自動検出

自動検出

Pandora FMS ドキュメント一覧に戻る

自動検出

Pandora FMS 自動検出とは

Pandora FMS バージョン 732 以上に存在します。

自動検出は、ウィザードを通して簡単に監視をするためのツールです。我々のビデオチュートリアル "Introduction to Pandora FMS Discovery" も参照ください。

自動検出タスク一覧

Pandora FMS 自動検出ツールでは、コンソールとサーバ両方における計画されているすべてのタスクの一覧を表示できます。

E アプリケーション検出

新たな管理コンソールから MySQL®、Oracle®、VMware® 環境を監視することができます。

E クラウド検出

この機能により、Amazon Web Services®、EC2、または AWS RDS のリレーショナルデータベースで作成された仮想マシンから、Azure Compute® で実行されている仮想マシンに至るまで、クラウドインフラストラクチャを監視できます。

E コンソールタスク

レポートの設定、バックアップの作成、Pandora FMS コンソールからのカスタマイズしたスクリプトの実行など、検出システム内のコンソールタスクを自動化できます。

ホストおよびデバイスの検出

ネットワークのデバイスや機器を発見し、登録するために必要なツールが含まれています。

アプリケーション検出

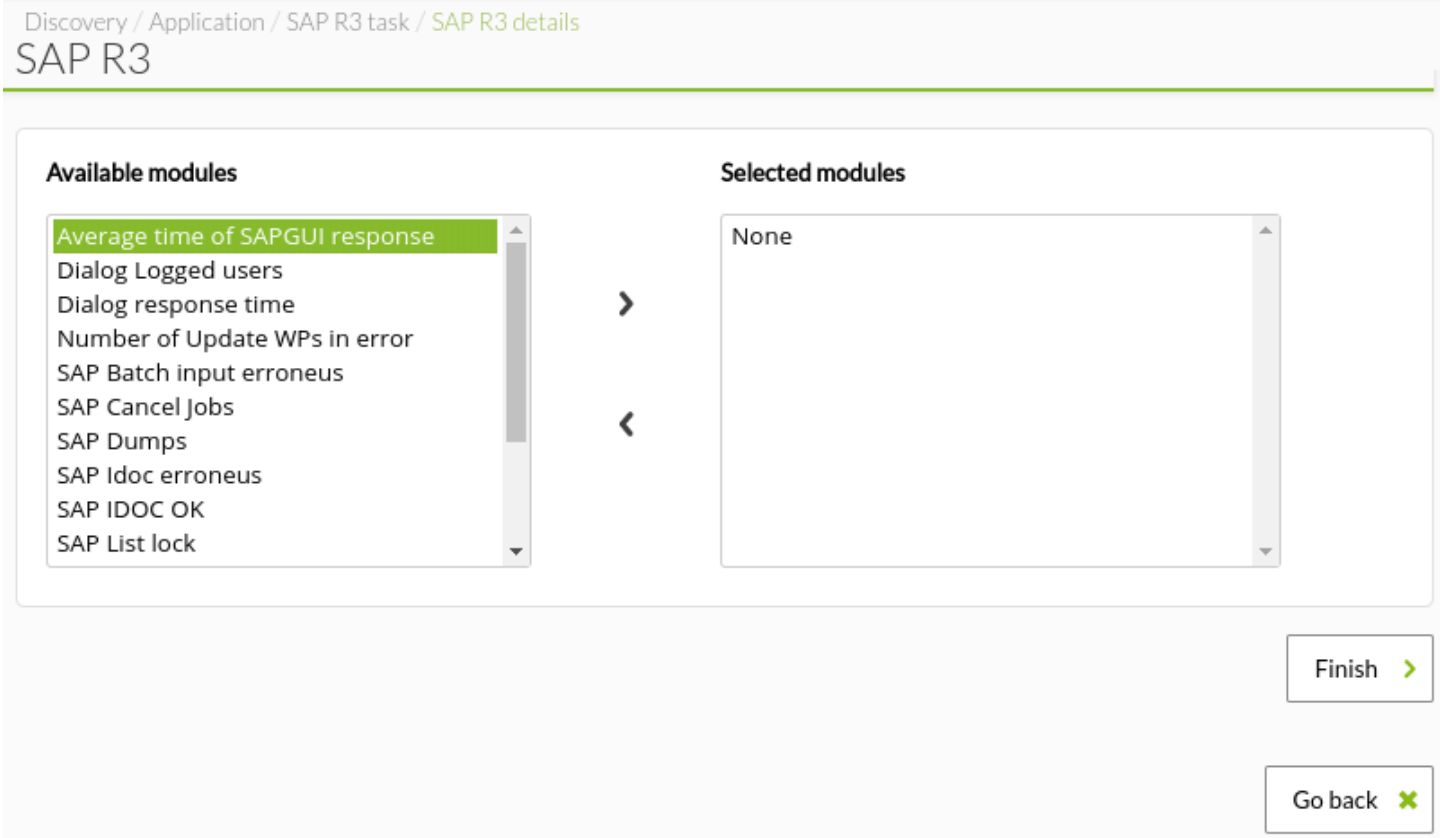
E *アプリケーション検出(Discovery Applications)* を用いて、アプリケーションをリモートで監視することができます。

アプリケーション検出: SAP

バージョン NG 741 以上

Eシステムは、必要に応じて SAP を設定する各ステップに沿ってガイドをします。ビデオチュートリアル «SAP Monitoring with Pandora FMS Discovery» もご覧ください。同じタスクを定義して、同様の構成のシステムを監視できます。(バージョン 741 から 768)

異なる設定を監視する必要がある場合は、それぞれの設定のタスクを作成します。



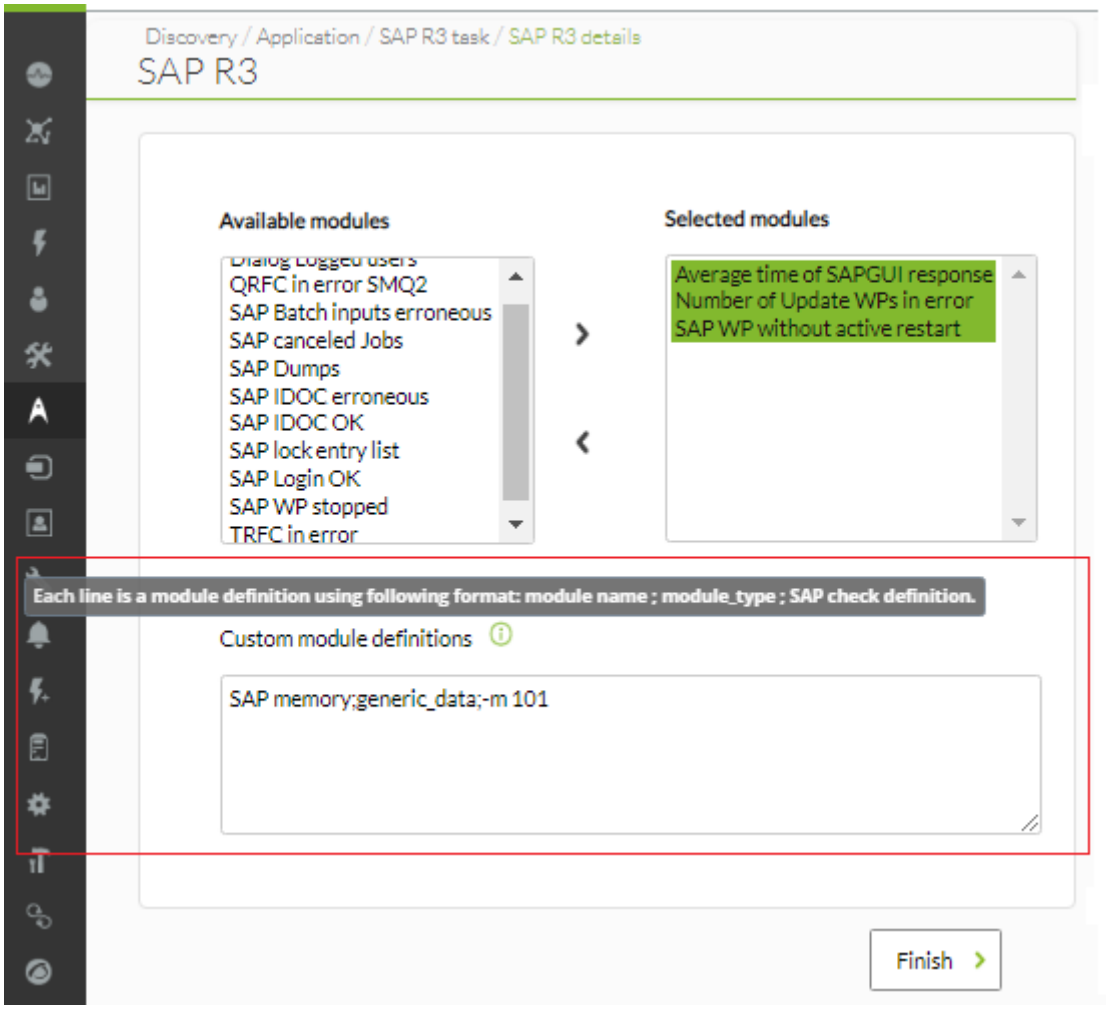
Pandora FMS 自動検出は、情報の収集を担当し、定義された SAP ホスト名(SAP Hostnames) で表される(バージョン 741 から 768)または、SAP ホスト名(SAP Hostname) で定義される(バージョン 769 以降)エージェントに情報を保存します。

