IBM Cloud Pak for Multicloud Management Integration Installation guide

This document provides a detailed step by step guide for installation of the IBM Cloud Pak for Multicloud Management integration components:

- **Sysdig Agent**
- **Sysdig Secure Event Forwarding**
- **OpenID Single Sign On**
- **Navigation Menu Shortcuts**

v1.0.3

Overview

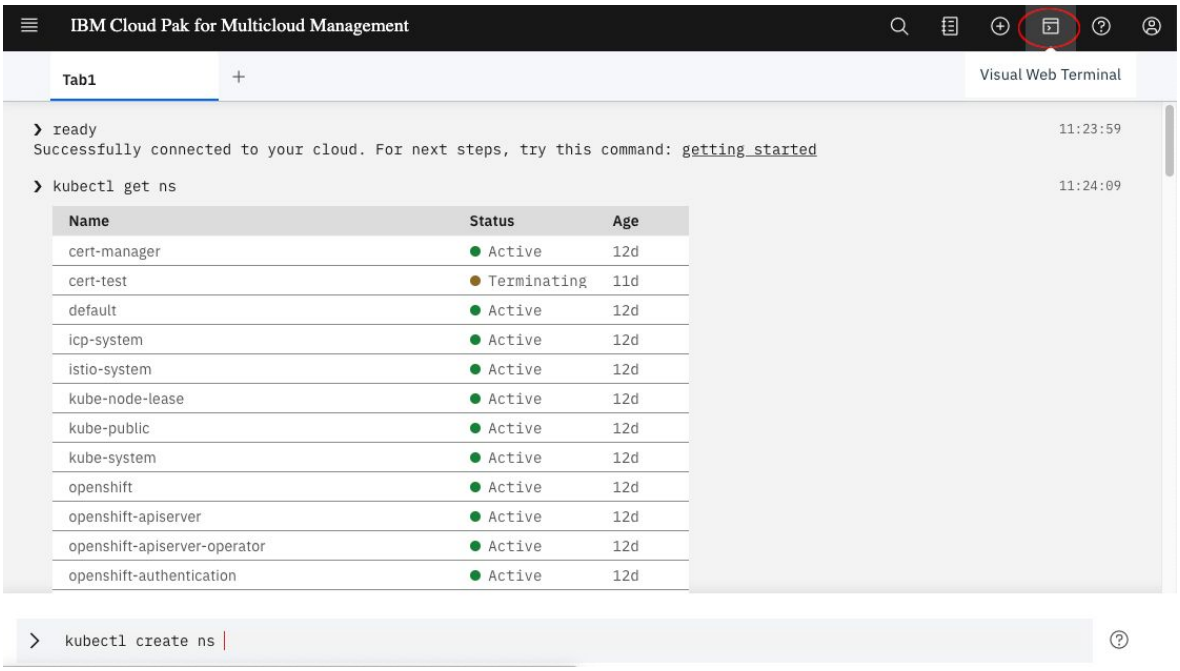
Sysdig integration with IBM Cloud Pak for Multicloud Management is composed of several components. Currently each component is installed and configured independently.

General requirements

Some component configuration requires the user to execute *kubectl*, *cloudctl* or *helm* commands on the command line.

- Install and Set Up kubectl
- Installing IBM Cloud Pak CLI (cloudctl)
- Installing Helm

Alternatively, the *kubectl*, *cloudctl* and *helm* commands can be executed in the **Visual Web Terminal** that is available directly in the top navigation bar of the IBM Cloud Pak for Multicloud Management console:



Sysdig agent

The Sysdig agent deploys on every node of your infrastructure, and monitors system calls depending on your defined policies and rules to detect undesired activities. Policies and rules are defined in Sysdig Secure. Whenever anything matching a defined policy occurs, the agent triggers a security event. The event is registered in Sysdig Secure for further analysis.

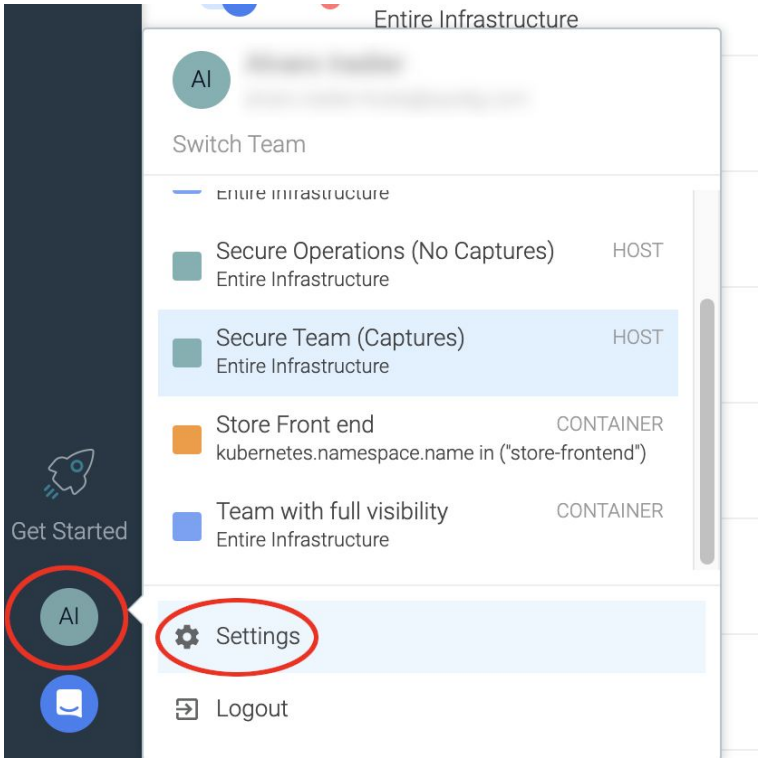
Requirements

- Kubernetes or Openshift cluster(s) managed by IBM Cloud Pak for Multicloud Management.
- A namespace where the Sysdig Agent is later deployed must exist.
    - The Sysdig Agent installation instructions in this information uses the **sysdig-agent** namespace. If it does not exist, create it by running the following command:
      `kubectl create ns sysdig-agent`
    - Otherwise, you can use a different pre-existing namespace (i.e. *kube-system*, or *default*).
- An IBM Cloud Pak for Multicloud Management account with administrator privileges.
- A Sysdig Secure installation (either SaaS license, or On-Prem version).
- A Sysdig Secure *Agent Installation Key* (obtained in the installation instructions).

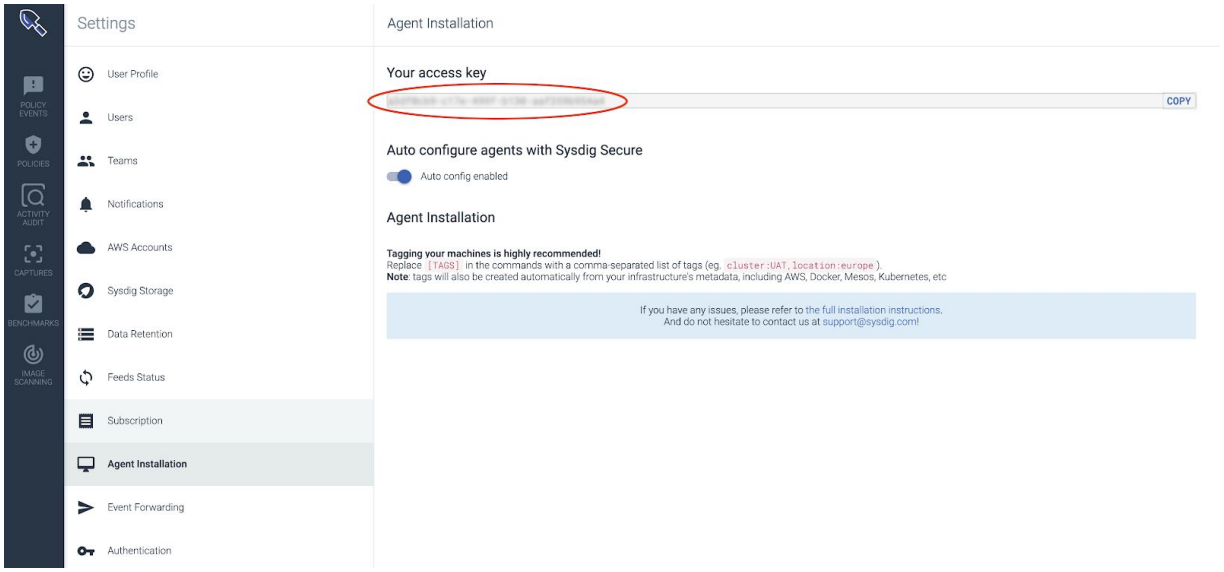
Installation

1. Navigate to Sysdig Secure.
    a. For SaaS, navigate to https://secure.sysdig.com/.
    b. For On-Prem, navigate to https://HOSTNAME/secure, where HOSTNAME is the address of your On-Prem instance.
2. Enter the credentials (email and password) for the admin user.
3. In Sysdig Secure, obtain the *Agent Installation Key* in the *Agent installation* section:

a. Click the green circle with your user initials at the bottom left of the screen, and then click on *Settings* on the pop-up menu to go to Account *Settings*.

