

安全监控模板部署文档

目录

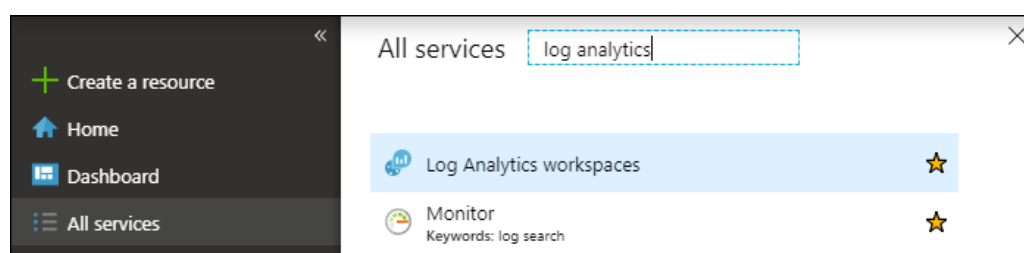
一．连接数据源.....	2
1. 部署 Log Analytics 工作区.....	2
2. 连接数据源到 Log Analytics 工作区	3
二．部署安全规则和工作流.....	8
1. 部署自动化账户.....	8
2. 部署安全规则模板	11
3. 部署安全规则工作流模板	12
4. 设置告警邮件工作流.....	13
5. 验证安全规则执行工作流	18
6. 使用模板分析查询结果	20
三．管理安全规则	21
1. 如何导出当前部署的安全规则	21
2. 如何修改当前部署的安全规则	22
3. 如何添加新的安全规则	26
4. 如何从 query pack 中删除安全规则	28
四．部署工作簿模板和共享仪表盘模板	29
1. 部署仪表盘模板.....	29
2. 部署工作簿模板.....	31
五．使用工作簿和仪表盘.....	35
1. 使用共享仪表盘.....	35
2. 使用工作簿.....	37
3. 使用导入的查询.....	38
六．配置安全中心告警的自动响应	40
1. 部署 Logic App	40
2. 设置安全中心工作流自动化.....	44
3. 验证工作流自动化.....	45

一 . 连接数据源

1. 部署 Log Analytics 工作区

如果之前没有部署过 Log Analytics 工作区，请在相关订阅中启用 Log Analytics 工作区。如果有现有的工作区，请忽略以下的步骤。

- 1) 在 Azure 门户中，单击“所有服务”。在资源列表中，键入“Log Analytics”。开始键入时，会根据输入筛选该列表。选择“Log Analytics 工作区”。



- 2) 单击“添加”，然后为以下各项选择选项：
 - a) 为新的 Log Analytics 工作区提供名称，如 DefaultLAWorkspace。此名称在所有 Azure Monitor 订阅中必须是全局唯一的。
 - b) 如果选择的默认值不合适，请从下拉列表中选择要链接到的 订阅。
 - c) 对于 资源组，选择要使用已设置的现有资源组，还是要创建一个新资源组。
 - d) 选择可用 位置。有关详细信息，请参阅可在哪些区域中使用 Log Analytics，并在“搜索产品”字段中搜索 Azure Monitor。
 - e) 如果在 2018 年 4 月 2 日后创建的新订阅中创建工作区，则它将自动使用“每 GB”定价计划，并且不提供用于选择定价层的选项。如果是为 4 月 2 日之前创建的现有订阅创建工作区，或者是为绑定到现有企业协议 (EA) 注册的订阅创建工作区，则可以选择首选定价层。有关特定层的详细信息，请参阅 Log Analytics 定价详细信息。

Dashboard > Log Analytics workspaces > Log Ar

Log Analytics workspace

Create new or link existing workspace

☒ Create New ☐ Link Existing

* Log Analytics Workspace ⓘ

ContosoWorkspace ✓

* Subscription

Standard Pay-in-Advance Offer ▼

* Resource group

(New) Contoso ▼

[Create new](#)

* Location

China East 2 ▼

* Pricing tier

Per GB (2018) >

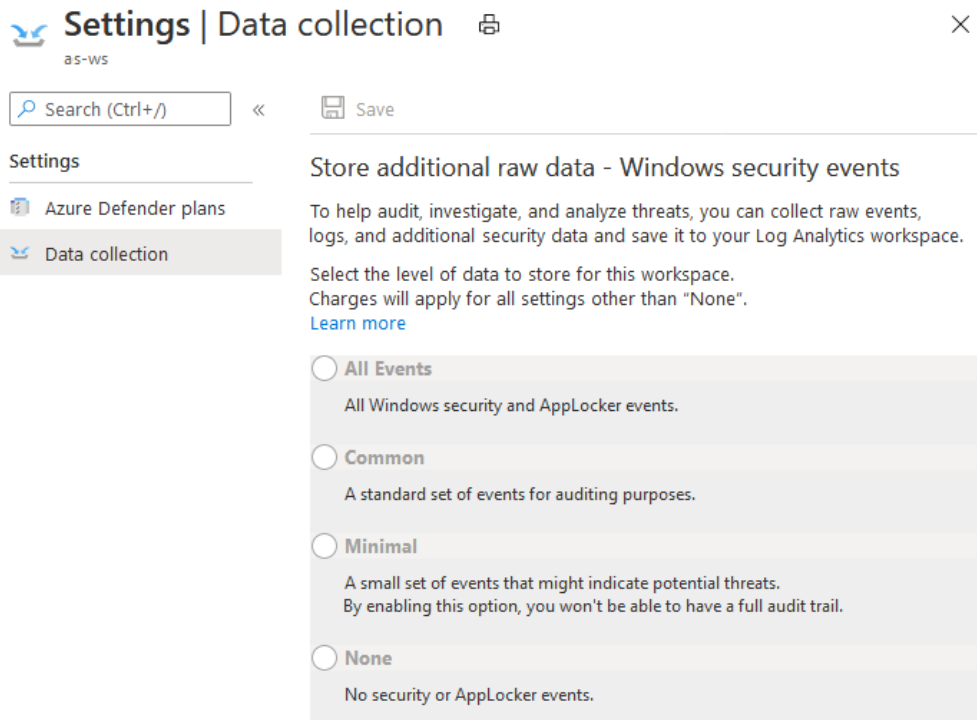
3) 在“Log Analytics 工作区”窗格上提供所需信息后，单击“确定”。

在验证信息和创建工作区时，可以在菜单中的“通知”下面跟踪操作进度。

2. 连接数据源到 Log Analytics 工作区

1.1 如果需要监控 Windows 安全日志，请完成以下的部署。否则，可以忽略此步骤。

- 1) 在 Azure 门户中，选择左上角的“所有服务”。在资源列表中，键入“Log Analytics”。开始键入时，会根据输入筛选该列表。选择“Log Analytics 工作区”。
- 2) 在 Log Analytics 工作区列表中，选择需要连接的 Log Analytics Workspace。
- 3) 在左侧菜单上的“工作区数据源”下，选择“虚拟机”。
- 4) 在“虚拟机”列表中，选择要在其中安装代理的 Windows 虚拟机。请注意，VM 的“Log Analytics 连接状态”指示其“未连接”。
- 5) 在虚拟机的详细信息中，选择“连接”。则会自动会为 Log Analytics 工作区安装并配置代理。此过程需要几分钟的时间，在此期间，“状态”显示“正在连接”。
- 6) 安装并连接代理后，会使用“此工作区”更新“Log Analytics 连接状态”。
- 7) 在 Azure 门户的“安全中心”菜单中，选择“定价和设置”。
- 8) 选择相关工作区。工作区的唯一数据收集事件是此页上描述的 Windows 安全事件。



Tips: 建议选择 minimal 或者 Common。具体涉及的安全日志列表可以参考:

<https://docs.azure.cn/zh-cn/security-center/security-center-enable-data-collection#what-event-types-are-stored-for-common-and-minimal>

9) 选择要存储的原始事件数据量，然后选择“保存”。

1.2 如果需要监控 Linux 的安全日志，请完成以下的部署。否则，可以忽略此步骤。

- 1) 在 Azure 门户中，选择左上角的“所有服务”。在资源列表中，键入“Log Analytics”。开始键入时，会根据输入筛选该列表。选择“Log Analytics 工作区”。
- 2) 在 Log Analytics 工作区列表中，选择需要连接的 Log Analytics Workspace。
- 3) 在左侧菜单上的“工作区数据源”下，选择“虚拟机”。
- 4) 在“虚拟机”列表中，选择要在其中安装代理的 Linux 虚拟机。请注意，VM 的“Log Analytics 连接状态”指示其“未连接”。
- 5) 在虚拟机的详细信息中，选择“连接”。则会自动为 Log Analytics 工作区安装并配置代理。此过程需要几分钟的时间，在此期间，“状态”显示“正在连接”。
- 6) 安装并连接代理后，会使用“此工作区”更新“Log Analytics 连接状态”。
- 7) 通过 Log Analytics 工作区的“高级设置”中的“数据”菜单，为 Log Analytics 工作区配置 Syslog。此配置将传递到每个 Linux 代理上的配置文件。
- 8) 可以通过以下方法添加新设施：首先选择选项“将下列配置应用到我的计算机”，然后输入其名称并单击“+”。对于每个设施，将仅收集具有所选严重级别的消息。检查要收集的特定设施的严重级别。不能向筛选消息提供任何其他条件。监测 Linux 安全日志需要配置 auth 和 authpriv facility 的收集。例如：

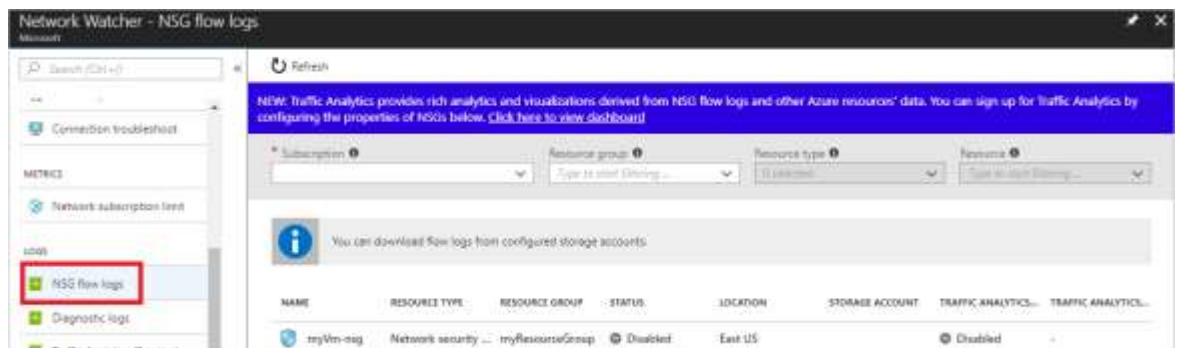
Collect syslogs from the following facilities ☒ Apply below configuration to my machines

Enter the name of a facility to monitor

FACILITY NAME	EMERGENCY	ALERT	CRITICAL	ERROR	WARNING	NOTICE	INFO	DEBUG	
auth	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Remove
authpriv	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Remove

1.3 如果需要收集 NSG flow 日志，请完成以下的部署。否则，可以忽略此步骤。

- 1) 在门户中，选择“所有服务”。在“筛选器”框中，输入“网络观察程序”。结果中出现“网络观察程序”后，将其选中。
- 2) 在“日志”下选择“NSG 流日志”，如下图所示：



- 3) 从 NSG 列表中选择需要监控 VM 流量所在虚拟网络的 NSG。
- 4) 在“流日志设置”下选择“启用”。
- 5) 选择流日志记录版本。版本 2 包含流会话统计信息（字节和数据包）
- 6) 选择保存日志到 Log Analytics workspace。
- 7) 在门户左上角选择“所有服务”。在“筛选器”框中，键入“网络观察程序”。搜索结果中出现“网络观察程序”后，将其选中。
- 8) 选择“保存”。

注意：

NSG flow 日志需要注册 Microsoft.Insights。如果无法使用网络观察程序，请检查是否已经注册 Microsoft.Insights:

<https://docs.azure.cn/zh-cn/network-watcher/network-watcher-nsg-flow-logging-portal#register-insights-provider>

- 9) 如果需要批量开启 NSG flow logs，可以使用以下的 Powershell 脚本（需要修改参数）。

```
# Please replace the below parameters:
# Location = actual Locations for Network Security Groups. Such as
chinaeast,chinaeast2,chinanorth,chinanorth2
# storageAccountName = storage account which will store NSG flow logs. This storage
account should be in the same location as network security group
# workspcename = your actual log analytics workspace name
```

TrafficAnalyticsInterval = NSG flow log analytics interval. Value can be 10 or 60 minutes

nsglogFormatVersion = NSG flow logs format version. Value can be 1 or 2. when set the format version to 2, packet size will be stored in Log A workspace. 1 is enough for used workbooks.

```
$location = "<location_of_target_network_security_group>"
```

```
$storageAccountName = "<storage_account_name>"
```

```
$workspacename = "<Log_analytics_workspace_name>"
```

```
$TrafficAnalyticsInterval = 10
```

```
$nsglogFormatVersion = 1
```

```
$NetworkWatcherResourceGroup = "NetworkWatcherRG"
```

```
$storageAccount = Get-AzStorageAccount | where {($_.storageaccountname -eq  
$storageAccountName) -and ($_.PrimaryLocation -eq $location)}
```

```
$workspace = Get-AzOperationalInsightsWorkspace | where {$_ .name -eq  
$workspacename}
```

```
if ( (($storageAccount | measure-object).count -eq 0) -or (($workspace | measure-  
object).count -eq 0) ){
```

```
    write-host "there is no storage account existing in the target location or Log  
Analytics workspace does not exist"
```

```
} else {
```

```
    $NW = Get-AzNetworkWatcher -Location $location -erroraction ignore
```

```
    if (($NW | measure-object).count -eq 0) {
```

```
        $NWRG = get-azresourcegroup -name $NetworkWatcherResourceGroup -erroraction  
ignore
```

```
        if (($NWRG | measure-object).count -eq 0) {
```

```
            New-AzResourceGroup -Name $NetworkWatcherResourceGroup -Location  
$location  
        }
```

```
        Register-AzResourceProvider -ProviderNamespace Microsoft.Insights
```

```
        $NWName = "NetworkWatcher_" + $location
```

```
        $NW = New-AzNetworkWatcher -Location $location -ResourceGroupName  
$NetworkWatcherResourceGroup -Name $NWName  
    }
```

```
$nsgs = Get-AzNetworkSecurityGroup | where {$_ .Location -eq $location}
```

```
foreach ($nsg in $nsgs) {
```

```

Set-AzNetworkWatcherConfigFlowLog -NetworkWatcher $NW -TargetResourceId
$nsg.Id -StorageAccountId $storageAccount.Id -EnableFlowLog $true -FormatType Json
-FormatVersion $nsgLogFormatVersion -EnableTrafficAnalytics -
TrafficAnalyticsInterval $TrafficAnalyticsInterval -WorkspaceResourceId
$workspace.ResourceId -WorkspaceGUID $workspace.CustomerId -WorkspaceLocation
$workspace.Location
}

}

