



Curso SC 200

Microsoft Security Operation Analitcs



Curso de Preparação para Realização do Exame de Certificação SC 200.





Instrutor: Célio Ramos

Formação: Graduado em Segurança da Informação e Pós-graduado em Gerenciamento de Projetos e MBA Gestão de Qualidade de Software e 14x Microsoft Azure





Meio de Contato:

Celio Ramos

Senior Presales Solutions Architect |
Membro ANPPD® | Membro ANADD...



never
plan



Certification areas (SC-200)

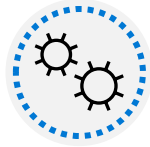
Study areas	Weights
Mitigate threats using Microsoft 365 Defender – OK	25-30%
Mitigate threats using Microsoft Defender for Cloud – OK	25-30%
Mitigate threats using Microsoft Sentinel	40-45%

- This course maps to the exam SC-200: Microsoft Security Operations Analyst
- Percentages indicate the relative weight of each area on the exam.
- The higher the percentage, the more questions you are likely to see in that area.

Agenda



Connect data to Microsoft Sentinel using data connectors



Connect Microsoft services to Microsoft Sentinel



Connect Microsoft 365 Defender to Microsoft Sentinel



Connect Windows hosts to Microsoft Sentinel



Connect Common Event Format logs to Microsoft Sentinel



Connect syslog data sources to Microsoft Sentinel



Connect threat indicators to Microsoft Sentinel

Connect data to Microsoft Sentinel using data connectors



Introduction

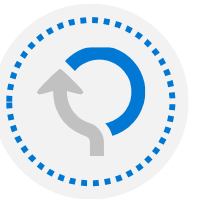
After completing this module, you will be able to:



Explain the use of data connectors in Microsoft Sentinel



Describe the Microsoft Sentinel data connector providers

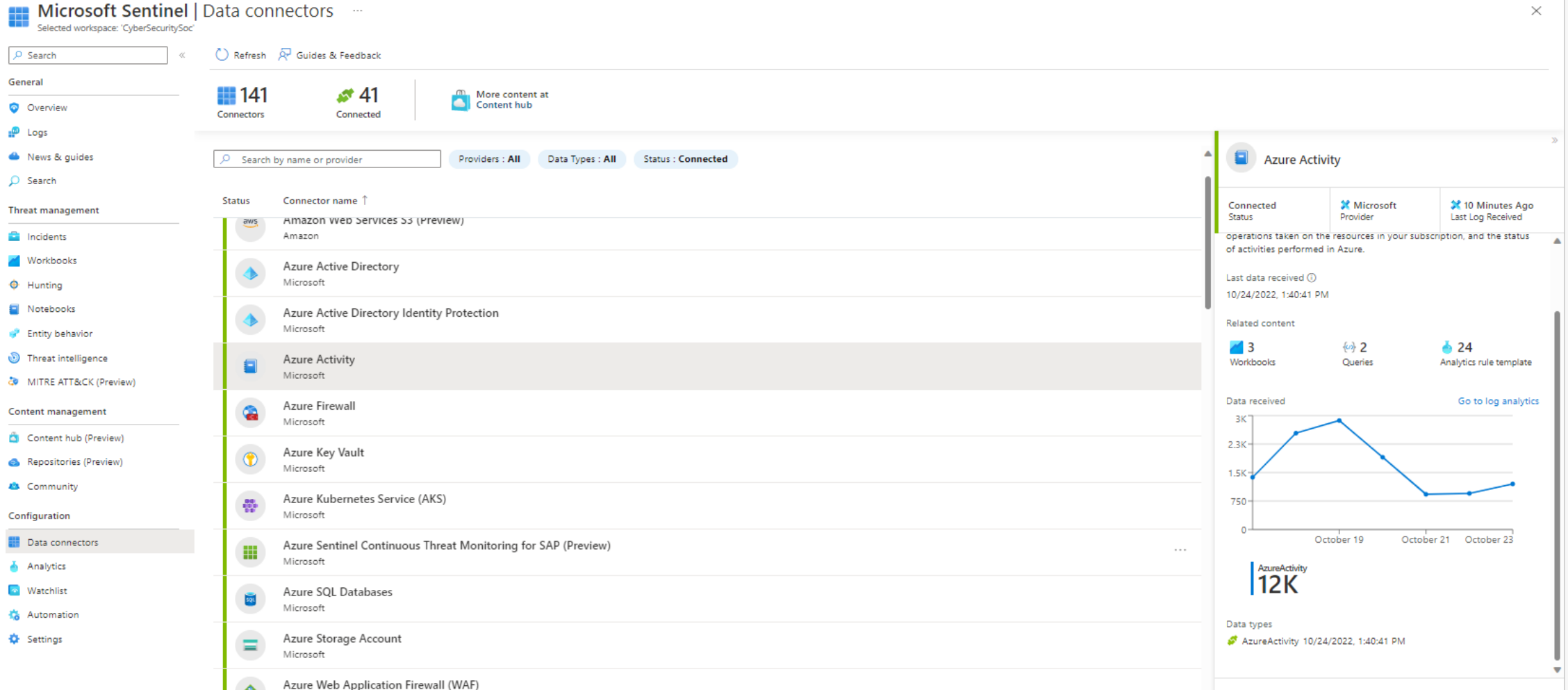


Explain the Common Event Format and Syslog connector differences in Microsoft Sentinel



Ingest log data with Data connectors

Para coletar dados de log, você precisa conectar suas fontes de dados com o Microsoft Sentinel Connectors. A página Conector de Dados mostra os conectores que estão conectados.



Microsoft Sentinel | Data connectors
Selected workspace: 'CyberSecuritySoc'

Search: Refresh Guides & Feedback

General

- Overview
- Logs
- News & guides
- Search

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK (Preview)

Content management

- Content hub (Preview)
- Repositories (Preview)
- Community

Configuration

- Data connectors**
- Analytics
- Watchlist
- Automation
- Settings

Connectors 141 **Connected** 41 [More content at Content hub](#)

Search by name or provider Providers: All Data Types: All Status: Connected

Status	Connector name ↑
Connected	Amazon Web Services S3 (Preview) Amazon
Connected	Azure Active Directory Microsoft
Connected	Azure Active Directory Identity Protection Microsoft
Connected	Azure Activity Microsoft
Connected	Azure Firewall Microsoft
Connected	Azure Key Vault Microsoft
Connected	Azure Kubernetes Service (AKS) Microsoft
Connected	Azure Sentinel Continuous Threat Monitoring for SAP (Preview) Microsoft
Connected	Azure SQL Databases Microsoft
Connected	Azure Storage Account Microsoft
Connected	Azure Web Application Firewall (WAF) Microsoft

Azure Activity

Connected Status Microsoft Provider 10 Minutes Ago Last Log Received

operations taken on the resources in your subscription, and the status of activities performed in Azure.

Last data received ⓘ
10/24/2022, 1:40:41 PM

Related content

3 Workbooks 2 Queries 24 Analytics rule template

Data received [Go to log analytics](#)

3K
2.3K
1.5K
750
0

October 19 October 21 October 23

AzureActivity
12K

Data types
AzureActivity 10/24/2022, 1:40:41 PM

Describe data connector providers



Microsoft 365 Defender and related Defender services



Microsoft 365 and Azure Services



Vendor connectors



Custom connectors (see next slide)



Common Event Format (CEF) and Syslog connector

Describe data connector providers - continued

Custom Connectors



Codeless Connector Platform (CCP)



Log Analytics Agent



Logstash plugin



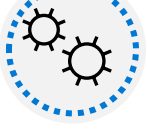
Logic Apps



PowerShell



The Log Analytics API



Azure Functions

Connect Microsoft services to Microsoft Sentinel



Introduction

After completing this module, you will be able to:



Connect Microsoft service connectors



Explain how connectors auto-create incidents in Microsoft Sentinel



Connect the Microsoft Office 365 connector

The Office 365 activity log connector provides insight into ongoing user activities. You will get details of operations such as file downloads, access requests sent, changes to group events, set-mailbox, and details of the user who performed the actions.

Microsoft Azure Search resources, services, and docs (G+/)

Home > Microsoft Sentinel > Microsoft Sentinel > Office 365

Office 365

Office 365

Not connected Status | Microsoft Provider | -- Last Log Received

Description
The Office 365 activity log connector provides insight into ongoing user activities. You will get details of operations such as file downloads, access requests sent, changes to group events, set-mailbox and details of the user who performed the actions. By connecting Office 365 logs into Microsoft Sentinel you can use this data to view dashboards, create custom alerts, and improve your investigation process.