Pandora FMS をパッケージからインストールしている場合もしくは□NG741 より前のバージョンの場合は、Pandora FMS サーバに公式 SAP プラグインをインストールし、SAP 自動検出コネクタ手動インストール に従って手動で設定します。

カスタム SAP

バージョン NG 747 以上

Pandora FMS の 利用可能なモジュール とは別に、多くの追加モジュール を カスタムモジュール 定義 セクションを通して追加できます。



追加する各行は、フィールド区切り文字としてセミコロンを使用して、次のフォーマットを使用する必要があります。

```
<module name>**;**<module_type>**;**<sap definition check>
```

SAP システムの情報を得るための例:

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

必要な数のカスタムモジュールを追加してから、前のセクションで説明したのと同じ方法でプロセスを続行できます。

アプリケーション検出: VMware

Pandora FMS サーバで autocreate_group が有効な場合、
ウィザードの設定ではなく、指定された ID に対応するグループが優先されます。

基本的な設定が完了したら、次の設定を行います。

- 最大スレッド(Max threads): VMware 監視スクリプトで使用されるスレッド数は、データ収集を高速化するために選択します。
- イベントモード(Event mode): VCenter のみ です VMware VCenter のイベントベースの監視が有効になります。この作業モードは排他的であり、標準の監視とは独立しています。
- 追加設定(Extra settings): VMware の監視をカスタマイズするために必要な詳細設定は、テキストモードでここで行う必要があります。

アプリケーション検出: MS SQL

この新たな Pandora FMS 統合機能により Microsoft SQL サーバデータベースの監視が可能です。それには、ODBC を Pandora FMS サーバが動作するシステムにインストールする必要があります。

MS SQL のアプリケーション検出タスク設定

Microsoft SQL サーバデータベースの監視タスクを作成は、自動検出(自動検出(Discovery) → アプリケーション(Applications) → Microsoft SQL Server)を通して行います。

Microsoft SQL サーバタスクを選択したら、次のようにインスタンスを定義します。

```
IP\Instance
```

ポートを指定したい場合は次のようにします。

```
IP:Port\Instance
```

デフォルトで存在するモジュール

監視に使用するユーザは、対応する操作を実行するために、接続するデータベースに対して必要な権限を持っている必要があります。

名前	説明
MSSQL connection	MS SQL サーバの接続をチェックします。
queries: delete	前回の実行以降に実行された delete クエリの量。
queries: insert	前回の実行以降に実行された insert クエリの量。
queries: update	前回の実行以降に実行された update クエリの量。
queries: select	前回の実行以降に実行されたクエリの量。

名前	説明
restart detection	データベースサービスが継続して実行されている時間をチェックします。
session usage	利用可能な最大セッションに対する開いているセッションの割合です。モジュールの説明に現在値と最大値を表示します。

クラウド検出

Enterprise クラウド検出では Amazon Web Services®, Google Cloud Platform® および Microsoft Azure® を単一ツールで監視できます。

AWS および Microsoft Azure 両方の各アカウントの管理は、プロファイル(Profiles) > エージェントグループ管理(Manage agent groups) > 認証情報ストア(Credential Store) もしくは、管理(Management) > 設定(Configuration) > 認証情報ストア(Credential store) から行います。

クラウド検出: Amazon Web Services (AWS)

Enterprise Amazon Web Service のインフラストラクチャを監視するには、ウィザードのページをたどる必要があります。

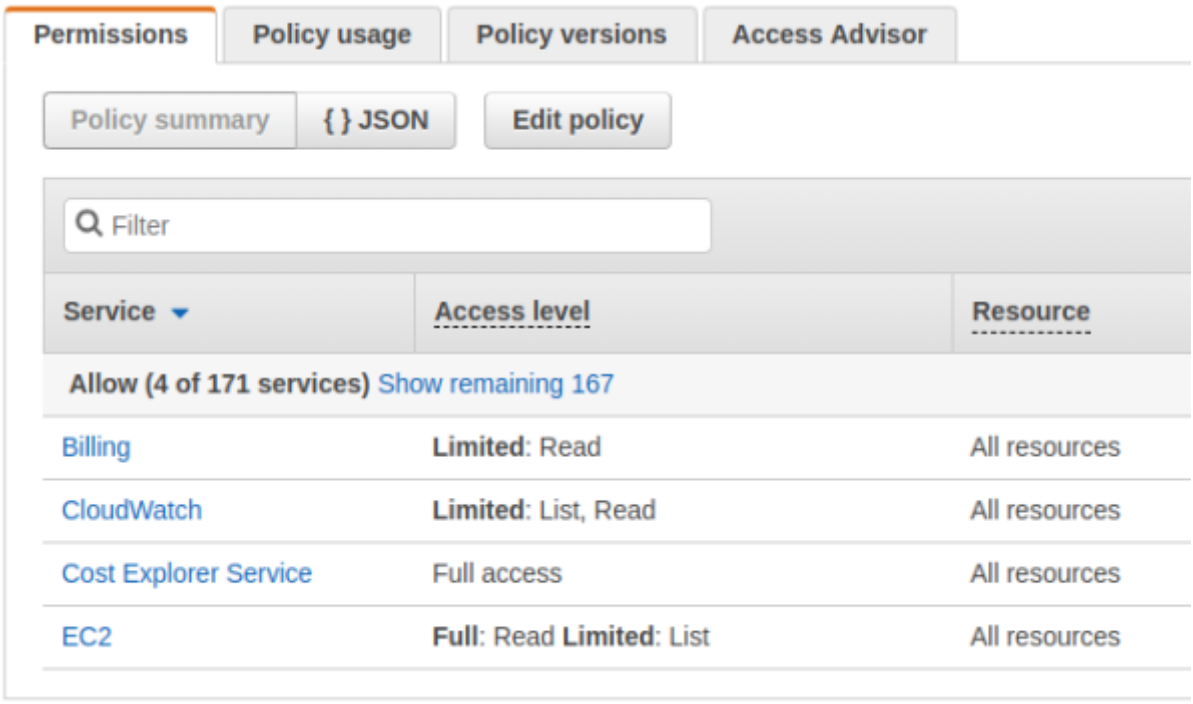
AWS 認証情報の確認

Pandora FMS では、複数の AWS アカウントを管理できます Amazon Web Services メニューにアクセスすると、ナビゲーションは自動的にサービスへアクセスするアカウントを選択するウィンドウにリダイレクトされます。 以前のバージョンの Pandora FMS で作成済のアカウントがある場合、それは imported_aws_account として表示されます。

AWS アカウントのドロップダウンの隣の アカウント管理(Manage Accounts) を通して必要な数のアカウントを追加できます。プロファイル(Profile) の 認証情報ストア(Credential store) > エージェントグループ管理(Manage agent groups) に、作成済のすべての Amazon Web Services® アカウントが保存されます。

