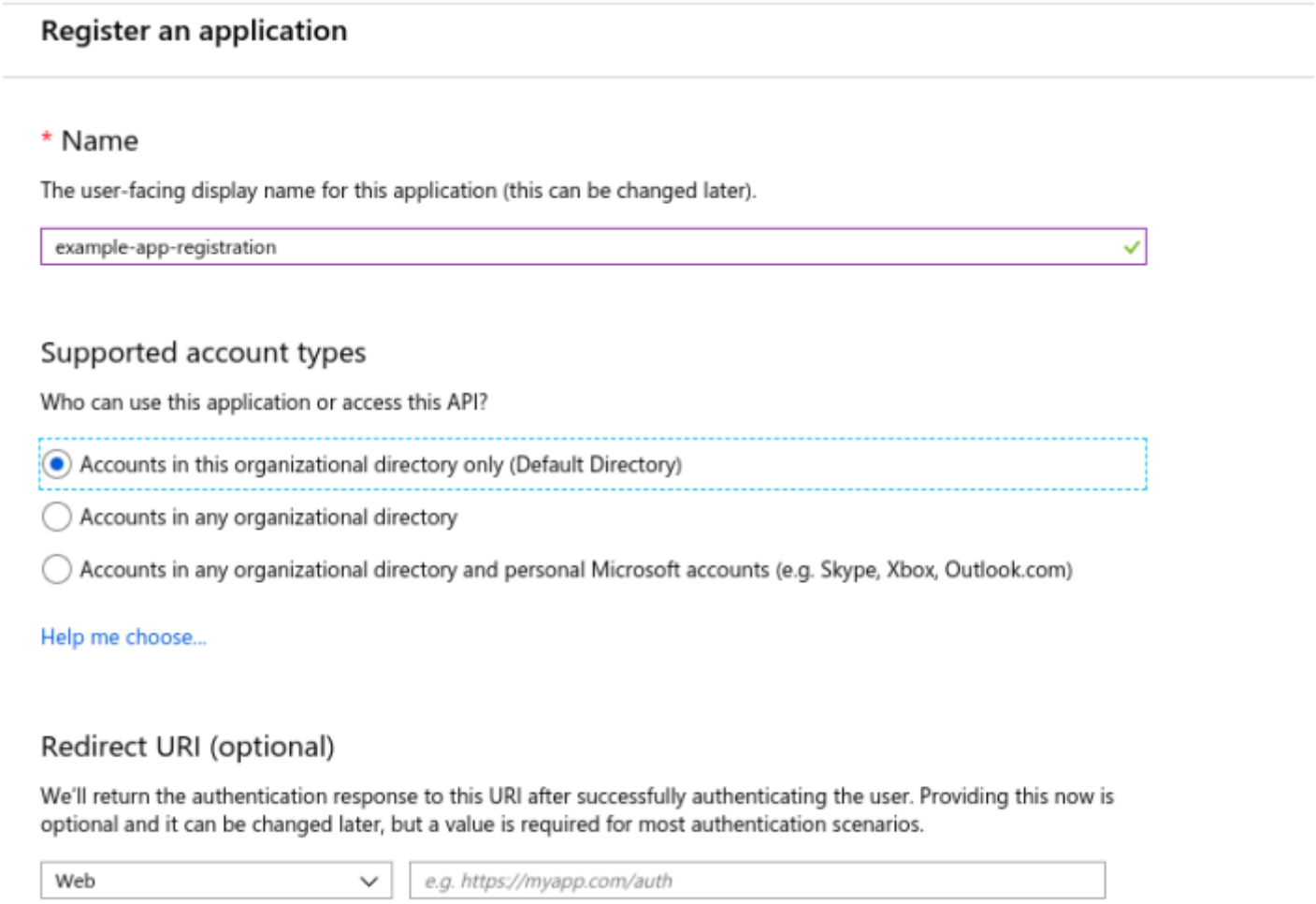
- You must access the Microsoft Azure® portal.
- The Azure Active Directory service opens:



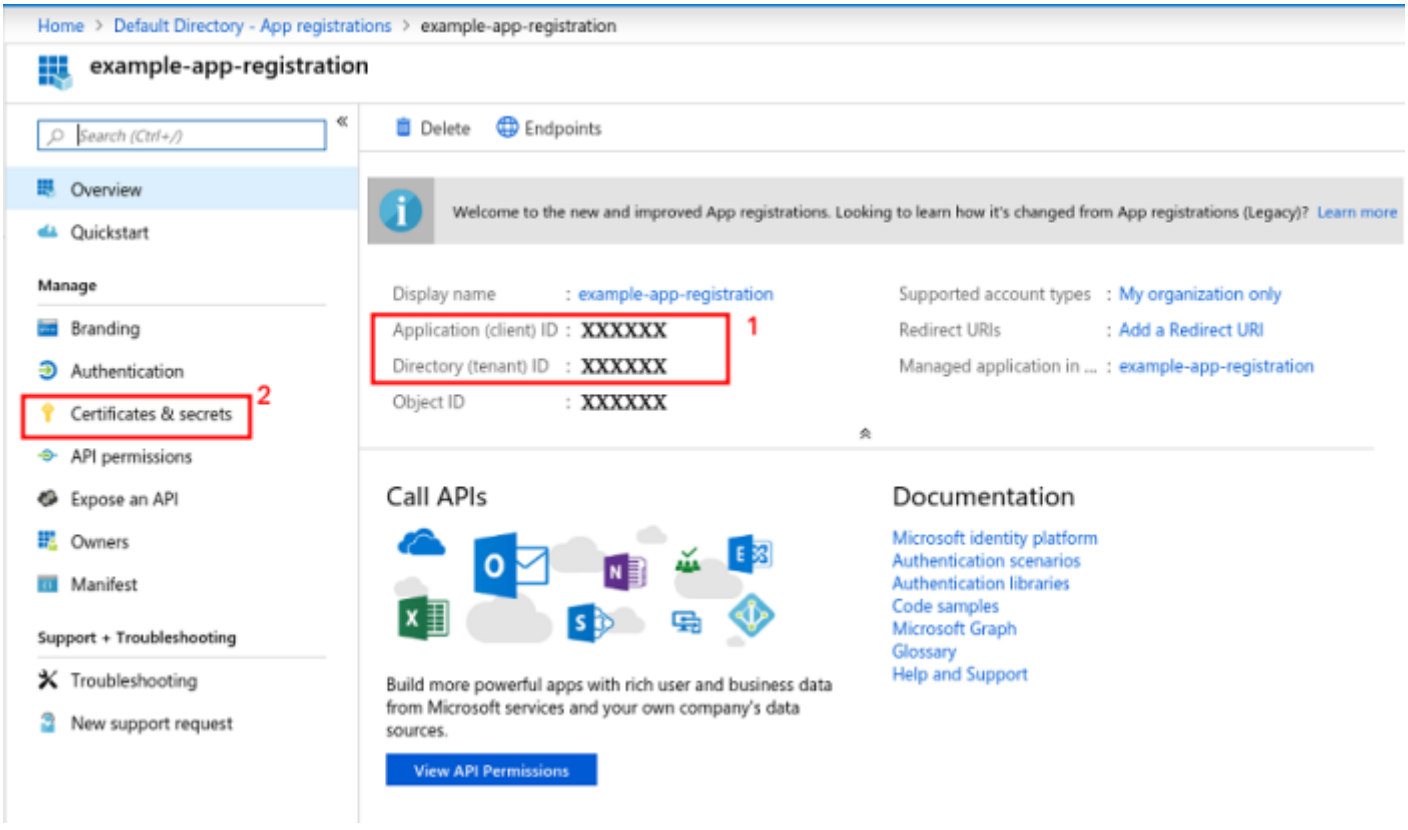
- App registrations → New registration:



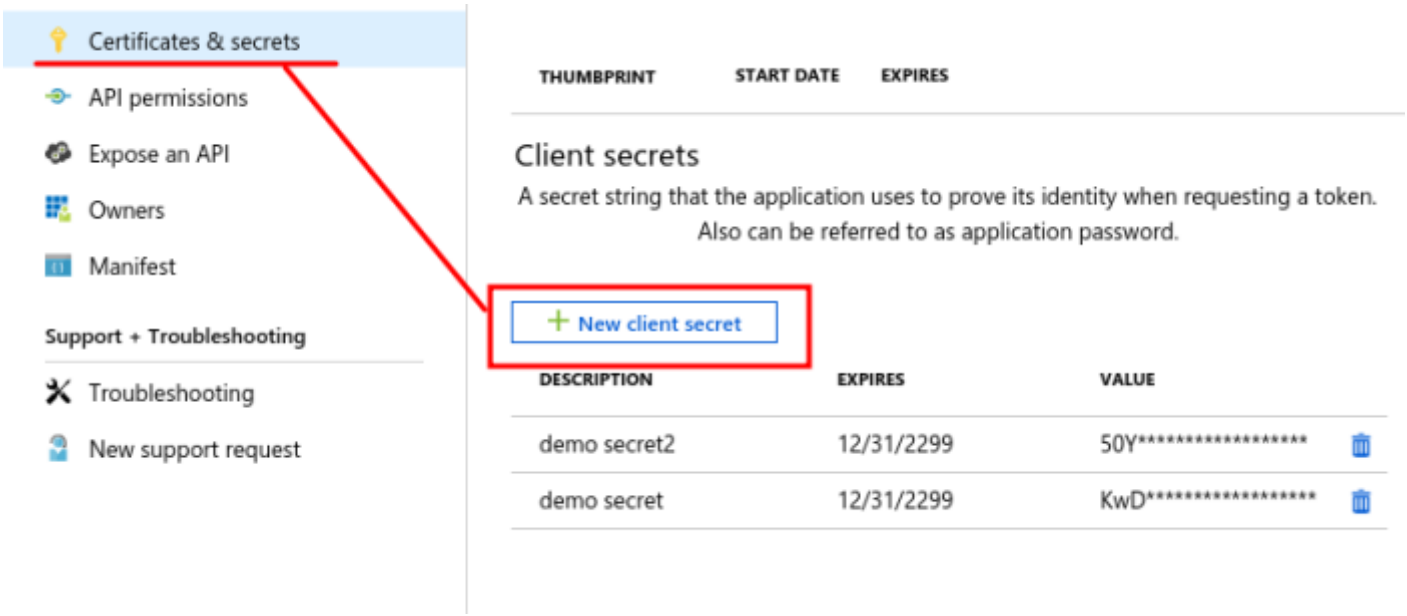
- Enter the following data:



- Take due note of the Application (client) ID`client_id` and Directory (tenant) ID`directory>` values



