警报目标/SIEM

Datadog 集成

配置后， 多云防御 警报将使用定义的警报服务配置文件和警报规则发送到 Datadog。

创建警报配置文件服务

Before you begin

要将警报发送到 Datadog，需要以下信息：

- Datadog 账户
- API 密钥

Tip

- 要注册 Datadog 账户，请参阅 Datadog 账户 (https://www.datadoghq.com/)。
- 要创建 Datadog API 密钥，请参阅 Datadog API 密钥 (https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api)。

步骤 1 导航到 **管理** > **警报配置文件** > **服务**。

步骤 2 点击**创建 (Create)**。

步骤 3 **名称** - 输入警报集成的唯一名称。示例 `多云防御-Datadog-profile`。

步骤 4 **说明** （可选）-输入此警报集成的说明。

步骤 5 **类型** - 使用下拉列表，选择 **Datadog**。

步骤 6 **API 密钥** - 指定用于对通信进行身份验证的 Datadog API 密钥。

步骤 7 点击**保存**。

What to do next

使用此新配置文件创建警报规则。

创建警报规则

Before you begin

要将警报发送到 Datadog，需要以下信息：

- Datadog 账户
- API 密钥

Tip

- 要注册 Datadog 账户，请参阅 Datadog 账户 (https://www.datadoghq.com/)。
- 要创建 Datadog API 密钥，请参阅 Datadog API 密钥 (https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api)。

步骤 1 导航到 **设置** > **警报配置文件** > **警报规则**。

步骤 2 点击**创建 (Create)**。

步骤 3 **配置文件名称** - 输入集成的唯一名称。示例 `多云防御-Datadog-alert-rule`。

步骤 4 **说明** （可选）-输入此警报的说明。

步骤 5 **警报配置文件** - 使用下拉列表，选择 PagerDuty 警报配置文件。例如，选择上面创建 `多云防御的配置文件-Datadog-profile`。

步骤 6 **类型** - 使用下拉列表，选择 **系统日志** 或 **发现**。

步骤 7 **子类型** - 对于类型 **系统日志**，子类型下拉列表选项为： **网关** 或 **账户**。对于类型 **发现**，子类型下拉列表选项为：**见解规则**。

步骤 8 **严重性** - 对于选定的类型 **系统日志**，并使用下拉列表从以下选项中选择严重性级别： `信息警告中高` 或 `严重`。对于类型 **发现**，请从以下选项中选择严重性级别： `信息中级严重`。

步骤 9 **已启用** - 使用此复选框，选中可启用此警报配置文件。

步骤 10 点击**保存 (Save)**。

Microsoft Sentinel 集成

配置后， 多云防御 警报将使用定义的警报服务配置文件和警报规则发送到 Microsoft Sentinel。

创建警报配置文件服务

Before you begin

要将警报发送到 Microsoft Sentinel，需要以下信息：

- 创建 Azure 日志分析工作空间。
- 定义 Azure 日志表。

步骤 1 导航到 **管理** > **警报配置文件** > **服务**。
步骤 2 点击**创建 (Create)**。
步骤 3 **名称** - 输入警报集成的唯一名称。示例 `mcd-mssentinel-profile`。
步骤 4 **说明** （可选）-输入此警报集成的说明。
步骤 5 **类型** - 使用下拉列表，选择 **Microsoft Sentinel**。
步骤 6 **API 密钥** - 指定在 Azure 中为 Azure 日志分析工作空间创建的共享密钥。
步骤 7 **Azure 日志表名称** - 指定创建 Azure 日志分析工作空间时定义的 Azure 日志的名称。
步骤 8 **Azure 日志分析工作空间 ID** - 指定 Azure 日志分析工作空间的 ID。
步骤 9 点击**保存**。

What to do next

使用此新配置文件创建警报规则。

创建警报规则

Before you begin

要将警报发送到 Microsoft Sentinel，需要以下信息：

- 创建 Azure 日志分析工作空间。
- 定义 Azure 日志表。

步骤 1 导航到 **设置** > **警报配置文件** > **警报规则**。
步骤 2 点击**创建 (Create)**。

步骤 3 **配置文件名称** - 输入集成的唯一名称。示例 `mcd-mssentinel-alert-rule`。

步骤 4 **说明** （可选）-输入此警报的说明。

步骤 5 **警报配置文件** - 使用下拉列表，选择 PagerDuty 警报配置文件。例如，选择上面创建的配置文件 `mcd-mssentinel-profile`。

步骤 6 **类型** - 使用下拉列表，选择 **系统日志** 或 **发现**。

步骤 7 **子类型** - 对于类型 **系统日志**，子类型下拉列表选项为： **网关** 或 **账户**。对于类型 **发现**，子类型下拉列表选项为： **见解规则**。

步骤 8 **严重性** - 对于选定的类型 **系统日志**，并使用下拉列表从以下选项中选择严重性级别： 信息警告中高 或 严重。对于类型 **发现**，请从以下选项中选择严重性级别： 信息中级严重。