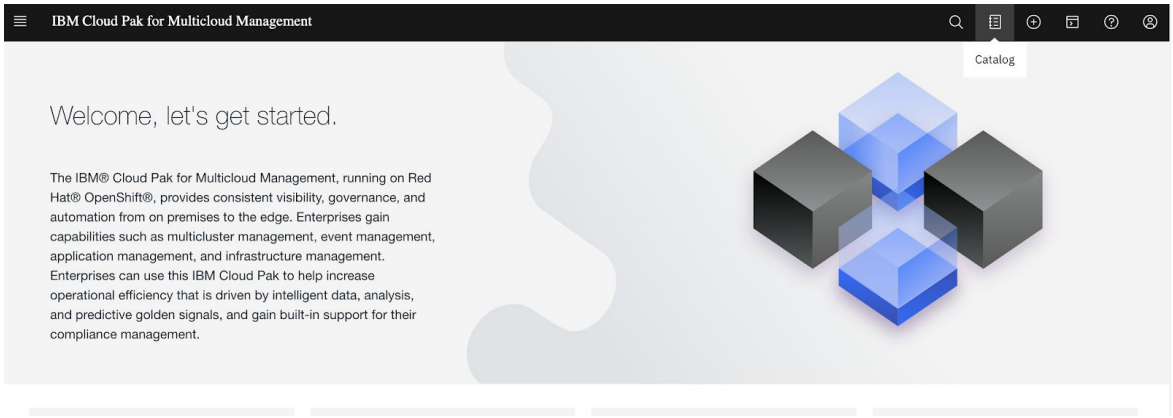


b. Copy the ***Agent access key*** that will be used during the agent installation:

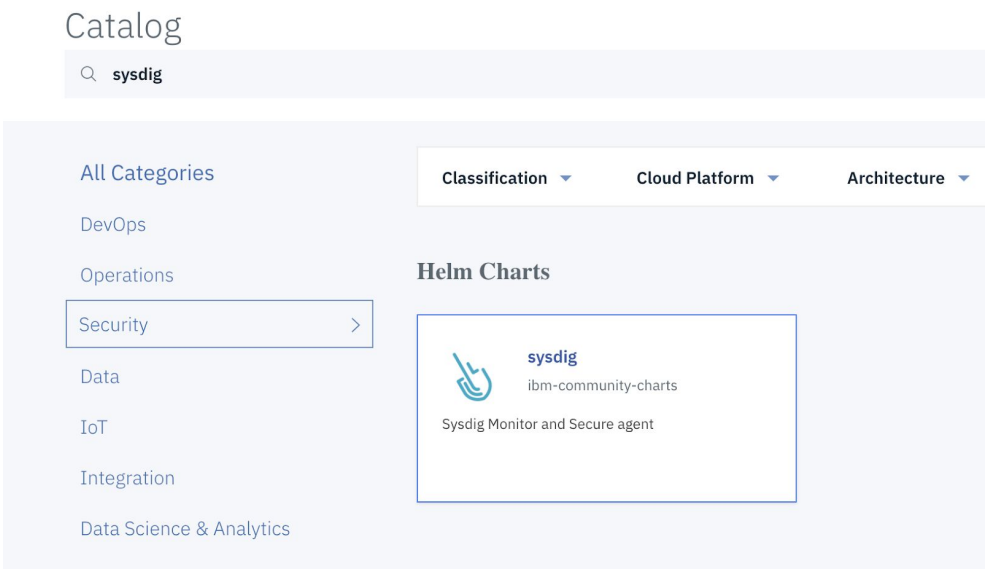


Online installation

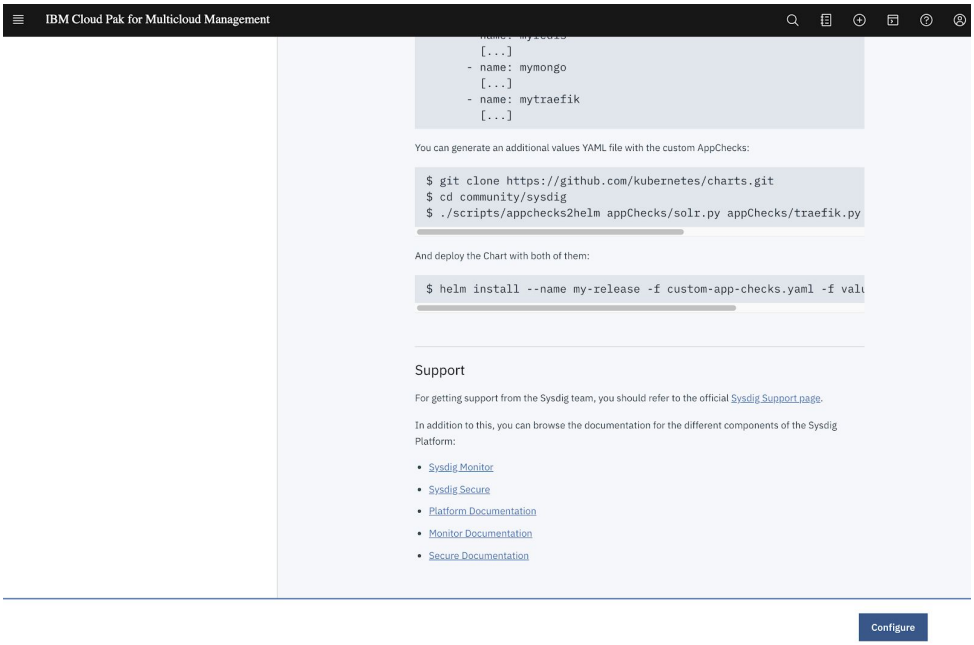
1. Login to IBM Cloud Pak console
2. Go to the Catalog clicking on the catalog icon located at the the icon bar on the header of the console screen.



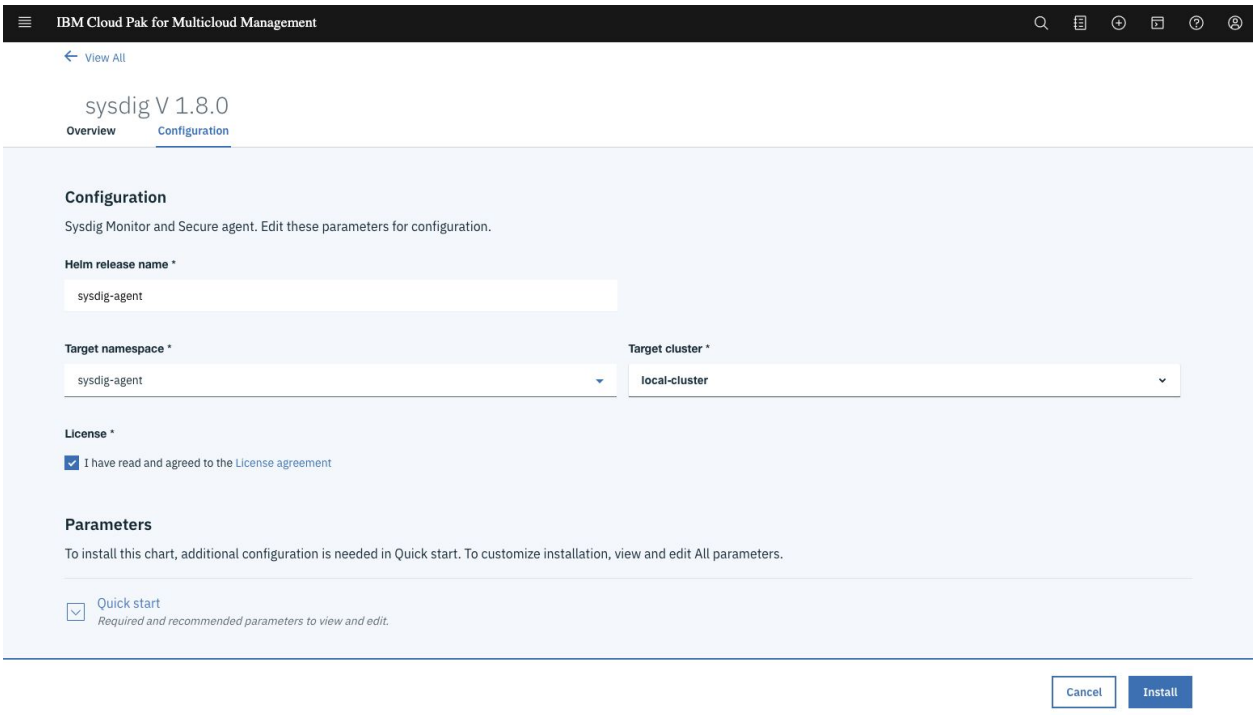
3. In the *Catalog*, search for the *Sysdig* Helm chart by entering “sysdig” in the search field. Click the Helm chart:



4. This guide describes how to install the Sysdig agent from the IBM Cloud Pak console, so ignore the command-line installation instructions, and just click the *Configure* button:



5. Provide a release name, choose the namespace where the agent will be installed, and select the cluster or clusters where it will be deployed:



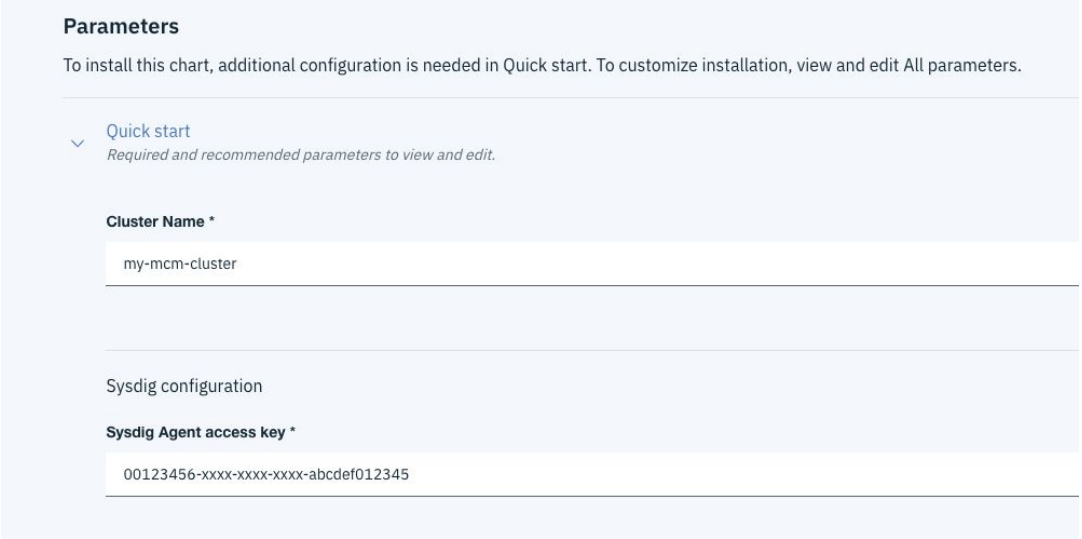
Recommended values:

- *Helm release name*: **sysdig-agent**
- Target *namespace*: **sysdig-agent**

NOTE: The namespace must exist on the Target cluster, so you need to create it first.