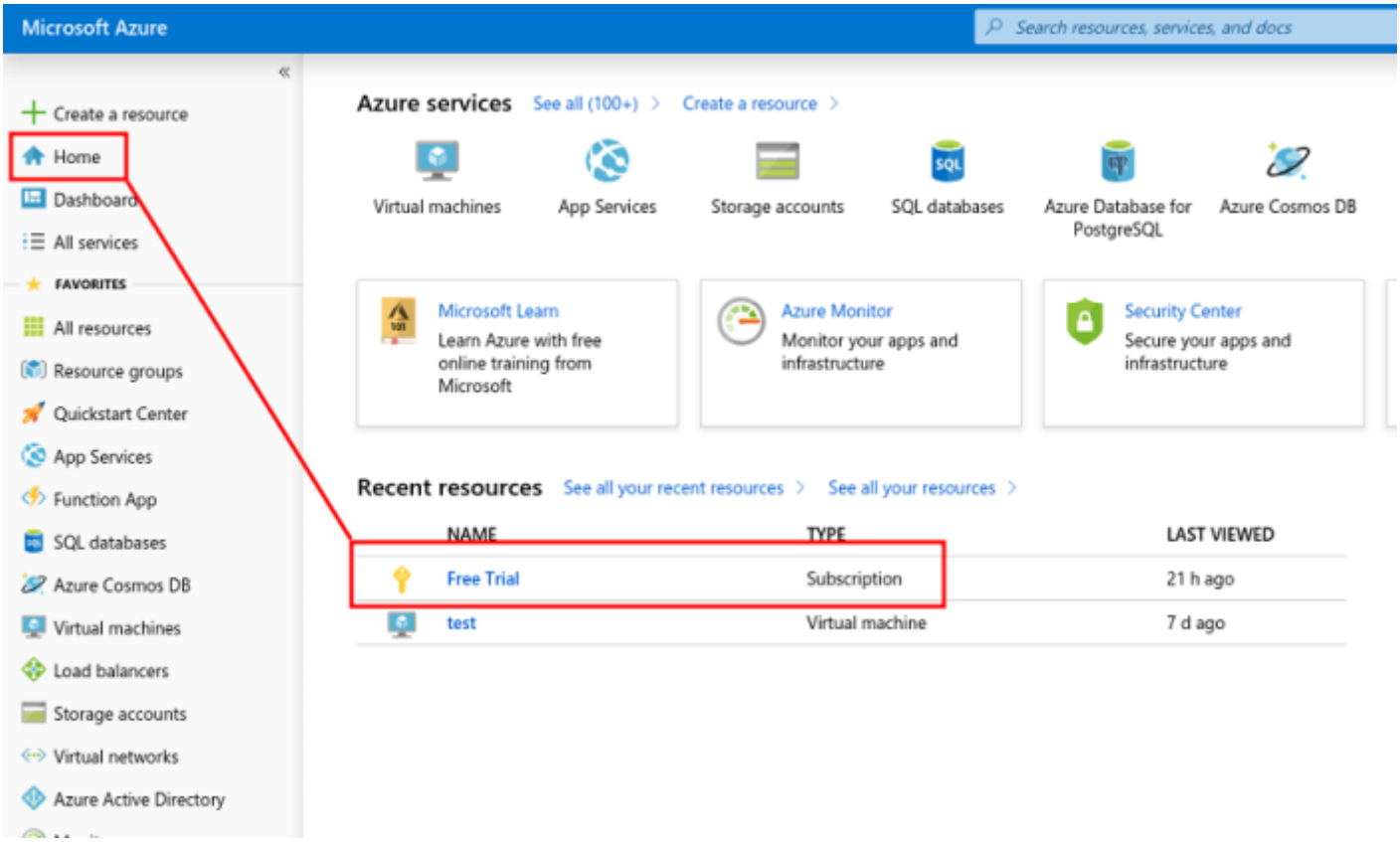
- In certificates & secrets a new one is added:



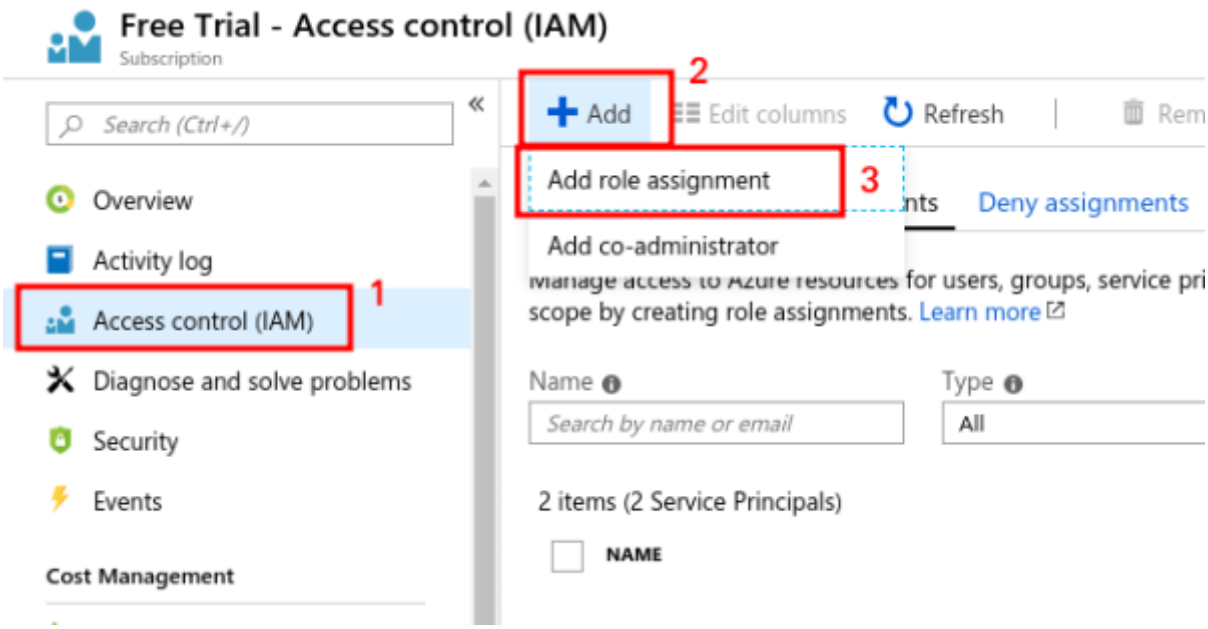
It will be necessary to write down the key that is movedstra, is the `application_secret`.

Permission Assignment

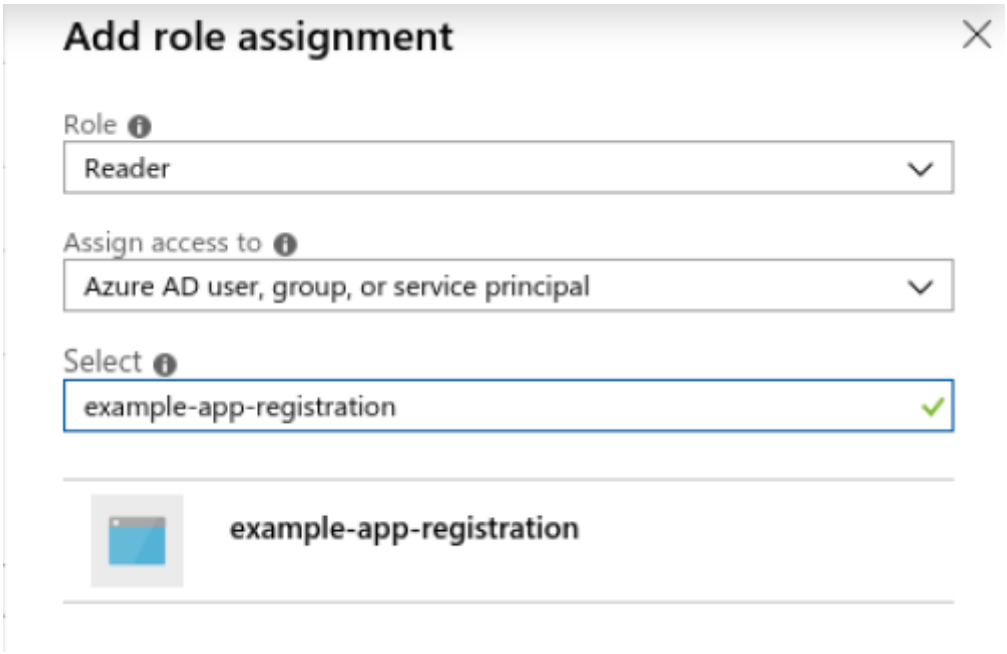
A role must be assigned to the account with which the app will operate, to do so, access Home → Suscription:



Access control (IAM) is selected:



A new role assignment will be added, Reader is placed for the created app:



Save the changes by clicking Save .