Last data received
--

Related content
7 Workbooks | 3 Queries | 32 Analytics rules templates

Data received
100
80
60
40
20
0
November 23 November 25 November 27
Total data received Total data received Total data received
0 0 0
Go to log analytics
SharePoint
Exchange
Teams

Instructions Next steps

Prerequisites

To integrate with Office 365 make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Tenant Permissions:** required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.

Configuration

Connect Office 365 activity logs to your Microsoft Sentinel.
Select the record types you want to collect from your tenant and click **Apply Changes**.

☐ Exchange
☐ SharePoint
☐ Teams

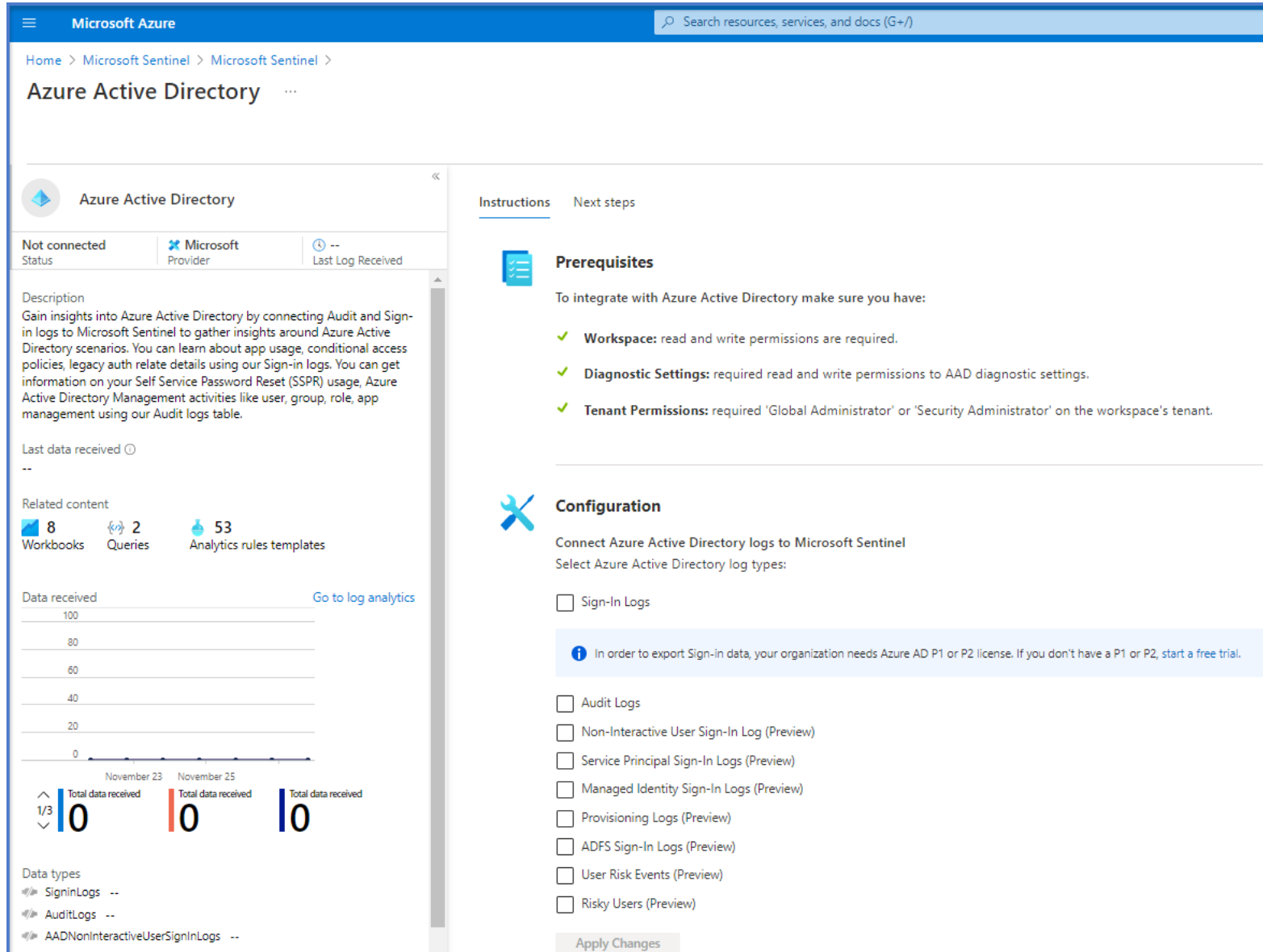
Apply Changes

2. Previously connected tenants
Microsoft Sentinel now enables Office 365 single-tenant connection. You can modify your previously connected tenants and click **Save**.

Save Refresh

Connect the Azure Active Directory connector

Gain insights into Azure Active Directory by connecting Audit and Sign in logs to Microsoft Sentinel to gather insights around Azure Active Directory scenarios.



The screenshot displays the Microsoft Azure portal interface for connecting the Azure Active Directory (AAD) connector to Microsoft Sentinel. The page is titled "Azure Active Directory" and shows the connector's status as "Not connected".

Instructions

Prerequisites

To integrate with Azure Active Directory make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Diagnostic Settings:** required read and write permissions to AAD diagnostic settings.
- ✓ **Tenant Permissions:** required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.

Configuration

Connect Azure Active Directory logs to Microsoft Sentinel

Select Azure Active Directory log types:

- ☐ Sign-In Logs
- ☐ Audit Logs
- ☐ Non-Interactive User Sign-In Log (Preview)
- ☐ Service Principal Sign-In Logs (Preview)
- ☐ Managed Identity Sign-In Logs (Preview)
- ☐ Provisioning Logs (Preview)
- ☐ ADFS Sign-In Logs (Preview)
- ☐ User Risk Events (Preview)
- ☐ Risky Users (Preview)

[In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, start a free trial.](#)

[Apply Changes](#)

Data received

100
80
60
40
20
0

November 23 November 25

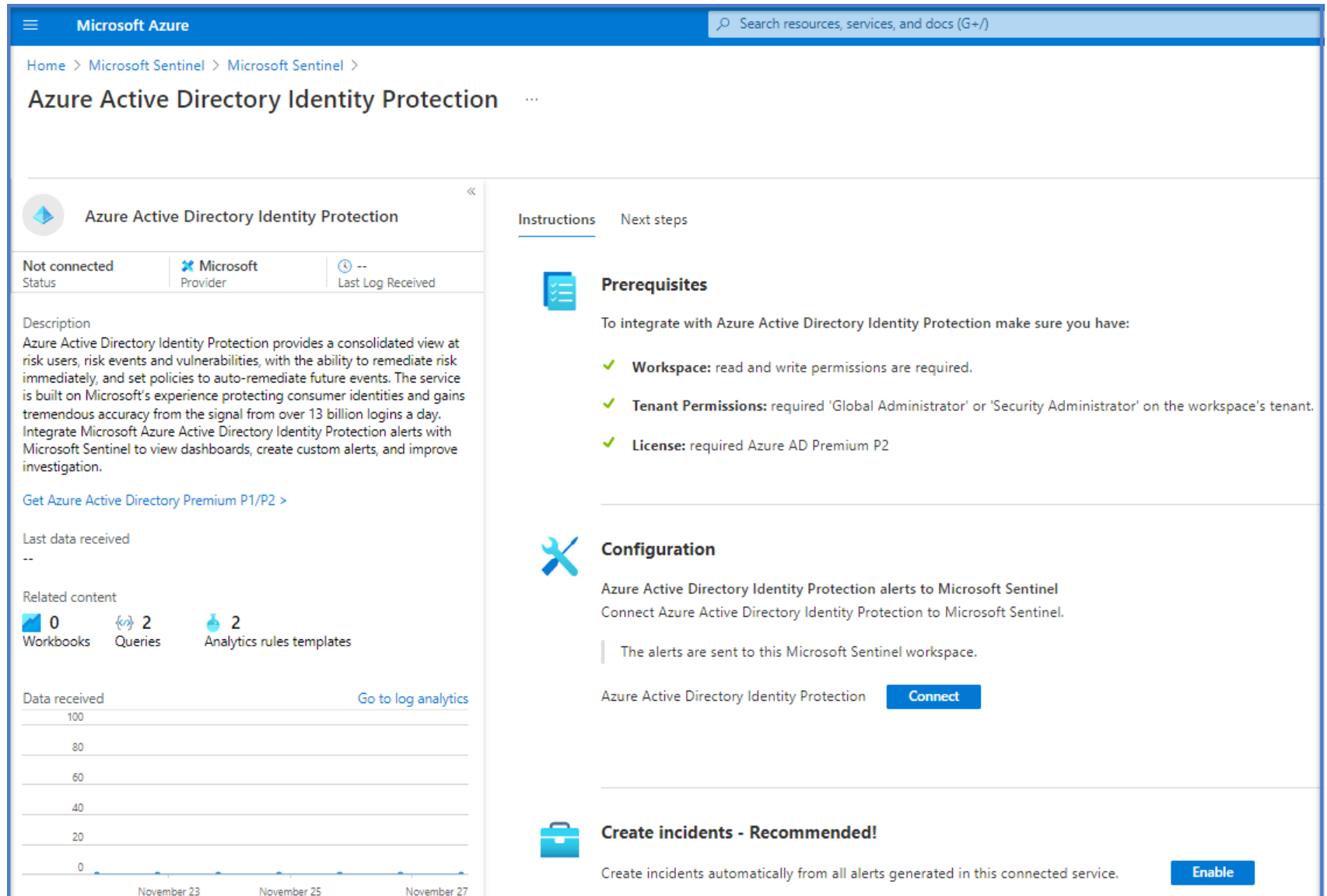
Total data received 0 Total data received 0 Total data received 0