認証情報ストア内のアカウントごとに Amazon EC2 自動検出で実行できるタスクは 1 つだけです。

以下の権限で Amazon AWS のアカウントを作成する必要があります。



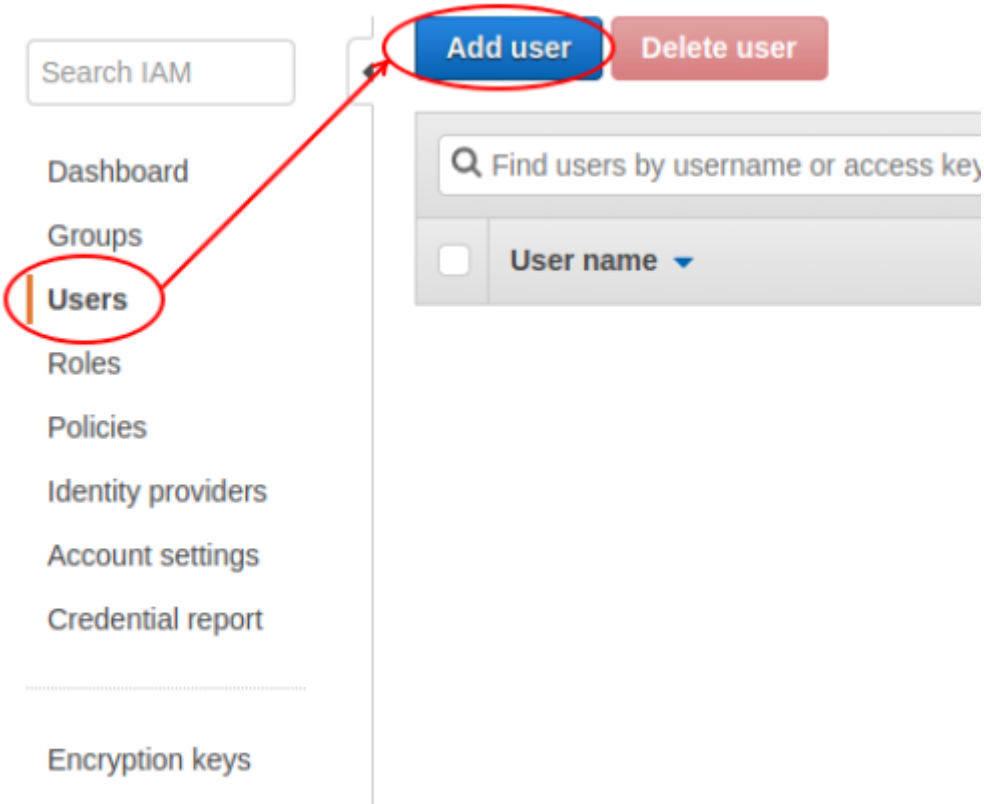
JSON でのポリシーは以下の通りです。

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

ポリシーを新規ユーザに割り当てる必要があります。



Pandora FMS へ戻り、登録したアカウントをリンクして使用できるようにしAWS 監視にアクセスできます。

pandora-cm-api をインストールしていない場合

は、Pandora Cloud Monitoring API から入手できます。

AWS のクラウド検出

Enterprise 権限を確認したら、クラウド検出(Discovery Cloud) → Amazon Web Services のメニューからアクセスします。認証情報ストア(Credential store) に追加されたアカウントごとに、そのアカウントに保存されている EC2 環境を監視できます。

AWS.EC2 のクラウド検出

Enterprise EC2 の監視では以下があります。

- 費用監視
- AWS.EC2 で記録されたリソースの概要
- 特定インスタンスの監視
- ボリュームおよび elastic IP の監視

監視処理を開始するためには、名前、それを実行する自動検出サーバ、グループおよび間隔などの基本的なデータが必要です。

Amazon Web Services の費用監視には追加の費用が発生します。 詳細については、次のリンク Amazon cost management pricing を確認してください。

全体コストとリージョンごとの個別のコストの両方を監視できます。

すべてのリージョンの全体的な予約情報を収集するには、自動検出 で スキャンと一般的な監視(Scan and general monitoring) オプションを有効にする必要があります。

AWS.EC2 特定インスタンスの監視

特定のインスタンスの以下の情報を監視することができます。

- CPUUtilization: 平均 CPU 使用率
- DiskReadBytes: 読み出しバイト数 (ディスク)
- DiskWriteBytes: 書き込みバイト数 (ディスク)
- DiskReadOps: 読み出し操作数 (ディスク)
- DiskWriteOps: 書き込み操作数 (ディスク)
- NetworkPacketsIn: 入力パケット数 (ネットワーク)
- NetworkPacketsOut: 出力パケット数 (ネットワーク)

特定のインスタンスを表すエージェントは、それらが所属しているリージョンを表すエージェントを親として持ちます。Pandora FMS サーバの設定でトークン *update_parent* を 1に設定し、親子関係

を最新の状態に保つようにしておく必要があります。

AWS.EC2 追加

この最後の画面では、リザーブドインスタンスによって使用されているボリュームを監視するかどうかを指定できます。リージョンのエージェントに以下の 2つの追加モジュールがあります。

- リザーブドボリュームの総量(GB)
- 記録された総量(数)

Elastic IP addresses トークンを有効化することもできます。AWS EC2 アカウントで登録されている elastic IP の数を報告します。

常に 自動検出タスク一覧(Discovery task list) で実行プロセスを確認できます。

AWS.RDS のクラウド検出

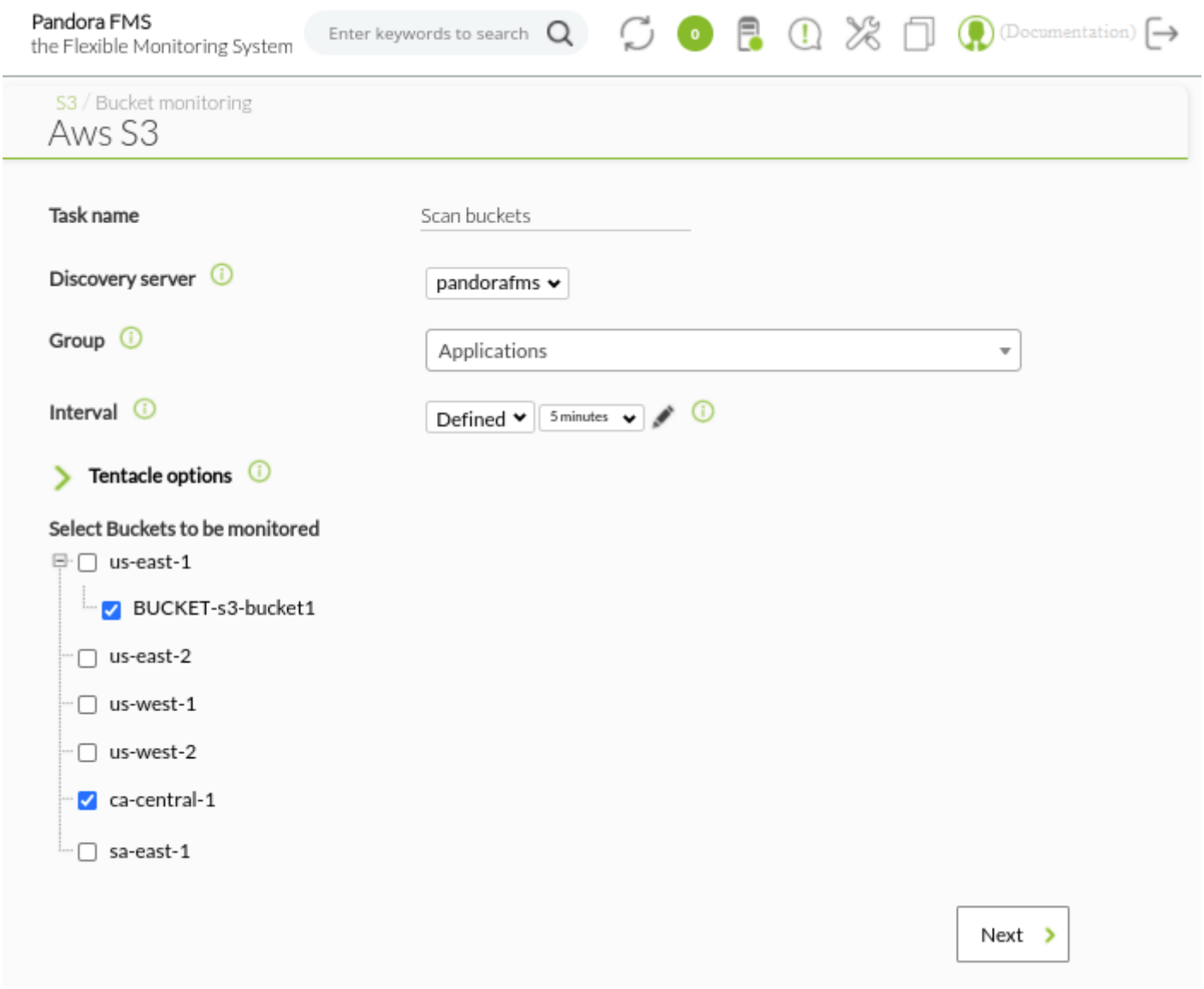
Enterprise RDS サービスはデータベースサーバを提供し、そのデータベースに関連するインスタンスの作成を可能にします。 さらに、RDS は、SSMS、MySQL ワークベンチなどのクライアント、または JDBC または ODBC DB API を介して接続することができます。

AWS RDS との統合は、Oracle, MySQL および Mariadb のみ対応しています。

S3 バケットのクラウド検出

Enterprise S3 バケット サービスは、エンタープライズアプリケーション、データレイク、ウェブサイト、ビッグデータ分析、モバイルアプリケーション、バックアップと復元処理など、オブジェクトと呼ばれるファイルのストレージを提供します。

登録済み認証情報 を使用して、検出タスクの作成にアクセスし、監視対象のオブジェクトを 1 つずつまたは地域ごとに選択します。



次(Next) をクリックして次のステップに進みます。バケットサイズやバケット要素数による監視を選択します。 完了(Finish) をクリックして保存します AWS グローバルおよび監視対象リージョンのエージェントができ、新しいモジュールは次のようになります。

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

リージョンの監視の場合、バケットが検出および監視され、
その後削除されると、対応するすべてのモジュールが 不明
状態のままになります。

一般的な表示

E クラウド検出では Amazon Web Services のインフラストラクチャの重要な点の概要を確認できます Pandora FMS は、存在するアカウントにもとづいて異なるマップを表示できます。

