Alert Destinations / SIEMs

A service rule that includes an alert destination typically defines how and where notifications or alerts should be sent when certain conditions are met. Service rules monitor specific conditions or events, such as system thresholds being exceeded, errors occurring, or security incidents being detected and when the predefined conditions are met, the service rule triggers an alert. Alerts are sent to web services or applications via webhooks for further processing or automation. This ensures that critical events do not go unnoticed.

Datadog

Once configured, Multicloud Defense alerts will sent to Datadog using the defined Alert Service Profile and Alert Rule.

Create an Alert Profile Service

Before you begin

In order to send alerts to Datadog, the following information is required:

- Datadog account
- API Key

Tip

- To Sign up for a Datadog account, refer to Datadog Account (https://www.datadoghq.com/).
- To create a Datadog API Key, refer to Datadog API Key (https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api).

Procedure

Step 1 Navigate to **System and Accounts** > **Service Alerts** > **Services**.
Step 2 Click **Create**.
Step 3 **Name** - Enter unique name for the alert integration. Example `multicloud defense-Datadog-profile`.
Step 4 **Description** (optional) - Enter a description for the alert integration.
Step 5 **Type** - Using the pulldown, choose **Datadog**.
Step 6 **API Key** - Specify the Datadog API Key used to authenticate the communication.
Step 7 Click **Save**.

What to do next

Create an alert rule with this new profile.

Create an Alert Rule

Before you begin

In order to send alerts to Datadog, the following information is required:

- Datadog account
- API Key

Tip

- To Sign up for a Datadog account, refer to Datadog Account (https://www.datadoghq.com/).
- To create a Datadog API Key, refer to Datadog API Key (https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api).

Procedure

Step 1 Navigate to **System and Accounts** > **Service Alerts** > **Alert Rules**.
Step 2 Click **Create**.
Step 3 **Profile Name** - Enter unique name for the integration. Example `multicloud defense-Datadog-alert-rule`.
Step 4 **Description** (optional) - Enter a description for the alert rule.
Step 5 **Alert Profile** - Using the pulldown, choose a PagerDuty Alert Profile. As example, select profile created above `multicloud defense-Datadog-profile`.
Step 6 (Optional)**Description** - Enter a description for the aler trule.
Step 7 **Alert Profile** - Expand the drop-down menu and select a Microsoft Teams alert profile.
Step 8 **Type** - Expand the drop-down menu and select one of the following types:

- System Logs
- Audit Logs
- Discovery

If you select **Audit Logs**, there are no other configurable items. Click **Save** to finalize the rule.

Step 9 If you select either System Logs or Discovery as your Type, then expand the **Sub Type** drp-down menu and select one of the following options:

- Gateway
- Account
- Controller

Step 10 Expand the **Severity**drop-down menu and select one of the following labels. Note that the options below are dependent on the **Type** you selected in step 7.

- Info
- Warning
- Medium
- High
- Critical

Step 11 **Enabled** - This option is checked by default to enable and implement this alert immediately after saving. Unceck this box if you do not to immediately apply the rule to your environment.

Step 12 Click **Save**.

Microsoft Sentinel

Once configured, Multicloud Defense alerts will sent to Microsoft Sentinel using the defined Alert Service Profile and Alert Rule.

Create an Alert Profile Service

Before you begin

In order to send alerts to Microsoft Sentinel, the following information is required:

- Create an Azure Log Analytics Workspace.
- Define an Azure Log Table.

Procedure

Step 1 Navigate to **System and Accounts** > **Service Alerts** > **Services**.
Step 2 Click **Create**.
Step 3 **Name** - Enter unique name for the alert integration. Example `mcd-mssentinel-profile`.
Step 4 **Description** (optional) - Enter a description for the alert integration.
Step 5 **Type** - Using the pulldown, choose **Microsoft Sentinel**.
Step 6 **API Key** - Specify the Shared Key created in Azure for the Azure Log Analytics Workspace.
Step 7 **Azure Log Table Name** - Specify the name of the Azure Log defined when creating the Azure Log Analytics Workspace.
Step 8 **Azure Log Analytics Workspace ID** - Specify the ID of the Azure Log Analytics Workspace.
Step 9 Click **Save**.