Data types

- SignInLogs --
- AuditLogs --
- AADNonInteractiveUserSignInLogs --

Connect the Azure Active Directory Identity Protection connector

Azure Active Directory Identity Protection provides a consolidated view of at-risk users, risk events, and vulnerabilities, with the ability to remediate risk immediately and set policies to auto remediate future events.



The screenshot displays the Microsoft Azure portal interface for the Azure Active Directory Identity Protection connector. The top navigation bar shows the Microsoft Azure logo and a search bar. The breadcrumb trail indicates the path: Home > Microsoft Sentinel > Microsoft Sentinel > Azure Active Directory Identity Protection. The main heading is "Azure Active Directory Identity Protection".

The connector status is "Not connected". The provider is "Microsoft". The last log received is "--".

Description
Azure Active Directory Identity Protection provides a consolidated view at risk users, risk events and vulnerabilities, with the ability to remediate risk immediately, and set policies to auto-remediate future events. The service is built on Microsoft's experience protecting consumer identities and gains tremendous accuracy from the signal from over 13 billion logins a day. Integrate Microsoft Azure Active Directory Identity Protection alerts with Microsoft Sentinel to view dashboards, create custom alerts, and improve investigation.

[Get Azure Active Directory Premium P1/P2 >](#)

Last data received: --

Related content

- 0 Workbooks
- 2 Queries
- 2 Analytics rules templates

Data received [Go to log analytics](#)

The data received chart shows a line graph with the y-axis ranging from 0 to 100 and the x-axis showing dates from November 23 to November 27. The data points are all at 0.

Instructions [Next steps](#)

Prerequisites

To integrate with Azure Active Directory Identity Protection make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Tenant Permissions:** required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.
- ✓ **License:** required Azure AD Premium P2

Configuration

Azure Active Directory Identity Protection alerts to Microsoft Sentinel
Connect Azure Active Directory Identity Protection to Microsoft Sentinel.

The alerts are sent to this Microsoft Sentinel workspace.

Azure Active Directory Identity Protection [Connect](#)

Create incidents - Recommended!

Create incidents automatically from all alerts generated in this connected service. [Enable](#)

Other Azure related connectors



Azure Activity



Azure DDoS Protection



Azure Firewall



Azure Key Vault



Azure SQL Databases



Azure Web Application Firewall

Connect Microsoft 365 Defender to Microsoft Sentinel



Introduction

After completing this module, you will be able to:



Activate the Microsoft 365 Defender connector in Microsoft Sentinel



Activate the Microsoft Defender for Cloud connector in Microsoft Sentinel



Plan for Microsoft 365 Defender connectors



Microsoft 365 Defender (Preview)



Microsoft Defender for Office 365 (Preview)



Microsoft Defender Legacy connectors



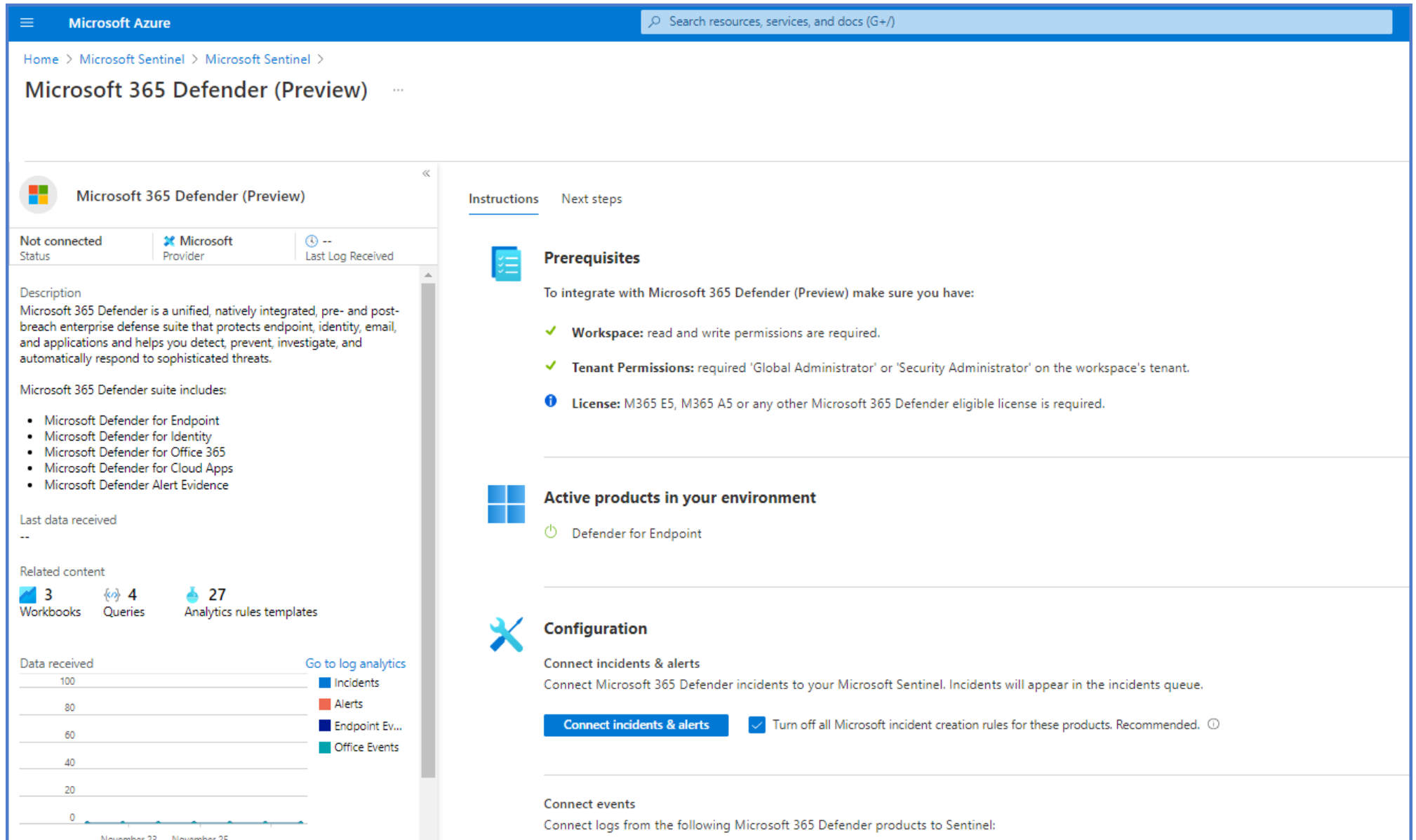
Microsoft Defender for Cloud



Microsoft Defender for IoT

Connect the Microsoft 365 Defender connector


O conector do Microsoft 365 Defender permite que você transmita logs de caça avançados - um tipo de dados brutos de eventos - do Microsoft 365 Defender.



Microsoft Azure Search resources, services, and docs (G+/I)

Home > Microsoft Sentinel > Microsoft Sentinel >

Microsoft 365 Defender (Preview) ...