- 現在の費用

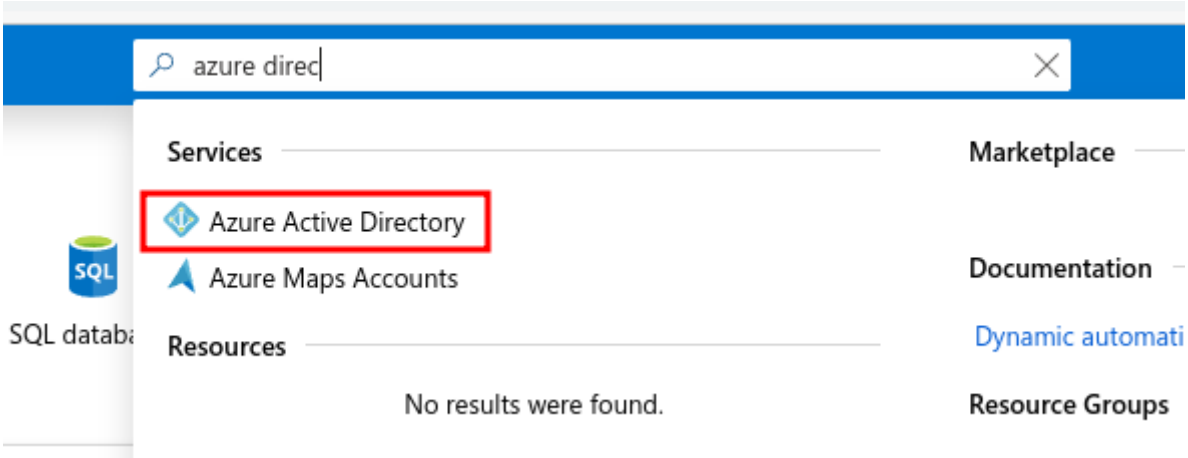
- 前期間の費用
- 費用の推移グラフ (6ヵ月)
- リザーブ/インスタンスの推移グラフ (1ヵ月)
- リージョンごとの、インスタンスの数を含んだリージョンのマップ

クラウド検出: Microsoft Azure

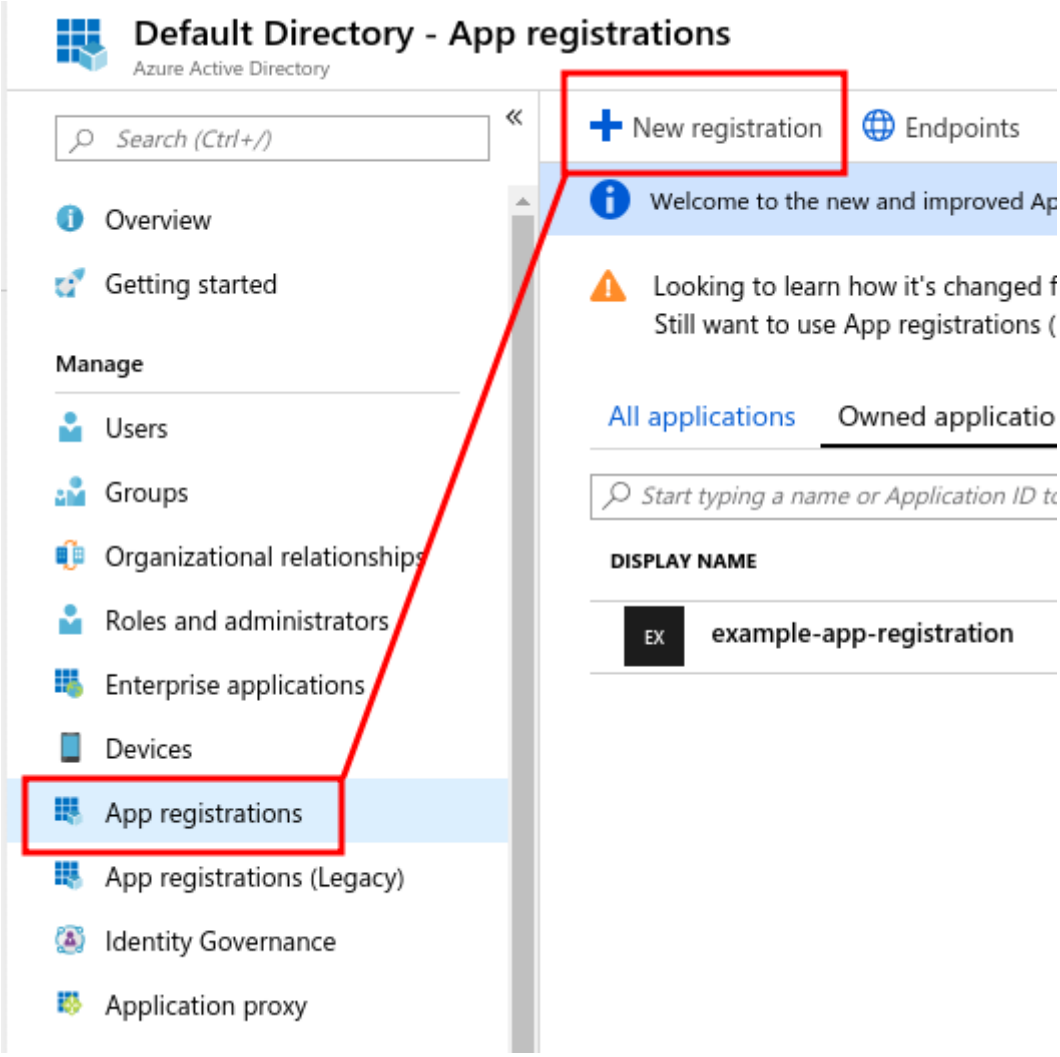
Microsoft Azure のインフラ監視のためには、以下の手順を実施します。

Azure API を利用するためのユーザ登録方法

- Microsoft Azure® ポータルへ行きます。
- “Azure Active Directory” サービスを開きます。



- 'App registrations'> 'New registration' へ行きます。


Default Directory - App registrations
Azure Active Directory
Search (Ctrl+/)
New registration
Endpoints
Overview
Getting started
Manage
Users
Groups
Organizational relationships
Roles and administrators
Enterprise applications
Devices
App registrations
App registrations (Legacy)
Identity Governance
Application proxy
Welcome to the new and improved Ap
Looking to learn how it's changed f
Still want to use App registrations (
All applications
Owned applicatio
Start typing a name or Application ID to
DISPLAY NAME
EX
example-app-registration

- **データを入力します。**

Register an application

* Name

The user-facing display name for this application (this can be changed later).

example-app-registration

Supported account types

Who can use this application or access this API?

- (●) Accounts in this organizational directory only (Default Directory)
- ( ) Accounts in any organizational directory
- ( ) Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

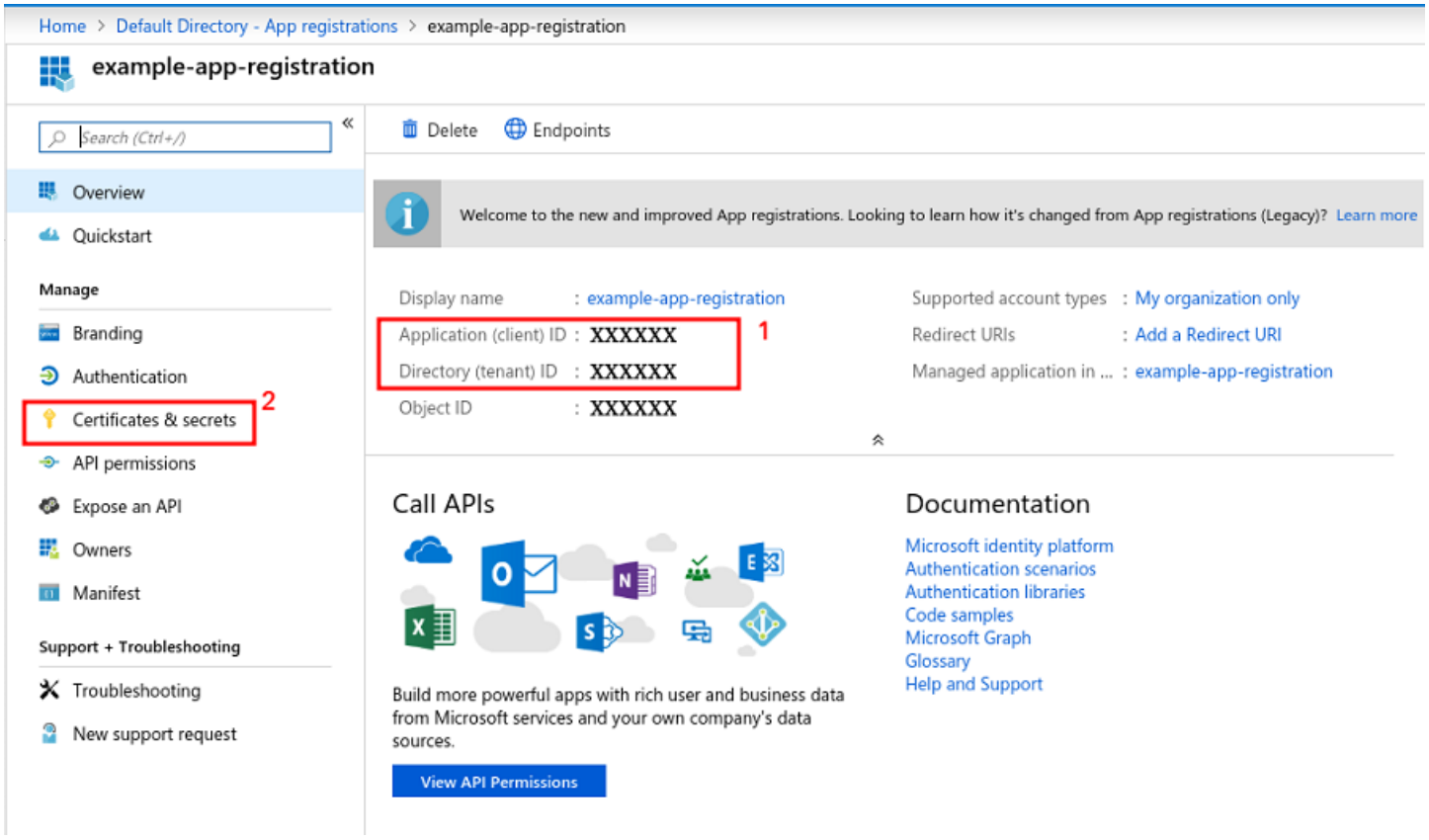
Help me choose...