What to do next

Create an alert rule with this new profile.

Create an Alert Rule

Before you begin

In order to send alerts to Microsoft Sentinel, the following information is required:

- Create an Azure Log Analytics Workspace.
- Define an Azure Log Table.

Procedure

Step 1 Navigate to **System and Accounts** > **Service Alerts** > **Alert Rules**.
Step 2 Click **Create**.
Step 3 **Profile Name** - Enter unique name for the integration. Example `mcd-mssentinel-alert-rule`.
Step 4 (Optional)**Description** - Enter a description for the aler trule.
Step 5 **Alert Profile** - Expand the drop-down menu and select a Microsoft Teams alert profile.
Step 6 **Type** - Expand the drop-down menu and select one of the following types:

- System Logs
- Audit Logs
- Discovery

If you select **Audit Logs**, there are no other configurable items. Click **Save** to finalize the rule.

Step 7 If you select either System Logs or Discovery as your Type, then expand the **Sub Type** drp-down menu and select one of the following options:

- Gateway
- Account
- Controller

Step 8 Expand the **Severity**drop-down menu and select one of the following labels. Note that the options below are dependent on the **Type** you selected in step 7.

- Info
- Warning
- Medium
- High
- Critical

Step 9 **Enabled** - This option is checked by default to enable and implement this alert immediately after saving. Unceck this box if you do not to immediately apply the rule to your environment.

Step 10 Click **Save**.

PagerDuty

Once configured, Multicloud Defense alerts will sent to a PagerDuty API gateway using the defined Alert Service Profile and Alert Rule.

Create an Alert Profile Service

Before you begin

In order to complete the steps in this guide, you will need:

- A PagerDuty account with an API Key configured.

Tip

- Sign up for a PagerDuty account (https://www.servicenow.com/my-account/sign-up.html).
- Setup the API Key (https://developer.pagerduty.com/api-reference).

Procedure

Step 1 Navigate to **System and Accounts** > **Service Alerts** > **Services**.

Step 2 Click **Create**.

Step 3 **Name** - Enter unique name for the alert integration. Example `mcd-pagerduty-profile`.

Step 4 **Description** (optional) - Enter a description for the alert integration.

Step 5 **Type** - Using the pulldown, choose **PagerDuty**.

Step 6 **API Key** - Copy the PagerDuty API key generated above, or other PagerDuty API Key as desired.

Step 7 Click **Save**.

What to do next

Create an alert rule with this new profile.

Create an Alert Rule

Before you begin

In order to complete the steps in this guide, you will need:

A PagerDuty account with an API Key configured.

Tip

- Sign up for a PagerDuty account (https://www.servicenow.com/my-account/sign-up.html).
- Setup the API Key (https://developer.pagerduty.com/api-reference).

Procedure

Step 1 Navigate to **System and Accounts** > **Service Alerts** > **Alert Rules**.

Step 2 Click **Create**.

Step 3 **Profile Name** - Enter unique name for the integration. Example `mcd-pagerduty-alert-rule`.

Step 4 **Description** (optional) - Enter a description for the alert rule.

Step 5 (Optional)**Description** - Enter a description for the aler trule.

Step 6 **Alert Profile** - Expand the drop-down menu and select a Microsoft Teams alert profile.

Step 7 **Type** - Expand the drop-down menu and select one of the following types:

- System Logs
- Audit Logs
- Discovery

If you select **Audit Logs**, there are no other configurable items. Click **Save** to finalize the rule.

Step 8 If you select either System Logs or Discovery as your Type, then expand the **Sub Type** drp-down menu and select one of the following options:

- Gateway

- Account
- Controller

Step 9 Expand the **Severity**drop-down menu and select one of the following labels. Note that the options below are dependent on the **Type** you selected in step 7.

- Info
- Warning
- Medium
- High
- Critical

Step 10 **Enabled** - This option is checked by default to enable and implement this alert immediately after saving. Unceck this box if you do not to immediately apply the rule to your environment.

Step 11 Click **Save**.

ServiceNow

Once configured, Multicloud Defense alerts will sent to a ServiceNow API gateway using the defined Alert Service Profile and Alert Rule.