From that moment you will be able to connect with the service and make requests through pandora-cm-api.

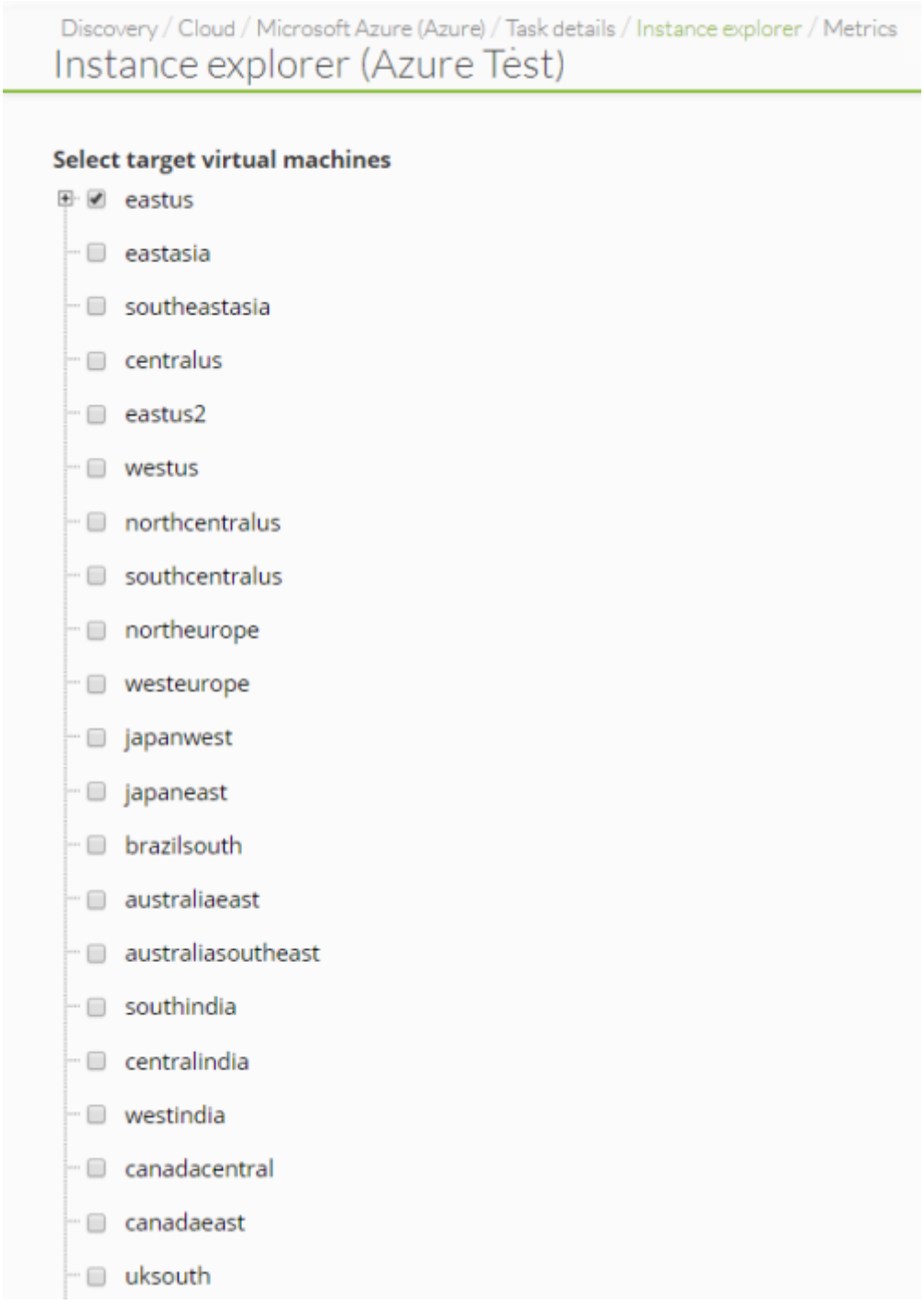
Configure the task in Pandora FMS

Pandora FMS allows the management of several Microsoft Azure® accounts. You can add as many accounts as you need via the Manage Accounts option found next to the Account dropdown.