**Microsoft 365 Defender (Preview)**

Not connected
Status

Microsoft
Provider

--
Last Log Received

Description

Microsoft 365 Defender is a unified, natively integrated, pre- and post-breach enterprise defense suite that protects endpoint, identity, email, and applications and helps you detect, prevent, investigate, and automatically respond to sophisticated threats.


Microsoft 365 Defender suite includes:


- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender Alert Evidence


Last data received

--

Related content

 **3**
Workbooks

 **4**
Queries

 **27**
Analytics rules templates

Data received

Go to log analytics

100
80
60
40
20
0

Incidents
Alerts
Endpoint Ev...
Office Events

Instructions Next steps

Prerequisites

To integrate with Microsoft 365 Defender (Preview) make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Tenant Permissions:** required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.
- ! **License:** M365 E5, M365 A5 or any other Microsoft 365 Defender eligible license is required.

Active products in your environment

Defender for Endpoint

Configuration

Connect incidents & alerts

Connect Microsoft 365 Defender incidents to your Microsoft Sentinel. Incidents will appear in the incidents queue.

Connect incidents & alerts ☒ Turn off all Microsoft incident creation rules for these products. Recommended. ⓘ

Connect events

Connect logs from the following Microsoft 365 Defender products to Sentinel:

Connect alerts from Microsoft Defender for Office 365

Com os alertas do Microsoft Defender para Office 365, você pode incorporar informações sobre ameaças baseadas em email e URL em sua análise de risco mais ampla e criar cenários de resposta de acordo.

The screenshot displays the Microsoft Azure portal interface for configuring Microsoft Defender for Office 365 (Preview). The top navigation bar shows the Microsoft Azure logo and a search bar. The breadcrumb trail indicates the path: Home > Microsoft Sentinel > Microsoft Sentinel > Microsoft Defender for Office 365 (Preview).

The main content area is divided into two sections: **Instructions** and **Next steps**. The **Instructions** section is currently active and contains the following information:

- Prerequisites:** To integrate with Microsoft Defender for Office 365 (Preview) make sure you have:
 - ✓ **Workspace:** read and write permissions are required.
 - ✓ **Tenant Permissions:** required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.
 - ✓ **License:** required Microsoft Defender for Office 365 Plan 2 (included with the Office 365 E5, Office 365 A5, and Microsoft 365 E5 licenses, and available for purchase separately)
- Configuration:** Connect Microsoft Defender for Office 365 alerts to Microsoft Sentinel. Connecting Microsoft Defender for Office 365 will cause your data that is collected by Microsoft Defender for Office 365 service to be stored and processed in the location that you have configured your Microsoft Sentinel workspace.

A **Connect** button is visible under the Configuration section. Below it, a note states: "Microsoft Defender for Office 365 (Preview) alerts are connected through the Microsoft 365 Defender connector and automatically grouped into incidents. Incidents can be seen in the incidents queue."

The **Create incidents - Recommended!** section at the bottom suggests creating incidents automatically from all alerts generated in this connected service, with an **Enable** button.

The sidebar on the left provides additional context and navigation options:

- Microsoft Defender for Office 365 (Preview)** status: Not connected, Microsoft Provider, Last Log Received: --.
- Description:** Microsoft Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links (URLs) and collaboration tools. By ingesting Microsoft Defender for Office 365 alerts into Microsoft Sentinel, you can incorporate information about email- and URL-based threats into your broader risk analysis and build response scenarios accordingly.
- The following types of alerts will be imported:**
 - A potentially malicious URL click was detected
 - Email messages containing malware removed after delivery
 - Email messages containing phishing URLs removed after delivery
 - Email reported by user as malware or phishing
 - Suspicious email sending patterns detected
 - User restricted from sending email
- These alerts can be seen by Office customers in the Office Security and Compliance Center.**
- Last data received:** --
- Related content:**
 - 0 Workbooks
 - 1 Queries
 - 2 Analytics rules templates
- Data received:** 100 (Go to log analytics)

Legacy Connectors

- Microsoft Defender para Endpoint

- Microsoft Defender para Office 365

- Microsoft Defender para Aplicativos em Nuvem

- Microsoft Defender para Identidade

The screenshot displays the Microsoft Azure portal interface for configuring the Microsoft Defender for Endpoint connector. The top navigation bar shows the Microsoft Azure logo and a search bar. The breadcrumb trail indicates the path: Home > Microsoft Sentinel > Microsoft Sentinel > Microsoft Defender for Endpoint. The main content area is divided into two columns. The left column contains a summary card for the connector, showing its status as 'Not connected', the provider as 'Microsoft', and the last log received as '--'. Below this, there is a description of the connector, a section for 'Last data received' showing '--', and a 'Related content' section with links to '0 Workbooks', '1 Queries', and '3 Analytics rules templates'. At the bottom of the left column is a 'Data received' chart showing a line graph with data points for November 23, 25, and 27, and a 'Total data received' count of 0. The right column contains instructions and configuration steps. The 'Instructions' tab is active, showing 'Prerequisites' (Workspace, Tenant Permissions, License) and 'Configuration' (Connect Microsoft Defender for Endpoint alerts to Microsoft Sentinel). A 'Connect' button is visible next to the 'Microsoft Defender for Endpoint alerts' text. Below the configuration section, there is a 'Create incidents - Recommended!' section with an 'Enable' button.

Microsoft Azure

Search resources, services, and docs (G+/I)

Home > Microsoft Sentinel > Microsoft Sentinel > Microsoft Defender for Endpoint

Microsoft Defender for Endpoint

Not connected Status

Microsoft Provider

Last Log Received

Description

Microsoft Defender for Endpoint is a security platform designed to prevent, detect, investigate, and respond to advanced threats. The platform creates alerts when suspicious security events are seen in an organization. Fetch alerts generated in Microsoft Defender for Endpoint to Microsoft Sentinel so that you can effectively analyze security events. You can create rules, build dashboards and author playbooks for immediate response.

Last data received

--

Related content

0 Workbooks

1 Queries

3 Analytics rules templates

Data received

Go to log analytics

100

80

60

40

20

0

November 23

November 25

November 27

Total data received

0

Instructions

Next steps

Prerequisites

To integrate with Microsoft Defender for Endpoint make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Tenant Permissions:** required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.
- ✓ **License:** requires Microsoft Defender for Endpoint.

Configuration

Connect Microsoft Defender for Endpoint alerts to Microsoft Sentinel

Connecting Microsoft Defender for Endpoint will cause your data that is collected by Microsoft Defender for Endpoint service to be stored and processed in the workspace.

Microsoft Defender for Endpoint alerts

Connect

Microsoft Defender for Endpoint Advanced Hunting raw logs are available as part of the Microsoft 365 Defender (Preview) connector

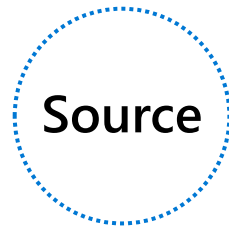
Create incidents - Recommended!

Create incidents automatically from all alerts generated in this connected service.

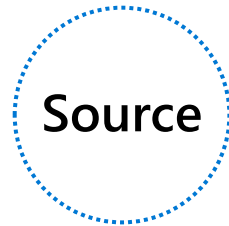
Enable

Connect other Microsoft Defender connectors

O Microsoft Sentinel fornece conectores internos para outras soluções do Microsoft Defender.



Microsoft Defender for Cloud



Microsoft Defender for IoT

Connect Windows hosts to Microsoft Sentinel



Introduction

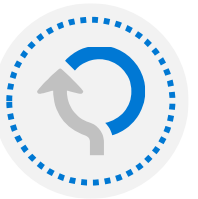
After completing this module, you will be able to:



Connect Azure Windows Virtual Machines to Microsoft Sentinel



Connect non-Azure Windows hosts to Microsoft Sentinel



Configure agent to collect Sysmon events



Planejar o conector de eventos de segurança dos hosts do Windows

Ingestion Options

Windows Security Events via
AMA Connector

Security Events via Legacy
Agent Connector

Windows Forwarded Events
(Preview) connector

Windows DNS Events via
AMA (Preview) Connector

Windows Security Events via AMA Connector

Benefits:

- Gerenciar configurações de coleção em escala
- Agente de Monitoramento do Azure compartilhado com outras soluções
- Melhorias de desempenho
- Melhorias de segurança

Limitations:

- Em Visualização pública do Microsoft Defender para Nuvem
- Nem todos os recursos estão disponíveis no momento
-

Requirements:

- Regras de Coleta de Dados (DCR)
- VMs/dispositivos que não sejam do Azure exigem o Azure Arc
-

Security Events via Legacy Agent Connector

Microsoft Azure

Search resources, services, and docs (G+/I)

Home > Microsoft Sentinel > Microsoft Sentinel >

Security Events via Legacy Agent

Security Events via Legacy Agent

Not connected
Status

Microsoft
Provider

--
Last Log Received

Description

You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

Last data received
--

Related content

9
Workbooks

1
Queries

73
Analytics rules templates

Data received

Go to log analytics

10

Total data received

Data types

SecurityEvents --

Instructions

Next steps

Prerequisites

To integrate with Security Events via Legacy Agent make sure you have:

✓ **Workspace:** read and write permissions are required.