```

1.4 其他的数据源的配置，请参考以下的列表：

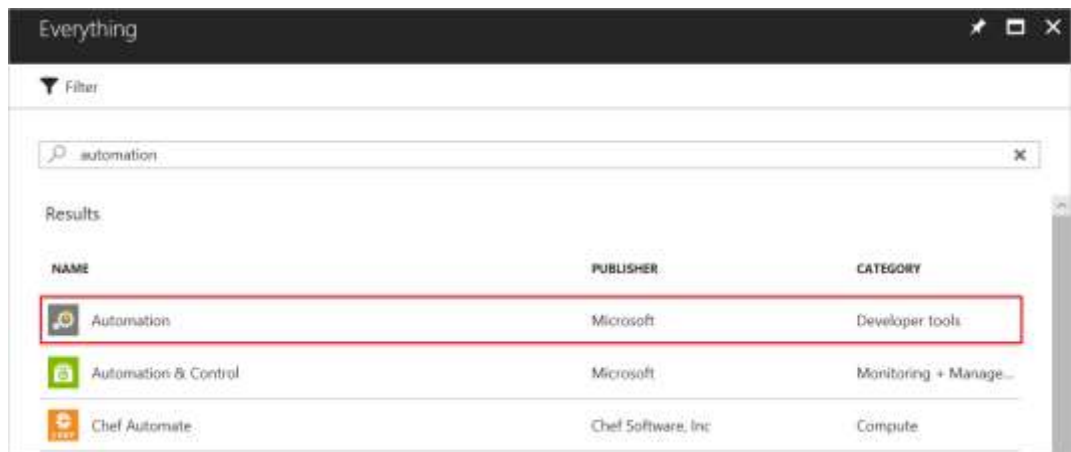
数据源	目标表名	启用文档
AzureActiveDirectory	AuditLogs	https://docs.azure.cn/zh-cn/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics
AzureActiveDirectory	SigninLogs	https://docs.azure.cn/zh-cn/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics
AzureActivity	AzureActivity	https://docs.azure.cn/zh-cn/azure-monitor/platform/diagnostic-settings
AzureMonitor(Keyvault)	AzureDiagnostics	https://docs.azure.cn/zh-cn/azure-monitor/insights/azure-key-vault
SecurityEvents	SecurityEvents	https://docs.azure.cn/zh-cn/security-center/security-center-enable-data-collection#data-collection-tier
Syslog	Syslog	https://docs.microsoft.com/en-us/azure/sentinel/connect-syslog
AzureMonitor(IIS)	W3CIISLog	https://docs.azure.cn/zh-cn/azure-monitor/platform/data-sources-iis-logs
AzureMonitor(Azure Firewall)	AzureDiagnostics	https://docs.microsoft.com/en-us/azure/firewall/firewall-diagnostics

数据源	目标表名	启用文档
AzureMonitor(Application Gateways/WAF)	AzureDiagnostics	https://docs.azure.cn/zh-cn/application-gateway/application-gateway-diagnostics#enable-logging-through-the-azure-portal
AzureSecurityCenter	SecurityAlert	https://docs.azure.cn/zh-cn/security-center/security-center-enable-data-collection
CEF	CommonSecurityLog	https://docs.microsoft.com/en-us/azure/sentinel/connect-common-event-format
CiscoASA	CommonSecurityLog	https://docs.microsoft.com/en-us/azure/sentinel/connect-common-event-format
ProcessAuditing	AuditLog_CL	https://msticpy.readthedocs.io/en/latest/data_acquisition/CollectingLinuxAuditLogs.html
TrafficAnalytics	AzureNetworkAnalytics_CL	https://docs.azure.cn/zh-cn/network-watcher/traffic-analytics
UpdateManagement	Update	https://docs.azure.cn/zh-cn/automation/update-management/update-mgmt-overview or https://docs.azure.cn/zh-cn/security-center/security-center-enable-data-collection
Compliance	SecurityBaseline	https://docs.azure.cn/zh-cn/security-center/security-center-enable-data-collection

二．部署安全规则和工作流

1. 部署自动化账户

- 1) 在 Azure Portal 中选择“+ 创建资源”。
- 2) 搜索“自动化”。在搜索结果中，选择“自动化”。



- 3) 在下一个屏幕上，选择“新建”。
- 4) 在“添加自动化帐户”窗格的“名称”字段中，输入新自动化帐户的名称。选择后，将无法更改此名称。如果有多个订阅，请使用“订阅”字段指定用于新帐户的订阅。对于“资源组”，请输入或选择新的或现有的资源组。对于“位置”，请选择 ChinaEast2(中国东部 2)数据中心位置。

[主页](#) > [自动化帐户](#) >

添加自动化帐户

名称 * ⓘ


订阅 *

资源组 *

[新建](#)

位置 *

创建 Azure 运行方式帐户 * ⓘ
☒ 是 ☐ 否



此操作将在自动化帐户中创建 Azure 运行方式帐户，这些帐户可用于向 Azure 进行身份验证，从而通过自动化 Runbook 管理 Azure 资源。请注意，创建 Azure 运行方式帐户可能会影响订阅的安全性。[了解详细信息](#)

- 5) 对于“创建 Azure 运行方式帐户”选项，请确保选择“是”，然后单击“创建”。

- 6) 完成创建后，在自动化账户界面的连接配置中，可以看到对应创建的 Azure 运行方式帐户 AzureRunAsConnection。



- 7) 在 Azure Portal 中，搜索"Log Analytics"。选择对应的 Log Analytics 工作区。在工作区界面的访问控制设置中，选择添加角色分配。



- 8) 在添加角色分配界面，选择角色"Log Analytics 参与者"。在选择中输入自动化账户名。选中出现的账户。选择添加。

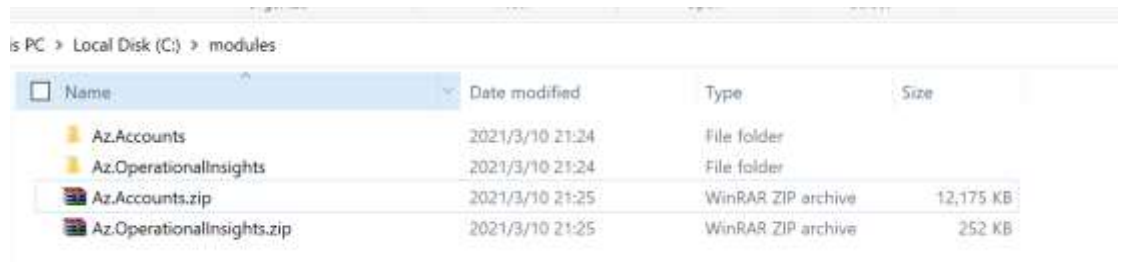


- 9) 通过以下的命令行下载 PowerShell 模块到本地目录（例如: C:\modules）：

Save-Module -Name az.accounts -Path C:\Modules -Repository PSGallery

Save-Module -Name Az.Operationallnsights -Path C:\Modules -Repository PSGallery

- 10) 完成下载后，在对应目录中，把 module 目录压缩成.ZIP 包



11) 回到 Azure Portal. 在自动化账户的模块界面, 选择添加模块。从本地目录选中之前步骤中创建的 ZIP 包。请先添加 Az.Accounts。在 Az.Accounts 模块显示状态为可用后, 再导入 Az.Operationallnsights。



2. 部署安全规则模板

1) 下载以下链接中的 ARM 模板

<https://github.com/simonxin/sentinel-like-queries-for-mooncake/blob/master/template/securityquerypack.json>

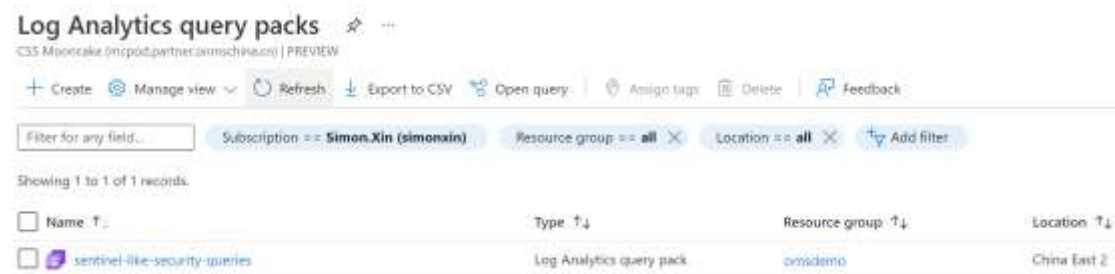
2) 执行以下的脚本部署模板 (需要替换脚本中的参数)

```
# resourcegroup = resource group you want to deploy the security rule query packs
# templatefile = downloaded ARM template file
# do group deployment
New-AzResourceGroupDeployment -ResourceGroupName $resourcegroup -Name "securityquerypack" `
-TemplateFile $templatefile `
-verbose
```

3) 完成部署后, 访问以下的连接:

<https://portal.azure.cn/#blade/HubsExtension/BrowseResource/resourceType/Microsoft.OperationalInsights%2Fquerypacks>

确认以下的 Query Pack 部署成功



3. 部署安全规则 workflow 模板

- 1) 下载以下链接中的 ARM 模板

<https://github.com/simonxin/sentinel-like-queries-for-mooncake/blob/master/template/securityworkflows.json>

- 2) 执行以下的脚本部署模板（需要替换脚本中的参数）

```
# Please replace the below parameters:
# workspace = your actual log analytics workspace name
# workspaceResourcegroup = resource group you want to deploy the template which is
# also the same as the Log Analytics resource group
# automationaccount = automation account name
# auaccountResourcegroup = automation account name resource group
# recipientaddress like xxx@yourdomain.com
# templatefile = downloaded ARM template file
# Use chinaeast2 as the location as log analytics service only available in this
region
$workspace = "<workspace_name>"
$workspaceResourcegroup = "<workspace_resource_group>"
$automationaccount = "<automation_account_name>"
$auaccountResourcegroup = "<automation_account_resource_group>"

$templatefile = "<full_path_of_downloaded_template_file>"
$recipientAddress = "<email_address_for_notification>"

# Define parameters
$params = @{
    workspaceName = $workspace
    workspaceResourcegroup = $workspaceResourcegroup
```

```

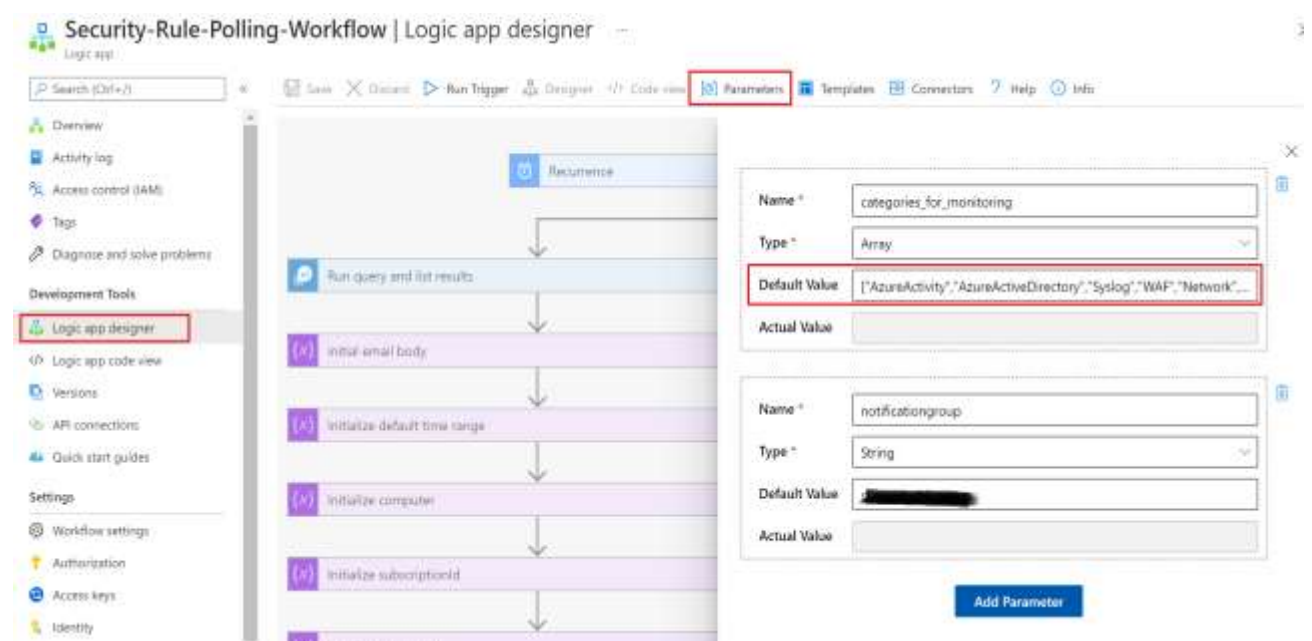
    auaccountname = $automationaccount
    auaccountresourcegroup = $auaccountresourcegroup
    recipientAddress = $recipientAddress
}

# do group deployment
New-AzResourceGroupDeployment -ResourceGroupName $workspaceresourcegroup -Name
"securityworkflows" `
-TemplateFile $templatefile `
-TemplateParameterObject $params `
-verbose