Redirect URI (optional)

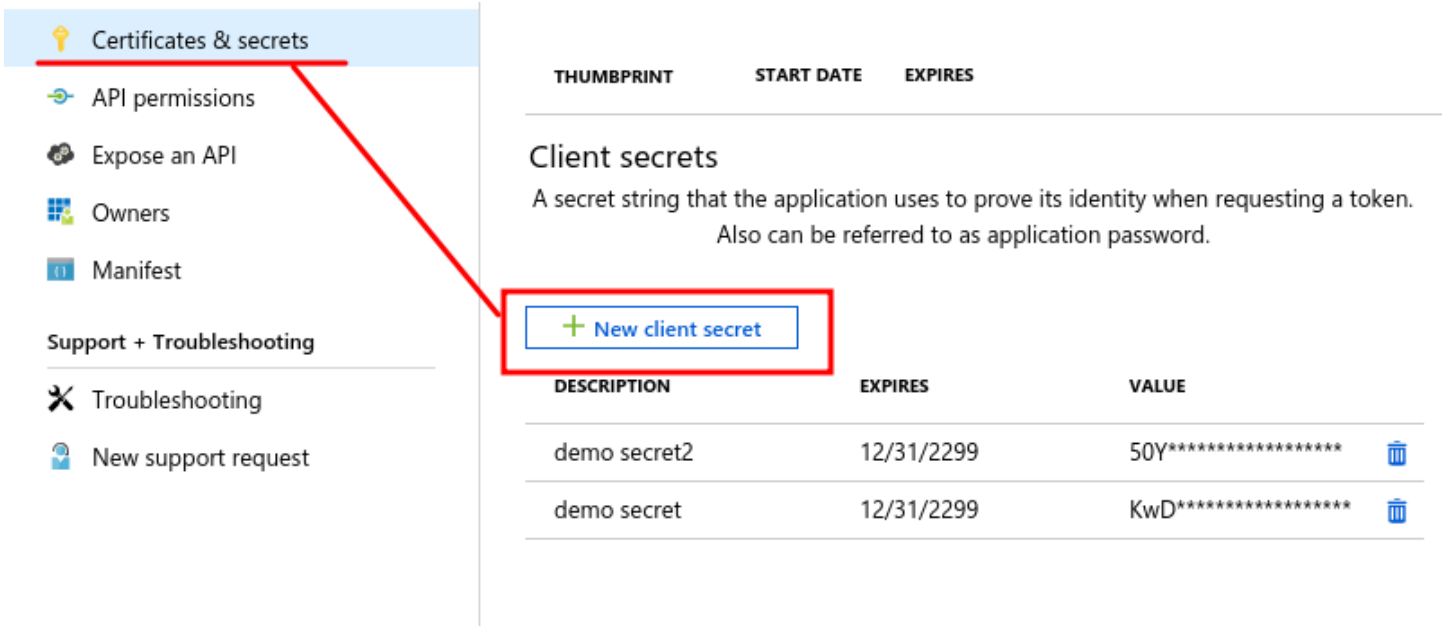
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | e.g. https://myapp.com/auth

- Application (client) ID `client_id` および Directory (tenant) ID `directory` を控えておきます。



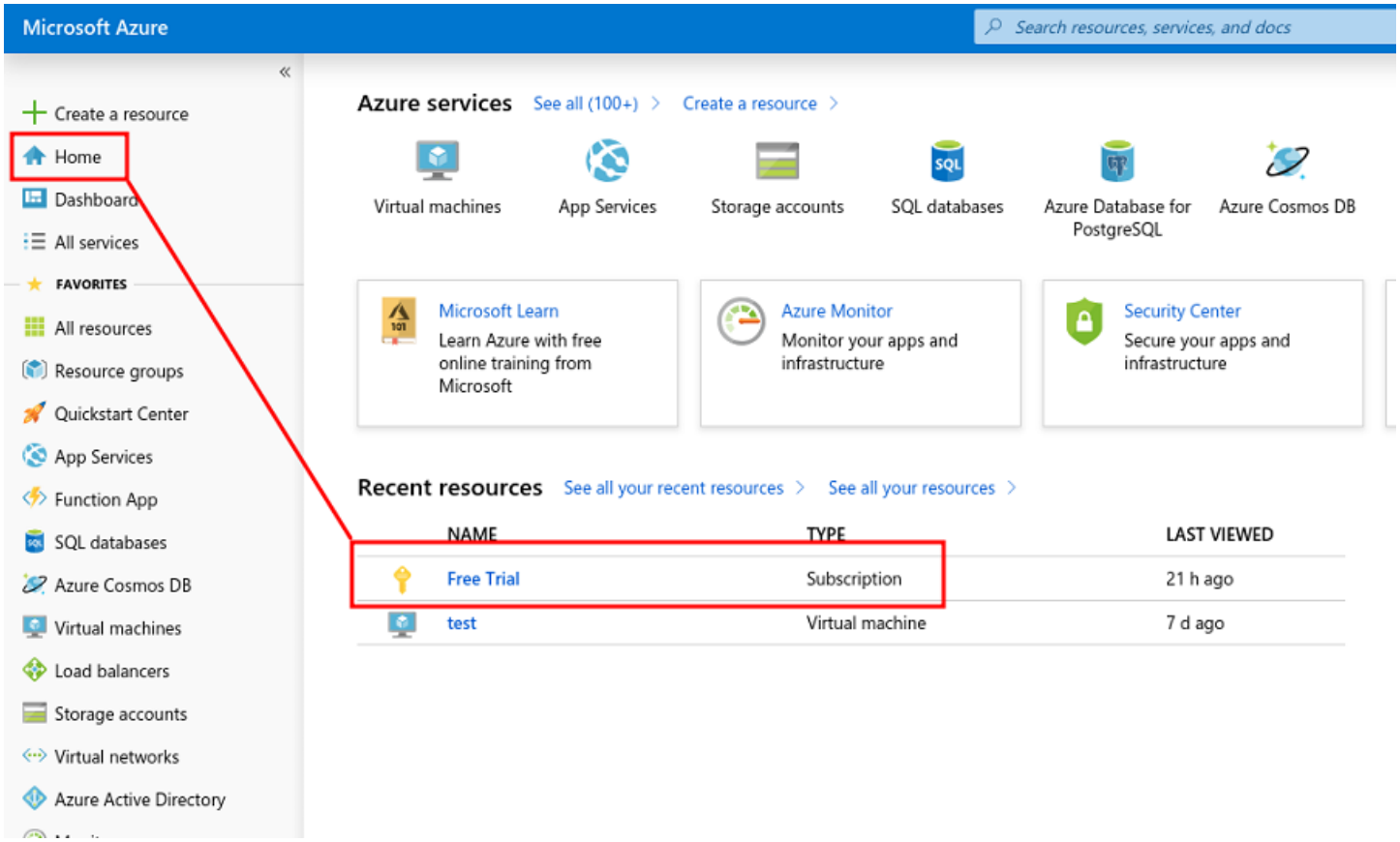
- 次に、'certificates & secrets' へアクセスし、新規作成します。