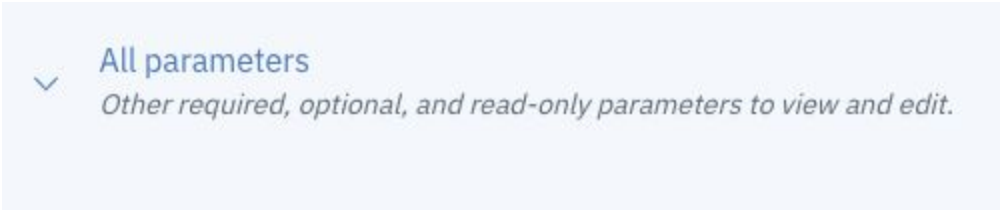
6. Read the License agreement and check the "*I have read and agreed to the License agreement*" checkbox:

7. In the *Quick Start* section under *Parameters*, provide a *Cluster Name* and the ***Sysdig Agent access key*** in the corresponding fields:

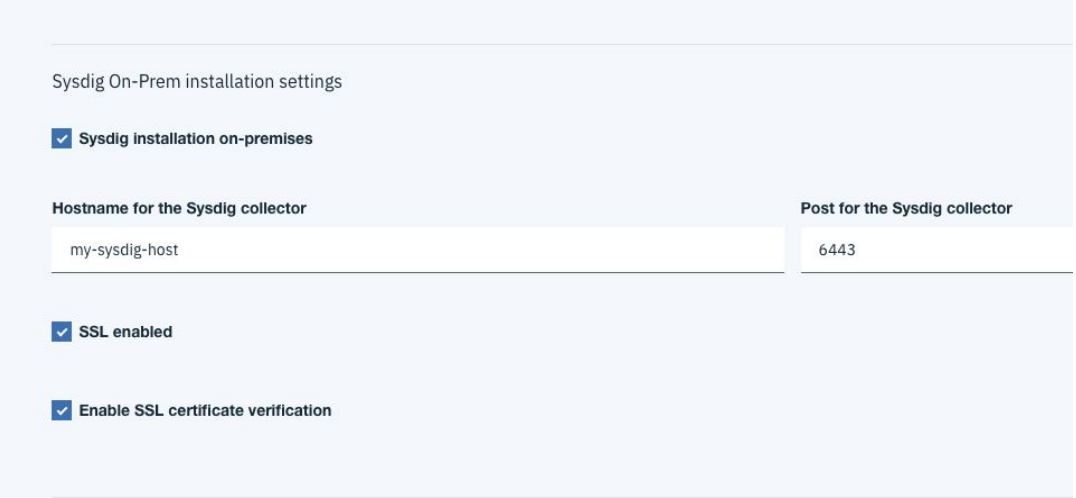


The *Cluster Name* will be included in the events detected by Sysdig Secure. As you need to provide a different cluster name for each cluster where the agent is deployed, **you'll need to deploy once per cluster**.

8. For additional settings, expand the *All Parameters* section:

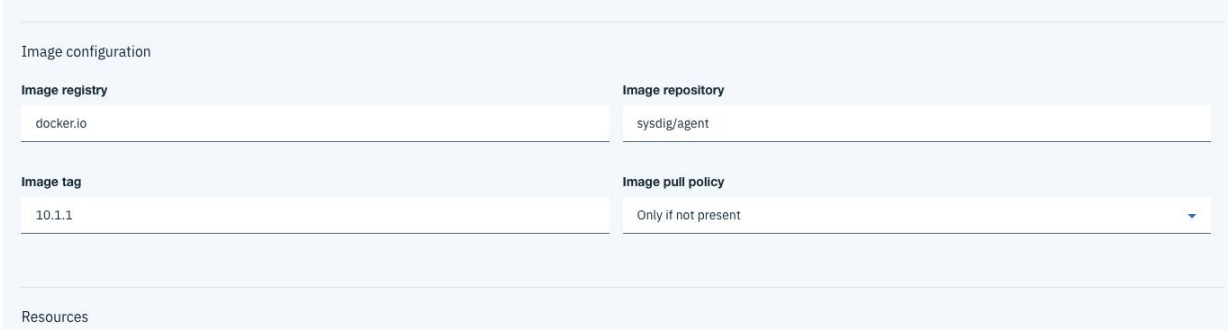


9. Only for Sysdig On-Prem, you need to provide the *Hostname for the Sysdig collector* of your Sysdig installation by checking the *Sysdig Installation on-premises* option in *Sysdig On-Prem installation settings* section, and providing the *collector* host and port:



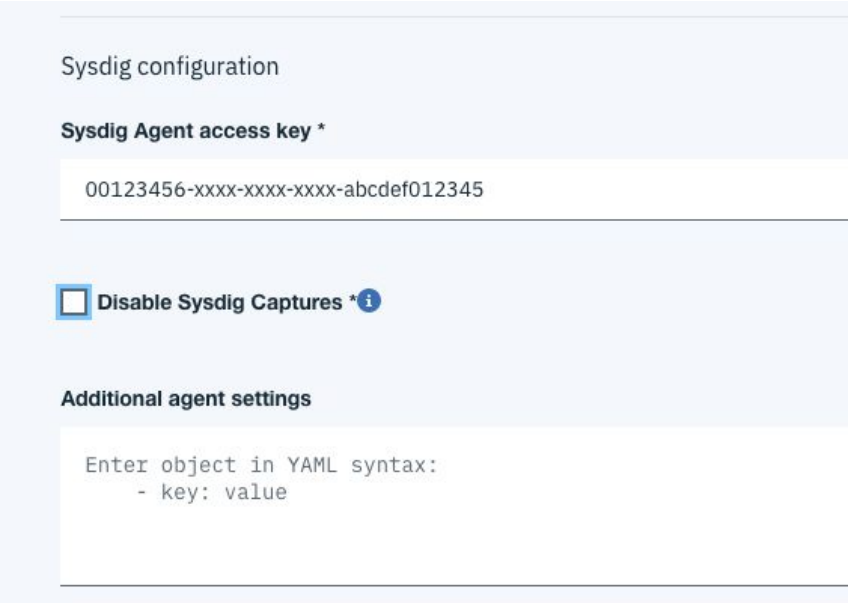
Additionally you can disable *ssl*, or disable the *SSL certificate verification* if not using a valid SSL certificate.

10. If you want to install a different version of the agent set it in the *Image configuration* subsection, by changing the value of *Image Tag*:

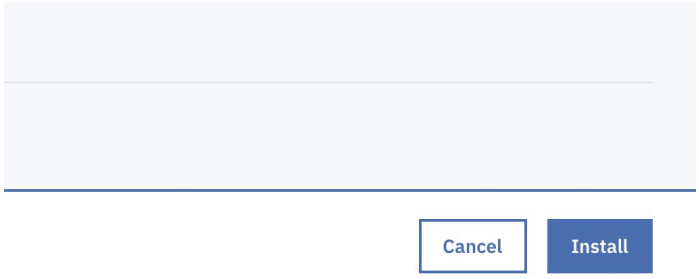


11. To enable the Sysdig captures functionality (see more details in https://docs.sysdig.com/en/disable-captures.html), which is disabled by default, uncheck the

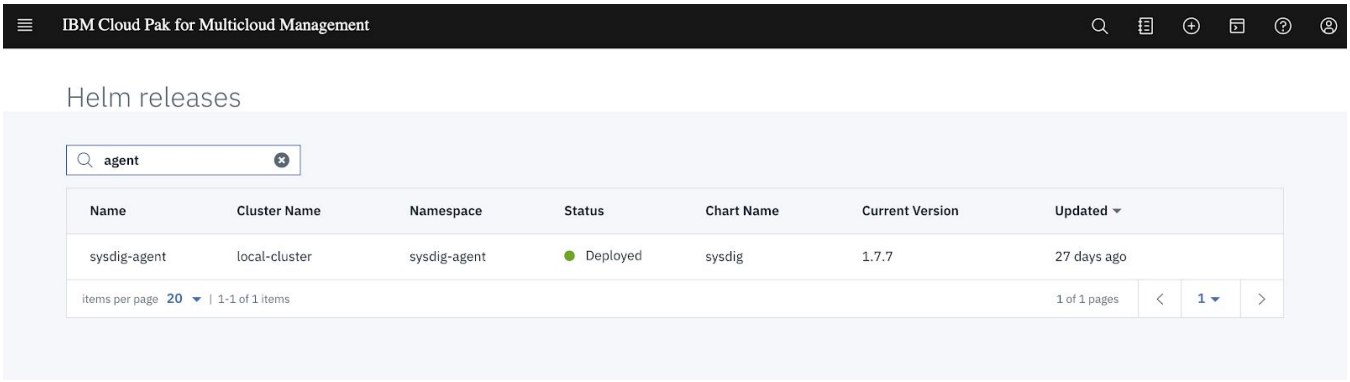
Disable Sysdig Captures checkbox in the *Sysdig Configuration* section:



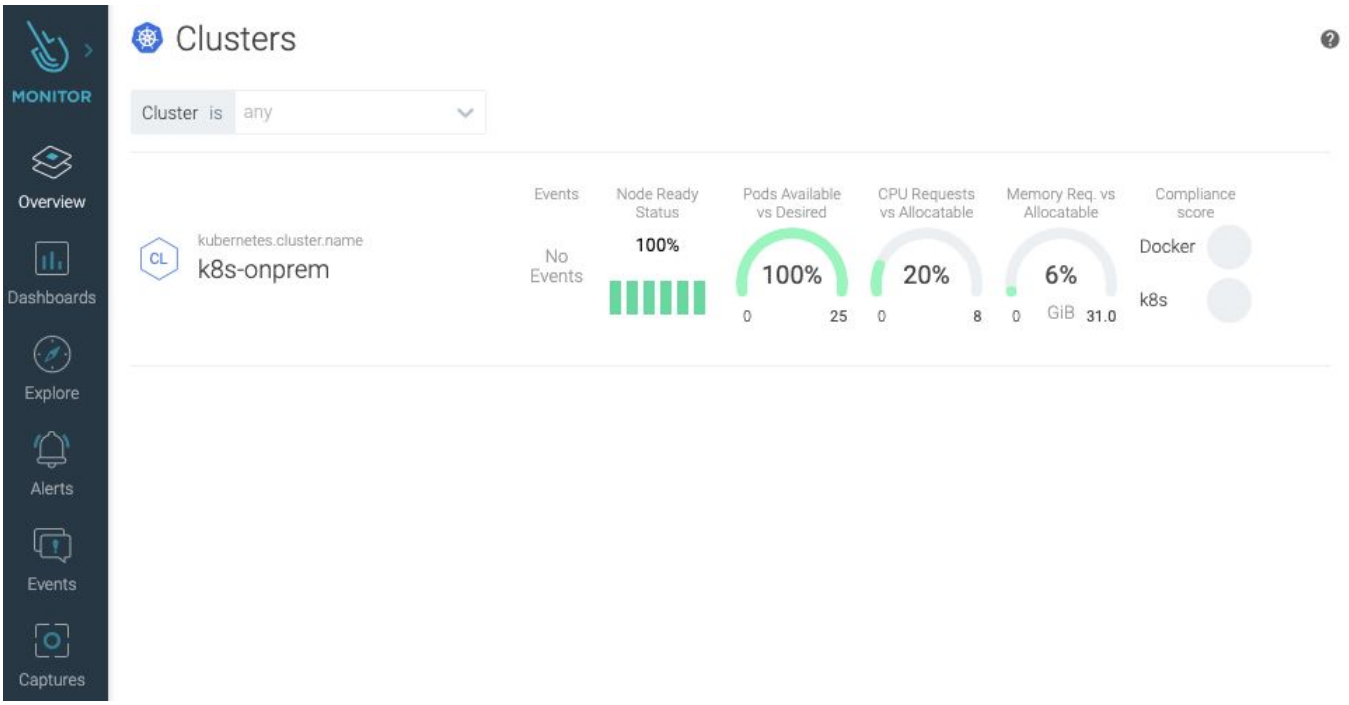
12. You can enter additional agent settings as described in the Configuring System Agent document.
    Additional settings for different environments are available at:
    a. Kubernetes (Vanilla): https://docs.sysdig.com/en/steps-for-kubernetes--vanilla-.html
    b. IKS: https://docs.sysdig.com/en/agent-install--iks--ibm-cloud-with-sysdig-.html
    c. OpenShift: https://docs.sysdig.com/en/steps-for-openshift.html
    d. Others: https://docs.sysdig.com/en/agent-installation.html
13. Click the *Install* button at the bottom left to trigger the deployment of the agent



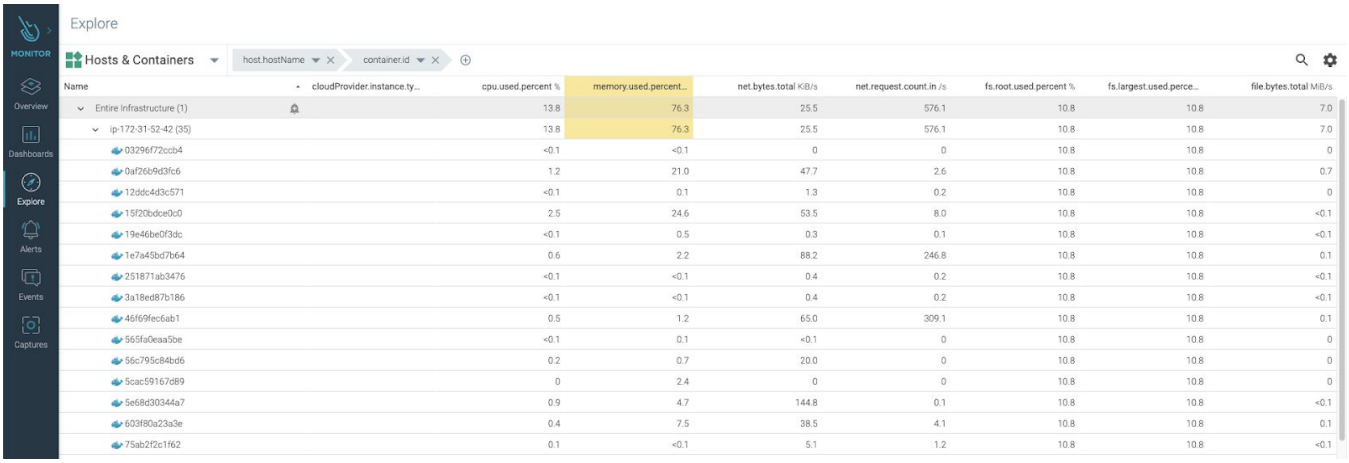
14. The *sysdig-agent* installation should appear in list of *Helm releases* under *Monitor health -> Helm releases:*



15. After a few minutes, you should see the new cluster under the Sysdig Monitor *Overview* by clusters section. Open Sysdig Monitor and click on the *Overview* icon on the side navigation bar, then choose *Kubernetes -> Clusters* in the pop-up menu:



or in the *Explore* section:



16. The agent installation is finished and ready.

Airgapped installation

See the **README** file in the tarball for instructions to complete the airgapped installation.

Event Forwarding

Sysdig Secure Event Forwarding integration allows you to receive security events detected in Sysdig directly into the Govern & Risk Security Findings dashboard in IBM Cloud Pak for Multicloud Management. From the dashboard you can directly jump into Sysdig Secure event to perform further incident analysis and response.

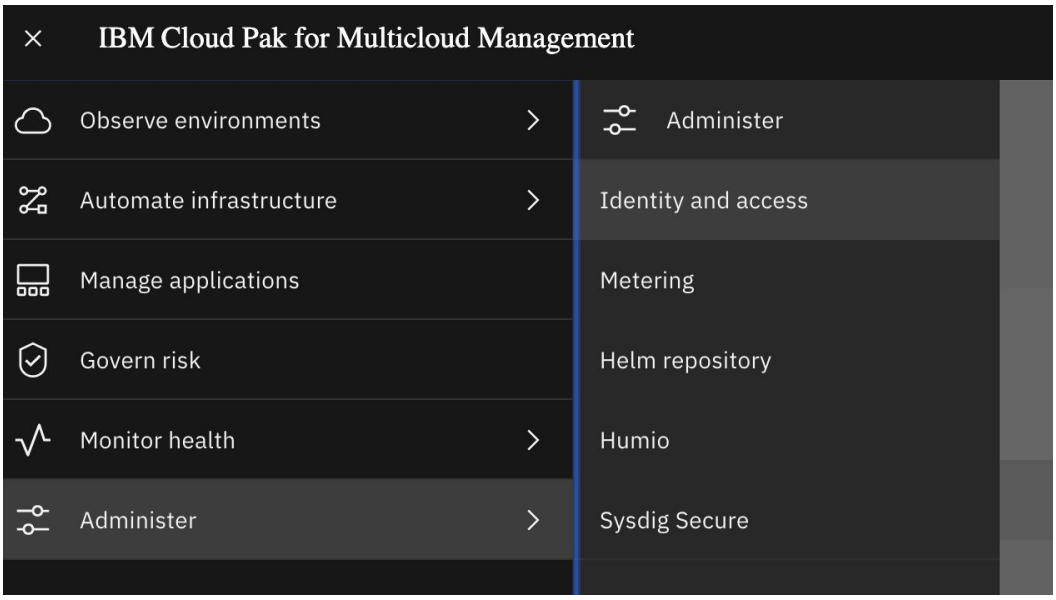
Requirements

- Kubernetes or Openshift cluster(s) managed by IBM Cloud Pak for Multicloud Management.
- An IBM Cloud Pak for Multicloud Management account with administrator privileges.
- A Sysdig Secure installation (either SaaS license, or On-Prem version).
- Sysdig Agent already installed on the cluster.
- A *grafeas-service-admin-id* API Key in IBM Cloud Pak for Multicloud Management (created in the installation instructions).

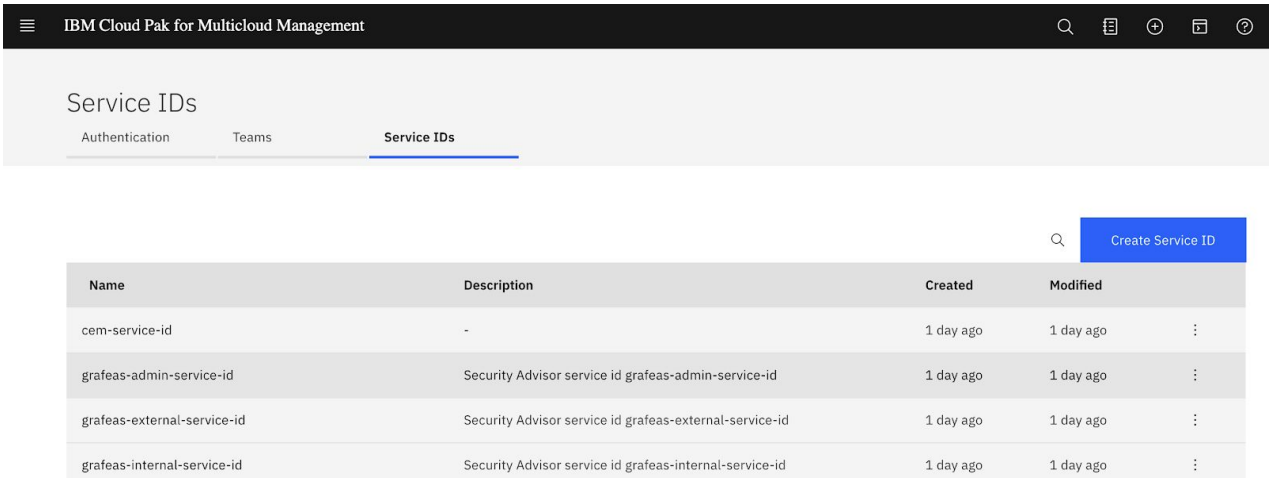
Installation

1. Login to IBM Cloud Pak console with an administrator account.

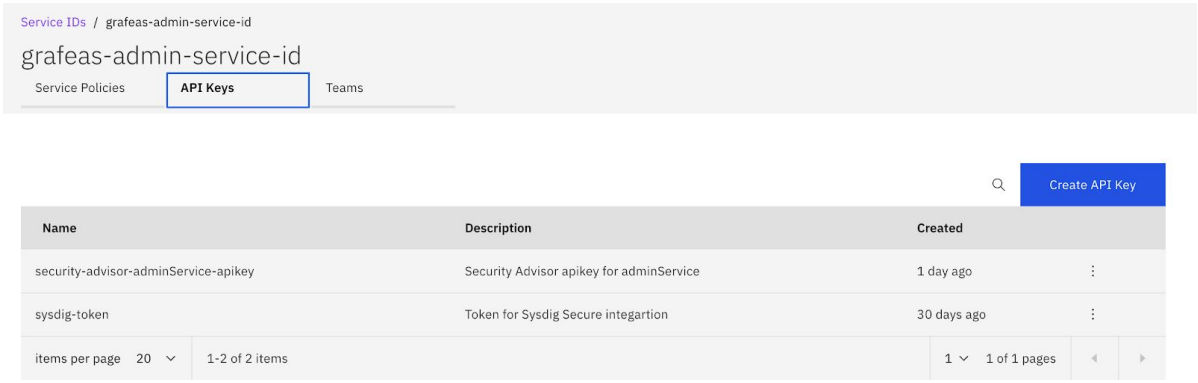
2. Go to *Administer -> Identify and access*



