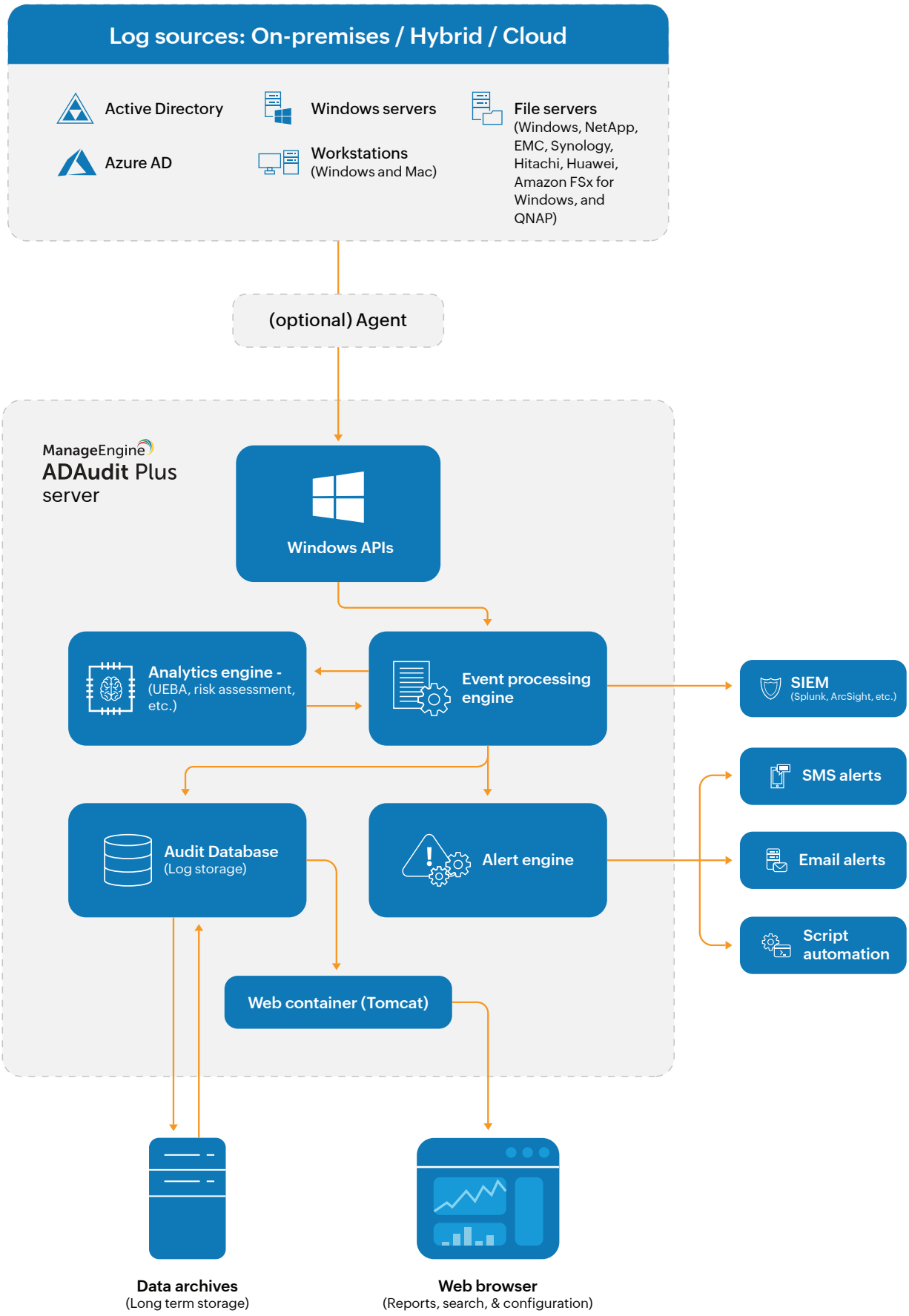
ManageEngine
ADAudit Plus

Architecture


Log sources: On-premises / Hybrid / Cloud
Active Directory
Azure AD
Windows servers
Workstations
(Windows and Mac)
File servers
(Windows, NetApp, EMC, Synology, Hitachi, Huawei, Amazon FSx for Windows, and QNAP)
(optional) Agent
ManageEngine
ADAudit Plus
server
Windows APIs
Analytics engine -
(UEBA, risk assessment, etc.)
Event processing engine
SIEM
(Splunk, ArcSight, etc.)
SMS alerts
Email alerts
Script automation
Audit Database
(Log storage)
Alert engine
Web container (Tomcat)
Data archives
(Long term storage)
Web browser
(Reports, search, & configuration)

Modules that ADAudit Plus has to offer

Event processing engine

All events that are fetched from the network are processed here before they are stored in the database or a corresponding alert is triggered. It filters logs which aren't needed—as configured by the administrator—and normalizes raw logs to standard formats.

Alerts engine

Sends out email or SMS notifications based on the configured alert profiles.

Audit Database

Stores raw and normalized log information from configured devices across your network. ADAudit Plus comes bundled with a PostgreSQL database, users can also choose to use Microsoft SQL databases if needed.

DataEngine

Stores and retrieves large volumes data faster & is more scalable when compared to the database.

Analytics engine

Collects information and models a baseline of normal activities to define dynamic thresholds. When an anomaly is detected, an alert is triggered.

External interfaces that ADAudit Plus interacts with

User interface

A web interface that runs on a browser and connects to the web server component of tomcat which listens on port number 8081.

Database interface

ADAudit Plus comes with an in-built PostgreSQL database which listens on port number 33307. The interactions between the product and the database happen using the Java Database Connectivity (JDBC) interfaces. The product also provides support to connect to MSSQL and MySQL databases.

Active Directory Services Interface (ADSI)

ADAudit Plus interacts with Active Directory through via ADSI. ADSI is a set of Component Object Model (COM) interfaces provided by Microsoft to access the features of the directory services.

Windows Event log

ADAudit Plus uses the Windows Eventlog API to query event logs from Windows Servers and workstations.

SIEM forwarding

ADAudit Plus can forward all events to an SIEM solution of your choice. Currently, the tool offers out-of-the-box support for Splunk, ArcSight(CEF) and syslog standards.

Email/SMS

ADAudit Plus can send critical alerts to users via email or SMS. An SMTP server configuration is used for sending emails and an SMS provider configuration is used to send SMSes.