步骤 9 **已启用** - 使用此复选框，选中可启用此警报配置文件。

步骤 10 点击**保存 (Save)**。

PagerDuty 集成

配置后， 多云防御 警报将使用定义的警报服务配置文件和警报规则发送到 PagerDuty API 网关。

创建警报配置文件服务

Before you begin

为了完成本指南中的步骤，您需要：

- 配置了 API 密钥的 PagerDuty 账户。

Tip

- 注册 PagerDuty 账户 (https://www.servicenow.com/my-account/sign-up.html)。
- 设置 API 密钥 (https://developer.pagerduty.com/api-reference)。

步骤 1 导航到 **管理** > **警报配置文件** > **服务**。

步骤 2 点击**创建 (Create)**。

步骤 3 **名称** - 输入警报集成的唯一名称。示例 `mcd-pagerduty-profile`。

步骤 4 **说明** （可选）-输入此警报集成的说明。

步骤 5 **类型** - 使用下拉列表，选择 **PagerDuty**。

步骤 6 **API 密钥** - 复制上面生成的 PagerDuty API 密钥，或根据需要复制其他 PagerDuty API 密钥。

步骤 7 点击**保存**。

What to do next

使用此新配置文件创建警报规则。

创建警报规则

Before you begin

为了完成本指南中的步骤，您需要：

配置了 API 密钥的 PagerDuty 账户。

Tip

- 注册 PagerDuty 账户 (https://www.servicenow.com/my-account/sign-up.html)。
- 设置 API 密钥 (https://developer.pagerduty.com/api-reference)。

步骤 1 导航到 **管理警报配置文件警报规则**。

步骤 2 点击**创建 (Create)**。

步骤 3 **配置文件名称** - 输入集成的唯一名称。示例 `mcd-pagerduty-alert-rule`。

步骤 4 **说明** （可选）-输入此警报的说明。

步骤 5 **警报配置文件** - 使用下拉列表，选择 PagerDuty 警报配置文件。例如，选择上面创建的配置文件 `mcd-pagerduty-profile`。

步骤 6 **类型** - 使用下拉列表，选择 **系统日志** 或 **发现**。

步骤 7 **子类型** - 对于类型 **系统日志**，子类型下拉列表选项为： **网关** 或 **账户**。对于类型 **发现**，子类型下拉列表选项为：**见解规则**。

步骤 8 **严重性** - 对于选定的类型 **系统日志**，并使用下拉列表从以下选项中选择严重性级别： 信息警告中高或严重。对于类型 **发现**，请从以下选项中选择严重性级别： 信息中级严重。

步骤 9 **已启用** - 使用此复选框，选中可启用此警报配置文件。

步骤 10 点击**保存 (Save)**。

ServiceNow 集成

配置后， 多云防御 警报将使用定义的警报服务配置文件和警报规则发送到 ServiceNow API 网关。

创建警报配置文件服务

Before you begin

为了完成本指南中的步骤，您需要：

- 具有传入 Webhook URL 的 ServiceNow 账户。
- 已配置 API 密钥。

Tip

- 注册 ServiceNow 账户 (https://www.servicenow.com/my-account/sign-up.html)
- 设置 Webhook 和 API 密钥 (https://docs.servicenow.com/search?q=setup%20webhook)

步骤 1 导航到 **管理** > **警报配置文件** > **服务**。
步骤 2 点击**创建 (Create)**。
步骤 3 **名称** - 输入警报集成的唯一名称。示例 `mcd-servicenow-profile`。
步骤 4 **说明** （可选）-输入此警报集成的说明。
步骤 5 **类型** - 使用下拉列表，选择 **ServiceNow**。
步骤 6 **API 密钥** - 指定上面生成的 ServiceNow API 密钥，或根据需要指定其他 ServiceNow API 密钥。
步骤 7 **API URL** - 指定上面生成的 ServiceNow Webhook URL，或根据需要指定其他 ServiceNow Webhook URL。
步骤 8 点击**保存**。

What to do next

使用此新配置文件创建警报规则。

创建警报规则

Before you begin

为了完成本指南中的步骤，您需要：

- 具有传入 Webhook URL 的 ServiceNow 账户。
- 已配置的 API 密钥。

Tip

- 注册 ServiceNow 账户 (https://www.servicenow.com/my-account/sign-up.html)
- 设置 Webhook 和 API 密钥 (https://docs.servicenow.com/search?q=setup%20webhook)

步骤 1 导航到 **管理** > **警报配置文件** > **警报规则**。
步骤 2 点击**创建 (Create)**。
步骤 3 **配置文件名称** - 输入集成的唯一名称。示例 `mcd-servicenow-alert-rule`。

步骤 4 **说明** （可选）-输入此警报的说明。

步骤 5 **警报配置文件** - 使用下拉列表，选择 ServiceNow 警报配置文件。例如，选择上面创建的配置文件 `mcd-servicenow-profile`。

步骤 6 **类型** - 使用下拉列表，选择 **系统日志** 或 **发现**。

步骤 7 选择 **子类型**。

- 对于类型 **系统日志**，选项为 **网关** 或 **账户**。
- 对于类型 **发现**，唯一的选项是 **见解规则**。

步骤 8 选择 **严重性**。

- 对于选定的类型 **系统日志**，并使用下拉列表从以下选项中选择严重性级别： **信息警告中高或严重**。
- 对于类型 **发现**，选择 **信息中关键**。