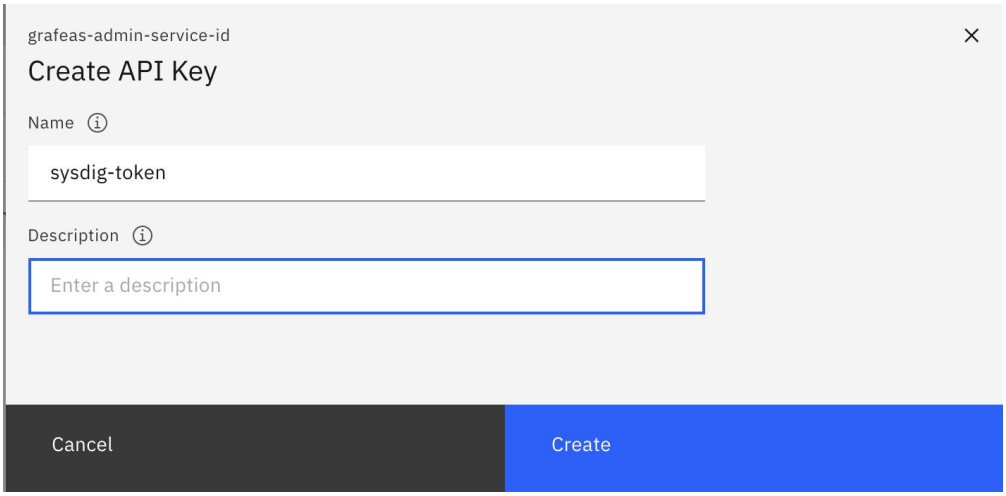
3. Click the *Service IDs* tab, and then click on the *grafeas-admin-service-id* entry.



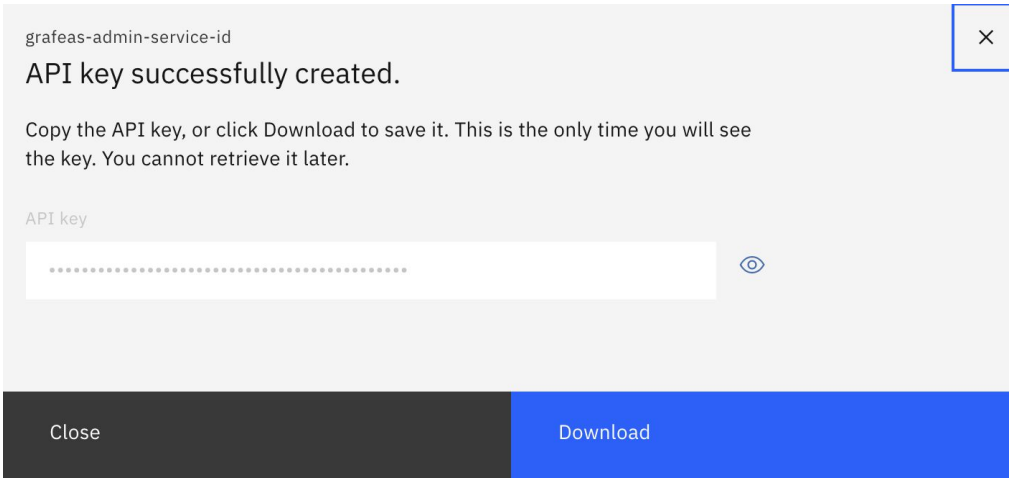
4. Click on the *API Keys* tab, then on the *Create API Key* button:



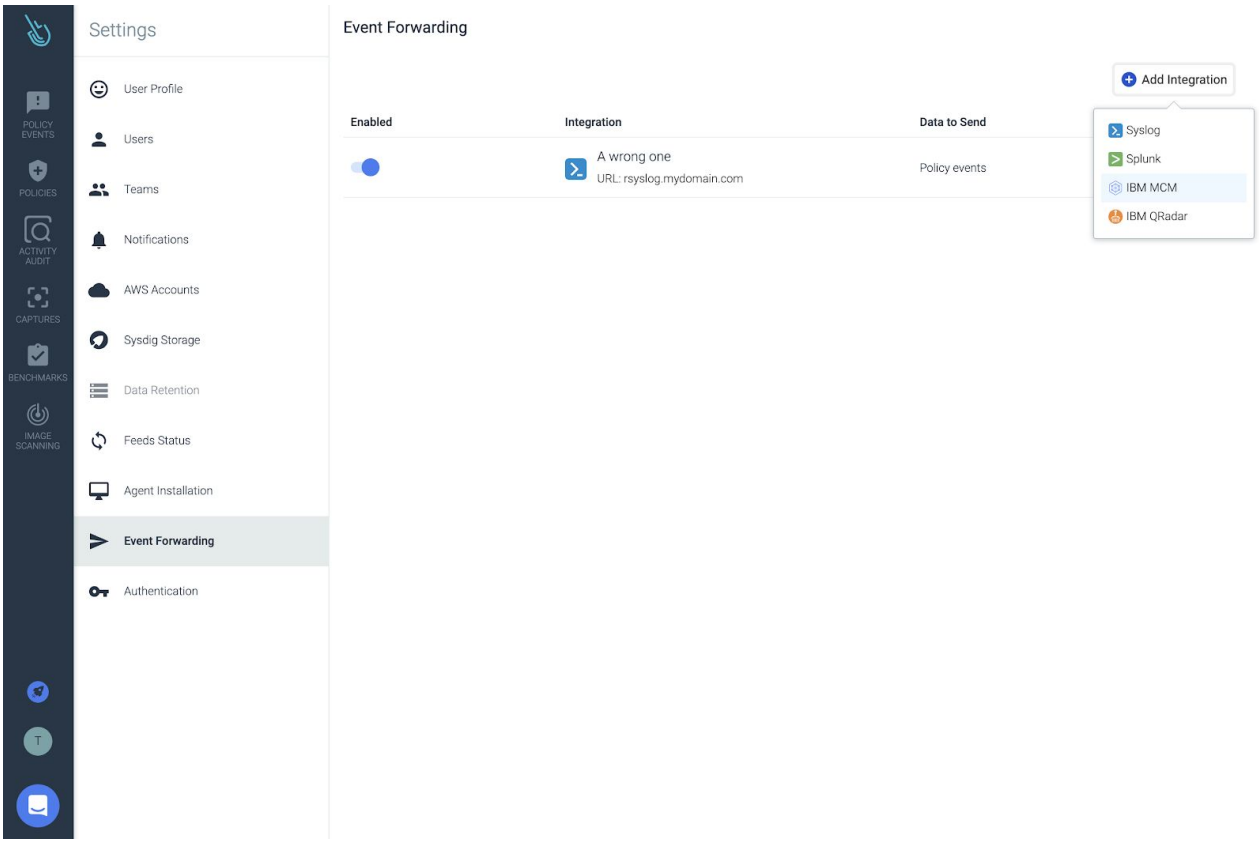
5. Provide a name (i.e. *sysdig-token*) and optionally a description, and click *Create*:



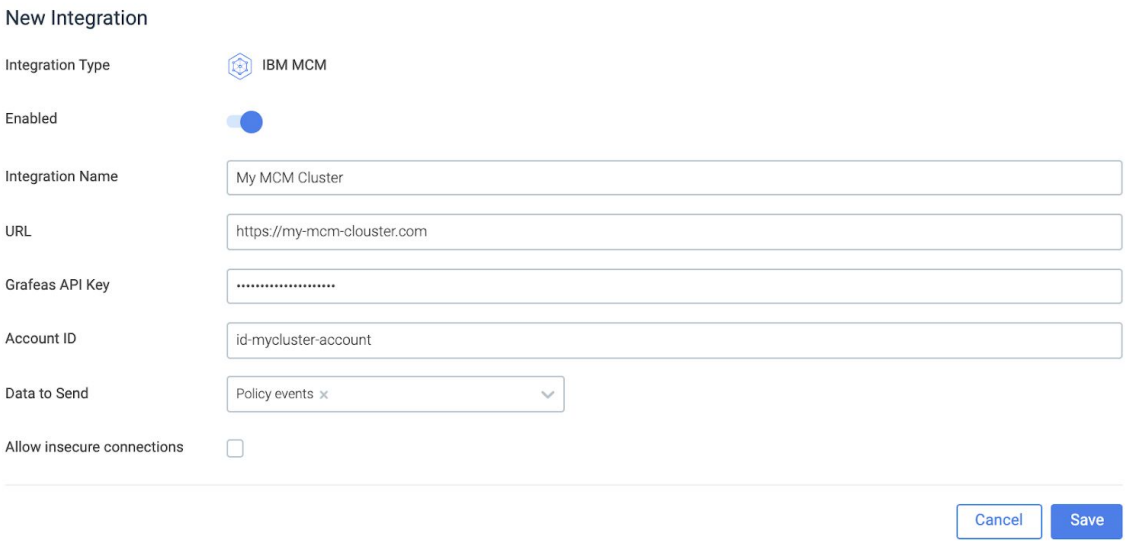
6. Copy and store, or download, the created API Key. You will need it later for configuring the Event Forwarder:



7. Login to Sysdig Secure, go to the Account *settings* using the account menu on the bottom left, and then go to the *Event Forwarding* section. Click on the *Add integration* button and choose IBM MCM:



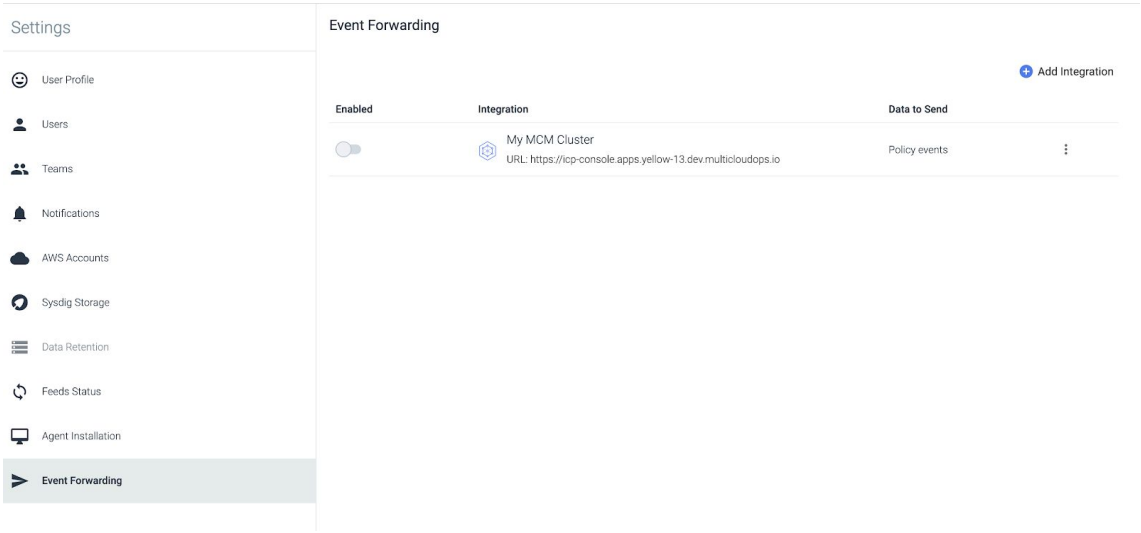
8. Fill up the configuration details, using the IBM Cloud Pak for Multicloud Management API Endpoint of your cluster and the Grafeas API Key previously created:



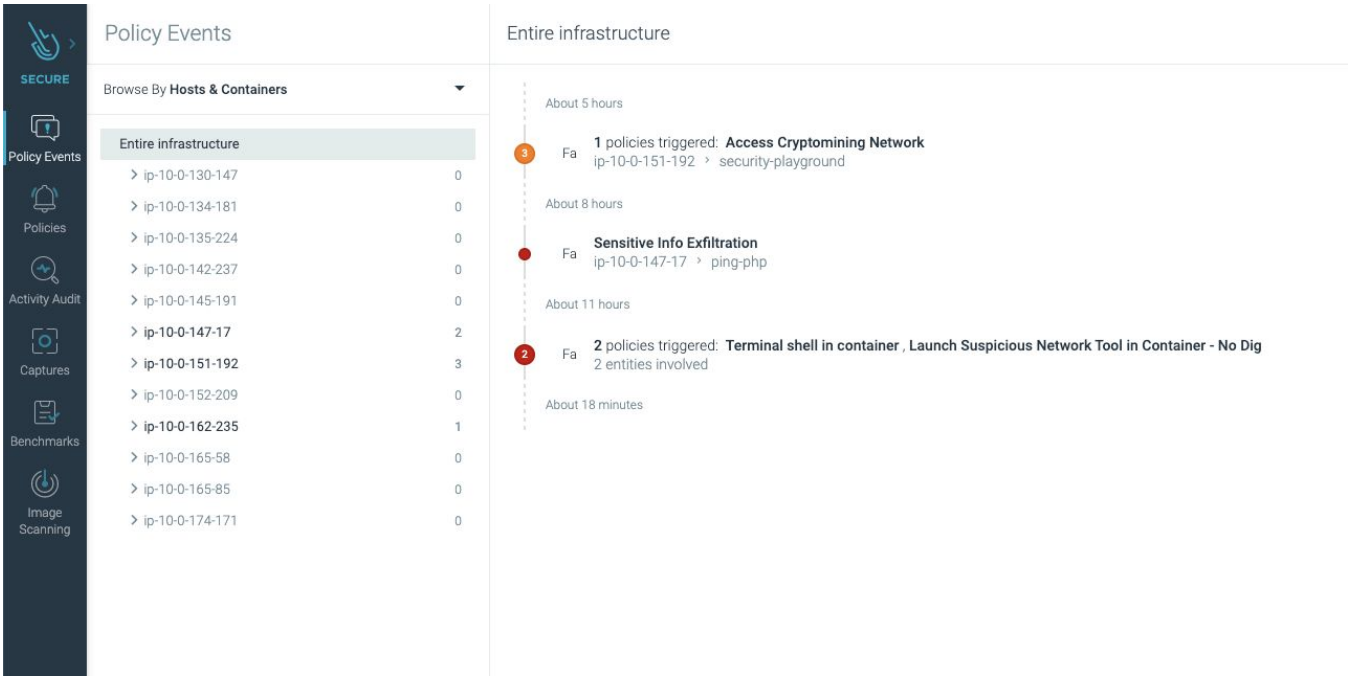
Integration Name: enter any name to identify this event forwarder.
URL: The URL, including https:// and port if it is not the default 443, to your IBM Cloud Pak for Multicloud Management API endpoint. This URL should be the same you use to connect to the IBM Cloud Pak for Multicloud Management console.
Grafeas API Key: The API key you obtained in Step 6.
Account ID: You can leave it blank to use the default value of *id-mycluster-account*. If you want to use a different account name, provide it here. You can list the existing accounts in your cluster using *cloudctl iam accounts* command.
Data to Send: select the types of events that you want to forward to IBM Cloud Pak for Multicloud Management.

9. Click *Save* to complete the configuration.

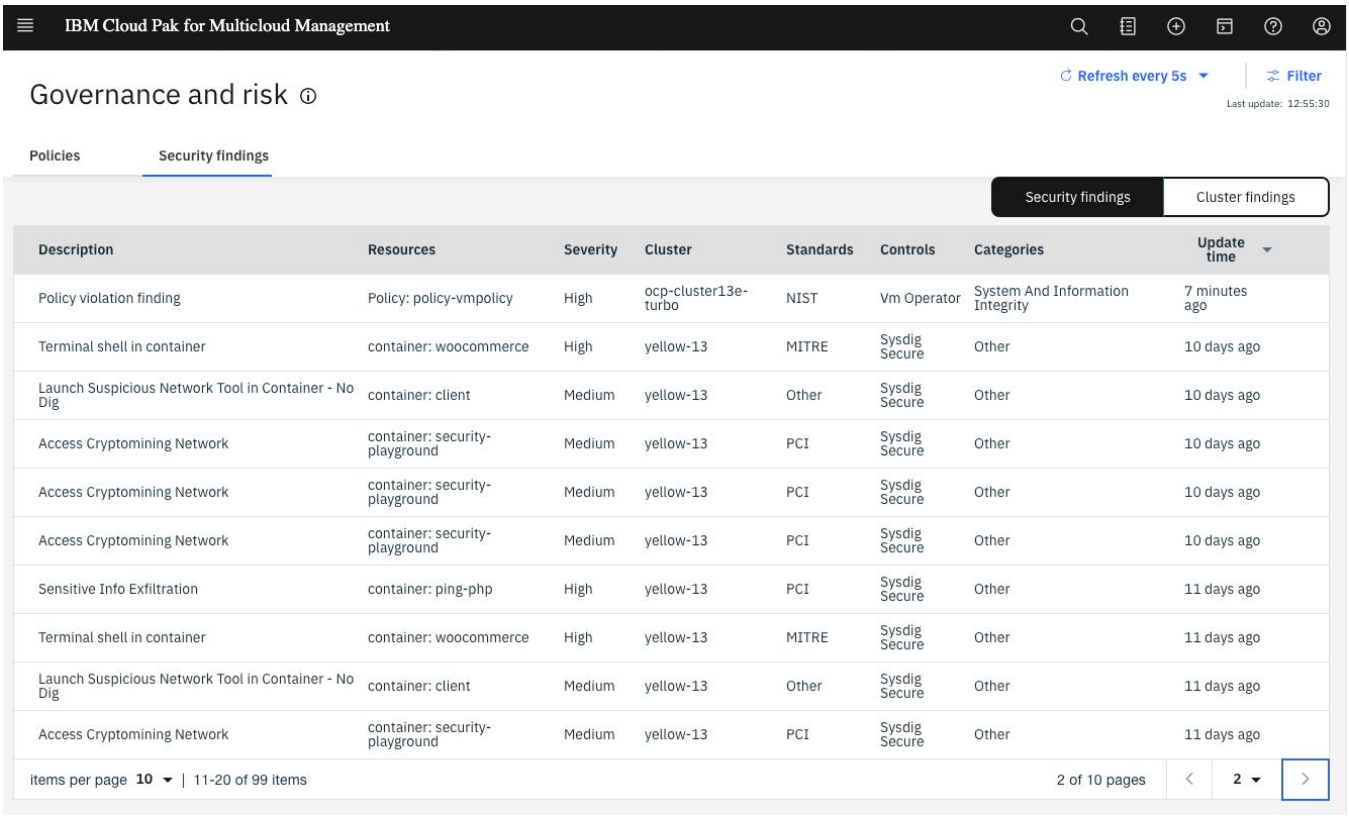
10. The new Event Forwarder will now be listed in the *Event Forwarding* screen.