Create an Alert Rule

Before you begin

In order to complete the steps in this guide, you will need:

- A ServiceNow account with an Incoming Webhook URL.
- An API Key configured.

Tip

- Sign up for a ServiceNow account (https://www.servicenow.com/my-account/sign-up.html)
- Setup Webhook and API Key (https://docs.servicenow.com/search?q=setup%20webhook)

Procedure

Step 1 Navigate to **System and Accounts** > **Service Alerts** > **Alert Rules**.

Step 2 Click **Create**.

Step 3 **Profile Name** - Enter unique name for the integration. Example `mcd-servicenow-alert-rule`.

Step 4 (Optional)**Description** - Enter a description for the aler trule.

Step 5 **Alert Profile** - Expand the drop-down menu and select a Microsoft Teams alert profile.

Step 6 **Type** - Expand the drop-down menu and select one of the following types:

- System Logs
- Audit Logs
- Discovery

If you select **Audit Logs**, there are no other configurable items. Click **Save** to finalize the rule.

Step 7 If you select either System Logs or Discovery as your Type, then expand the **Sub Type** drp-down menu and select one of the following options:

- Gateway
- Account
- Controller

Step 8 Expand the **Severity**drop-down menu and select one of the following labels. Note that the options below are dependent on the **Type** you selected in step 7.

- Info
- Warning
- Medium
- High
- Critical

Step 9 **Enabled** - This option is checked by default to enable and implement this alert immediately after saving. Unceck this box if you do not to immediately apply the rule to your environment.

Step 10 Click **Save**.

Create an Alert Profile Service

Before you begin

In order to complete the steps in this guide, you will need:

- A ServiceNow account with an Incoming Webhook URL.
- API Key configured.

Tip

- Sign up for a ServiceNow account (https://www.servicenow.com/my-account/sign-up.html)
- Setup Webhook and API Key (https://docs.servicenow.com/search?q=setup%20webhook)

Procedure

Step 1 Navigate to **System and Accounts** > **Service Alerts** > **Services**.
Step 2 Click **Create**.
Step 3 **Name** - Enter unique name for the alert integration. Example `mcd-servicenow-profile`.
Step 4 **Description** (optional) - Enter a description for the alert integration.
Step 5 **Type** - Using the pulldown, choose **ServiceNow**.
Step 6 **API Key** - Specify the ServiceNow API key generated above, or other ServiceNow API Key as desired.
Step 7 **API URL** - Specify the ServiceNow Webhook URL generated above, or other ServiceNow Webhook URL as desired.
Step 8 Click **Save**.

What to do next

Create an alert rule with this new profile.

Slack

Once configured, Multicloud Defense alerts will sent to a Slack Incoming Webhook URL using the defined Alert Service Profile and Rule.

Create a Slack Alert Rule

Before you begin

You must create a Slack alert profile before you create an alert rule.

Procedure

Step 1 Navigate to **System and Accounts** > **Service Alerts** > **Alert Rules**.
Step 2 Click **Create**.
Step 3 **Profile Name** - Enter unique name for the integration. Example `mcd-slack-alert-rule`.
Step 4 (Optional)**Description** - Enter a description for the aler trule.
Step 5 **Alert Profile** - Expand the drop-down menu and select a Microsoft Teams alert profile.
Step 6 **Type** - Expand the drop-down menu and select one of the following types:

- System Logs
- Audit Logs
- Discovery

If you select **Audit Logs**, there are no other configurable items. Click **Save** to finalize the rule.

Step 7 If you select either System Logs or Discovery as your Type, then expand the **Sub Type** drp-down menu and select one of the following options:

- Gateway
- Account
- Controller

Step 8 Expand the **Severity**drop-down menu and select one of the following labels. Note that the options below are dependent on the **Type** you selected in step 7.

- Info
- Warning
- Medium
- High
- Critical

Step 9 **Enabled** - This option is checked by default to enable and implement this alert immediately after saving. Unceck this box if you do not to immediately apply the rule to your environment.

Step 10 Click **Save**.

Create an Alert Profile Service

Before you begin

In order to complete the steps in this guide, you will need:

- A Slack account with an incoming webhook URL configured.