This allows access to the Credential store section located in Profiles → Manage agent groups and which will act as a store for all previously created and registered Microsoft Azure® accounts.

A new task has to be configured:

- A new key is added to the Credential store .
- Access Discovery → Cloud → Azure and validate the Azure account.
- From this point on, it is necessary to define the name, the server that will execute the task, the group at and the execution interval.
- Once the task data is defined, the regions of the created Azure account that will be monitored are selected. Each region will in turn allow you to select the desired instances.



- The last step will be to select the metrics to obtain from the agents that Pandora FMS will create for each instance found in Microsoft Azure®. Once this section is configured, the task can be launched and Pandora FMS will automatically create the agents based on the instances requested in the previous steps.

Plugins in Pandora FMS

- " Pandora Azure Storage ".

Discovery Cloud: Google Cloud Platform (GCP)

This functionality is available from version 750 of Pandora FMS.

Google Cloud Platform (GCP) credential validation

To access the Google Cloud console, the JSON key must be registered.

- Accesses the security settings in GCP IAM. The access account to register will be a service account with the following privileges:

- It is accessed in Pandora FMS in Credential Store located in Profiles → Manage agent groups → Credential Store with the Add key button.
- In the Product dropdown, choose Google and add the JSON key of the GCP account (the user field will be filled in automatically).
- Then go to Discovery → Cloud → Google Cloud Platform and validate the GCP account by defining a Discovery GCP task.

Configure the task in Pandora FMS

To define the task, you specify a name, the Discovery server in charge of it, along with the monitoring group and interval. Once the task data has been defined, the regions of the GCP account that will be monitored must be selected. Each region will in turn allow you to select the desired instances.

Selecting a zone will automatically monitor new instances detected within that zone. Selecting an instance will explicitly monitor it even if its zone is not monitored.

The last step is to select the metrics to obtain from the agents that Pandora FMS will create for each instance found in Google Cloud Platform®:

- Scan and general monitoring.

- CPU performance summary.
- IOPS performance summary.
- Disk performance summary.
- Network performance summary.

A generic agent called Google or GCP in which all the modules related to google monitoring will appear.

Those instances that disappear from a zone that is constantly monitored will appear in a critical or removed state and all other modules in unknown. In case entire instance goes to unknown you can use auto-disable mode.

Later you can also view a map from the GCP task list.

Discovery Console Tasks

Similarly to Task List, Console Tasks allows you to create new tasks taking into account the group to which it will belong, periodicity, console that executes it, etc.

Discovery Host&Devices

NetSdog

NetScan allows you to discover devices on a network and apply different monitoring rules. When creating a task, the group to which it will belong is established in advance and you must select the option in the recognition:

- Load a file in CSV format with the specific devices to be checked (in Use CSV file definition: you can select a file).
- Or via network, in Network you can specify networks or FQDNs of a specific host, separated by commas, for example: `192.168.50.0/24` or `192.168.60.0/ 24, hostname.pandorafms.com`. If necessary, enable the Name resolution option for domain names.

Intervals selected as manual will need to be launched manually.
Discovery will not launch a manual task automatically. Agents detected by NetScan are remote agents without a configuration file. You won't be able to apply local monitoring policies or add configuration changes in bulk if you don't deploy an agent to the targets.

