LOGZILLA

AI-Powered Log Intelligence
www.logzilla.net

AI Copilot

Transform Log Analysis with Natural Language AI

What is LogZilla AI Copilot?

An AI-powered assistant that transforms how operators interact with log data. Ask questions in plain English, get expert-level analysis in seconds.

- **Natural Language Queries** – No query syntax to learn
- **Automated Reports** – Incident analysis with remediation steps
- **Deep Integration** – Direct access to LogZilla data and context
- **Flexible Deployment** – Cloud AI or on-premises with Ollama

Key Capabilities

Natural Language Querying

Ask questions like you would ask a colleague:

```
"Show me all authentication failures from the last hour"
"What caused the network outage at 3 AM?"
"Which hosts are generating the most errors?"
```

Intelligent Analysis

- **Pattern Recognition** – Identify anomalies automatically
- **Root Cause Suggestions** – AI-assisted troubleshooting
- **Correlation Detection** – Link related events across systems
- **Baseline Comparison** – Detect deviations from normal

Automated Reporting

- Executive summaries with business impact
- Priority matrices with confidence levels
- Remediation playbooks with CLI commands
- MITRE ATT&CK mapping for security events

Deployment Options

Cloud AI

Connect to leading AI providers with simple API key configuration:

- Anthropic
- OpenAI
- Scaleway

On-Premises AI (Ollama)

Full AI capabilities with zero external connectivity:

- Llama, Mistral, Mixtral
- No data leaves your network
- CMMC/FedRAMP compliant
- No per-query API costs

What Makes It Different

- **Deep LogZilla Integration** – Direct access to events, stats, config
- **Context-Aware** – Understands your infrastructure
- **Actionable Output** – Copy-paste CLI commands, not generic advice
- **Vendor-Specific** – Knows Cisco, Palo Alto, Juniper syntax

AI Domains

LogZilla AI Copilot provides specialized analysis across six operational domains:

SecOps
Threat detection, IOC extraction, MITRE ATT&CK mapping

NetOps
Network analysis, topology impact, cascading failures

InfraOps
Server health, capacity planning, resource trending

AppOps
Error clustering, dependency mapping, performance

CloudOps
Multi-cloud correlation, K8s health, cost anomalies

DevOps
CI/CD analysis, build failures, pipeline optimization

Compliance
PCI, HIPAA, GDPR, SOX evidence gathering

Executive
Business impact summaries, trend dashboards

AI SecOps: Security Operations Analysis

User Request

"Generate a security incident report with threat intelligence, IOCs, and MITRE ATT&CK mapping."

AI-Generated Threat Intel

Source IP	Country	Threat	Action
45.142.xxx.xxx	Russia	Brute Force	Blocked
185.220.xxx.xxx	Germany	Port Scan	Blocked
23.94.xxx.xxx	US	DNS Amp	Rate Ltd

MITRE ATT&CK Mapping

Technique	Tactic	Evidence
T1110.001	Credential Access	12,453 SSH failures
T1498.002	Impact	DNS amplification
T1046	Discovery	Port scanning
T1071.004	C2	Suspicious DNS

AI-Generated Report

Finding	Severity	Events
DNS Amplification Attacks	Critical	847
Failed SSH Authentication	High	12,453
Firewall Deny Events	Medium	156,892
Certificate Failures	Medium	2,341

Automated Remediation

```
# Cisco ASA - Block attacker
access-list OUTSIDE_IN deny ip host 45.142.xxx.xxx
any

# Palo Alto - Create EDL block
set address "Threat-Actor-1" ip-netmask
45.142.xxx.xxx/32

# Fortinet - Block and log
config firewall address
  edit "blocked-attacker"
  set subnet 45.142.xxx.xxx/32
```

AI NetOps: Network Operations Analysis

User Request

"Analyze network operations events from the last 2 hours, compare to baseline, identify anomalies, and provide remediation steps."