```

4. 设置告警邮件 workflow

- 1) 部署完成后，在 Azure Portal 中找到部署的 logic App。缺省名: Security-Rule-Polling-Workflow
- 2) 在 Logic App 页面，选择"Logic app designer"。选择"Parameters"。



- 3) 修改 Default Value 可以控制需要执行的安全规则。

例如：

["AzureActivity","AzureActiveDirectory","Syslog","WAF","Network","HIDS","DSM","honeypot"]

注意：目前的安全规则支持以下的类型：

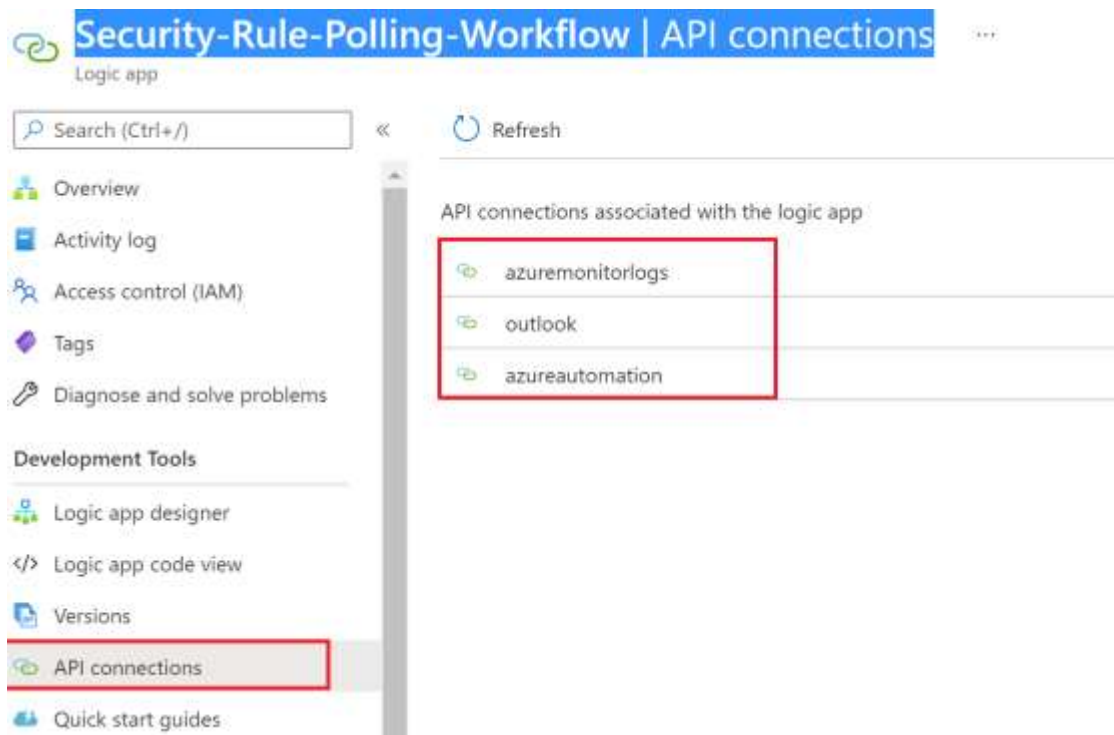
"AzureActivity": Azure 活动日志

"AzureActiveDirectory": Azure AD 审计

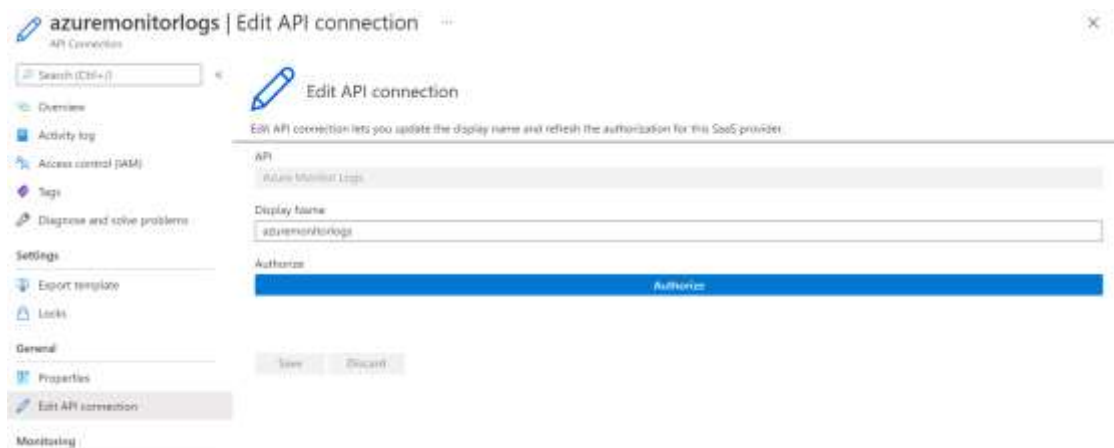
"Syslog": Linux VM
"Heartbeat": OMS Agent version check
"SecurityEvents": Windows VM
"AzureSecurityCenter": Azure 安全中心
"WAF": Azure application gateway (WAF)
"Network": Azure Network watcher logs
"HIDS": HIDS events
"DSM": DSM events
"honeypot": Honey pot security events

3) 在 notificationgroup 中定义的告警邮件中设置的告警邮件接收者地址。

4) 在 API connectors 页面。找到需要配置的 connector.



5) 选中 azuremonitorlogs。在 Edit API connectionu 页面。点击"Authorize"



完成登录。选择"Allow Access"

Confirmation required

You are about to provide access to



Azure Monitor Logs

to a connection created by user .

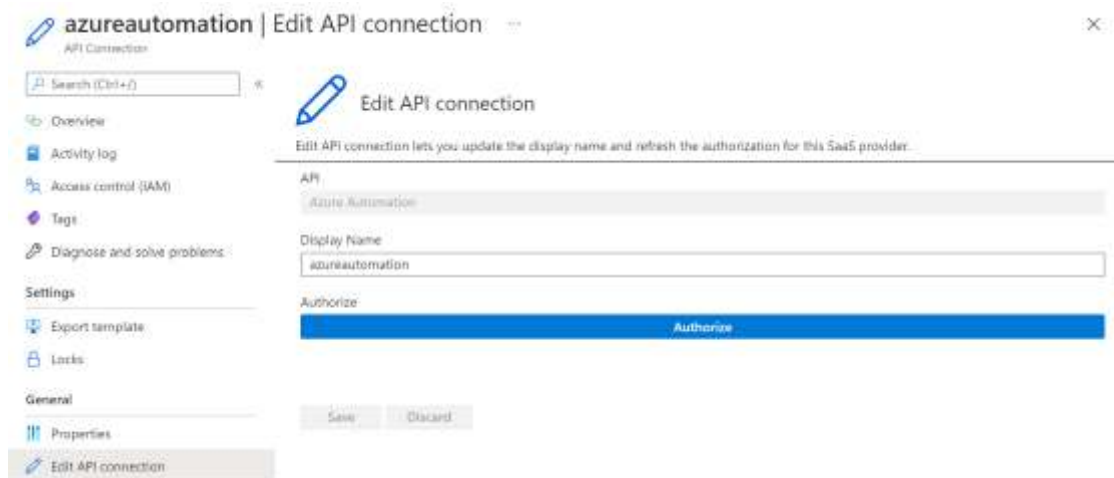
Allow access

Cancel

选择"Save".

6) 选择 azureautomation 连接。

7) 在 Edit API connection 页面。点击 Authorize.。



完成登录。选择"Allow Access"

Confirmation required

You are about to provide access to



Azure Automation

to a connection created by user .

Allow access

Cancel

- 8) 选择 Outlook Connector。在 Edit API connectionu 页面。点击"Authorize"
- 9) 使用你的 outlook 邮箱登录（例如：xxx@live.com）。完成登陆后，选择"Allow Access"。选择"Save"。

Confirmation required

You are about to provide access to



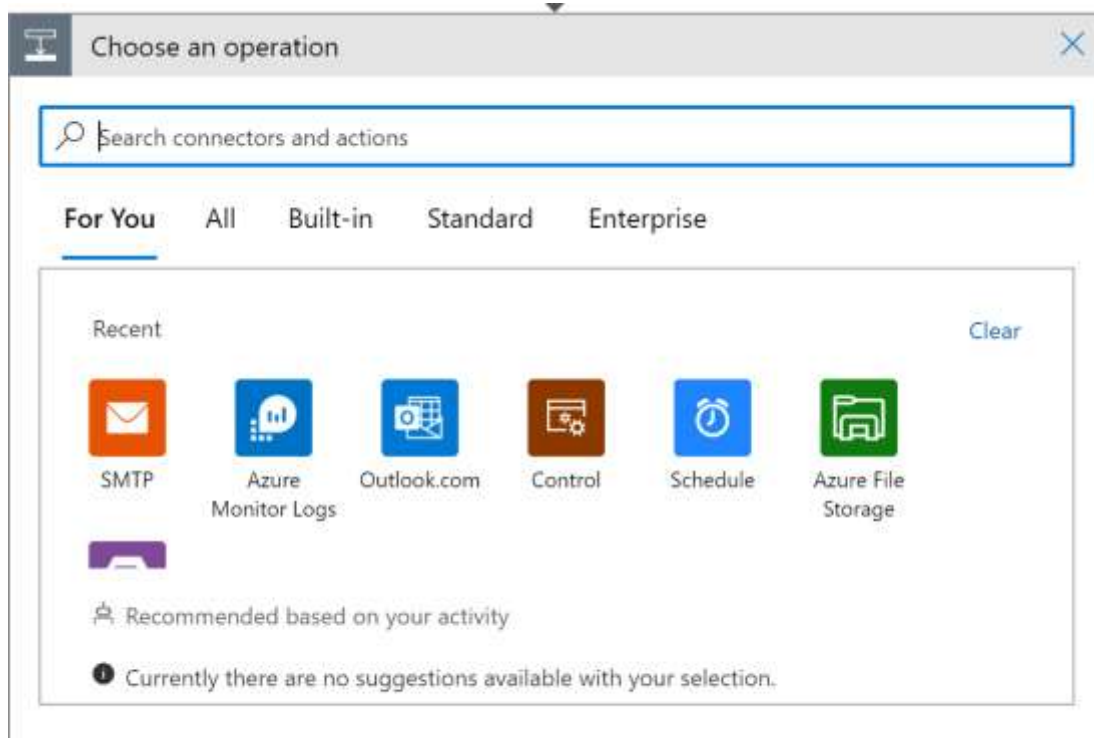
Outlook.com

to a connection created by user .

Allow access

Cancel

- 10) 如果没有 outlook 邮箱，也可以配置 SMTP 邮箱的连接器来发送告警。方法是在 Logic App designer 中，展开 For each。选择 "Add an action"。
- 11) 在模板中选择 SMTP。



12) 配置对应的 SMTP 连接。

SMTP

* Connection name: Enter name for connection

* SMTP Server Address: SMTP Server Address

User Name: User Name

Password: Password

SMTP Server Port: SMTP Port Number (example: 587)

Enable SSL? ☐ Enable SSL? (True/False)

Create

13) 复制邮件格式可以参考部署的 logic app 里的"send email (v2)"里的设置。

5. 验证安全规则执行 workflow

- 1) Logic App 工作流每 10 分钟触发一次。在完成 logic app parameters 和 API connection 配置后，可以在 Logic App Overview 页面，选择“run history”，确保配置触发的工作流执行状态为 Succeeded

The screenshot shows the Logic App Overview page for 'Security-Rule-Polling-Workflow'. The left sidebar has 'Overview' selected. The main content area shows the workflow's details, including Resource group (somsauto), Location (China East 2), Subscription (Simon.Xin (somsauto)), and Subscription ID (0f2daa80-6c16-44ee-8016-4a688e059ac). The 'Runs history' tab is selected, showing a table of recent runs.

Status	Start time	Identifier	Duration	Static Results
Succeeded	11/18/2021, 4:29 PM	08585643827064459389709459709CU25	48.05 Seconds	
Succeeded	11/18/2021, 4:19 PM	085856438330738620886648044490CU27	17.88 Seconds	

- 2) 如果出现错误，可以点开错误的工作流执行历史，看错误原因。
- 3) 如果工作流错误是执行 azure automation runbook 失败，可以在 Azure Portal 中，打开 automation 页面。部署的安全规则自动化执行 runbook 缺省命名为"SecurityRulePollingjob"

The screenshot shows the Azure Automation Runbooks page for the 'somsauto' Automation Account. The left sidebar has 'Runbooks' selected. The main content area shows a table of runbooks.

Name	Authoring status	Runbook type	Runtime version	Last modified	Tags
AzureAutomationTutorial	Published	Graphical PowerShell	5.1	3/10/2021, 5:48 PM	
AzureAutomationTutorial	Published	Python	2.7.12	3/10/2021, 5:48 PM	
AzureAutomationTutorial	Published	PowerShell	5.1	3/10/2021, 5:48 PM	
Inject-project-inf	In edit	PowerShell	5.1	10/8/2021, 5:07 PM	
SecurityRulePollingjob	Published	PowerShell	5.1	11/18/2021, 4:40 PM	
test	In edit	PowerShell	5.1	9/7/2021, 3:24 PM	

- 4) 在 runbook 页面，查看 Recent jobs.