✓ **Workspace data sources:** read and write permissions are required.

Configuration

1. Download and install the agent

Security Events logs are collected only from **Windows** agents.

Choose where to install the agent:

✓ Install agent on Azure Windows Virtual Machine

✓ Install agent on non-Azure Windows Machine

2. Select which events to stream

All events - All Windows security and AppLocker events.

Common - A standard set of events for auditing purposes.

Minimal - A small set of events that might indicate potential threats. By enabling this option, you won't be able to have a full audit trail.

None - No security or AppLocker events.

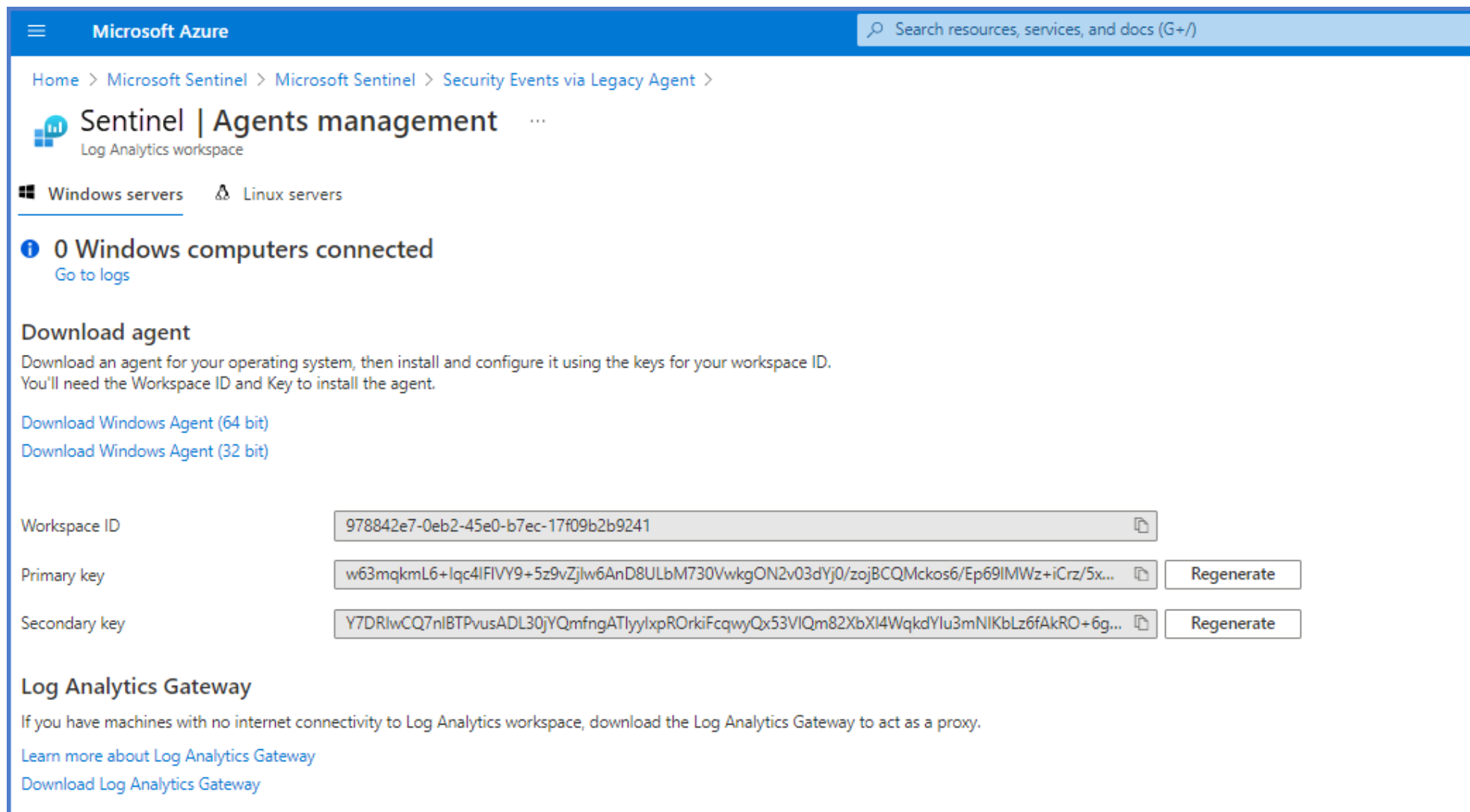
☒ None ☐ Minimal ☐ Common ☐ All Events

Apply Changes

Copyright Microsoft Corporation. All rights reserved.

Connect non-Azure Windows Machines

Ao conectar hosts Windows que não sejam do Azure, você precisa instalar manualmente o agente do cliente.



The screenshot displays the Microsoft Sentinel 'Agents management' page. At the top, the navigation bar includes the Microsoft Azure logo and a search bar. The breadcrumb trail reads: Home > Microsoft Sentinel > Microsoft Sentinel > Security Events via Legacy Agent >. The main heading is 'Sentinel | Agents management' with a sub-label 'Log Analytics workspace'. Below this, there are tabs for 'Windows servers' (selected) and 'Linux servers'. A status indicator shows '0 Windows computers connected' with a 'Go to logs' link. The 'Download agent' section provides instructions: 'Download an agent for your operating system, then install and configure it using the keys for your workspace ID. You'll need the Workspace ID and Key to install the agent.' It offers links to 'Download Windows Agent (64 bit)' and 'Download Windows Agent (32 bit)'. Below these are fields for 'Workspace ID' (978842e7-0eb2-45e0-b7ec-17f09b2b9241), 'Primary key' (w63mqkmL6+lqc4lFIVY9+5z9vZjIw6AnD8ULbM730VwkgON2v03dYj0/zojBCQMckos6/Ep69IMWz+iCrz/5x...), and 'Secondary key' (Y7DRlwCQ7nIBTPvusADL30jYQmfngATlyylxpROrkIFcqwyQx53VIQm82XbXI4WqkdYlu3mNIKbLz6fAkRO+6g...). Each key field has a 'Regenerate' button. The 'Log Analytics Gateway' section explains that if machines lack internet connectivity, the gateway can act as a proxy, with links to 'Learn more about Log Analytics Gateway' and 'Download Log Analytics Gateway'.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Microsoft Sentinel > Microsoft Sentinel > Security Events via Legacy Agent >

Sentinel | Agents management
Log Analytics workspace

Windows servers Linux servers

0 Windows computers connected
[Go to logs](#)

Download agent
Download an agent for your operating system, then install and configure it using the keys for your workspace ID. You'll need the Workspace ID and Key to install the agent.

[Download Windows Agent \(64 bit\)](#)
[Download Windows Agent \(32 bit\)](#)

Workspace ID: 978842e7-0eb2-45e0-b7ec-17f09b2b9241

Primary key: w63mqkmL6+lqc4lFIVY9+5z9vZjIw6AnD8ULbM730VwkgON2v03dYj0/zojBCQMckos6/Ep69IMWz+iCrz/5x... [Regenerate](#)

Secondary key: Y7DRlwCQ7nIBTPvusADL30jYQmfngATlyylxpROrkIFcqwyQx53VIQm82XbXI4WqkdYlu3mNIKbLz6fAkRO+6g... [Regenerate](#)

Log Analytics Gateway
If you have machines with no internet connectivity to Log Analytics workspace, download the Log Analytics Gateway to act as a proxy.