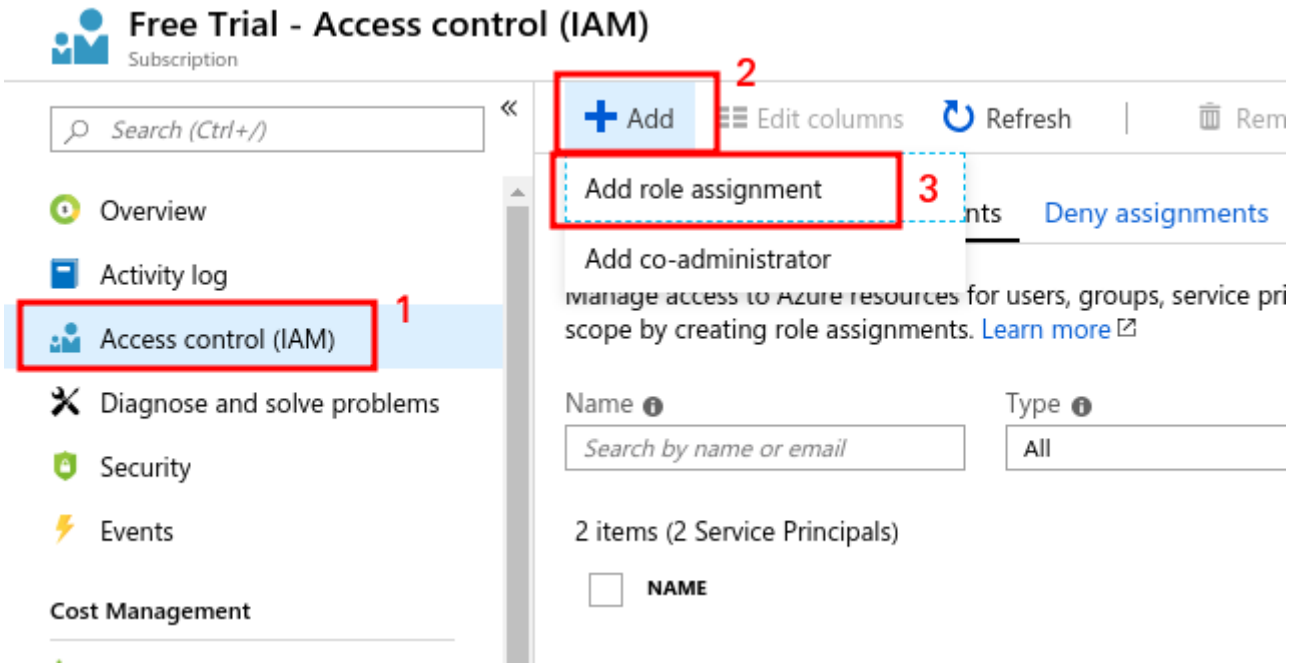
表示された鍵を控えておきます。`application_secret` になります。

権限の割り当て

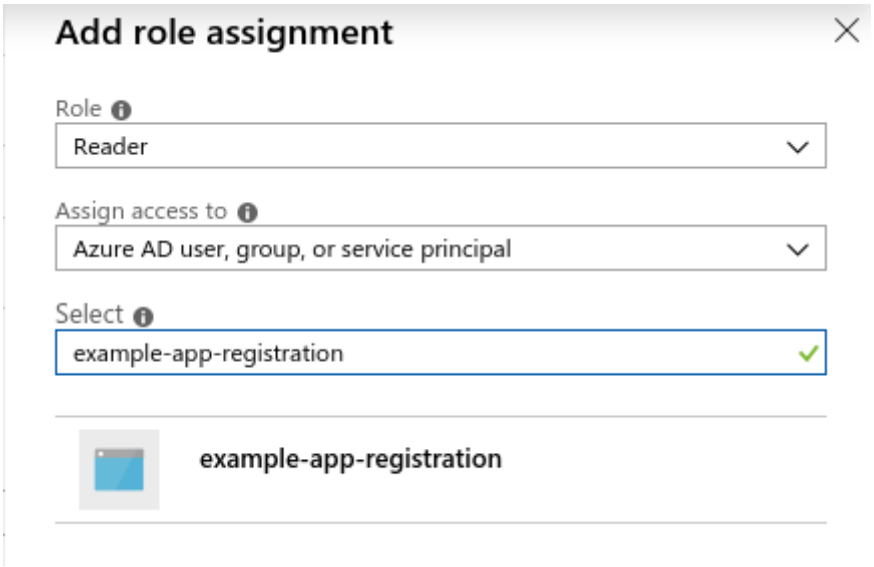
操作を行うアカウントに権限を割り当てます。そのためには“home” にアクセスしてサブスクリプションに入ります。



サブスクリプションで、“Access control (IAM)” を選択します。



新しい役割の割り当てを追加し、作成したアプリの “reader” の役割を選択します。



“save” をクリックして、変更を保存することが重要です。

これ以降、pandora-cm-api を通してサービスに接続し結果を得ることができます。

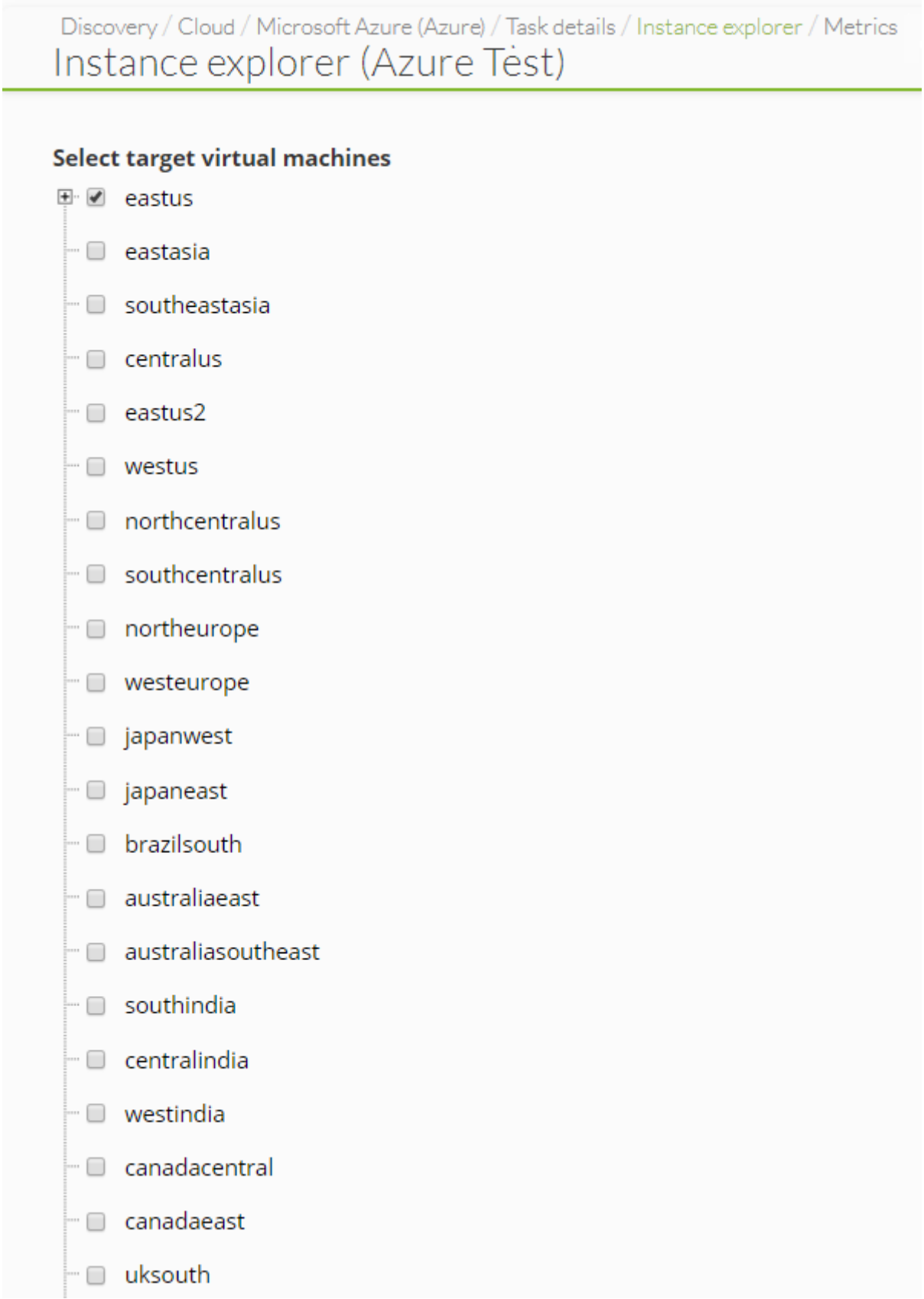
Pandora FMS における設定

Pandora FMS は、複数の Microsoft Azure® アカウントを管理できます。アカウントドロップダウンの横にある アカウント管理(Manage Accoutns) オプションを使用して、必要な数のアカウントを追加できます。

これにより、プロファイル(Profiles) > エージェントグループ管理(Manage agent groups) の 認証情報ストアへ(Credential store) のアクセスが許可され、登録済みの Microsoft Azure アカウントのストアとして機能します。

新たなタスクを設定するには、次のステップを実施します。

- 認証情報ストア(credential store) に新たなパスワードを追加します。
- 自動検出(Discovery) > クラウド(Cloud) > Azure へアクセスし、Azure アカウントを検証します。
- ここからは、自動検出タスクの名前、タスクを実行するサーバ、タスクが属するグループ、および実行間隔を定義する必要があります。
- タスクデータを定義したら、監視する Azure アカウントセクションを選択します。 各セクションでは、目的のインスタンスを順番に選択できます。



- 最後の手順は、Microsoft Azure で見つかった各インスタンスに対して Pandora FMS によって生成されたエージェントから取得するメトリックを選択することです。設定が完了したらタスクを起動でき Pandora FMS は前の手順で選択したインスタンスに対して、エージェントを自動的に作成します。

Pandora FMS のプラグイン

- “ Pandora Azure Storage ”.