SecurityRulePollingJob (somsauto/SecurityRulePollingJob)

Search (Ctrl+F)

Start View Edit Link to schedule Add webhook Delete Export Refresh

Overview

- Activity log
- Tags
- Diagnose and solve problems

Resources

- Jobs
- Schedules
- Webhooks

Runbook settings

- Properties
- Description
- Logging and tracing

Settings

- Export template
- Locks

Essentials

Resource group: **amsdemo**

Account: **somsauto**

Location: **China East 2**

Subscription: **Soms.Xia (somsauto)**

Subscription ID: **0f2ba90-6b16-44ee-8016-4a3b88e059ac**

Status: **Published**

Runbook type: **PowerShell**

Runtime version: **5.1**

Last modified: **11/18/2021, 4:40 PM**

Tags: (change) [Click here to add tags](#)

Recent Jobs

Status	Created	Last updated
✓ Completed	11/18/2021, 4:38:38 PM	11/18/2021, 4:40:18 PM
✓ Completed	11/18/2021, 4:29:39 PM	11/18/2021, 4:30:21 PM
✓ Completed	11/18/2021, 4:18:28 PM	11/18/2021, 4:19:55 PM

5) 如果是失败的记录，可以在 runbook job 页面查看 output, Errors, Exceptions

SecurityRulePollingJob 11/18/2021, 4:39 PM

Resume Stop Suspend Refresh

Essentials

ID: **eb4410b-ff0-4e5b-9d99-7e676c3460a6**

Status: **Completed**

Run: **Azure**

Run as: **User**

Created: **11/18/2021, 4:39:39 PM**

Last Update: **11/18/2021, 4:40:18 PM**

Runbook: **SecurityRulePollingJob**

Source image: **View source image**

Input **Output** Errors Warnings All Logs Exception

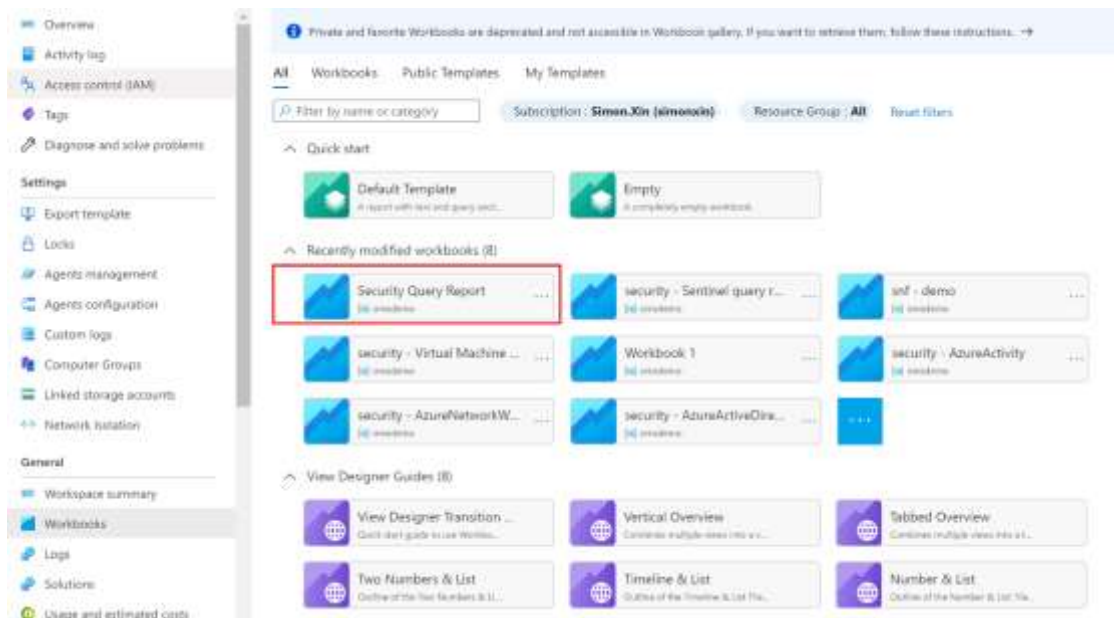
```

execution: 99
Logging in to Azure...

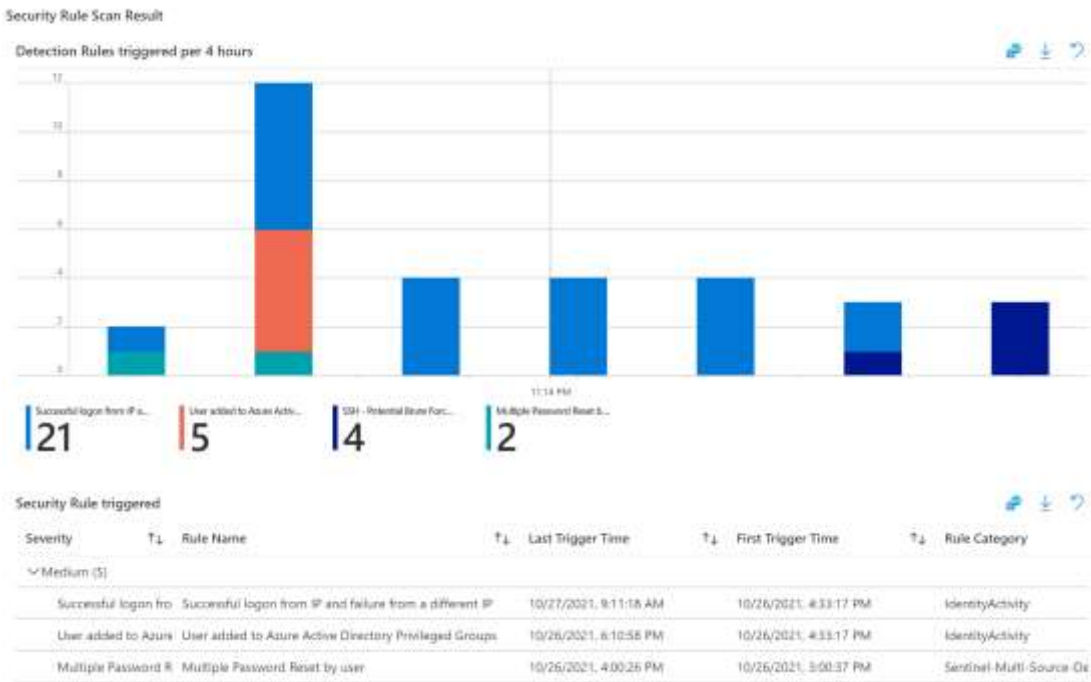
Environments
-----
[[AzureChinaCloud, AzureChinaCloud], [AzureCloud, AzureCloud], [AzureGermanCloud, AzureGermanCloud], [AzureSGovernance, AzureSGovernance]]
  
```

6. 使用模板分析查询结果

- 1) 在 Azure Portal Log Analytics 工作区的工作簿中，选中名为"security – Sentinel query report"的工作簿



- 2) 在工作簿中，会返回最后执行的 detection 和 hunting 查询中有数据的查询条目。选中发现的条目，在"Selected rule query details"表单中会显示具体的查询结果。



三．管理安全规则

1. 如何导出当前部署的安全规则

- 1) 下载以下链接中的 PowerShell 模板
- 2) 执行以下的 Powershell 语句

```
=====

import-module <full path of downloaded securityruletoolkit.ps1> -force

$environment = "Mooncake"

$subscriptionId = "<subscription ID which you have deployed Azure Query Pack>"

$resourcegroup = "<resource group you have used to deploy Azure Query Pack>"

$querypackname = "sentinel-like-security-queries"

$exportfile = "<full path of target file you want export, like c:\case\rules.csv>"

# run below command to export the query pack

export-savedqueries -environment $environment -subscriptionId $subscriptionId -
resourceGroup $resourcegroup -querypackname $querypackname -exportpath $exportfile
```

- 3) 如果执行正确，可以打开导出的 CSV 文件。其中， ruleId 和 displayName 为安全规则的唯一标识。其他的部分为安全规则的属性。唯一标识不能修改。安全规则的属性，可以修改。

ruleId	displayName	isEnabled	type	severity	category	source	queryFrequency	queryPeriod	description	body
Zeta712b71ee	New internet-exposed SSH endpoints	TRUE	Detection	Medium	Syslog	Syslog	1d	7d	本规则用于检查 Syslog，当发现虚拟机异常行为是	let Pwntest = 92.141.72.1 let seqfrew let protobdi let startime let sub_Jcpi where Tin where Fau where Sp1 extend Sc \$[1:3][0:1] where son extend ip PwntestPre join Logins summarize publiccount by(EventId) summarize publicPloq logon, tim privatePlo logon, tim ms-apply (order by summa publicPloq Count]]

注意：

Enabled：支持的值为 TRUE 或 FALSE. 如果为 FALSE, 此条安全规则将被禁用

type：支持的值为 Detection 或 Hunting. 如果为 Hunting, 此条安全规则将被不会被自动触发

severity：安全规则优先级。支持的值为 High, Medium, Low, （高，中，低）

category：安全规则所属范围。如果修改，请确保在告警邮件工作流设置中已经添加此监控范围。否则，安全规则不会被执行

queryFrequency：安全规则执行频率。支持的格式是 xm (minutes), xh(hour), xd (day). 这里支持的最小单位为 10m (10 分钟)

queryPeriod：安全规则查询日志的时间范围。支持的格式是 xm (minutes), xh(hour), xd (day). 这里支持的最小单位为 10m (10 分钟)

description：安全规则说明。将显示在告警邮件中

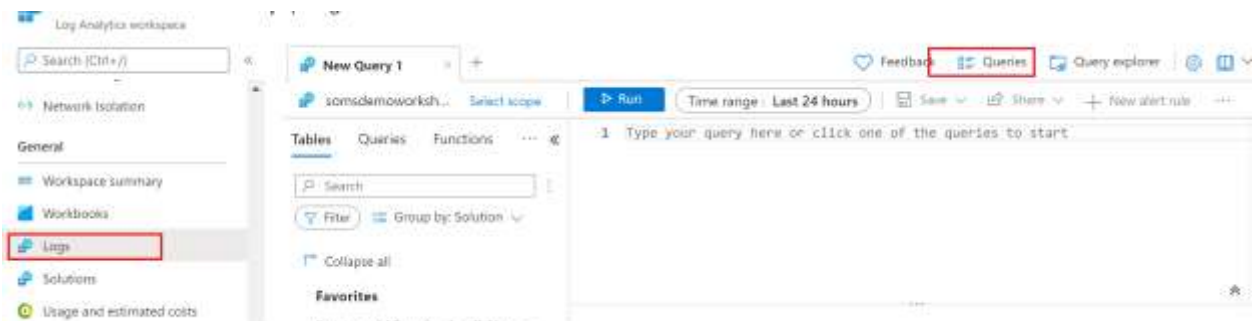
body：安全规则查询语句

2. 如何修改当前部署的安全规则

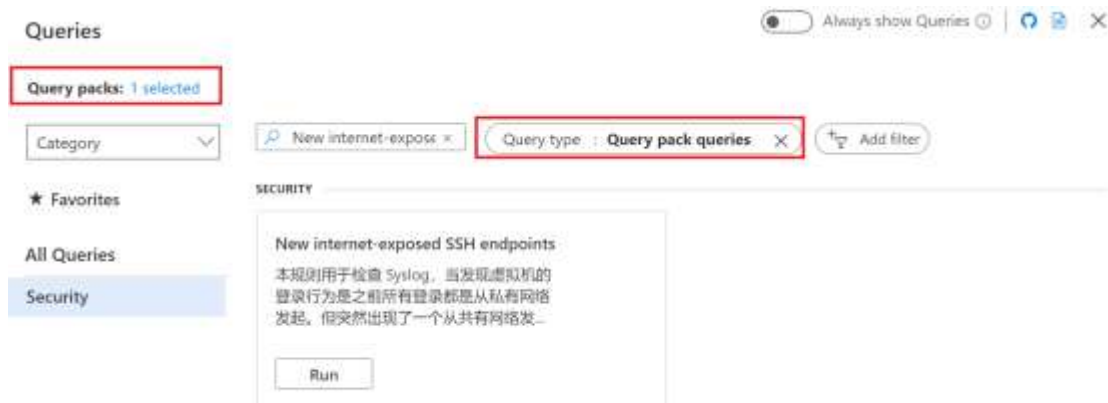
可以使用以下的方法之一来修改部署的安全规则

方法一：修改安全规则查询语句（Query）或说明(Description)

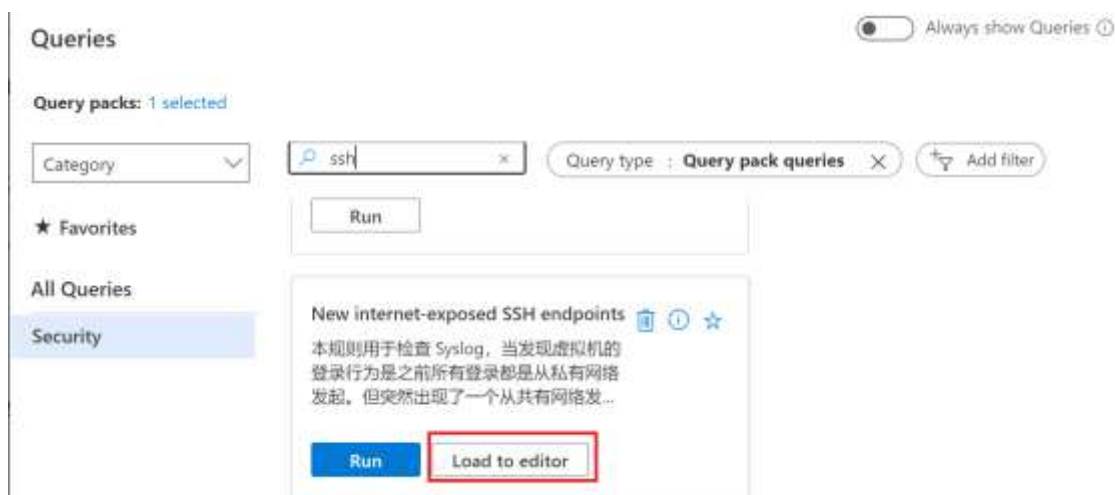
- 1) 打开 Azure Portal. 在 Log Analytics 页面，选择 Logs。在 Logs 查询页面，选择"Queries"



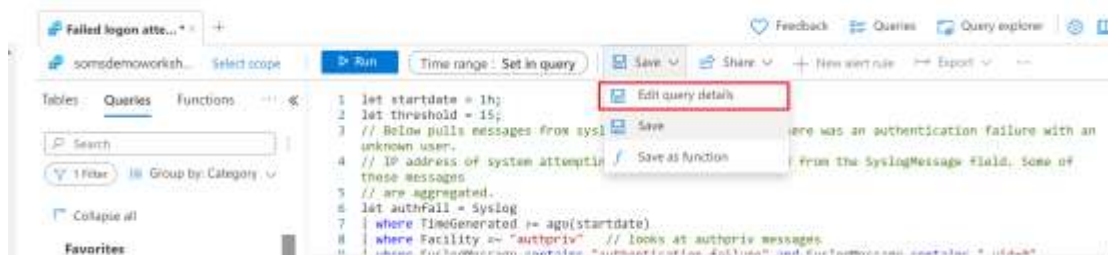
- 2) 在 Queries 查询页面，请确认 query packs 已经选择。在搜索页面，可以复制需要修改的安全规则名。如果有多个，可以点击"Add filter"。设置 query type 为 query pack queries.



