



10-09-2026

Microsoft

Microsoft helps your organization reach its full potential by relying on an integrated and open cloud platform that spans six critical areas—security, infrastructure, digital and app innovation, data and AI, business applications, and modern work. Azure can help you migrate, modernize, and maximize your cloud and on-premises investments. Microsoft 365 can help you reduce costs – but not productivity – and centralize your business. Additional services, such as Exchange, Hyper-V, and IIS Web Server help you keep your business running smoothly.

Before looking at documentation for specific data sources, review the Splunk Help information on general data ingestion for [Splunk Enterprise](#), [Splunk Cloud Platform](#) or [Splunk Observability Cloud](#).

Getting data in

For Azure users, we recommend starting with [Following best practices for ingesting data from your Azure environment](#) and then looking in more detail at options for the source types listed below.

Source	Add-ons and Apps	Guidance
Windows • Windows security logs have over 400 loggable events. We recommend following Microsoft’s official guidance for “Stronger” security visibility. The audit policy recommendations page from Microsoft TechNet provides detailed configuration settings for operating systems from Windows 7/Server 2008 and later. In the Common Information Model, Windows security log data can be mapped to the Authentication, Updates, Vulnerabilities, Endpoint, Event Signatures, Performance, and Change data models, depending on the field. • Windows process launch logs are a subset of security audit logs that track program activation, process exit, handle duplication, and indirect object access. The most common events related to process launches are:	Splunk platform • Splunk Add-on for Microsoft Windows	Configuration • Splunk Add-on for Microsoft Windows • Splunk Add-on for Microsoft Security Splunk Lantern Articles • Maintaining Microsoft Windows

Source

Add-ons and Apps

Guidance

- [4688\(S\): A new process has been created.](#)
- [4696\(S\): A primary token was assigned to process.](#)
- **Windows event logs** contain important events relating to applications, system services and the operating system. The events describe errors, warnings or information details about activity taking place on each system. This information is used to monitor and troubleshoot each system. In the Common Information Model, Windows event logs can be mapped to the [Endpoint](#), [Inventory](#), [Updates](#), [Change](#), and [Performance](#) data models, depending on the field.

[systems with the Splunk platform](#)

- [Enabling Windows event log process command line logging via group policy object](#)
- [Configuring Windows event logs for Enterprise Security use](#)
- [Configuring Windows security audit policies for Enterprise Security visibility](#)
- [Installing Splunk Enterprise 9.x on Windows](#)
- [Using ingest actions to filter Windows event logs](#)
- [Reducing Windows security event log volume with Splunk Edge Processor](#)
- [Maintaining Microsoft Windows systems with Infrastructure Monitoring](#)

Source

Add-ons and Apps

Guidance

- [Monitoring Windows account access](#)
- [Detecting the use of randomization in cyberattacks](#)
- [Detecting Netsh attacks](#)
- [Creating a timebound picture of network activity](#)
- [Investigating a ransomware attack](#)
- [Recovering lost visibility of IT infrastructure](#)
- [Managing printers in a Windows environment](#)
- [Identifying new Windows local admin accounts](#)
- [Running common General Data Protection Regulation \(GDPR\) compliance searches](#)
- [Detecting brute force access behavior](#)
- [Visualizing](#)

Source

Add-ons and Apps

Guidance

- [processes and their parent/child relationships](#)
- [Detecting print spooler attacks with Splunk Enterprise Security](#)
- [Recognizing improper use of system administration tools with Splunk Security Essentials](#)
- [Using ingest actions to filter Windows event logs](#)
- [Monitoring access to Operational Technology environments outside business hours](#)
- [Monitoring remote access to Operational Technology environments](#)
- [Investigating user login issues and account lockouts](#)

Splunk platform

Splunk Lantern Articles

Source

Add-ons and Apps

Guidance

Active Directory

Microsoft Active Directory (AD) is a directory service that stores information about network objects such as users, computers, and other devices, and provides authentication and authorization services. Data from Active Directory includes security logs related to user logins, group policy changes, object modifications, and replication events, which are critical for identity and access management, security monitoring, and compliance auditing.

- [Splunk Supporting Add-on for Active Directory](#)

Splunk SOAR

- [AD LDAP](#)
- [MS Graph for Active Directory](#)

- [Detecting password spraying attacks within Active Directory environments](#)
- [Detecting cloud federated credential abuse in Windows](#)
- [Enabling an audit trail from Active Directory](#)

Azure

Microsoft Azure is a comprehensive suite of cloud computing services that includes virtual machines, storage, databases, networking, analytics, and AI. Data from Azure services includes activity logs, diagnostic logs, and metrics, providing insights into resource usage, performance, security events, and operational health across your cloud infrastructure.