[Learn more about Log Analytics Gateway](#)
[Download Log Analytics Gateway](#)

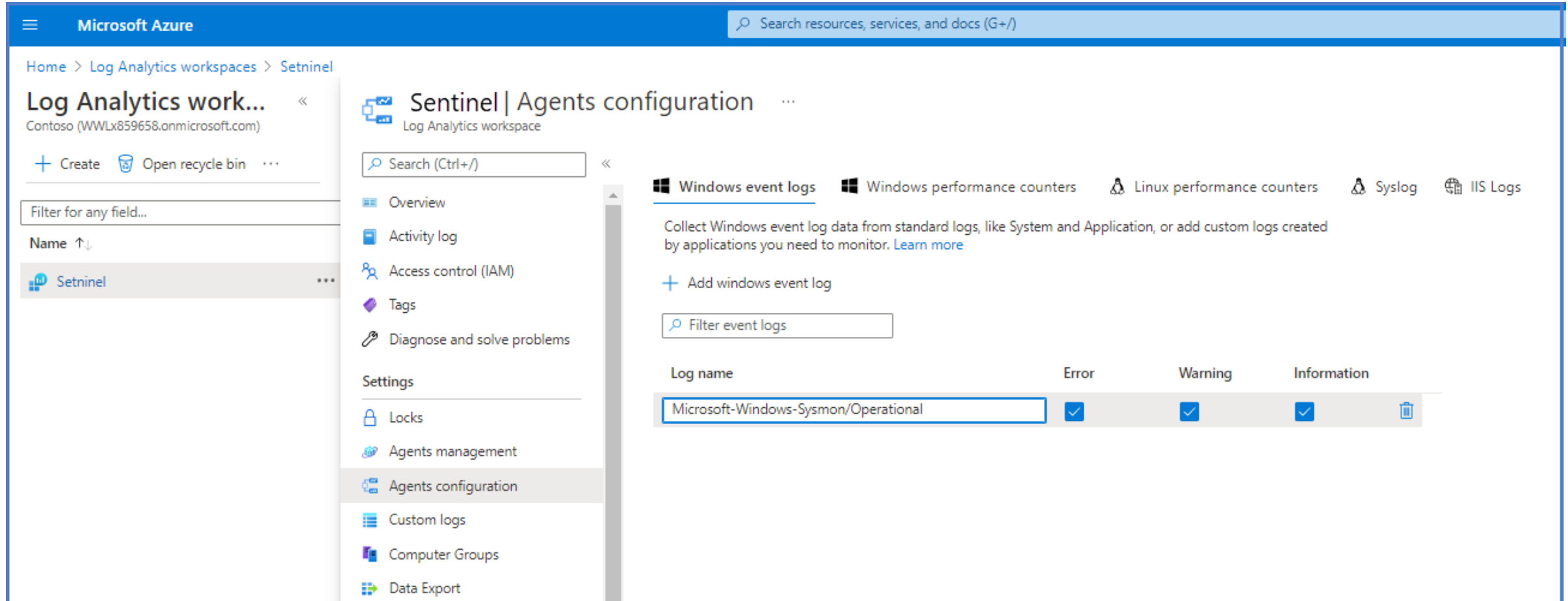
View connected hosts

- O número de hosts Windows e Linux conectados ao Agente do Azure Monitor ou ao agente do Log Analytics está disponível no espaço de trabalho do Log Analytics.
- Você pode exibir os hosts conectados na página Gerenciamento de Agentes de Espaço de Trabalho do Log Analytics.

The screenshot displays the 'CyberSecuritySOC | Agents management' interface within a 'Log Analytics workspace'. On the left, a sidebar contains a search bar and a list of navigation items: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Locks, and Agents management (which is highlighted). The main content area is titled 'Windows servers' and 'Linux servers'. It shows two status cards: '3 Windows computers connected via Azure Monitor Windows agent' and '20 Windows computers connected via Log Analytics Windows agent (legacy)'. Both cards include a green checkmark icon and a link to 'See them in Logs'. Below these cards, there is a prompt: 'Want to setup the new Azure Monitor agent? Go to 'Data Collection Rules'', followed by a blue button labeled 'Data Collection Rules'. At the bottom, there is a section titled 'Log Analytics agent instructions' with a downward arrow icon.

Collect Sysmon event logs

A entrada Microsoft-Windows-Sysmon/Operational é necessária nos logs de eventos do Windows.



The screenshot shows the Microsoft Azure Sentinel interface. The left sidebar contains the navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Locks, Agents management, Agents configuration (selected), Custom logs, Computer Groups, and Data Export. The main content area is titled 'Sentinel | Agents configuration' and shows the configuration for Windows event logs. A table lists the logs to be collected, with 'Microsoft-Windows-Sysmon/Operational' highlighted. The table has columns for Log name, Error, Warning, and Information, all of which are checked for the selected log.

Log name	Error	Warning	Information
Microsoft-Windows-Sysmon/Operational	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Connect Common Event Format logs to Microsoft Sentinel



Introduction

After completing this module, you will be able to:



Explicar as opções de implantação do conector Common Event Format no Microsoft Sentinel



Executar o script de implantação para o conector Common Event Format



Plan for Common Event Format (CEF) connector



Implanta um servidor Syslog Forwarder para oferecer suporte à comunicação entre o dispositivo e o Microsoft Sentinel.



O servidor consiste em uma máquina Linux dedicada com o agente Log Analytics para Linux instalado.



Muitos dos conectores de dados do Microsoft Sentinel que são específicos do fornecedor utilizam o conector CEF.



As opções de implantação incluem o Azure e o local.



O CEF é recomendado sobre o conector Syslog porque o CEF fornece dados de mensagem analisados

Connect your external solution using the CEF connector

Usando o link fornecido na página do conector, você executará um script na máquina designada.

Microsoft Azure Search resources, services, and docs (G+/I)

Home > Microsoft Sentinel > Microsoft Sentinel > Common Event Format (CEF) ...

Common Event Format (CEF)

Not connected Status Any Provider Last Log Received --

Description
Common Event Format (CEF) is an industry standard format on top of Syslog messages, used by many security vendors to allow event interoperability among different platforms. By connecting your CEF logs to Microsoft Sentinel, you can take advantage of search & correlation, alerting, and threat intelligence enrichment for each log.

Last data received --

Related content
0 Workbooks 1 Queries 14 Analytics rules templates

Data received Go to log analytics
100
80
60
40
20
0
November 23 November 25 November 27

Total data received
0

Data types
CommonSecurityLog --

Instructions Next steps

Prerequisites

To integrate with Common Event Format (CEF) make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Keys:** read permissions to shared keys for the workspace are required. [See the documentation to learn more.](#)

Configuration

1. Linux Syslog agent configuration

Install and configure the Linux agent to collect your Common Event Format (CEF) Syslog messages and forward them to Microsoft Sentinel.

Notice that the data from all regions will be stored in the selected workspace

1.1 Select or create a Linux machine

Select or create a Linux machine that Microsoft Sentinel will use as the proxy between your security solution and the CEF collector.

1.2 Install the CEF collector on the Linux machine

Install the Microsoft Monitoring Agent on your Linux machine and configure the machine to listen on the CEF collector port.

1. Make sure that you have Python on your machine using the following command: `python --version`
2. You must have elevated permissions (sudo) on your machine.

Run the following command to install and apply the CEF collector:

```
sudo wget -O cef_installer.py https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/scripts/cef_installer.py
```

Connect syslog data sources to Microsoft Sentinel



Plan for the syslog connector

Overview

Transmita eventos de máquinas ou dispositivos baseados em Linux e compatíveis com Syslog para o Microsoft Sentinel usando o agente do Log Analytics para Linux.

O daemon Syslog nativo do host coletará eventos locais dos tipos especificados e os encaminhará localmente para o agente, que os transmitirá para o espaço de trabalho do Log Analytics.