Tip

1. Create a Slack account (https://slack.com/get-started#/create).
2. Create an incoming Webhook (https://slack.com/help/articles/115005265063-Incoming-webhooks-for-Slack#set-up-incoming-webhooks).

Procedure

Step 1 Navigate to **System and Accounts** > **Service Alerts** > **Services**.

Step 2 Click **Create**.

Step 3 **Name** - Enter unique name for the alert integration. Example `mcd-slack-profile`.

Step 4 **Description** (optional) - Enter a description for the alert integration.

Step 5 **Type** - Using the pulldown, choose **Slack**.

Step 6 **API URL** - Specify the Slack Webhook URL generated above, or other Slack Webhook URL as desired.

What to do next

Create an alert rule with this new profile.

Microsoft Teams

Create an alert profile and then use that profile in a service alert rule to generate alerts specifically for Microsoft Teams using a uique incoming webhook from the service.

Create a Microsoft Teams Alert Profile Service

Before you begin

You must do the following items before you finalize the alert profile for your Microsoft account:

- You **must** create an Incoming Webhook in the Microsoft Teams UI. See Microsoft documentation for more information.
- You **must** save the unique API URL generated from creating an incoming webhook for the procedure below.

Procedure

Step 1 Navigate to **System and Accounts** > **Service Alerts** > **Services**.

Step 2 Click **Create**.

Step 3 **Name** - Enter unique name for the alert integration.

Step 4 (Optional) **Description** - Enter a description for the alert integration.

Step 5 **Type** - Using the pulldown, choose **Microsoft Teams**.

Step 6 **API URL** - Enter the API URL that is generated from creating an incoming webhook. Copy the URL from your Microsoft Teams UI and paste it in this text field.

Step 7 Click **Save**.

What to do next

Create an alert rule with this new profile.

Create a Microsoft Teams Service Rule

Before you begin

You must create a Microsoft Teams service profile before you create a service rule.

Procedure

Step 1 Navigate to **System and Accounts** > **Service Alerts** > **Alert Rules**.

Step 2 Click **Create**.

Step 3 **Profile Name** - Enter unique name for the integration. An example would be similar to `mcd-microsoft-alert-rule`.

Step 4 (Optional)**Description** - Enter a description for the aler trule.

Step 5 **Alert Profile** - Expand the drop-down menu and select a Microsoft Teams alert profile.

Step 6 **Type** - Expand the drop-down menu and select one of the following types:

- System Logs
- Audit Logs
- Discovery

If you select **Audit Logs**, there are no other configurable items. Click **Save** to finalize the rule.

Step 7 If you select either System Logs or Discovery as your Type, then expand the **Sub Type** drp-down menu and select one of the following options:

- Gateway
- Account
- Controller

Step 8 Expand the **Severity**drop-down menu and select one of the following labels. Note that the options below are dependent on the **Type** you selected in step 7.

- Info
- Warning
- Medium
- High
- Critical

Step 9 **Enabled** - This option is checked by default to enable and implement this alert immediately after saving. Unceck this box if you do not to immediately apply the rule to your environment.

Step 10 Click **Save**.

Webex

Once configured, Multicloud Defense alerts will sent to a Webex API gateway using the defined Alert Service Profile and Alert Rule.

Create an Alert Profile Service

Use the following procedure to create an alert profile for the Webex service:

Before you begin

In order to complete the steps in this guide, you will need:

- A Webex account with an Incoming Webhook URL.
- API Key configured.

Note

1. Create or access a Webex account.
2. Create a Webex Incoming Webhook.
3. Accept the Incoming Webhook permissions.
4. Provide a Name and select a Webex Space.
5. Copy the Webex Webhook URL to use in the configuration of the Alert Service Profile.

Procedure

Step 1 Navigate to **System and Accounts** > **Service Alerts** > **Services**.

Step 2 Click **Create**.

Step 3 **Name** - Enter unique name for the alert integration.

Step 4 (Optional) **Description** - Enter a description for the alert integration.

Step 5 **Type** - Using the pulldown, choose **Webex**.

Step 6 **API URL** - Specify the Webex Webhook URL generated as part of the prerequisites, or other Webex Webhook URL as desired.

Step 7 Click **Save**.

What to do next

Create an alert rule with this new profile.