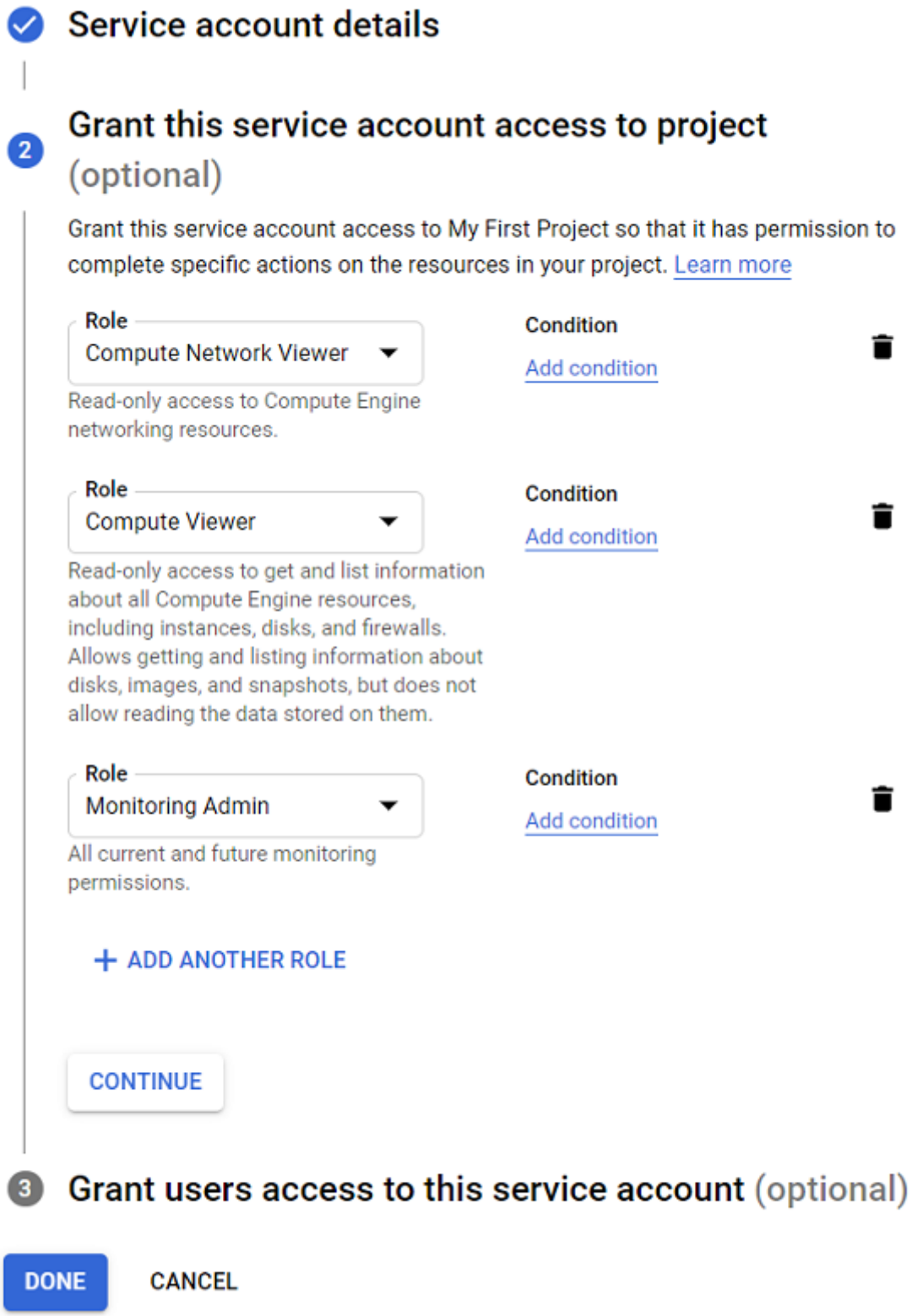
クラウド検出: Google Cloud Platform (GCP)

この機能は、Pandora FMS バージョン 750 からです。

Google Cloud Platform (GCP) 認証情報の検証

Google Cloud コンソールへアクセスするための JSON キーを登録する必要があります。次のステップを行います。

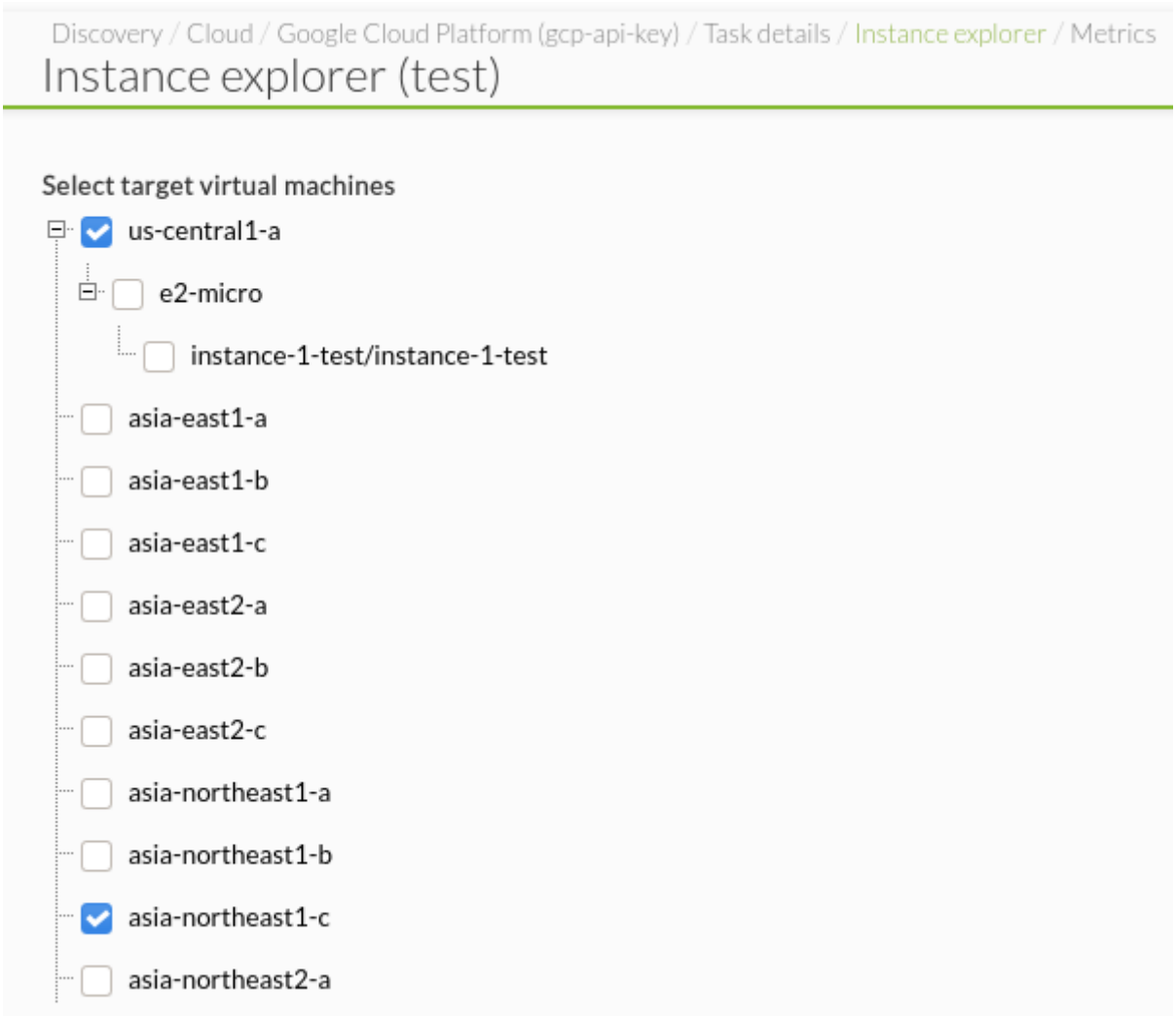
- GCP IAM のセキュリティ設定 にアクセスします。登録するログインアカウントは、次の権限を持つサービスアカウントになります。



- Pandora FMS の **プロファイル**(Profiles) → **エージェントグループ**管理(Manage agent groups) → 認証情報**ストア**(Credential Store) **から、**認証情報**ストア**(Credential Store) **へアクセスし、**“ 鍵の追加(Add key)” **をクリックします。**
- 製品(Product) **のドロップダウンで** Google **を選択し、**GCP **アカウントの** JSON key **を追加します。**
- 自動検出(Discovery) > **クラウド**(Cloud) > Google Cloud Platform **へアクセスし、**GCP 自動検出**タスクを定義することにより** GCP **アカウントの検証をします。**