For general recommendations or different methods of data ingestion, see the [Getting Microsoft Azure data into the Splunk platform](#).

Azure Local clusters represent Microsoft Azure in your private environment. In connected scenarios they act as an extension of Azure cloud services. In disconnected deployments they are sovereign private instances of Azure. Azure Local cluster nodes emit rich audit data via syslog forwarding. For disconnected, hyperconverged, and disaggregated deployments, the events are Windows Server shaped so you can use familiar ingestion and analysis workflows.

For more information, see [Manage syslog forwarding for Azure local](#).

Splunk platform

- [Splunk Add-on for Microsoft Cloud Services](#)

Splunk SOAR

- [Microsoft Azure SQL](#)
- [Microsoft Azure Compute](#)

Configuration

- [Microsoft Azure Services in Splunk Observability Cloud](#)
- [Deploy Splunk Enterprise on Windows](#)
- [Syslog data collection](#)

Splunk Lantern Articles

- [Getting started with Microsoft Azure Event Hub data](#)
- [Managing Azure cloud infrastructure](#)

Source

Add-ons and Apps

Guidance

Cloud Services

Microsoft Cloud Services refer to a broad range of hosted applications and infrastructure, including Azure, Microsoft 365, and Dynamics 365. These services generate various logs, such as audit logs for user and administrative activities, security logs for threat detection, and operational logs for performance monitoring, all essential for maintaining visibility and control over cloud environments.

Splunk platform

- [Splunk Add-on for Microsoft Cloud Services](#)

Configuration

- [Splunk Add-on for Microsoft Cloud Services](#)

Entra ID

Microsoft Entra ID (formerly Azure Active Directory) is a cloud-based identity and access management service that enables organizations to manage users, groups, and application access across cloud and hybrid environments. It provides core directory services, application access management, and identity protection capabilities. Data from Entra ID includes sign-in logs, audit logs, provisioning logs, and risk detection events, which are critical for monitoring authentication activity, detecting identity-based threats, managing access policies, and supporting compliance requirements.

Splunk platform

- [Splunk Add-on for Microsoft Cloud Services](#)

Splunk Lantern Articles

- [Integrating SOAR with Azure AD SAML](#)
- [Configuring SAML authentication for the Splunk platform](#)

Exchange

Microsoft Exchange Server is a mail server and calendaring server developed by Microsoft. It stores email messages, calendars, contacts, and tasks, and provides services for email communication and collaboration. Exchange logs include message tracking logs, protocol logs, and connectivity logs, offering detailed insights into email flow, server health, and potential security incidents.

Splunk platform

- [Splunk Add-on for Microsoft Exchange](#)
- [Splunk Add-on for Microsoft Exchange Indexes](#)

Configuration

- [Splunk Add-on for Microsoft Exchange](#)

Splunk SOAR

- [Microsoft Exchange On-](#)

Source

Add-ons and Apps

Guidance

[Premise EWS](#)

IIS Web Server

Microsoft Internet Information Services (IIS) is an extensible web server software with a large number of features. IIS can be:

- used to host ASP.NET web applications and static websites.
- used as an FTP server, host WCF services.
- extended to host web applications built on other platforms such as PHP.
- used with built-in authentication options such as Basic, ASP.NET, and Windows auth.
- managed via the CLI or using PowerShell.
- used to produce IIS websites with a number of tools, including WebDav and Microsoft Visual Studio.

In the Common Information Model, Microsoft IIS data is typically mapped to the [Web](#) data model.

Splunk platform

- [Splunk Add-on for Microsoft IIS](#)

Configuration

- [Splunk Add-on for Microsoft IIS](#)

Splunk Lantern Articles

- [Reconstructing a website defacement](#)
- [Managing web server performance](#)
- [Monitoring web application performance](#)
- [Monitoring NIST SP 800-53 rev5 control families](#)
- [Identifying slowly loading web pages](#)
- [Identifying web users by country](#)

Microsoft 365

Microsoft Office 365 produces service status, service messages, and management activity logs that are all useful for system administrators. In the Common Information Model, Microsoft O365 data can be mapped to any of the following data models: [Authentication](#), [Change](#), [Data Access](#).