11. Once the Event Forwarder is ready, new Policy Events in Sysdig Secure should be forwarded to the *Govern risk* findings section in BM Cloud Pak for Multicloud Management.
    For example, the following events from Sysdig Secure:



Will be available in *Govern risk* dashboard, inside *Security Findings* section



Description	Resources	Severity	Cluster	Standards	Controls	Categories	Update time
Policy violation finding	Policy: policy-vmpolicy	High	ocp-cluster13e-turbo	NIST	Vm Operator	System And Information Integrity	7 minutes ago
Terminal shell in container	container: woocommerce	High	yellow-13	MITRE	Sysdig Secure	Other	10 days ago
Launch Suspicious Network Tool in Container - No Dig	container: client	Medium	yellow-13	Other	Sysdig Secure	Other	10 days ago
Access Cryptomining Network	container: security-playground	Medium	yellow-13	PCI	Sysdig Secure	Other	10 days ago
Access Cryptomining Network	container: security-playground	Medium	yellow-13	PCI	Sysdig Secure	Other	10 days ago
Access Cryptomining Network	container: security-playground	Medium	yellow-13	PCI	Sysdig Secure	Other	10 days ago
Sensitive Info Exfiltration	container: ping-php	High	yellow-13	PCI	Sysdig Secure	Other	11 days ago
Terminal shell in container	container: woocommerce	High	yellow-13	MITRE	Sysdig Secure	Other	11 days ago
Launch Suspicious Network Tool in Container - No Dig	container: client	Medium	yellow-13	Other	Sysdig Secure	Other	11 days ago
Access Cryptomining Network	container: security-playground	Medium	yellow-13	PCI	Sysdig Secure	Other	11 days ago

Rules configuration and IBM Cloud Pak for Multicloud Management Context mapping

Policy Events forwarded to Security Findings are mapped to the IBM Cloud Pak for Multicloud Management context:

- Resource Type
- Resource Name
- Namespace
- Cluster Name

The mapping is performed based on two different sources: event **fields** and event **labels**. Please consider the following guidelines to allow an optimal mapping to IBM Cloud Pak for Multicloud Management Context.

Event labels

Kubernetes events in Sysdig Secure are enriched with a set of labels including:

- kubernetes.cluster.name
- kubernetes.namespace.name
- kubernetes.pod.name
- ...

as described in the Sysdig Event Forwarding documentation. These labels are included by default, but can be removed by using the *exclude* option in the agent configuration. **This should not be necessary and will prevent the mapping from working correctly, so please don't use this option in the agent settings.**

Event fields

When a Policy Event is triggered from a defined Falco rule, the event will include all the **fields** that are used in the Falco rule output. For example, the following rule, coming from the Kubernetes Audit source:

```
- rule: Ingress Object Without TLS Cert Created                                    Secure UI
  condition: ( kactivity and kcreate and ingress and response_successful and not ingress_tls )
  output: K8s Ingress Without TLS Cert Created (user=%ka.user.name ingress=%ka.target.name\
        \ namespace=%ka.target.namespace)
  source: k8s_audit
  description: Detect any attempt to create an ingress without TLS certification
  tags: k8s, network
```

will include the fields:

- ka.user.name
- ka.target.name

- ka.target.namespace

The full list of available fields is available in https://falco.org/docs/rules/supported-fields/

The available fields help mapping the event to the IBM Cloud Pak for Multicloud Management context for *k8s_audit* (Kubernetes Audit log) source. So in case you define a custom rule for *k8s_audit* **please include relevant fields in the output**:

- ka.target.name (for the Resource Name).
- ka.target.resource (contains the Resource Type).
- ka.target.namespace (contains the Namespace).

OpenID Connect SSO

Single-sign-on (SSO) integration simplifies the registration and login experience of IBM Cloud Pak for Multicloud Management users in Sysdig Monitor and Sysdig Secure.

IBM Cloud Pak for Multicloud Management acts as an OpenID Connect identity provider, so any user can login in the Sysdig platform with the same credentials they are using in IBM Cloud Pak for Multicloud Management. If they have already logged in, the same session is used and the user won't need to identify again. Newly onboarded users are assigned to a default team in Sysdig applications

Requirements

- Kubernetes or Openshift cluster(s) managed by IBM Cloud Pak for Multicloud Management.
- A IBM Cloud Pak for Multicloud Management account with administrator privileges.
- Users in IBM Cloud Pak for Multicloud Management must have an email attribute.
- A Sysdig Secure installation (either SaaS license, or On-Prem version).
- A Sysdig Monitor installation (either SaaS license, or On-Prem version).
- For SaaS only, your Sysdig Secure / Sysdig Monitor *customer name*, which is associated with your license and account. You can ask Sales to set and provide your *customer name*.
- IBM Cloud Pak for Multicloud Management console must have a valid TLS certificate. If that is not the case, check how to include external CA certificates:
    - Use CA Certs for External SSL Connection (Kubernetes)
    - Use CA Certs for External SSL Connection (Openshift)

Installation

SSO configuration is a three stepwise process. First, you need to create a new "client registration" in IBM Cloud Pak for Multicloud Management, which is the Identity Provider in the OpenID Connect protocol. Then, you configure the client side on both Sysdig Secure and Sysdig Monitor.

Client registration in IBM Cloud Pak for Multicloud Management

This document covers the client registration using *cloudctl* tool. Additional information and other ways of performing this registration are detailed in:
https://www.ibm.com/support/knowledgecenter/SSFC4F_1.3.0/iam/3.4.0/auth_onboard.html

1. Download and install *cloudctl* tool, if not already installed. Download and installation instructions are available here:
   https://www.ibm.com/support/knowledgecenter/SSFC4F_1.3.0/cloudctl/install_cli.html
2. Login to your cluster using the *cloudctl login* command using a user with administrator permissions. You'll be asked for your user and password:
   `cloudctl login -a https://your-cluster-ip-endpoint`
3. Create a *registration.json* following the template described in the onboarding docs. The *registration.json* file should look like:

```
{
  "token_endpoint_auth_method":"client_secret_basic",
  "client_id": "your-client-id",
  "client_secret": "<some-random-secret-string>",
  "scope":"openid profile email",
  "grant_types":[
     "authorization_code",
     "client_credentials",
     "password",
     "implicit",
     "refresh_token",
     "urn:ietf:params:oauth:grant-type:jwt-bearer"
  ],
  "response_types":[
     "code",
     "token",
     "id_token token"
  ],
  "application_type":"web",
  "subject_type":"public",
  "preauthorized_scope":"openid profile email general",
  "introspect_tokens":true,
```

```
  "trusted_uri_prefixes":[ "https://secure.sysdig.com/"],
  "post_logout_redirect_uris":[
     "https://secure.sysdig.com/api/oauth/openid/logout"
   ],
  "redirect_uris":[
    "https://secure.sysdig.com/api/oauth/openid/secureAuth",
    "https://app.sysdigcloud.com/api/oauth/openid/auth"
  ]
}
```

4. In the previous *registration.json* file, choose a *client_id* and generate a random *client_secret*. Adjust the *redirect_uris* and *post_logout_redirect_uris* to contain the OpenID redirect URIs for On-Prem as described in https://docs.sysdig.com/en/openid-connect--on-prem-.html (the example URIs are for SaaS).
    a. For SaaS:

```
"trusted_uri_prefixes":[ "https://secure.sysdig.com/"],
"post_logout_redirect_uris":[
     "https://secure.sysdig.com/api/oauth/openid/logout"
],
"redirect_uris": [
    "https://secure.sysdig.com/api/oauth/openid/secureAuth",
    "https://app.sysdigcloud.com/api/oauth/openid/auth"
]
```

    b. For onPrem, use (replace HOSTNAME by the host name of your Sysdig instance and include the port even if it is the standard 443):

```
"trusted_uri_prefixes":[ "https://HOSTNAME:PORT/"],
"post_logout_redirect_uris":[
     "https://HOSTNAME:PORT/api/oauth/openid/logout"
],
"redirect_uris": [
    "https://HOSTNAME:PORT/api/oauth/openid/secureAuth",
    "https://HOSTNMAME:PORT/api/oauth/openid/auth"
]
```

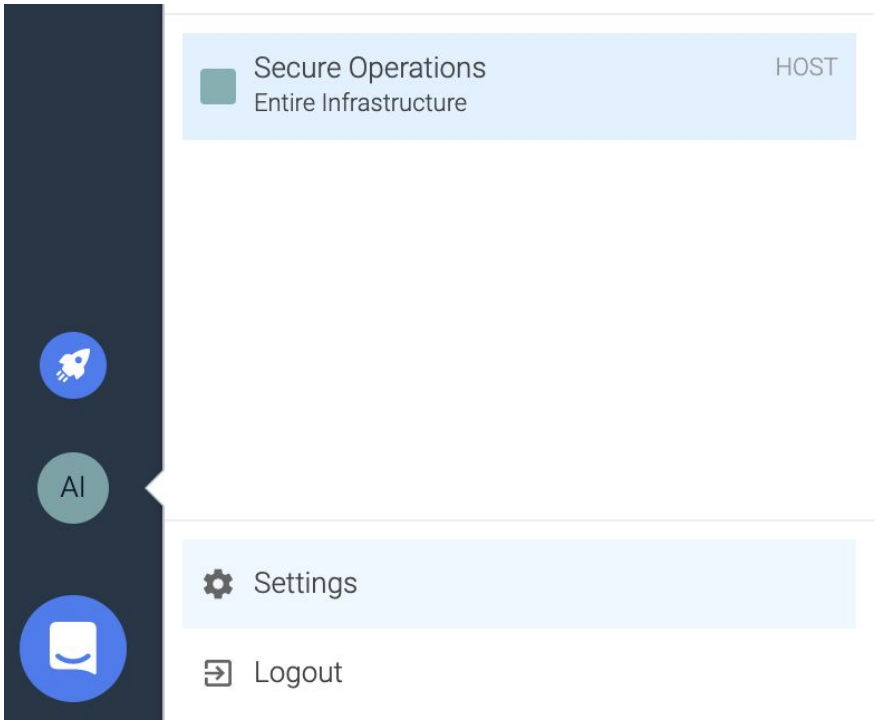
5. Create the client registration using the *cloudtcl iam oauth-client-register* command:

```
 $ cloudctl iam oauth-client-register -f registration.json
OK
client_name:            your-client-id
client_id:              your-client-id
client_secret:          <some-random-secret-string>
```