AI-Generated Priority Matrix

Priority	Issue	Confidence
P1	PKI Certificate Failure (20+ devices)	95%
P1	AD Connector DNS Failure	90%
P2	Wireless Auth Failures (92K events)	80%
P2	DHCP Error Storm	85%

Anomaly Detection

Metric	Current	Baseline	Delta
Total Events	5.06M	3.90M	+29.6%
Critical Events	273	231	+18.2%
Avg/5min	221K	163K	+36.3%

AI-Generated Remediation

```
# Verify CA Server Status
ping <CA_SERVER_IP>
show crypto pki trustpoints
show crypto pki certificates sdn-network-infra-iwan

# Manual Certificate Renewal
conf t
crypto pki authenticate sdn-network-infra-iwan
crypto pki enroll sdn-network-infra-iwan
```

Topology Impact Analysis

Device	Role	Downstream Impact
core-sw-01	Distribution	847 endpoints
wlc-primary	Wireless	2,341 clients
fw-dmz-01	Perimeter	All external

AI InfraOps: Infrastructure Operations Analysis

> **User Request**
>
> *"Analyze infrastructure health, identify capacity issues, and provide remediation for any critical problems."*

Server Health Summary

Category	Healthy	Warning	Critical
Physical Servers	142	8	2
Virtual Machines	1,247	34	5
Storage Arrays	12	1	0
Backup Systems	8	2	1

Resource Trending

Resource	Current	7-Day Avg	Trend
CPU (cluster)	67%	54%	Increasing
Memory (cluster)	78%	72%	Stable
Storage (SAN)	71%	68%	Increasing
Network I/O	2.4 Gbps	1.8 Gbps	Spike

Critical Issues Identified

Server	Issue	Action
db-prod-03	Disk 95% full	Expand /var/lib/mysql
esxi-host-07	Memory overcommit	Migrate VMs
backup-srv-01	Job failures	Check tape library

Automated Remediation

```
# Linux - Disk space analysis
df -h /var/lib/mysql
du -sh /var/lib/mysql/* | sort -hr | head -20

# VMware ESXi - Host diagnostics
esxcli system health status get
esxcli hardware memory get
```

AI AppOps: Application Operations Analysis

> **User Request**
>
> *"Analyze application errors across all services, identify root causes, and suggest fixes."*

Error Summary by Service

Service	Errors	Rate	Top Error
payment-api	1,247	2.3%	DB timeout
user-auth	892	1.8%	Token expired
inventory-svc	456	0.9%	Cache miss
order-processor	234	0.5%	Queue full

Performance Analysis

Endpoint	Avg	P95	Errors
/api/checkout	2.4s	8.7s	3.2%
/api/search	180ms	450ms	0.1%
/api/auth/login	340ms	890ms	1.8%
/api/inventory	95ms	210ms	0.4%

Root Cause Correlation

Symptom	Root Cause	Conf.
Checkout timeouts	DB connection pool exhausted	92%
Auth failures	Redis cache eviction	85%
Slow search	ES index fragmentation	78%

Automated Remediation

```
# Database connection pool
SHOW PROCESSLIST;
SET GLOBAL max_connections = 500;

# Redis cache diagnostics
redis-cli INFO memory
redis-cli INFO stats | grep evicted
```

AI CloudOps: Multi-Cloud Operations Analysis

User Request

"Analyze cloud security posture across all accounts, check Kubernetes health, and identify cost anomalies."