步骤 9 **已启用** - 使用此复选框，选中可启用此警报配置文件。

步骤 10 点击**保存 (Save)**。

Slack 集成

配置后， 多云防御 警报将使用定义的警报服务配置文件和规则发送到 Slack 传入 Webhook URL。

创建警报配置文件服务

Before you begin

为了完成本指南中的步骤，您需要：

- 配置了传入 Webhook URL 的 Slack 账户。

Tip

1. 创建 Slack 账户 (https://slack.com/get-started#/create)。
2. 创建传入 Webhook (https://slack.com/help/articles/115005265063-Incoming-webhooks-for-Slack#set-up-incoming-webhooks)。

步骤 1 导航到 **管理** > **警报配置文件** > **服务**。

步骤 2 点击**创建 (Create)**。

步骤 3 **名称** - 输入警报集成的唯一名称。示例 `mcd-slack-profile`。

步骤 4 **说明** （可选）-输入此警报集成的说明。

步骤 5 类型 - 使用下拉列表，选择 **Slack**。

步骤 6 **API URL** - 指定上面生成的 Slack Webhook URL，或根据需要指定其他 Slack Webhook URL。

What to do next

使用此新配置文件创建警报规则。

创建警报规则

Before you begin

为了完成本指南中的步骤，您需要：

配置了传入 Webhook URL 的 Slack 账户。

Tip

1. 创建 Slack 账户 (https://slack.com/get-started#/create)。
2. 创建传入 Webhook (https://slack.com/help/articles/115005265063-Incoming-webhooks-for-Slack#set-up-incoming-webhooks)。

步骤 1 导航到 **管理** > **警报配置文件** > **警报规则**。

步骤 2 点击**创建 (Create)**。

步骤 3 **配置文件名称** - 输入集成的唯一名称。示例 `mcd-slack-alert-rule`。

步骤 4 **说明** （可选）-输入此警报的说明。

步骤 5 **警报配置文件** - 使用下拉列表，选择 Slack 警报配置文件。例如，选择上面创建的配置文件 `mcd-slack-profile`。

步骤 6 **类型** - 使用下拉列表，选择 **系统日志** 或 **发现**。

步骤 7 **子类型** - 对于类型 **系统日志**，子类型下拉列表选项为： **网关** 或 **账户**。对于类型 **发现**，子类型下拉列表选项为：**见解规则**。

步骤 8 **严重性** - 对于选定的类型 **系统日志**，并使用下拉列表从以下选项中选择严重性级别： 信息警告中高或严重。对于类型 **发现**，请从以下选项中选择严重性级别： 信息中级严重。

步骤 9 **已启用** - 使用此复选框，选中可启用此警报配置文件。

步骤 10 点击**保存 (Save)**。

Webex 集成

配置后， 多云防御 警报将使用定义的警报服务配置文件和警报规则发送到 Webex API 网关。

创建警报配置文件服务

开始之前

为了完成本指南中的步骤，您需要：

- 具有传入 Webhook URL 的 Webex 帐户。
- 已配置 API 密钥。

注释

1. 创建或访问 Webex 帐户。
2. 创建 Webex 传入 Webhook。
3. 接受传入 Webhook 权限。
4. 提供名称并选择 Webex Space。
5. 复制要在警报服务配置文件配置中使用的 Webex Webhook URL。

步骤 1 导航到 **管理** > **警报配置文件** > **服务**。

步骤 2 点击**创建 (Create)**。

步骤 3 **名称** - 输入警报集成的唯一名称。例如， `mcd-servicenow-profile`。

步骤 4 （可选） **说明** - 输入警报集成的说明。

步骤 5 **键入** - 使用下拉列表，选择 **Webex**。

步骤 6 **API URL** - 指定作为必备条件生成的 Webex Webhook URL，或根据需要指定其他 Webex Webhook URL。

下一步做什么

使用此新配置文件创建警报规则。

创建警报规则

步骤 1 导航到 **管理** > **警报配置文件** > **警报规则**。

步骤 2 点击**创建 (Create)**。

步骤 3 **配置文件名称** - 输入集成的唯一名称。例如， `mcd-servicenow-alert-rule`。

步骤 4 （可选） **说明** -输入此警报规则的说明。

步骤 5 **警报配置文件** - 使用下拉列表，选择 **Webex 警报配置文件**。例如，选择上面创建的配置文件 mcd-servicenow-profile。

步骤 6 **类型** - 使用下拉列表，选择 **系统日志** 或 **发现**。

步骤 7 选择 **子类型**。

- 对于类型系统日志，选项包括 **网关** 或 **账户**。
- 对于类型发现，唯一的选项是 **见解规则**。

步骤 8 选择 **严重性**。

- 对于选定的类型系统日志，并使用下拉列表选择 **信息警告中高** 或 **严重**。
- 对于类型发现，选择 **信息中关键**。

步骤 9 **已启用** - 使用此复选框，选中可启用此警报配置文件。

步骤 10 点击**保存 (Save)**。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。