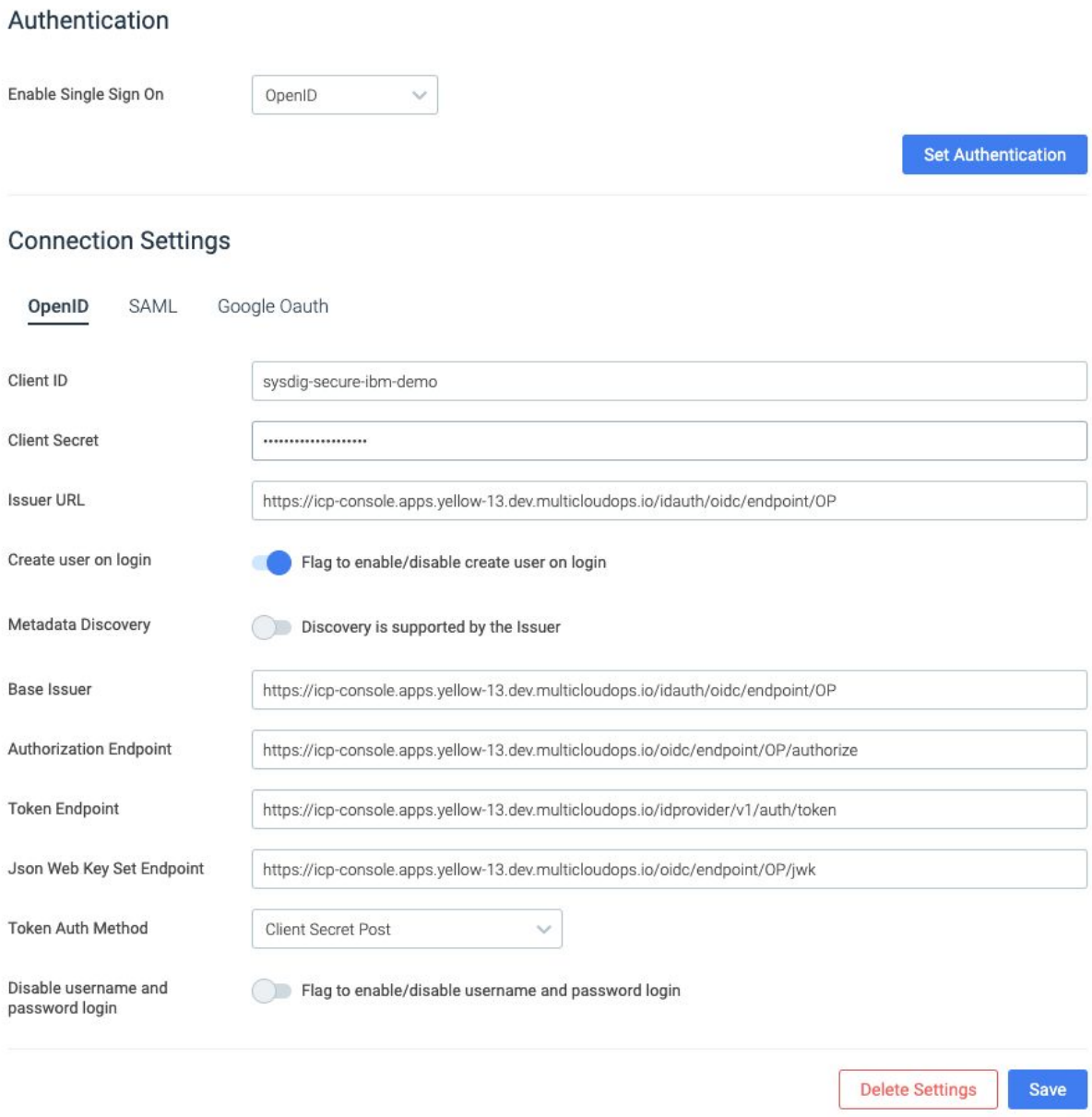
6. Your client is now registered. Keep the *client_secret* string that you used for the registration, as it will be used when configuring the client side in Sysdig Secure and Sysdig Monitor.

OpenID configuration in Sysdig Secure

1. Login to Sysdig Secure using an account with administrator privileges.
2. Go to Account -> *Settings* using the user icon on the bottom left of the screen:



3. Go to the *Authentication* section and choose *OpenID* in connection settings. Let's suppose https://my-mcm-cluster/ is the base URL for your IBM Cloud Pak for Multicloud Management cluster API endpoint. Fill up all the fields with the following values:



- *Client ID*: **your-client-id** (same value as in *registration.json*)

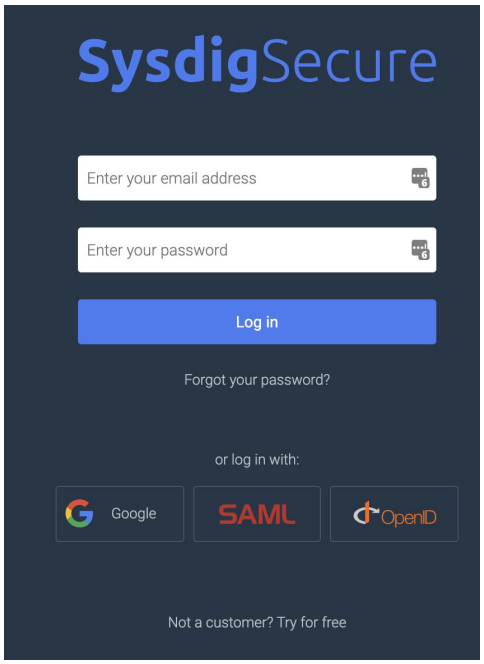
- *Client Secret*: **<some-random-secret-string>** (same value as in *registration.json*)
- Issuer URL: **https://my-mcm-cluster/idauth/oidc/endpoint/OP**
- *Create user on login*: **Enabled** if you want all users in IBM Cloud Pak for Multicloud Management identity provider to be automatically onboarded in Sysdig Secure. Otherwise, **disable** it and manually add users in Sysdig Secure before they are able to login.
- *Metadata Discovery*: **Disabled**
- *Base Issuer*: **https://my-mcm-cluster/idauth/oidc/endpoint/OP**
- *Authorization Endpoint*: **https://my-mcm-cluster/oidc/endpoint/OP/authorize**
- *Token Endpoint*: **https://my-mcm-cluster/idprovider/v1/auth/token**
- *Json Web Key Set Endpoint*: **https://my-mcm-cluster/oidc/endpoint/OP/jwk**
- *Token Auth Method*: **Client Secret Post**

4. ⚠Please note that the prefix for ***Tokend Endpointt*** field differs from the other endpoints (it is /idprovider/v1/auth/).
5. Click *Save* button, and then at the top of the same screen, choose *OpenID* in the *Enable Single Sign On* drop-down, and click the *Set Authentication* button.
6. For SaaS, you'll need to obtain your *company name* ID for your Sysdig Secure account (sales support can provide it to you, in case you don't know it already).

Once this is ready, you should be able to trigger OpenID Connect SSO authentication by using the following URLs:

- On-Prem: https://HOSTNAME/api/oauth/openid?product=SDS
- SaaS: https://secure.sysdig.com/api/oauth/openid/<company name>?product=SDS
- Using the Sysdig Secure link from the Navigation Menu shortcuts in the IBM Cloud Pak for Multicloud Management console.
- Using the *Review event in Sysdig Secure* link from a Sysdig Secure security finding details in the Govern Risk console.

Or by clicking the OpenID button on the login page:



and for SaaS, then enter your *company name* when prompted:

OpenID configuration in Sysdig Monitor

Sysdig Monitor OpenID Single Sign On configuration is exactly the same as configuring Sysdig Secure.

Once the configuration is finished, you should be able to trigger OpenID Connect SSO authentication by using the following URLs:

- On-Prem: https://HOSTNAME/api/oauth/openid
- SaaS: https://app.sysdigcloud.com/api/oauth/openid/<company name>
- Using the Sysdig Monitor link from the Navigation Menu shortcuts in the IBM Cloud Pak for Multicloud Management console.

User onboarding in Sysdig Secure and Sysdig Monitor

Users will get automatically onboarded in Sysdig Secure and Sysdig Monitor the first time they login using Single Sign-On, and added to the *Default* team in the corresponding application on first login.

As *teams* are independent in Sysdig Secure and Sysdig Monitor, a user that logs in first in Sysdig Secure won't belong to any team in Sysdig Monitor, and **login will be denied**. The opposite also applies, so if it first logs in Sysdig Monitor, the user won't be in any Sysdig Secure team.

Login as an administrator user in the corresponding application (Sysdig Secure or Monitor), and navigate to Settings -> Users and add the user to any team in order to allow it to login to the application.

Navigation Menu Shortcuts

The Navigation Menu integration includes direct links from IBM Cloud Pak for Multicloud Management menu to launch Sysdig Secure and Sysdig Monitor.

Requirements

- Kubernetes or Openshift cluster(s) managed by IBM Cloud Pak for Multicloud Management.
- A IBM Cloud Pak for Multicloud Management account with administrator privileges.
- Navigation menu Helm Charts.

Online Installation

1. Download and install Helm (version 3.x preferred)
2. Add the *sysdiglabs* Helm chart repository:

```
helm repo add sysdiglabs https://sysdiglabs.github.io/charts/
```

If you are using **Helm 2** and it is not initialized, you might get an error message like:

```
Error: Couldn't load repositories file ...

You might need to run `helm init` (or `helm init --client-only` if tiller is
already installed)
```

In that case, run the suggested command:

```
helm init --client-only
```

And **repeat step 2 again**. Now it should work.

3. Refresh the repositories cache:

```
helm repo update
```

4. Create the *sysdig-navmenu* namespace:

```
kubectl create ns sysdig-navmenu
```

5. **For Helm 3 or higher (check running "`helm version`").**
    a. For Sysdig SaaS, use the command:

```
helm install -n sysdig-navmenu \
      --set saas=true,companyName=<my-company-name> \
      sysdig-navmenu sysdiglabs/sysdig-mcm-navmenu
```

where **<my-company-name>** is replaced with your company name ID.

    b. For On-Prem, use:

```
helm install -n sysdig-navmenu \
      --set saas=false,sysdigURL=<https://HOSTNAME> \
      sysdig-navmenu sysdiglabs/sysdig-mcm-navmenu
```

where **<https://HOSTNAME>** is replaced with your on-prem installation URL.

6. **For Helm 2 (check running "helm version").**
    a. For Sysdig SaaS, use the command:

```
helm install --namespace sysdig-navmenu \
      --set saas=true,companyName=<my-company-name> \
      -n sysdig-navmenu sysdiglabs/sysdig-mcm-navmenu --tls
```

where **<my-company-name>** is replaced with your company name ID.

b. For On-Prem, use:

```
helm install --namespace sysdig-navmenu \
      --set saas=false,sysdigURL=<https://HOSTNAME> \
      -n sysdig-navmenu sysdiglabs/sysdig-mcm-navmenu --tls
```

where **<https://HOSTNAME>** is replaced with your on-prem installation URL.