Pandora FMS でのタスクの設定

タスクを定義するには、名前、そのタスクを担当する検出サーバー、グループおよび監視間隔を指定します。 タスクデータを定義したら、監視する GCP アカウントからリージョンを選択します。各リージョンでは、希望するインスタンスを順番に選択できます。



ゾーンを選択すると、そのゾーン内で検出された新しいインスタンスが 自動的に 監視されます。 インスタンスを選択すると、そのゾーンが監視されていない場合でも、明示的に 監視されます。

最後のステップは、Pandora FMS が Google Cloud Platform® で検出したインスタンスごとに作成するエージェントから取得するメトリックを選択することです。

- スキャンおよび一般監視
- CPU パフォーマンス概要
- IOPS パフォーマンス概要
- ディスクパフォーマンス概要
- ネットワークパフォーマンス概要

Google または GCP と呼ばれる汎用エージェントに、Google 監視に関連するすべてのモジュールが含まれます。

常に監視されている領域から消えたインスタンスは、障害または削除されたステータスで表示され、他のすべてのモジュールは不明で表示されます。 インスタンス全体が不明になる場合は、自動無効化モードを使用できます。

GCP タスクリストからマップを確認することもできます。

コンソールの自動検出タスク

以前にタスクリストに表示されていたものとほぼ同じコンソールタスクの場合、次のパラメーター Eを考慮して新しいタスクを作成できます。

ホストおよびデバイスの検出

ネットスキャン(NetScan)

NetScan ツールでは、ネットワーク内のデバイスを検出し、異なる監視設定を適用することができます。タスクを作成するときは、そのタスクが属するグループと、自動検出の対応するオプションを事前に設定する必要があります。

- チェックする特定のデバイスを含む CSV 形式のファイルをアップロードします (CSV ファイル定義を利用(Use CSV file definition) : ファイルを選択できます)
- または、ネットワーク(Network) を通して: カンマくぐりで特定のネットワークまたは FQDN を設定することができます。例: `192,168,50,0/24` や `192,60,0/24`, `hostname.artica.es`。必要に応じて、ドメイン名の名前解決オプションを有効にします。

間隔で手動を選択した場合は手動で検出タスクを起動する必要があります。 自動検出は、手動設定のタスクを自動的には実行しません。 ネットスキャンによって検出されたエージェントは、設定ファイルを持たないリモートエージェントです。対象ににエージェントをデプロイしない場合、ローカル監視ポリシーや設定変更をまとめて適用することはできません。

ネットスキャンオプションは次の通りです。

- 認識済ハードウエアの自動検出(Auto discover known hardware): 以前に *プライベートエンタープライズ番号* セクションに追加されたテンプレートを動的に適用します。 詳細については、こちらにアクセスしてください。
- モジュールテンプレート(Module templates): 選択したテンプレートからモジュールの適用を行います。実行がテストに合格しない場合、それらは監視リストに追加されません。
- 自動設定ルールの適用(Apply autoconfiguration rules): 検出されたエージェントに事前定義された自動設定ルールを適用します。詳細については、エージェント設定の概要を参照してください。

- SNMP 有効化(SNMP activated): 検出されたネットワークデバイスから取得した情報を活用するには、SNMPを有効にします。 検出された対象で使用可能な SNMP 情報をスキャンすることにより、検出が向上します。 このトークンが有効になると、さらに次の 2つのオプションが表示されます。
  - SNMP バージョン(SNMP version): スキャンされるネットワークデバイスで設定されている SNMP バージョンを選択します。SNMP バージョン 1、2、2c、3 をサポートしています。
  - NG 766 以降: 無効なインターフェイスの参照を回避するには、無効なインターフェイスをスキップ(Skip non-enabled interfaces) オプションを使用します。
  - 試行する SNMP コミュニティ(SNMP communities to try with): 設定されているコミュニティを示します。以降のボックスにコミュニティを入力して、必要なだけコミュニティを追加できます。
- WMI 有効化(WMI enabled): WMI スキャンを有効化できます。認証情報ストア で事前設定した認証情報を 利用認証情報(Credentials to try with) で選択するだけです。

検出された WMI をサポートする対象に対して提供されるさまざまな資格情報がテストされ、CPU、メモリ、およびディスクの使用状況について報告するモジュールによる監視が補完されます。

- 親の再帰(Parent recursion): 親の検出を改善し、処理に再帰を追加します。
- VLAN 有効化(VLAN enabled): さまざまなデバイスが接続されているVLANを検出します。

自動エージェントデプロイ

コンソールからエージェントをデプロイする手順は次の通りです。

- エージェントリポジトリにデプロイするソフトウエアエージェントのバージョンを登録: デプロイするエージェントのインストーラが必要です。カスタムエージェントを利用することもできます。
- 認証情報ストアで対象へ接続するために利用する認証情報を登録: 検出または指定された対象へのアクセスのテストに使用する認証情報を指定します。
- デプロイの準備ができかた確認します。
  - デプロイ対象 の定義。
  - 公開アクセスURL の定義。
  - ソフトウエアをデプロイするインストーラ の登録。

このシステムは、プッシュ処理は実行しません。すべてのデプロイは、ターゲットに対してソフトウェアを *提供* し、インストールする指示が送られることにより行われます。エージェントの自動デプロイが正しく動作するためには、サーバのバージョンが EL7 (Red Hat Eenterprise Linux) 以降である必要があります。 GNU/Linux Debian および関連ディストリビューション (Ubuntu など) では、curl コマンドがすでにインストールされているはずです。

対象の検索

E デプロイ対象

新たなターゲットを定義するには、ターゲットのスキャン(Scan for targets)、ターゲット追加(Add target)、または ターゲット読み込み(Load targets) を利用します。

対象が存在する一つ以上のネットワークのスキャン

対象をスキャンするボタンを押すと、以下のフィールドのポップアップが表示されます。

- ネットワーク/マスク(Network/mask): スキャンするネットワーク(カンマ区切り)
- 適切なエージェントバージョン(Desired agent version): 検出した対象に想定するソフトウエアエージェントのバージョン
- 対象サーバ IP(Target server IP): ソフトウェアエージェントがインストールされたときに、それが指し示すサーバの IP (エージェント設定ファイルにおける “server_ip” フィールドに設定されます)

エージェントの展開に関連する検出タスクは 一時的な タスクです。完了すると、それらは自動的に削除されます。 成功または失敗の両方について、スキャンまたはデプロイに関する情報は、デプロイセンター自体から参照できます。

対象の情報の CSV ファイルでのアップロード

この CSV インポーターは自動検出タスクは実行しません。CSV で提供された名前、IP、OS タイプ、説明、およびグループで空のエージェントを作成します。

対象を複数登録したい場合は、以下のフォーマットの CSV ファイルをアップロードします。

```
エージェントの別名, IP アドレス, OS ID, 間隔, グループ ID, 説明
```

- エージェントの別名: 将来のエージェントの別名。名前として別名を利用 オプションを選択すると、名前は別名と同じになります。
- IP アドレス: エージェントがインストールされたコンピュータの IP アドレス。
- OS ID: OS を特定する番号。AIX, BSD, HP-UX, Linux, Solaris, Windows など。
- 間隔: 各チェックの秒単位の間隔
- グループ ID: エージェントが所属するグループの ID 番号。

ソフトウエアのデプロイ

認証情報とデプロイするソフトウェアバージョンの両方を指定して、情報が完全なターゲットに対してのみ展開をスケジュールできます。

一覧に対象がある場合、エージェントのデプロイを起動します。一覧(正しい対象のみ表示されます)

から対象の IP を選択し、エージェントのデプロイを開始するには デプロイ(Deploy) ボタンをクリックします。

バックグラウンドでのデプロイするための検出タスクが自動的に作成され、指定した対象にエージェントをインストールします。デプロイセンターの対象のリストから、エージェントが正常にインストールされたことを確認できます。

CSV でのデバイス一覧のインポート

エージェントインポートウィザードを用いてCSV でデバイスの一覧をエージェントとしてインポートできます。

この機能は、Pandora FMS でリモート監視用のエージェントのみを作成します。

使用する区切り文字、インポート先のサーバ、データを含むファイルを選択して、Go をクリックします。

カスタムネットスキャン

ネットワーク検出タスクを実行するためのカスタムスクリプトの実行ができます。所属するグループと実行間隔を指定します。 タスクの作成処理が完了したら、実行するスクリプトとその実行に必要な指定ファイルを指定します。

ネットスキャンスクリプト

このセクションでは、カスタム検出タスク用に作成されたさまざまなスクリプトを表示します。管理(Management) > 自動検出(Discovery) > ホスト&デバイス(Host&devices) > スキャンスクリプト管理(Manage scan scripts) からアクセスします。

andora FMS では、スクリプトを追加することにより、必要なネットワークの監視と検出を容易にすることができます。スクリプトを作成することにより、それを正しく実行するために必要なすべてのパラメータを定義するマクロを追加できます。