3) 选中需要修改的安全规则. 点击"load to editor".



4) 完成修改后, 在 Save 下拉列表, 选择"Edit query details"



5) 在 Edit Query Details, 可以修改 Description.

注意: 请不要修改 Query Name。 否则将保存为一个新的安全规则。

Edit query details ✕

Query name *
Failed logon attempts in authpriv ✓

Description
本规则将检查 Syslog authpriv 日志。如果出现来自未知用户的失败登录尝试超过阈值（默认阈值为 15）将产生报警。表明

Path
☐ Save to the default query pack ⓘ

Subscription
Simon.Xin (simonxin) ▼

Resource group
prsdemo ▼

Log Analytics query pack
sentinel-like-security-queries ▼

Tags

Resource type
Log Analytics workspaces ▼

Category
Security ▼

Label
D selected ▼
[Create new label](#)

方法二：使用 Powershell 修改单条安全规则属性(可以修改除了 ruleId, displayName 外所有的属性)

1) 执行以下的 Powershell 语句

=====

```
import-module <full path of downloaded securityruletoolkit.ps1> -force
```

```
$environment = "Mooncake"
```

```
$subscriptionId = "<subscription ID which you have deployed Azure Query Pack>"
```

```
$resourcegroup = "<resource group you have used to deploy Azure Query Pack>"
```

```
$querypackname = "sentinel-like-security-queries"
```

```
$rulename = "<target rule name you want change>"
```



```
# run below command to export the query pack

$securityrule = get-savedqueries -environment $environment -subscriptionId $subscriptionId -resourceGroup $resourcegroup -querypackname $querypackname -rulename $rulename

# get rule ID
$ruleId = $securityrule.Name

# change properties
# update the rule severity from Low to High
$securityrule.properties.properties.severity = 'Low'
$securityrule.properties.properties.queryFrequency = '1h'
$securityrule.properties.properties.queryPeriod = '1h'
$properties = $securityrule.properties

# update the security rule properties
update-savedqueries -environment $environment -subscriptionId $subscriptionId -resourceGroup $resourcegroup -querypackname $querypackname -ruleid $ruleid -properties $properties
```

方法三：在导出的 excel 中，修改多条安全规则属性(可以修改除了 ruleId, displayName 外所有的属性)，

- 1) 在导出的 Excel 中，修改所有需要修改的安全规则属性（ruleId, displayName 不可修改）
- 2) 执行以下的 Powershell 语句

```
=====

import-module <full path of downloaded securityruletoolkit.ps1> -force

$environment = "Mooncake"

$subscriptionId = "<subscription ID which you have deployed Azure Query Pack>"

$resourcegroup = "<resource group you have used to deploy Azure Query Pack>"

$querypackname = "sentinel-like-security-queries"

$importfile = "<full path of target file you want import, like c:\case\rules.csv>"

# run below command to export the query pack

import-savedqueries -environment $environment -subscriptionId $subscriptionId -resourceGroup $resourcegroup -querypackname $querypackname -sourcefile $importfile
```

3. 如何添加新的安全规则

可以使用以下的 powershell 脚本来部署新的安全规则

1) 执行以下的 Powershell 语句

=====

```
import-module <full path of downloaded securityruletoolkit.ps1> -force

$environment = "Mooncake"

$subscriptionId = "<subscription ID which you have deployed Azure Query Pack>"

$resourcegroup = "<resource group you have used to deploy Azure Query Pack>"

$querypackname = "sentinel-like-security-queries"


# generate a new GUID for your rule

$ruleId = $([guid]::NewGuid()).toString()


# full fill rule proeptries

$displayname = "test rule"

$description = "测试规则"

$related = [PSCustomObject]@{

    categories = @('security')

    resourceTypes = @('microsoft.operationalinsights/workspaces')

}

$body = @'

Heartbeat / Limit 1
```

'@

```
$ruleproperty = [PSCustomObject]@{
```

```
    enabled="false"
```

```
    type="Detection"
```

```
    severity="Low"
```

```
    category="Heartbeat"
```

```
    source="Heartbeat"
```

```
    queryFrequency="1d"
```

```
    queryPeriod="1d"
```

```
}
```

```
$properties = [PSCustomObject]@{
```

```
    displayName = $displayname
```

```
    description = $description
```

```
    body = $body
```

```
    related = $related
```

```
    properties = $ruleproperty
```

```
}
```

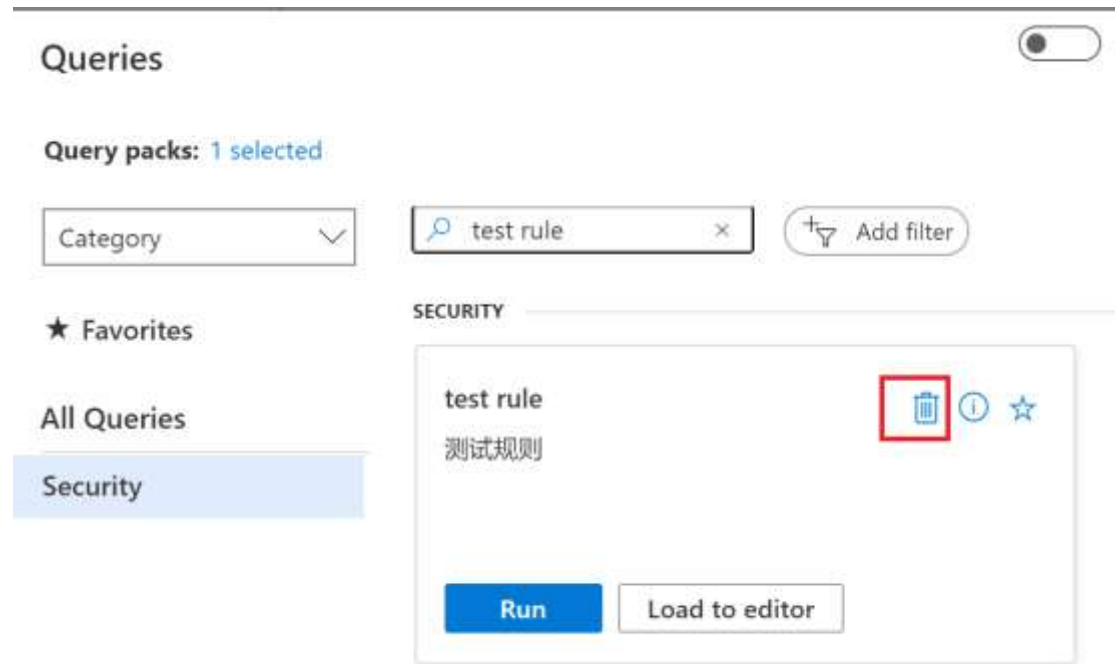
```
# add new rules
```

```
update-savedqueries -environment $environment -subscriptionId $subscriptionId -  
resourceGroup $resourcegroup -querypackname $querypackname -ruleid $ruleId -  
properties $properties
```

4. 如何从 query pack 中删除安全规则

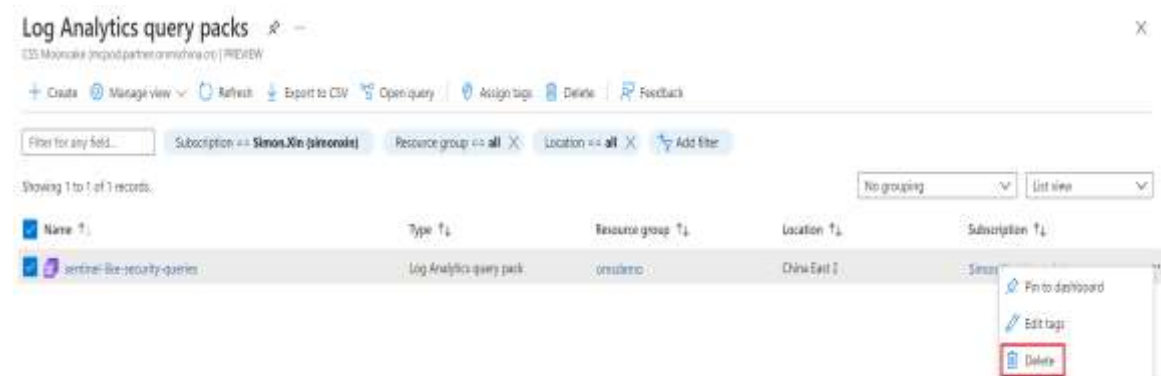
方法一:

- 1) 在 Azure portal 的 log analytics 页面, 选择 logs -> Queries. 找到需要删除的安全规则。
- 2) 点击“垃圾箱”标记。在弹出窗口中, 选择 delete。



方法二:

- 1) 修改 ARM 模板 securityquerypack.json。删除安全规则定义。
- 2) 从以下的连接访问 Azure Query Pack:
<https://portal.azure.cn/#blade/HubsExtension/BrowseResource/resourceType/Microsoft.OperationalInsights%2FQuerypacks>
选中 Query Pack, 选择 delete。



- 3) 导入更新后的 ARM 模板

四 . 部署工作簿模板和共享仪表盘模板

完成日志收集后，可以参考以下的步骤部署模板。导入用于分析日志的工作簿， 查询和仪表盘。

1. 部署仪表盘模板

1.1 下载仪表盘模板到本地。

请参考以下列表，下载对应的 ARM 模板到本地

category	Descriptions	required data source	template
Azure AD Signing	Azure dashboard which will show overview of Azure AD signin operations	SigninLogs	azureadsignins.json
Azure AD Operations	Azure dashboard which will provide overview of sensitive Azure AD operations like grant permissions or add new users etc	AuditLog	Azure AD Audit logs.json
Azure Activity	Azure dashboard which will show overview of Azure activities like resource creation, updating and deletion	AzureActivity	Azure Activity.json

category	Descriptions	required data source	template
Network Flows	Azure Dashboard which will show overview analysis on network flows such as: 1) Malicious traffic over IPs and Protocols, 2) Allowed and Denied flows trends over NSG, 3) Most Attacked resources	AzureNetworkAnalytics_CL	azurenetworkwatcher.json
Virtual Machine Performance	Azure Dashboard which will show performance overview on monitored Azure VMs	Perf	PerformLATemplate.json
Windows Security Events	Azure Dashboard which will show overview analytics on collected Windows Security Events from Windows VM with Azure Security Center license	SecurityEvent	identity and access.json
Application Gateway - WAF	Azure Dashboard which will show overview analytics on collected WAF access logs	AzureDiagnostics	Microsoft_WAF.json

1.2 执行 powershell 脚本部署模板（需要替换脚本中的参数）

```

# Please replace the below parameters:
# workspce = your actual log analytics workspace name
# resouworkspaceresourcegroup = your actual log analytics workspace resource group
# targetresourcegroup = resource group you want to deploy the dashboard
# templatefile = downloaded ARM template file
# Use chinaeast2 as the location as log analytics service only available in this
region
$workspace = "<your_LogA_workspace_name>"
$workspaceresourcegroup = "<your_LogA_workspace_resource_group>"
$subscriptionId = "<subscriptionId_for_LogA_workspace>"
$targetresourcegroup = "<resource_group_for_dashboard>"
$templatefile = "<downloaded_json_file_full_path>"
$location = "chinaeast2"

# Define parameters
$params = @{
    workspace = $workspace
    resourcegroup = $workspaceresourcegroup
    subscriptionId = $subscriptionId
    location = $location
}

$rg = Get-AzResourceGroup -Name $targetresourcegroup -ErrorAction SilentlyContinue

if ($rg -eq $null) {
    $rg = New-AzResourceGroup $targetresourcegroup -Location $location
}

# do group deployment
New-AzResourceGroupDeployment -ResourceGroupName $targetresourcegroup -Name
$targetresourcegroup `
-TemplateFile $templatefile `
-TemplateParameterObject $params `
-Verbose