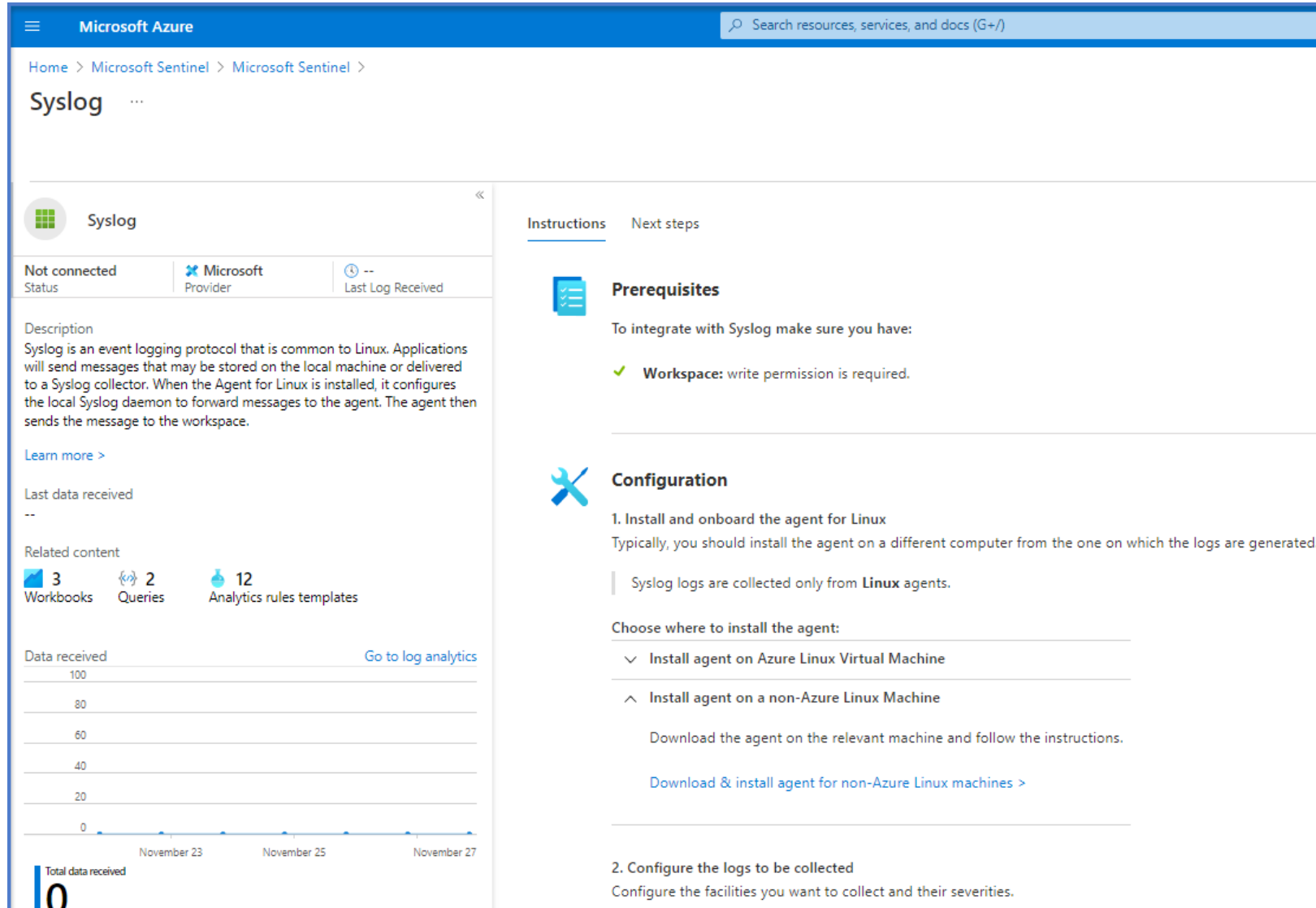
How it works

Syslog é um protocolo de log de eventos que é comum ao Linux. Quando o agente do Log Analytics para Linux é instalado na VM ou no dispositivo, a rotina de instalação configura o daemon Syslog local para encaminhar mensagens ao agente na porta TCP 25224.

Em seguida, o agente envia a mensagem para o espaço de trabalho do Log Analytics por HTTPS, onde é analisada em uma entrada de log de eventos no Syslog table in *Microsoft Sentinel > Logs*.

Collect data from Linux-based sources using syslog

O conector Syslog tem duas opções de implantação: Máquina Virtual Linux do Azure e agente em uma Máquina Linux que não seja do Azure. A VM Linux do Azure é um simples botão de conexão.



The screenshot displays the Microsoft Azure portal interface for the Syslog connector. The top navigation bar shows the Microsoft Azure logo and a search bar. The breadcrumb trail indicates the path: Home > Microsoft Sentinel > Microsoft Sentinel > Syslog. The main content area is divided into two columns. The left column contains a Syslog connector card with a green grid icon. It shows a status of 'Not connected', the provider as 'Microsoft', and the last log received as '--'. Below this is a description of Syslog as an event logging protocol. Further down, there are links for 'Learn more', 'Last data received' (showing '--'), and 'Related content' which includes 3 Workbooks, 2 Queries, and 12 Analytics rules templates. At the bottom of the left column is a 'Data received' chart showing a bar graph with a value of 100 and a 'Go to log analytics' link. The right column has tabs for 'Instructions' and 'Next steps'. Under 'Instructions', there are sections for 'Prerequisites' (noting that write permission is required for the workspace) and 'Configuration'. The configuration section lists two steps: 1. Install and onboard the agent for Linux, with a note that logs are collected only from Linux agents, and 2. Configure the logs to be collected. Step 1 includes a dropdown menu with options to 'Install agent on Azure Linux Virtual Machine' and 'Install agent on a non-Azure Linux Machine', followed by a link to download and install the agent for non-Azure Linux machines.

Microsoft Azure

Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Microsoft Sentinel > Syslog

Syslog

Not connected
Status

Microsoft
Provider

--
Last Log Received

Description
Syslog is an event logging protocol that is common to Linux. Applications will send messages that may be stored on the local machine or delivered to a Syslog collector. When the Agent for Linux is installed, it configures the local Syslog daemon to forward messages to the agent. The agent then sends the message to the workspace.

Learn more >

Last data received
--

Related content
3 Workbooks 2 Queries 12 Analytics rules templates

Data received
100
80
60
40
20
0
November 23 November 25 November 27

Go to log analytics

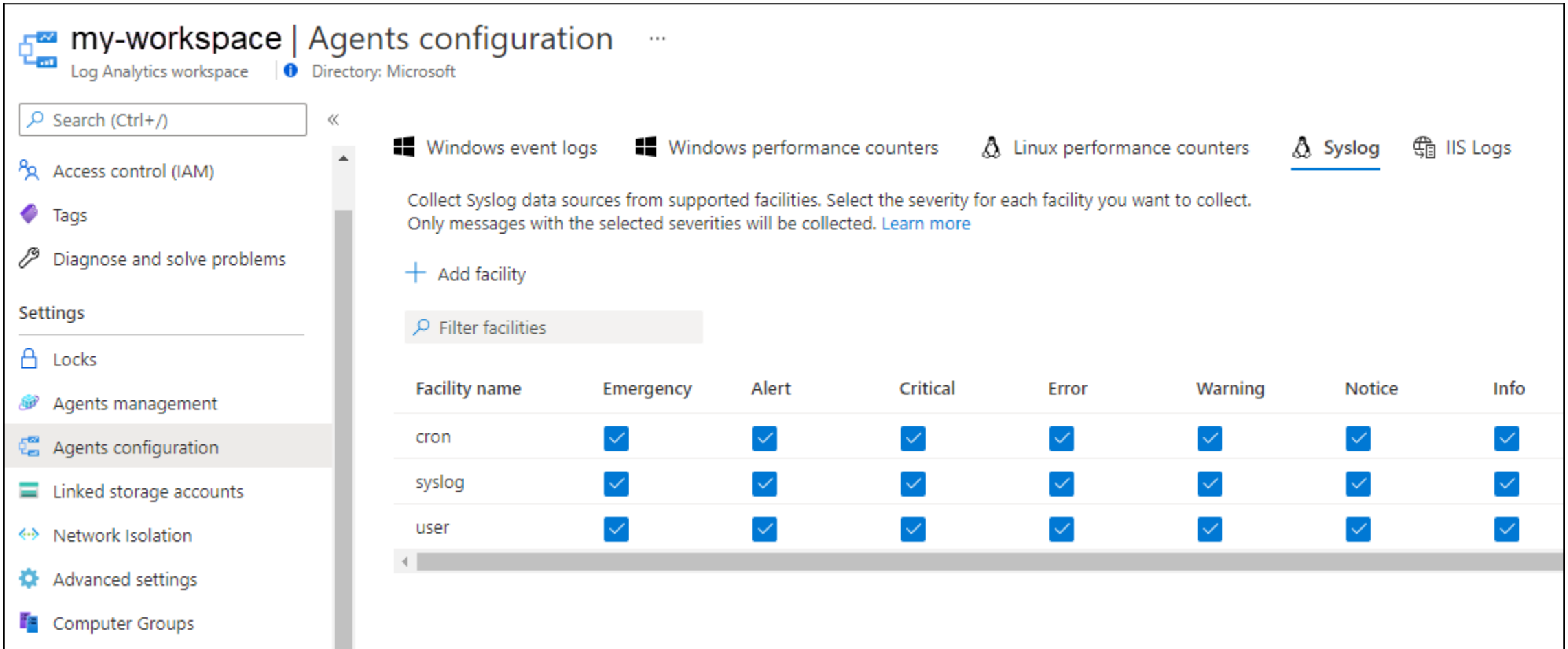
Instructions Next steps

Prerequisites
To integrate with Syslog make sure you have:
✓ **Workspace:** write permission is required.