Some NetScan options:

- Auto discover known hardware: Auto discover known hardware dynamically applies added templates that have been added via Private Enterprise Number.
- Modules templates: Try to apply the modules of the selected templates. If the execution fails the test, they will not be added to the watch list.
- Apply autoconfiguration rules: Applies the auto configuration rules previously defined to the detected agents. Automatic configuration allows you to apply policies, group and configuration changes, as well as launch custom events or run scripts on actions.
- SNMP enabled: To complete the information obtained from discovered network devices, SNMP must be enabled. This improves detection by scanning available SNMP information on discovered targets. By enabling this token, two additional options will appear:
  - SNMP version.
  - Version 766 or later: Use the Skip non-enabled interfaces option to avoid querying for disabled interfaces.
- WMI enabled: WMI scanning for MS Microsoft can be enabled with the credentials previously loaded in the keystore.

The different credentials provided will be tested against the detected targets that support WMI, complementing the monitoring with modules that will report on the use of CPU, memory and disk.

- Parent recursion: Improves parent detection by adding recursion to the process.
- VLAN enabled: Detects the VLANs to which the different devices are connected.

Automatic agent deployment

The steps to deploy Software Agents from the Console are:

- Register the versions of Software Agents to be deployed in the agents repository: You will need the installers of the agents to be deployed. You can also use custom agents.
- Register the credentials that will be used to connect to the targets in the credentials manager: You will need to specify the credentials with which access to the found or specified targets will be tested.
- Confirm that the environment is ready for deployment:
  - You must define targets for deployment.
  - You must define the Public Access URL.
  - You must register installers to deploy the software.

This system does not perform PUSH type operations; all deployments are broadcast offering the software and ordering the target to install it. The server will need to be running EL7 (Red Hat Enterprise Linux) or higher for automatic agent deployment to work. On GNU/Linux Debian and related distributions (Ubuntu, etc.) you should already have the curl command installed.

Goal Pursuit

Objectives for the deployment

You can use any of the Scan for targets, Add target or Load targets options to define targets.

Scan one or more networks for targets

Pressing the scan targets button will display a pop-up box with the following fields:

- Network/mask: The network (or networks, separated by commas) to scan.
- Desired agent version: The version of the Software Agent that registers as desired for the discovered targets.rtos.
- Target server IP: The IP of the target server where these Software Agents will point when they are installed (corresponds to the `server_ip` field of the agent configuration file).

When finished, a new running entry will appear in the task list.

Discovery tasks related to agent deployment are volatile tasks. Once completed, they will be automatically deleted. The information about a scan or deployment, both successful and erroneous, can be consulted from the deployment center itself.

Upload a CSV file with objective information

Attention, this CSV importer will not perform any Discovery tasks, it will only create empty agents with the name, IP address, OS type, description and group provided in the CSV file.

If you want to enroll goals in bulk, you can upload a CSV file in the following format:

```
Agent alias, IP address, OS id, Interval, Group id, Description
```

Deploy the software

You will only be able to schedule the deployment against targets whose information is complete, specifying both credentials and software versions to deploy.

As soon as you have possible targets on the list, you can launch the deployment of the agent. Select the IP addresses of the targets from the list (only valid targets will appear in Available targets) and with the Deploy button the agent deployment will start.

A Discovery task will automatically be created for deployment in the background, which will be in charge of installing the agent on the desired targets. You will be able to confirm that the agent has been successfully installed from the target list of the deployment center.

Import a list of your devices in CSV

A list of devices can be imported to represent them as agents using the agent import wizard via CSV.

This utility only creates the agents in Pandora FMS for
remote monitoring.

You must select the separator used, the server in which you want to import and the file that contains the data, then you must click on Go.

Custom NetScan

It allows the execution of custom scripts for the execution of network recognition tasks. The group to which it belongs and the execution interval must be specified. Once the task creation process is completed, it will be necessary to specify the script to be executed, as well as the configuration file necessary for its execution.

Net scan scripts

This section shows the different scripts that have been created for custom scan tasks, accessed through the Management menu → Discovery → Host&devices → Manage scan scripts.

Pandora FMS allows adding additional scripts to facilitate the monitoring and recognition of the required networks. With the creation of scripts it is possible to add macros with which you can define all the parameters that are necessary for the correct execution of the script.

Back to Pandora FMS documentation index