```

2. 部署工作簿模板

2.1 下载模板到本地

请参考以下列表，下载对应的 ARM 模板到本地。

category	Description	required data source	optional data source	ARM template Content
Azure Identity and Activity	Provide security analysis for unabnormal AAD signngs and Azure Actiities such as: 1) brute attacks and password spray attacks on AAD account, 2) Suspicioous permission granting, 3) anomalous change in signing location, 4) unexpected resource deployments	AuditLogs SigninLogsAzure Activity		Identity Activity.json
Network Flows	Provide security analysis on network flows such as: 1) Malicious traffic over IPs and Protocols, 2) Allowed and Denied flows trends over NSG, 3) Most Attacked resources	AzureNetworkAnalytics_CL	AzureActivity	networkwatcher.json

category	Description	required data source	optional data source	ARM template Content
Virtual Machine	<p>Provide security analysis on VMs such as:</p> <ol style="list-style-type: none"> 1) Linux/Windows logon analytics, 2) Linux/Windows VM compliances and update analytics, 3) Windows VM Security Event Analytics, 4) Windows VM process execution analytics 5) Access on Windows VM by protocol like SMB/Kerberos/NTLM 	<p>SecurityEvent Syslog Update</p>	<p>Event SecurityBaseline SecurityBaselineSummary SecurityAlert ProtectionStatus</p>	<p>azurevm.json</p>
Azure Diagnostic	<p>Provide security analysis on Azure Resource Diagnostic log such as:</p> <ol style="list-style-type: none"> 1) Azure KeyVault sensitive operations analytics, 2) WAF (Web Application Firewall) access log analytics, 3) Azure 	<p>AzureDiagnostics</p>		<p>azurediagnostics.json</p>

category	Description	required data source	optional data source	ARM template Content
	Firewall trace analytics			
IIS Log	Provide security analysis on IIS logs (limited to Windows VM only) to provide insights that checks	W3CIISLog		IIS.json
Common Event Format	Provide security analysis on CEF log such as: 1) Cisco CEF logs, 2) Hardware WAF CEF logs	CommonSecurityLog	SecurityAlerts	CEF.json

2.2 执行 powershell 脚本部署模板（需要替换脚本中的参数）

```
# Please replace the below parameters:
# workspace = your actual log analytics workspace name
# resouworkspaceresourcegroup = your actual log analytics workspace resource group
# targetresourcegroup = resource group you want to deploy the dashboard
# templatefile = downloaded ARM template file
# Use chinaeast2 as the location as log analytics service only available in this region
$workspace = "<your_LogA_workspace_name>"
$targetresourcegroup = "<resource_group_for_LogA_workspace>"
$templatefile = "<downloaded_json_file_full_path>"
$location = "chinaeast2"
# Define parameters
$params = @{
    workspace = $workspace
    location = $location
}

$rg = Get-AzResourceGroup -Name $targetresourcegroup -ErrorAction SilentlyContinue
```

```

if ($rg -eq $null) {
    $rg =New-AzResourceGroup $targetresourcegroup -Location $Location
}

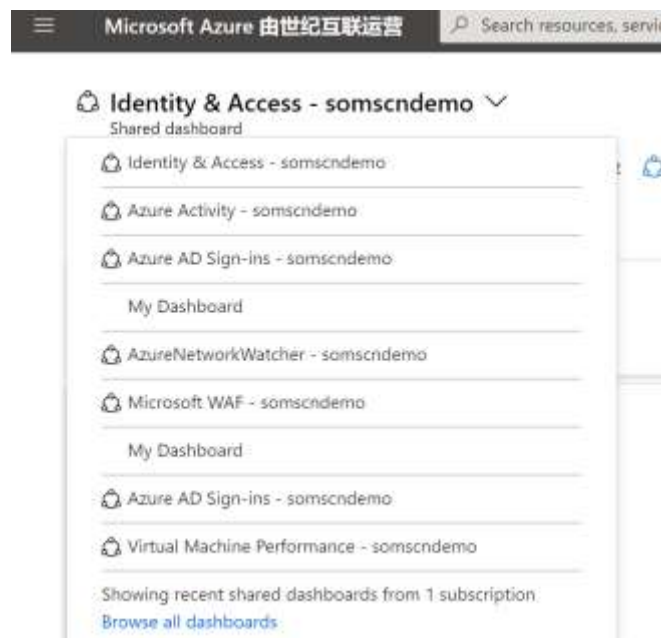
# do group deployment
New-AzResourceGroupDeployment -ResourceGroupName $targetresourcegroup -Name
$targetresourcegroup `
-TemplateFile $templatefile `
-TemplateParameterObject $params `
-Verbose

```

五．使用工作簿和仪表盘

1. 使用共享仪表盘

- 1.1 在 Azure 门户菜单上，选择“仪表盘”。缺省仪表盘将会显示。在共享仪表盘的下拉列表中，选择之前导入模板中的仪表盘。

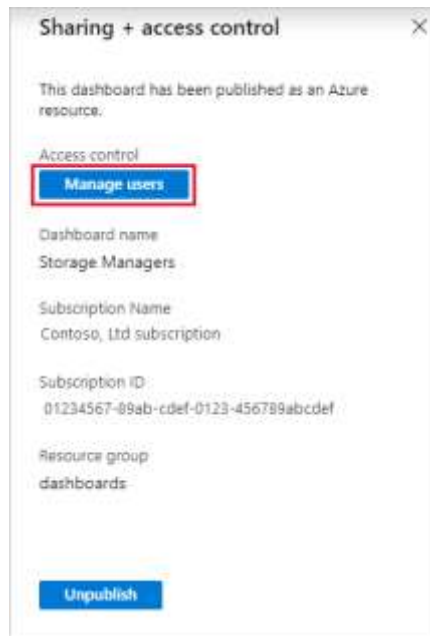


- 1.2 管理共享仪表盘的访问

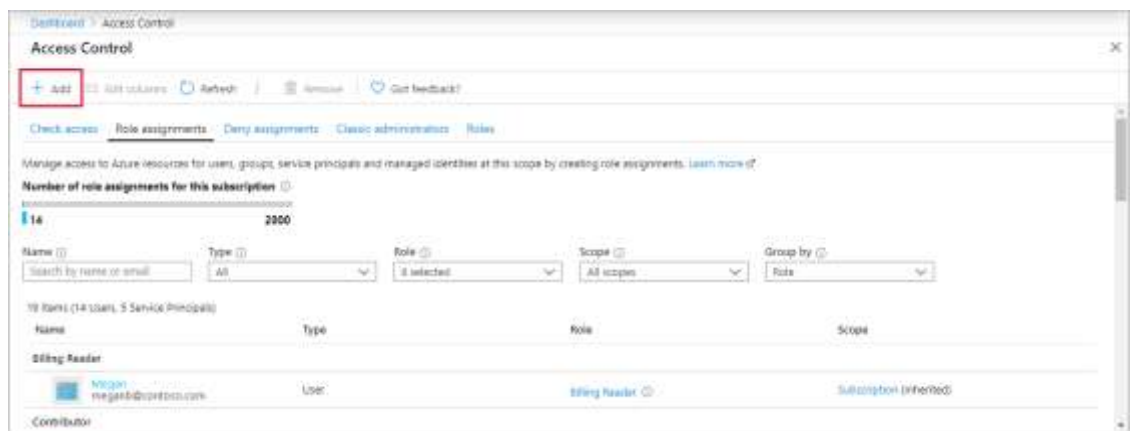
仪表盘可以通过角色的访问控制来共享给其他的 AAD 用户。具体步骤如下：

- 1) 发布仪表板后，选择“共享”或“取消共享”选项以访问“共享 + 访问控制”。

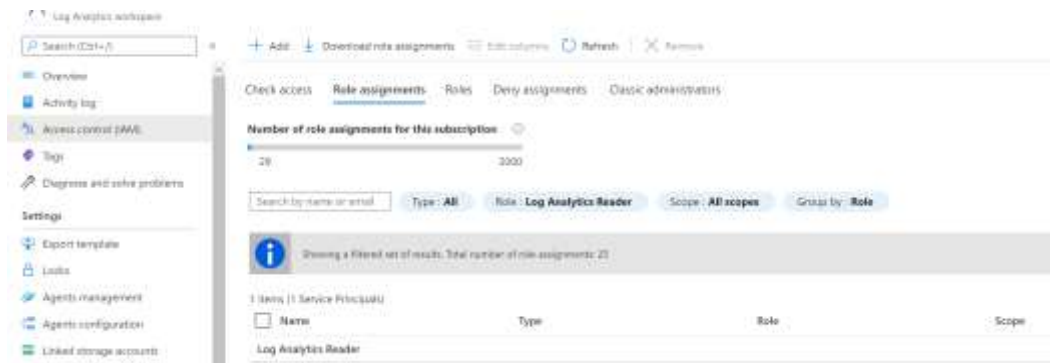
- 2) 在“共享 + 访问控制”中选择“管理用户”。



- 3) 选择“角色分配”，查看已为其分配此仪表板角色的现有用户。
- 4) 若要添加新用户或组，请选择“添加”，然后选择“添加角色分配”。

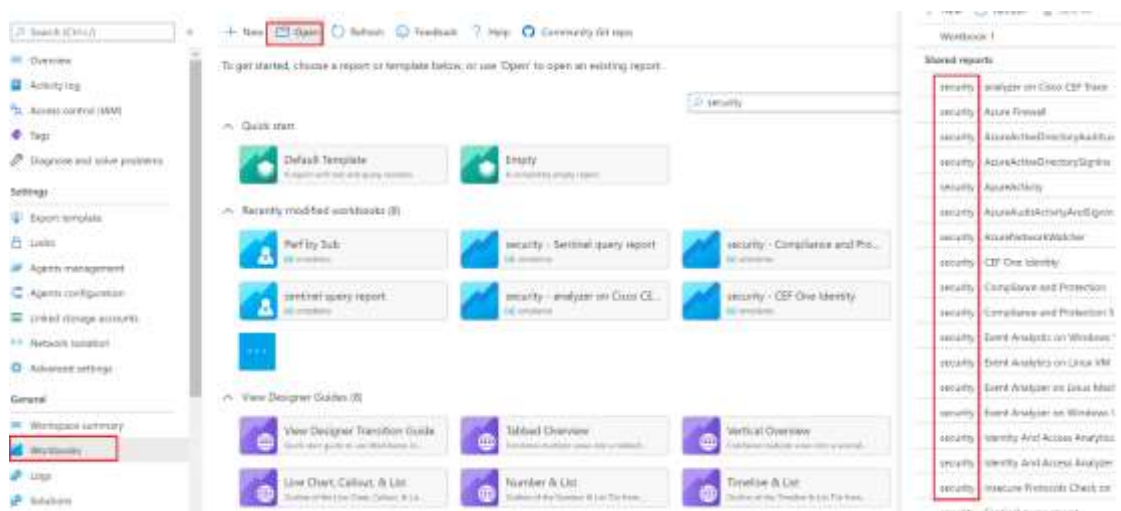


- 5) 选择表示要授予的权限的角色。对于此示例，请选择“参与者”。
- 6) 选择要分配到该角色的用户或组。如果在列表中没有看到要查找的用户或组，请使用搜索框。可用组列表取决于已在 Active Directory 中创建的组。
- 7) 完成添加用户或组后，请选择“保存”。
- 8) 安全监控中使用的仪表盘同时需要对 Log Analytics 工作区具有访问权限。使用以上步骤，分配 Log Analytics Reader 权限。



2. 使用工作簿

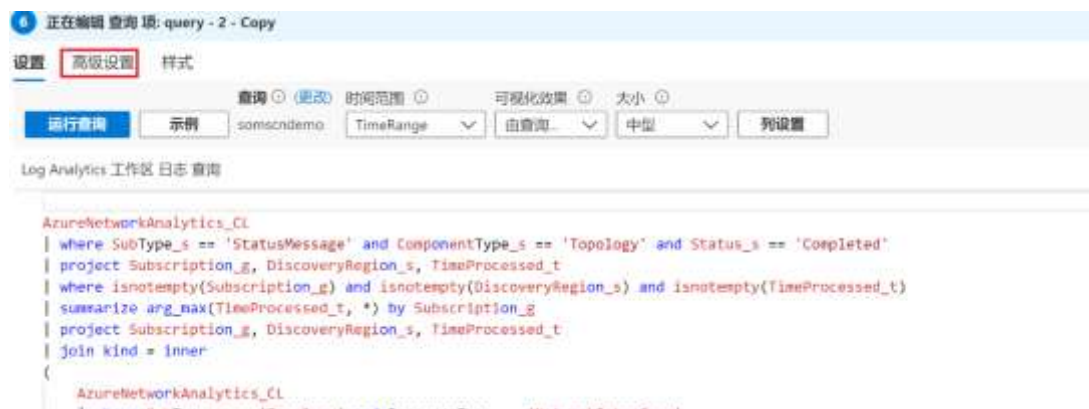
- 1) 在 Azure Portal 的 Log Analytics Workspace 界面，选择“工作簿”。
- 2) 在工作簿库中，点击“Open”，选择导入的工作簿（以 Security 做为命名开头）



- 3) 若要了解此工作簿模板的构成，需要选择“编辑”切换到编辑模式。



- 4) 切换到编辑模式后，你会发现右侧显示了一些“编辑”框，它们对应于工作簿的每个方面。选择需要修改的工作簿表。在 Log Analytics 工作区日志查询中可以修改查询。或者可以点击运行查询来测试。如果需要方便的切换到 Log Analytics 查询页面，点击高级设置。



- 5) 在高级设置中选“为编辑时显示打开外部查询按钮”。



6) 点击完成编辑。



可以看到在对应工作簿表的右上角会出现查询图标。点击查询图标可以跳转到 Log Analytics 查询界面。以便后续可以进一步排查。



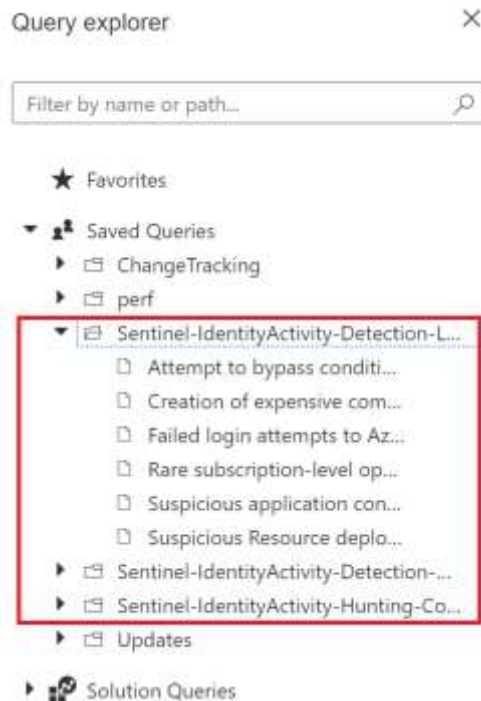
3. 使用导入的查询

1) 在 Azure Portal 的 Log Analytics workspace 界面，选择“日志”。点击“查询资源管理器”。



2) 在“已保存的查询”中，选择以 Security 开头的目录，找到特定的查询
注意：关于 detection 和 hunting 查询的具体定义，可以参考以下的文档：