Multi-Cloud Security Posture

Cloud	Crit	High	Med	Compliant
AWS (3 accounts)	2	8	23	89%
Azure (2 subs)	1	5	12	92%
GCP (1 project)	0	3	8	95%

Kubernetes Cluster Health

Cluster	Nodes	Pods	Failed	Pending
prod-eks-east	24	847	3	2
prod-aks-west	18	623	1	0
dev-gke	8	234	12	5

Cost Anomalies Detected

Resource	Account	Daily	Anomaly
EC2 i3.4xlarge	prod-aws	$892	+340%
Azure SQL	prod-azure	$456	Idle 72h
GCS Bucket	dev-gcp	$234	Egress spike

Automated Remediation

```
# AWS - Investigate SG change
aws cloudtrail lookup-events \
  --lookup-attributes AttributeKey=EventName,\
  AttributeValue=AuthorizeSecurityGroupIngress

# Kubernetes - Debug CrashLoopBackOff
kubectl describe pod <name> -n <ns>
kubectl logs <name> --previous
```

AI DevOps: CI/CD Pipeline Analysis

User Request

"Analyze CI/CD pipeline failures from the last 24 hours, identify patterns, and suggest optimizations."

Build Failure Matrix

Priority	Pipeline	Failure Type	Count
CRIT	main-deploy	Integration test fail	23
HIGH	api-build	Dependency resolution	18
MED	frontend-ci	Lint errors	31
LOW	docs-build	Asset compilation	17

Root Cause Analysis

Pipeline	Root Cause
main-deploy	Test "user-auth-flow" race condition
api-build	npm registry timeout (09:00-11:00 UTC)
frontend-ci	ESLint v9 introduced new rules
docs-build	Node heap size insufficient

Optimization Opportunities

Optimization	Time Saved
Cache npm dependencies	-4m 12s
Parallelize test suites	-2m 45s
Skip unchanged modules	-1m 30s

AI-Generated Fixes

```
# Fix flaky test with explicit waits (Playwright)
await page.waitForSelector('[data-testid="auth-
complete"]');

# Add npm registry mirror in .npmrc
registry=https://registry.npmjs.org/

# Increase Node heap for large builds
export NODE_OPTIONS="--max-old-space-size=4096"
```

Getting Started

Setup Steps

1. Navigate to **Settings > AI Copilot**
2. Set **AI Enabled** to "On"
3. Select **Model Type** (OpenAI, Anthropic, Ollama)
4. Enter **API Key** (not required for Ollama)
5. Click **Save** – access via `Copilot` menu link

Example Queries to Try

```
"Show me authentication failures from the last hour"
"What caused the network outage at 3 AM?"
"Generate a PCI compliance report for Q4"
"Analyze Kubernetes pod failures in production"
"Which CI/CD pipelines are failing most often?"
```

Technical Specifications

Min LogZilla Version	v6.36+
AI Providers	OpenAI, Anthropic, Ollama, Scaleway
Max Context Window	Per model/provider
Authentication	Inherits LogZilla RBAC
Data Residency	Cloud or On-Prem (your choice)

Air-Gapped Deployment

For classified or isolated environments:

- Ollama runs entirely on-premises
- No external network connectivity required
- Supports Llama, Mistral, Mixtral models
- CMMC/FedRAMP compliant architecture
- Full AI capability without cloud dependency

Supported Log Sources

LogZilla AI Copilot analyzes logs from any syslog-compatible source. App Store integrations include:

Security

Palo Alto, Fortigate, Cisco ASA/Firepower, Check Point, Zeek, Snort

Network

Cisco IOS/Nexus/WLC/Meraki, Juniper, Infoblox, Ubiquiti

Infrastructure

VMware vCenter/ESXi, Linux, Windows, Nimble, QNAP

Cloud

AWS CloudTrail/CloudWatch, Azure Monitor, GCP Logging, Kubernetes

Applications

Apache, Nginx, MySQL, PostgreSQL, Redis, Elasticsearch

DevOps

Jenkins, GitLab, GitHub Actions, Docker, containerd

Why LogZilla AI Copilot?

No Query Language

Ask in plain English. No SPL, KQL, or Lucene to learn.

Vendor-Specific

Get CLI commands for your actual equipment, not generic advice.

Works Air-Gapped

Full capability in classified environments with Ollama.

Context-Aware

Understands your infrastructure, not just generic patterns.

Contact: sales@logzilla.net | **www.logzilla.net**

AI-generated content should be verified before implementation. LogZilla Copilot continually improves through regular updates.