Splunk platform

- [Splunk Add-on for Microsoft Office 365](#)

Configuration

- [Splunk Add-on for Microsoft Office 365](#)

Splunk Lantern Articles

Source

Microsoft O365 reporting data allows you to determine if a message was received, rejected, deferred, or delivered by the service. It also shows what actions were taken on the message before it reached its final status. These logs also provide the following information:

- Message size
- Message ID
- To IP
- From IP
- Date

Add-ons and Apps

- [Splunk Add-on for Microsoft Security](#)

Splunk SOAR

- [Microsoft 365 Defender](#)
- [Microsoft Teams](#)
- [Microsoft OneDrive](#)

Guidance

- [Detecting Office 365 attacks](#)
- [Identifying and removing malicious emails with Splunk SOAR from within Microsoft 365 mailboxes](#)
- [Managing O365 workloads](#)
- [Detecting cloud federated credential abuse in Microsoft Office and Azure Active Directory](#)
- [Setting up a Microsoft 365 abuse mailbox asset in Enterprise Security](#)

SQL Server

Microsoft SQL Server is a relational database management system that stores and retrieves data as requested by other software applications. It generates various logs, including error logs, transaction logs, and audit logs, which provide critical information for database performance monitoring, security auditing, and troubleshooting.

Splunk platform

- [Splunk Add-on for Microsoft SQL Server](#)
- [Splunk DBX Add-on for Microsoft SQL](#)

Configuration

- [Splunk Add-on for Microsoft SQL Server](#)

Source

Add-ons and Apps

Guidance

[Server JDBC](#)

Splunk SOAR

- [Microsoft SQL Server](#)

Sysmon

Microsoft Sysmon, a component of Microsoft's Sysinternals suite of Windows utilities, is a powerful host-level tool that can assist you in detecting advanced threats on your network by providing intricate host-operation details in real time. In contrast to common Antivirus/Host-Based Intrusion-detection (HIDS) solutions, Sysmon performs system activity deep monitoring and logs high-confidence indicators of advanced attacks.

Sysmon is capable of producing extensive details that are useful in the early detection of malicious code execution or other nefarious behavior. These include:

- Process executions, including parent/child relationships, user that launched process, and hash data
- File creations
- File creation time changes
- Network activity, down to the process level
- Image loads
- Creation of remote threads
- Interprocess accesses
- Windows registry modifications
- NTFS alternate data stream (ADS) creations
- Pipe creations and connections
- WMI event monitoring

Splunk platform

- [Splunk Add-on for Sysmon](#)

Splunk Lantern Articles

- [Reconstructing a website defacement](#)
- [Investigating a ransomware attack](#)
- [Detecting Netsh attacks](#)
- [Checking for files created on a system](#)
- [Monitoring DNS queries](#)
- [Visualizing processes and their parent/child relationships](#)
- [Detecting indicators of Remcos RAT malware](#)
- [Detecting print spooler attacks with Splunk Enterprise Security](#)
- [Monitoring for](#)

Source

Add-ons and Apps

Guidance

- [signs of a Windows privilege escalation attack with Splunk Enterprise Security](#)
- [Monitoring command line interface actions with Splunk Enterprise Security](#)
- [Detecting Supernova web shell malware](#)
- [Monitoring removable media devices in Operational Technology environments](#)

System Center

Microsoft System Center is a suite of management products designed to help organizations manage their IT environments across various platforms. It includes tools like System Center Operations Manager (SCOM) for monitoring, System Center Configuration Manager (SCCM) for deployment and compliance, and System Center Virtual Machine Manager (SCVMM) for virtualization management. Data from System Center products provides insights into infrastructure health, software deployments, and configuration changes.

Splunk platform

- [Splunk Add-on for Microsoft System Center Operations Manager](#)

Splunk SOAR

- [Microsoft SCOM](#)
- [Microsoft SCCM](#)

Configuration

- [Splunk Add-on for Microsoft SCOM](#)

Source

Add-ons and Apps

Guidance

Teams

Microsoft Teams is a unified communication and collaboration platform that combines workplace chat, video meetings, file storage, and application integration. It generates data such as chat logs, call detail records, meeting events, and administrative audit logs, which are valuable for monitoring communication patterns, troubleshooting connectivity issues, and ensuring compliance.

Splunk platform

[Microsoft Teams Add-on for Splunk](#)

Splunk Lantern Articles

- [Getting started with the Microsoft Teams Add-on for Splunk](#)
- [Getting started with Microsoft Teams call record data](#)
- [Getting started with Microsoft Teams call record data and Azure Functions](#)
- [Analyzing Microsoft Teams data with Kollektive Technology and Splunk](#)