Create an Alert Rule

Procedure

Step 1 Navigate to **System and Accounts** > **Service Alerts** > **Alert Rules**.

Step 2 Click **Create**.

Step 3 **Profile Name** - Enter unique name for the integration. An example is `mcd-servicenow-alert-rule`.

Step 4 (Optional)**Description** - Enter a description for the aler trule.

Step 5 **Alert Profile** - Expand the drop-down menu and select a Microsoft Teams alert profile.

Step 6 **Type** - Expand the drop-down menu and select one of the following types:

- System Logs
- Audit Logs
- Discovery

If you select **Audit Logs**, there are no other configurable items. Click **Save** to finalize the rule.

Step 7 If you select either System Logs or Discovery as your Type, then expand the **Sub Type** drp-down menu and select one of the following options:

- Gateway
- Account
- Controller

Step 8 Expand the **Severity**drop-down menu and select one of the following labels. Note that the options below are dependent on the **Type** you selected in step 7.

- Info
- Warning
- Medium
- High
- Critical

Step 9 **Enabled** - This option is checked by default to enable and implement this alert immediately after saving. Unceck this box if you do not to immediately apply the rule to your environment.

Step 10 Click **Save**.

Splunk

Once configured, Multicloud Defense alerts will sent to an API gateway using the defined Alert Service Profile and Alert Rule.

Create a Splunk Profile Service

Use the following procedure to create an alert profile for the Splunk service:

Before you begin

You must have the following configured and ready:

- Create an API Key in Multicloud Defense and store both the key and secret. See Create an API Key in Multicloud Defense for more information.
- Set up the HTTP Event Collector (HEC) in Splunk Web. See Configure HTTP Event Collector on Splunk Cloud for more information.
- Your Splunk HEC must have the following configured:
  - HEC must be **enabled**.
  - You must have at least one active HEC token available.
  - You must use an active token to authenticate into HEC.
  - You must format the data that goes to HEC in a certain way. See Format events for HTTP Event Collector.

Procedure

Step 1 Navigate to **System and Accounts** > **Service Alerts** > **Services**.

Step 2 Click **Create**.

Step 3 **Name** - Enter unique name for the alert integration.

Step 4 **Description** (optional) - Enter a description for the alert integration.

Step 5 **Type** - Using the pulldown, choose **Splunk**.

Step 6 **API Key** - Copy the Splunk API key generated above, or other PagerDuty API Key as desired.

Step 7 Check the **Skip Verify Certificate** box if your server doesnt have certificates with SAN field matching with domain. If you server does have ceritficats with SAN fields matching the domain, leave this unchecked.

Step 8 **Index(default - main)** is Splunk's default index where all the processed data is stored. This is provided when you configure the Splunk HEC.

Step 9 Enter the **API URL** for the Splunk HTTP Event Collector. We recommend this URL `https://<host>:<port>/services/collector .`

Step 10 Click **Save**.

What to do next

Create an alert rule with this new profile.

Create a Splunk Rule

Use the following procedure to create a rule containing the splunk alert service:

Procedure

Step 1 Navigate to **System and Accounts** > **Service Alerts** > **Alert Rules**.

Step 2 Click **Create**.

Step 3 **Profile Name** - Enter unique name for the integration. Example `mcd-mssentinel-alert-rule`.

Step 4 (Optional)**Description** - Enter a description for the aler trule.

Step 5 **Alert Profile** - Expand the drop-down menu and select a Microsoft Teams alert profile.

Step 6 **Type** - Expand the drop-down menu and select one of the following types:

- System Logs
- Audit Logs
- Discovery

If you select **Audit Logs**, there are no other configurable items. Click **Save** to finalize the rule.

Step 7 If you select either System Logs or Discovery as your Type, then expand the **Sub Type** drp-down menu and select one of the following options:

- Gateway
- Account
- Controller

Step 8 Expand the **Severity**drop-down menu and select one of the following labels. Note that the options below are dependent on the **Type** you selected in step 7.

- Info
- Warning
- Medium
- High
- Critical

Step 9 **Enabled** - This option is checked by default to enable and implement this alert immediately after saving. Unceck this box if you do not to immediately apply the rule to your environment.

Step 10 Click **Save**.