<https://github.com/simonxin/sentinel-like-queries-for-mooncake/blob/master/query/detectionquery.csv>
<https://github.com/simonxin/sentinel-like-queries-for-mooncake/blob/master/query/huntingquery.csv>



3) 执行

```

29 tostring(parse_json(tostring(InitiatedBy.user)).IpAddress), tostring(parse_json(tostring(InitiatedBy.user)).userPrincipalName),
30 | extend InitiatedBy = iff(isnotempty(tostring(parse_json(tostring(InitiatedBy.user)).userPrincipalName)), tostring(parse_json(tostring(InitiatedBy.user)).userPrincipalName),
31 tostring(parse_json(tostring(InitiatedBy.user)).userPrincipalName), tostring(parse_json(tostring(InitiatedBy.user)).userPrincipalName))
32 | extend TargetResourceName = tolower(tostring(TargetResources.[@].displayName))
33 | parse TargetResources.[@].modifiedProperties with * "ConsentType: " ConsentType "]" *
34 | project TimeGenerated, InitiatedBy, IpAddress, TargetResourceName, Category, OperationName, Co
35 // Exclude previously seen audit activity for "Consent to application" that was seen in the look
36 // First for rare InitiatedBy
37 let RareConsentBy = RecentConsent | join kind= leftanti AuditTrail on OperationName, InitiatedBy
38 | extend Reason = "Previously unseen user consenting";
39 // Second for rare TargetResourceName

```

TimeGenerated [UTC]	InitiatedBy	IpAddress	TargetResourceName	Reason
2020-11-04T02:25:04.239Z	ms-mcsptg-00000000000000000000000000000000			Previously unseen user consenting

4. 如何查询告警的历史记录

可以使用以下的 log analytics 查询语句（请替换 time range 和 rulename 字段）：

```

let timerange = 30d;
let rulename="Detect malicious network flows";
sentinelscanreport_CL
| where type_s =~ "Detection"
| where TimeGenerated > ago(timerange)

```

```
| where rulename_s =~ rulename
| join
    (sentinelscanreportdetails_CL)
    on $left.pid_s == $right.pid_s
| project details = todynamic(details_s)
| evaluate bag_unpack(details)
```

六．配置安全中心告警的自动响应

1. 部署 Logic App

- 1) 下载以下链接中的 ARM 模板

https://github.com/simonxin/sentinel-like-queries-for-mooncake/blob/master/template/logicapp_approledefinition.json

https://github.com/simonxin/sentinel-like-queries-for-mooncake/blob/master/template/logicapp_blockbruteforceattachip.json

https://github.com/simonxin/sentinel-like-queries-for-mooncake/blob/master/template/logicapp_isolateinfectedvm.json

- 2) 执行以下的脚本部署模板（需要替换脚本中的参数-加黄部分）

```
=====
# define initial value
$ResourceGroupName = "<resource_group_for_logicapp>"
$templatefilepath = "<full_path_where_you_downloaded_ARM_Template>"
$location="chinaeast2"

$templatefile1=$templatefilepath+"/Logicapp_blockbruteforceattachip.json"
$templatefile2=$templatefilepath+"/Logicapp_isolateinfectedvm.json"
$templatefile3=$templatefilepath+"/Logicapp_logicapp_approledefinition.json"

$SenderAddress = "<account>n@<o365_tenant>.partner.onmschina.cn"
$recipientAddress = "<notify_email_account>"
$playbookname1 = "block-bruteforceattachip"
$playbookname2 = "isolate-infectedvm"
# note: by default, the logic app will have default name as block-bruteforceattachip
and isolate-infectedvm
```


if you want to use customer name, change the above line to use different name

Define template parameters

```
$params1 = @{  
    SenderAddress = $SenderAddress  
    recipientAddress = $recipientAddress  
    PlaybookName = $playbookname1  
}
```

```
$params2 = @{  
    SenderAddress = $SenderAddress  
    recipientAddress = $recipientAddress  
    PlaybookName = $playbookname2  
}
```

Do deployment

```
$rg = Get-AzResourceGroup -Name $ResourceGroupName -ErrorAction SilentlyContinue  
if ($rg -eq $null) {  
    $rg =New-AzResourceGroup $ResourceGroupName -Location $Location  
}
```

```
New-AzResourceGroupDeployment -ResourceGroupName $ResourceGroupName `  
-TemplateFile $templatefile1 `  
-TemplateParameterObject $params1 `  
-Verbose
```

```
New-AzResourceGroupDeployment -ResourceGroupName $ResourceGroupName `  
-TemplateFile $templatefile2 `  
-TemplateParameterObject $params2 `  
-Verbose
```

Create customized role and grant permissions for first Logic app

```
Connect-AzureAD -AzureEnvironmentName AzureChinaCloud
```

```
$App = Get-AzureADServicePrincipal -Filter "displayName eq '$PlaybookName1'"
```

```
$App.objectID
```

```
$rolepermission = @(  
    "Microsoft.Compute/virtualMachines/read",  
    "Microsoft.Network/networkSecurityGroups/read",  
    "Microsoft.Network/networkSecurityGroups/write",  
    "Microsoft.Network/networkSecurityGroups/securityRules/read",  
    "Microsoft.Network/networkSecurityGroups/securityRules/write",  
    "Microsoft.Network/networkInterfaces/read",
```

```
    "Microsoft.Network/networkInterfaces/effectiveNetworkSecurityGroups/action",
    "Microsoft.Network/virtualNetworks/subnets/read"
)
```

```
$params3 = @{
    PlaybookName = $PlaybookName1
    ObjectID = $App.objectID
    actions = $rolepermission
}
```

```
New-AzDeployment `
-TemplateFile $templatefile3 `
-TemplateParameterObject $params3 `
-Location $Location `
-Verbose
```

```
# Create customized role and grant permissions for second logic app
$App = Get-AzureADServicePrincipal -Filter "displayName eq '$PlaybookName2'"
```

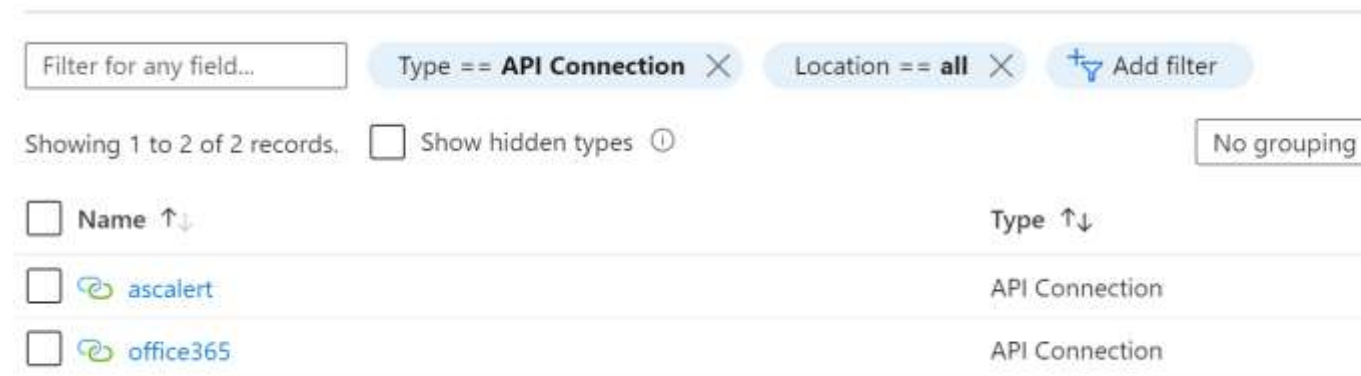
```
$rolepermission = @(
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/securityRules/read",
"Microsoft.Network/networkSecurityGroups/securityRules/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write"
"Microsoft.Network/networkInterfaces/effectiveNetworkSecurityGroups/action",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Compute/virtualMachines/deallocate/*",
"Microsoft.Compute/virtualMachines/start/*",
"Microsoft.Compute/virtualMachines/powerOff/*",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/virtualNetworks/subnets/join/action"

)
```

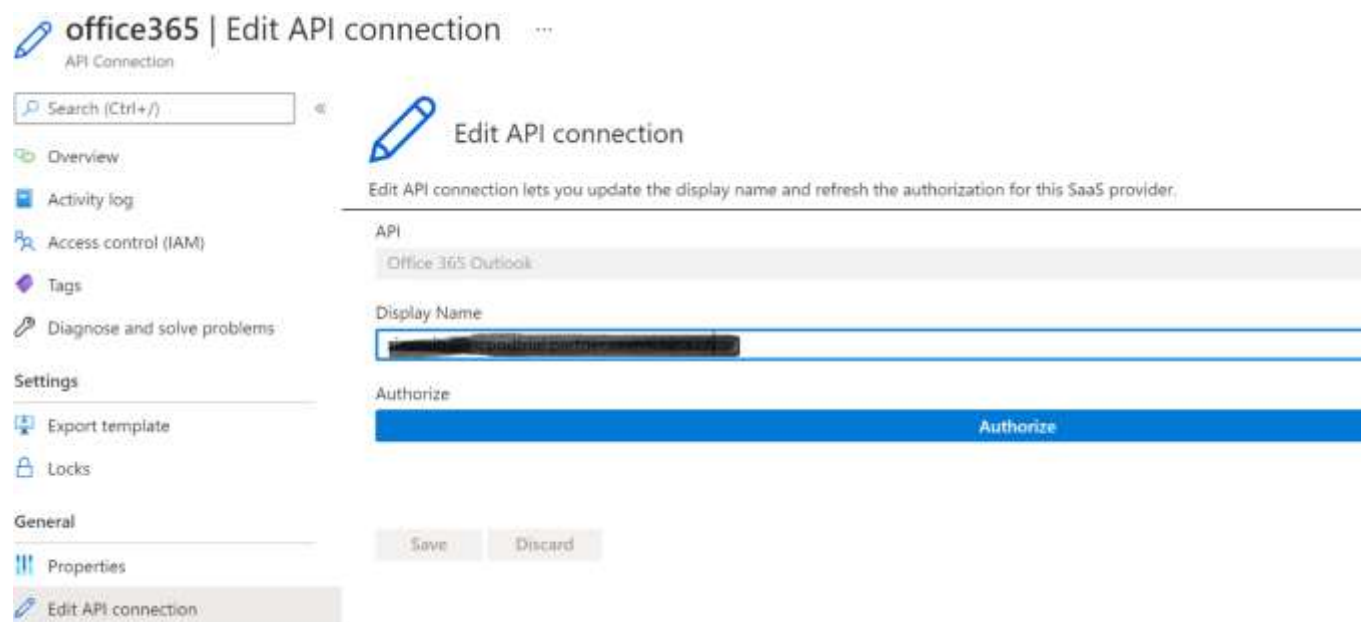
```
$params4 = @{
    PlaybookName = $PlaybookName2
    ObjectID = $App.objectID
    actions = $rolepermission
}
```

```
New-AzDeployment `
-TemplateFile $templatefile2 `
-TemplateParameterObject $params4 `
-Location $location `
-Verbose
```

3) 配置 o365 连接器。在 Azure Portal 中找到之前脚本中部署 logic app 的资源组。找到类型为"API Connection"的资源。缺省的名字为 office365 和 ascalert (如下图):



4) 选中名为 office365 的连接器。在 Edit API connection 页面，点击"Authorize"。



5) 输入你的 Office 365 账号并完成身份验证。完成验证后，点击"Allow Access".

注意：当前版本的 logic app 模板只支持 Office 365 邮箱账号（office 365 中国区账号）。如果你需要使用其他的 Email 连接器，请修改对应 Logic App。

Confirmation required

You are about to provide access to



Office 365 Outlook

to a connection created by user ,

Allow access

Cancel

- 5) 点击"Save"保存设置。

2. 设置安全中心工作流自动化

- 1) 从 Azure Portal 打开安全中心
- 2) 选择工作流自动化界面。选择“添加工作流自动化”:



- 3) 在添加工作流自动化界面。选中名为 block-bruteforceattackip 的 logic app. 在警报名称中， 输入"brute force attack".
完成其他常规属性选择， 点击创建来生成工作流自动化

添加工作流自动化

常规

名称 *

block-malicious-ip ✓

说明

订阅 ①

████████████████████ ✓

资源组 * ①

████████████████████ ✓

触发器条件 ①

选择用于自动触发已配置操作的触发条件。

选择安全中心数据类型 *

威胁检测警报 ✓

警报名称包含 ①

brute force attack ✓

警报严重性 *

已选择所有严重性 ✓

操作

配置将触发的逻辑应用。

选择现有逻辑应用或 [访问“逻辑应用”页](#) 以新建一个

显示以下订阅中的逻辑应用实例 *

████████████████████ ✓

逻辑应用名称 ①

block-bruteforceattackip (安全中心警报连接器) ✓

[刷新](#) [查看逻辑应用](#)

3. 验证工作流自动化

注意： 以下验证适用于 Linux Virtual Machines

1) 请参考以下文档中的内容，对测试 Linux 虚拟机发起模拟 Brute force 攻击

[Azure-Security-Center/Azure Security Center Linux Detections_v2.pdf at main · Azure/Azure-Security-Center \(github.com\)](#)

- 2) 等待一小时，在安全中心应该可以看到名为 **Failed SSH Brute force attack**(或者 **success SSH brute force attack**)的安全告警
- 3) 如果成功， 在 **Logic App** 的运行历史记录中应该可以看到成功的运行记录。



- 4) 作为结果，在被攻击的虚拟机的网络界面，可以看到以下的名为 **BlockBruteForce** 的入站端口规则

Priority	Name	Port	Protocol
100	BlockBruteForce-100	Any	Any
110	Port_443	443	Any

同时，可以收到以下的告警邮件



Azure Security Center

Brute force attack blocked!