Configuration
1. Install and onboard the agent for Linux
Typically, you should install the agent on a different computer from the one on which the logs are generated.
Syslog logs are collected only from **Linux** agents.
Choose where to install the agent:
▼ Install agent on Azure Linux Virtual Machine
▲ Install agent on a non-Azure Linux Machine
Download the agent on the relevant machine and follow the instructions.
Download & install agent for non-Azure Linux machines >
2. Configure the logs to be collected
Configure the facilities you want to collect and their severities.

Configure the log analytics agent

O agente do Log Analytics para Linux só coletará eventos com os recursos e severidades especificados em sua configuração.



The screenshot shows the 'Agents configuration' page in the Azure portal for a 'my-workspace' Log Analytics workspace. The left sidebar contains navigation links: Access control (IAM), Tags, Diagnose and solve problems, Settings, Locks, Agents management, Agents configuration (selected), Linked storage accounts, Network Isolation, Advanced settings, and Computer Groups. The main content area is titled 'Agents configuration' and shows a tab for 'Syslog'. Below the tabs, there is a description: 'Collect Syslog data sources from supported facilities. Select the severity for each facility you want to collect. Only messages with the selected severities will be collected. [Learn more](#)'. There is a '+ Add facility' button and a 'Filter facilities' search bar. A table lists facilities and their configured severities:

Facility name	Emergency	Alert	Critical	Error	Warning	Notice	Info
cron	<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"/>
syslog	<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"/>
user	<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"/>

Connect threat indicators to Microsoft Sentinel



Plan for threat intelligence connectors

Indicator Uses



Gere alertas e incidentes com base em correspondências de eventos de log de seus indicadores de ameaça.



As pastas de trabalho fornecem informações resumidas sobre os indicadores de ameaça



As consultas de caça permitem que os investigadores de segurança usem indicadores de ameaça



Os blocos de anotações podem usar indicadores de ameaça quando você investiga anomalias e procura comportamentos mal-intencionados.

Threat Intelligence Connectors



Inteligência de ameaças - TAXII



Plataformas de inteligência de ameaças

Connect the threat intelligence TAXII connector

O Microsoft Sentinel integra-se às fontes de dados TAXII 2.0 e 2.1 para habilitar o monitoramento, o alerta e a busca usando sua inteligência de ameaças.

The screenshot displays the Microsoft Azure portal interface for configuring the Threat intelligence - TAXII connector. The page is divided into two main sections: a left-hand navigation pane and a right-hand configuration pane.

Left-hand navigation pane:

- Threat intelligence - TAXII** (Selected)
- Not connected** (Status)
- Microsoft Provider** (Icon)
- Last Log Received** (Clock icon)
- Description**: Microsoft Sentinel integrates with TAXII 2.0 and 2.1 data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send threat indicators from TAXII servers to Microsoft Sentinel. Threat indicators can include IP addresses, domains, URLs, and file hashes.
- Last data received**: --
- Related content**:
 - 5 Workbooks
 - 2 Queries
 - 32 Analytics rules templates
- Data received**: A line chart showing data received over time (November 23 to November 27). The y-axis ranges from 0 to 100. The chart shows a single data point at 0.
- Total data received**: 0
- Data types**: ThreatIntelligenceIndicator --

Right-hand configuration pane:

- Instructions** (Selected) | Next steps
- Prerequisites**:
 - To integrate with Threat intelligence - TAXII make sure you have:
 - ✓ **Workspace**: read and write permissions are required.
 - ❗ **TAXII Server**: TAXII 2.0 or TAXII 2.1 Server URI and Collection ID are required
- Configuration**:
 - Configure TAXII servers to stream STIX 2.0 or 2.1 threat indicators to Microsoft Sentinel
 - You can connect your TAXII servers to Microsoft Sentinel using the built-in TAXII connector. For more information, see [TAXII connector](#).
 - Enter the following information and select Add to configure your TAXII server.
 - Friendly name (for server) ***:
 - API root URL ***:
 - Collection ID ***:
 - Username**:
 - Password**:
 - Import indicators**:
 - Polling frequency**:
 - Add** (Button)

Connect the threat intelligence platforms connector

O Microsoft Sentinel se integra às fontes de dados da API de Segurança do Microsoft Graph para habilitar o monitoramento, o alerta e a caça usando sua inteligência de ameaças. Use esse conector para enviar indicadores de ameaças ao Microsoft Sentinel a partir de sua TIP (Threat Intelligence Platform, plataforma de inteligência de ameaças)

The screenshot displays the Microsoft Azure portal interface for the Threat Intelligence Platforms (Preview) connector. The top navigation bar shows 'Microsoft Azure' and a search bar. The breadcrumb trail is 'Home > Microsoft Sentinel > Microsoft Sentinel > Threat Intelligence Platforms (Preview)'. The main content area is divided into two columns. The left column, titled 'Threat Intelligence Platforms (Preview)', shows the connector's status as 'Not connected', the provider as 'Microsoft', and the last log received as '--'. It includes a description of the connector's purpose, a section for 'Last data received' (showing '--'), and 'Related content' with links to '4 Workbooks', '2 Queries', and '32 Analytics rules templates'. At the bottom of this column is a 'Data received' chart showing a line graph with data points for November 23, 25, and 27. The right column contains 'Instructions' and 'Next steps'. The 'Instructions' section includes a 'Prerequisites' list (Workspace permissions, Tenant Permissions) and a 'Configuration' section with steps to connect the TIP to Microsoft Sentinel.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Microsoft Sentinel > Microsoft Sentinel > Threat Intelligence Platforms (Preview) ...

Threat Intelligence Platforms (Preview)

Not connected Status

Microsoft Provider

-- Last Log Received

Description

Microsoft Sentinel integrates with Microsoft Graph Security API data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send threat indicators to Microsoft Sentinel from your Threat Intelligence Platform (TIP), such as Threat Connect, Palo Alto Networks MindMeld, MISP, or other integrated applications. Threat indicators can include IP addresses, domains, URLs, and file hashes.

Last data received

--

Related content

4 Workbooks

2 Queries

32 Analytics rules templates

Data received

Go to log analytics

100

80

60

40

20

0

November 23 November 25 November 27

Instructions Next steps

Prerequisites

To integrate with Threat Intelligence Platforms (Preview) make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Tenant Permissions:** required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.

Configuration

You can connect your threat intelligence data sources to Microsoft Sentinel by either:

- Using an integrated Threat Intelligence Platform (TIP), such as Threat Connect, Palo Alto Networks MindMeld, MISP, and others.
- Calling the Microsoft Graph Security API directly from another application.

Follow These Steps to Connect your Threat Intelligence:

- 1) [Register an application](#) in Azure Active Directory.
- 2) [Configure permissions](#) and be sure to add the ThreatIndicators.ReadWrite.OwnedBy permission to the application.
- 3) Ask your Azure AD tenant administrator to [grant consent](#) to the application.
- 4) [Configure your TIP or other integrated application to push indicators to Microsoft Sentinel by specifying the following:](#)

View your threat indicators

Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | Logs

Selected workspace:

New Query 1*

ibol-law

Run

Time range : Last 24 hours

Save

Share

New alert rule

Export

Pin to dashboard

Feedback

Queries

Query explorer

1 ThreatIntelligenceIndicator

2 | project TimeGenerated, Description, NetworkIP, Url

Results

Chart

Columns

Add bookmark

Display time (UTC+00:00)

Group columns

Completed. Showing results from the last 24 hours.

00:02.0

312 records

	TimeGenerated [UTC]	Description	NetworkIP	Url
>	11:32:40.540 AM			
>	3:40:28.453 AM	TS ID: 326471959; iType: phish_url; State: ...		
>	3:40:28.535 AM	TS ID: 51642918002; iType: phish_url; Stat...		
>	3:40:28.535 AM	TS ID: 454369622; iType: phish_url; State:...		
>	3:40:28.536 AM	TS ID: 326476779; iType: phish_url; State:...		
>	3:40:28.536 AM	TS ID: 51915980027; iType: tor_ip; State: a...		

Schema and Filter

Page 1 of 7

50 items per page

1 - 50 of 312 items



Knowledge check



Check your knowledge
with the module quiz
in your course viewer