Azure security logging and auditing

10/31/2019 • 3 minutes to read •

In this article

Azure provides a wide array of configurable security auditing and logging options to help you identify gaps in your security policies and mechanisms. This article discusses generating, collecting, and analyzing security logs from services hosted on Azure.

> **Note**
>
> Certain recommendations in this article might result in increased data, network, or compute resource usage, and increase your license or subscription costs.

Types of logs in Azure

Cloud applications are complex with many moving parts. Logging data can provide insights about your applications and help you:

- Troubleshoot past problems or prevent potential ones
- Improve application performance or maintainability
- Automate actions that would otherwise require manual intervention

Azure logs are categorized into the following types:

- **Control/management logs** provide information about Azure Resource Manager CREATE, UPDATE, and DELETE operations. For more information, see Azure activity logs.
- **Data plane logs** provide information about events raised as part of Azure resource usage. Examples of this type of log are the Windows event system, security, and application logs in a virtual machine (VM) and the diagnostics logs that are configured through Azure Monitor.
- **Processed events** provide information about analyzed events/alerts that have been processed on your behalf. Examples of this type are Azure Security Center

alerts where Azure Security Center has processed and analyzed your subscription and provides concise security alerts.

The following table lists the most important types of logs available in Azure:

Log category	Log type	Usage	Integration
Activity logs	Control-plane events on Azure Resource Manager resources	Provides insight into the operations that were performed on resources in your subscription.	Rest API, Azure Monitor
Azure Resource logs	Frequent data about the operation of Azure Resource Manager resources in subscription	Provides insight into operations that your resource itself performed.	Azure Monitor
Azure Active Directory reporting	Logs and reports	Reports user sign-in activities and system activity information about users and group management.	Graph API
Virtual machines and cloud services	Windows Event Log service and Linux Syslog	Captures system data and logging data on the virtual machines and transfers that data into a storage account of your choice.	Windows (using Windows Azure Diagnostics [WAD] storage) and Linux in Azure Monitor
Azure Storage Analytics	Storage logging, provides metrics data for a storage account	Provides insight into trace requests, analyzes usage trends, and diagnoses issues with your storage account.	REST API or the client library
Network security group (NSG) flow logs	JSON format, shows outbound and inbound flows on a per-rule basis	Displays information about ingress and egress IP traffic through a Network Security Group.	Azure Network Watcher
Application insight	Logs, exceptions, and custom diagnostics	Provides an application performance monitoring (APM) service for web developers on multiple platforms.	REST API, Power BI

Log category	Log type	Usage	Integration
Process data / security alerts	Azure Security Center alerts, Azure Monitor logs alerts	Provides security information and alerts.	REST APIs, JSON

Log integration with on-premises SIEM systems

Integrating Security Center alerts discusses how to sync Security Center alerts, virtual machine security events collected by Azure diagnostics logs, and Azure audit logs with your Azure Monitor logs or SIEM solution.

Next steps

- Auditing and logging: Protect data by maintaining visibility and responding quickly to timely security alerts.
- Security logging and audit-log collection within Azure: Enforce these settings to ensure that your Azure instances are collecting the correct security and audit logs.
- Configure audit settings for a site collection: If you're a site collection administrator, retrieve the history of individual users' actions and the history of actions taken during a particular date range.
- Search the audit log in the Office 365 Security & Compliance Center: Use the Office 365 Security & Compliance Center to search the unified audit log and view user and administrator activity in your Office 365 organization.