Azure Security Center has detected a **Failed SSH brute force attack** on your machine **k8skindvm**. The attack was stopped by blocking the attacking IP address(es) ["52.131.233.242"] in the VM's Network Security Group (NSG). Please review the VM's network configuration and change it if necessary.

Resource details

Resource name	k8skindvm
Subscription ID	01201a80-8016-44ee-8016-4ad88b...ac
Resource type	
Resource location	
Resource ID	

Alert information

Alert name	Failed SSH brute force attack
Description	Failed SSH brute force attacks were detected on k8skindvm
Alert severity	Medium

Action items

1. Click [here](#) to open the alert's details page in Azure Defender.
2. Review the remediation steps and resolve all the issues.
3. If any alert isn't applicable to your resource, a security administrator can suppress further alerts by following the instructions [here](#).

七. 告警响应流程

1. 告警邮件格式

告警邮件按照不同的数据源有不同的格式。
一般的格式如下：

威胁发生时间	2022年03月06日 08:06:42	威胁唯一	202203061205#001
威胁类型	SecurityEvents	威胁来源	Sentinel
威胁名称	AD user enabled and password not set within 48 hours	威胁等级	Low
受影响资源	AccountCustomEntity : [REDACTED] Activity_4722 : 4722 - A user account was enabled. Computer_4722 : [REDACTED] HostCustomEntity : [REDACTED] Reason : User either has not yet attempted to set the initial password after account was enabled or it occurred after 48 hours SubjectAccount_Event4722 : [REDACTED] SubjectUserSid_Event4722 : [REDACTED] TargetAccount : [REDACTED] TargetSid : [REDACTED] Time_Event4722 : 2022-03-04 05:31:43.5570000		
规则说明	标识何时使用默认密码启用帐户，并且密码未在 48 小时内由用户设置。事件 4722 指示帐户已启用，并且在 48 小时内，没有发生事件 4723，表明用户没有尝试设置密码。这将显示 48 小时后发生的任何尝试（成功或失败）。这可能表明将密码设置过期时间太长。建议根据您的情况调整此时间段公司内部政策。		
所属订阅	-		

各个字段的含义：

字段名	字段内容
威胁发生时间	安全规则检测到威胁日志的时间。由于Log Analytics 日志收集的延迟和规则的执行时间的原因，会和实际的安全事件有一定的延迟
威胁类型	安全规则检测的数据源类型
威胁名称	安全规则名称
威胁唯一	告警在 Log Analytics中保存记录的唯一标识
威胁来源	安全规则所属来源（例如：Sentinel, HIDS, DSM, honeypot, AzureSecurityCenter）
威胁等级	威胁等级：High, Medium, Low, information
受影响资源	告警所涉及的资源（账号，IP地址，虚拟机等）
规则说明	安全规则说明
所属订阅	告警所涉及的资源所属订阅

2.查询告警详细信息

通过告警邮件中的“威胁唯一”链接，可以打开 Azure Portal 并跳转到 Azure Log Analytics 查询界面。执行查询可以得到告警的具体信息。

如果查询没有结果，请调整 time range 到合适的区间：

Logs somsdemoworkshop

New Query 1* x +

somsdemoworksh... Select scope Run Time range: Last 7 days Save Share

Tables Queries Functions ... <<

Search

Filter Group by: Solution

Collapse all

Favorites

You can add favorites by clicking on the ☆ icon

- ContainerInsights
- LogManagement
- Network Performance Monitor
- Security and Audit
- SecurityCenterFree
- Update Management
- Custom Logs

```
1 sentinelcanreport_CL
2 | where type_s =~ "Detection" and pid_s =~ "202203051203"
3 | project pid_s, TimeGenerated, rulename_s
4 | join kind=inner
5 | (sentinelcanreportdetails_CL)
6 | on $left.pid_s == $right.pid_s
7 | project details = todynamic(details_s), rulename_s, n...
```

Results Chart Columns Display time (UTC+00:00)

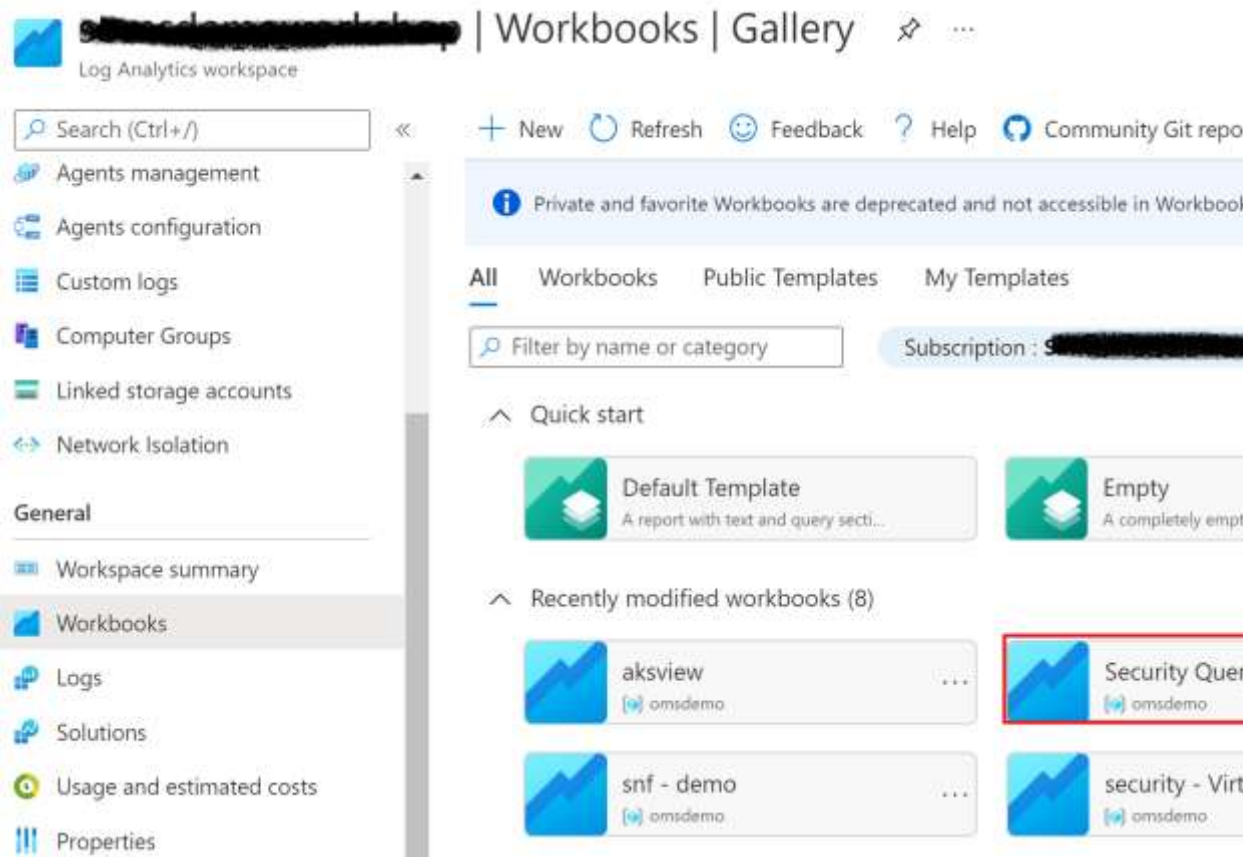
Completed. Showing results from the last 7 days.

TimeGenerated [UTC]	rule_name_s
DisplayName	Rare SVCHOST service group execut
EventTime [UTC]	2022-03-05T11:58:33.31Z
> ExtendedProperties	{"domain name": "██████████", "user na
HostCustomEntity	████████████████████
ProductComponentName	Virtual Machines
ProductName	Microsoft Defender for Cloud
ProviderName	MSTIC
> RemediationSteps	["1. Run Process Explorer and try to
Tactics	DefenseEvasion, Execution

3.使用 hunting rules

1. 使用 hunting rules 得到更多的安全信息

- 1) 在 Azure Portal 中选择 Log Analytics。在 Workbooks 界面, 选择 Security Query Report.



2) 根据威胁类型，选择需要查询的 hunting 安全规则，可以直接查询到相关记录。例如，发现告警规则：“Rare SVCHOST service group executed”，可以检查相关威胁所在时间内， 是否有不正常的本地账号安全组变动。

category: SecurityEvents

hunting rules which to look for more security logs details

Category	↑↓	Last Scan Time	↑↓	Rule Name	↑↓	Rule Category
SecurityEvents		3/10/2022, 8:11:22 AM		Invoke-PowerShellTcpOneLine Usage.		SecurityEvents
SecurityEvents		3/10/2022, 8:11:22 AM		Suspected LSASS Dump		SecurityEvents
SecurityEvents		3/10/2022, 8:11:22 AM		Suspicious Windows Login outside normal hours		SecurityEvents
SecurityEvents		3/10/2022, 8:11:22 AM		User created by unauthorized user		SecurityEvents
SecurityEvents		3/10/2022, 8:11:22 AM		Summary of user logons by logon type		SecurityEvents
SecurityEvents		3/10/2022, 8:11:22 AM		Rare Process Path		SecurityEvents
SecurityEvents		3/10/2022, 8:11:22 AM		New Child Process of W3WP.exe		SecurityEvents
SecurityEvents		3/10/2022, 8:11:22 AM		User account added or removed from a security group by...		SecurityEvents
SecurityEvents		3/10/2022, 8:11:22 AM		Host Exporting Mailbox and Removing Export		SecurityEvents
SecurityEvents		3/10/2022, 8:11:22 AM		Exchange PowerShell Snapin Added		SecurityEvents
SecurityEvents		3/10/2022, 8:11:22 AM		Nishang Reverse TCP Shell in Base64		SecurityEvents

query details

TimeGenerated	↑↓	Computer	↑↓	Account	↑↓
3/9/2022, 3:30:13 PM		[REDACTED]		[REDACTED]	

3) 如果安全规则来源于网络，可以查看 Exploration 列。通过对应的 IP 地址，VM Host name, Account Name 来找到关联信息。

例如：

给定 public IP 发生的所有网络流量

This page is used to show scheduled hunting query report

Security Rule Scan Result Exploration by public IP Exploration by host or local IP Exploration by account name

Time Range: Last 7 days

Ip Address: 40.80.238.189

Traffic Analytics for public IP Address

Calls↑↓	SourceIP	↑↓	DestinationIP	↑↓	Protocol	↑↓	Directory	↑↓	Status	↑↓
16	12.10.0.41		40.80.238.189		http(80)		Out		Allowed	

给定虚拟机产生的所有 internet 网络流量

Security Rule Scan Result Exploration by public IP Exploration by host or local IP Exploration by account name

Time Range: Last 7 days

VM Name: k8skindvm

VM IP Address: 12.10.0.41

Message contains: <unset>

Calls	Source IP	Destination IP	Protocol	Directory	Status
163	12.10.0.41	40.73.172.112	https(443)	Out	Allowed
66	12.10.0.41	151.139.128.10	https(443)	Out	Allowed
66	12.10.0.41	40.80.238.189	http(80)	Out	Allowed
46	12.10.0.41	91.189.91.157	ntp(123)	Out	Allowed
38	12.10.0.41	91.189.89.199	ntp(123)	Out	Allowed
27	12.10.0.41	40.73.192.6	domain(53)	Out	Allowed
24	12.10.0.41	91.189.91.39	http(80)	Out	Allowed

给定账号的登录信息

Security Rule Scan Result Exploration by public IP Exploration by host or local IP Exploration by account name

Time Range: Last 24 hours

AAD Account: [REDACTED]

AAD user login (UPN name required)

Account_UnstructuredName	Account_NTDomain	Account_AadUserId	IP_Address	IP_Location_Country	IP_Location
[REDACTED]	[REDACTED]	[REDACTED]	101.80.153.186	CN	Shanghai S
[REDACTED]	[REDACTED]	[REDACTED]	167.220.255.106	SG	Central Sin
[REDACTED]	[REDACTED]	[REDACTED]	167.220.255.42	SG	Central Sin

Host_Aux_StartTime	Host_Aux_EndTime	Host_UnstructuredName	Host_OSVersion	Host_Aux_Info
3/9/2022, 8:34:26 PM	3/9/2022, 8:34:40 PM	[REDACTED]	Windows	[{"UserDisplayName": "[REDACTED]", "UserPrincipalName": "ch..."}]
3/9/2022, 5:04:17 PM	3/10/2022, 10:30:55 AM	[REDACTED]	Windows 10	[{"UserDisplayName": "[REDACTED]", "UserPrincipalName": "ch..."}]

4.安全响应流程

参考文档:

<https://docs.microsoft.com/zh-cn/security/compass/incident-response-process>

以下是参考步骤：

1) 定义安全处理角色

Operations Roles	Responsibility	Scope	Escalation Path

2) 常规处理分类

威胁来源	类型	Operation Roles	Operations
HIDS	Security Patch		
	Weak Password		
	HIDS security alert		
DSM	DSM security Events		
Honeypot	Honeypot Events		
Sentinel	Network		
	SecurityEvents		
	Syslog		
	WAF		
	AzureFirewall		
	AzureActivity		
	AzureAcitveDirectory		
AzureSecurityCenter	SecurityAlert		

3) 处理流程

对象	常见处理流程	Playbook	Operation Roles
虚拟机	隔离终结点		
	恢复虚拟机和应用		
	虚拟机补丁部署		
IP Address	隔离恶意IP		
	黑/白名单处理		
	Azure Firewall rule		
AAD Accounts	禁用帐户并重置已泄露帐户的密码	密码喷发调查 Microsoft Docs	
Web Apps	快速修正应用漏洞		
	回滚 Devops 操作		

其他	其他自定义操作		
----	---------	--	--