LOGZILLA DOCUMENTATION

Event Correlation

LogZilla Event Correlation combines trigger-based stateless matching with Simple Event Correlator for stateful multi-event pattern detection across time windows

Event Correlation · Generated April 29, 2026 · logzilla.ai/docs/event-correlation

Event Correlation in LogZilla

Event correlation transforms individual log events into meaningful insights by identifying patterns, relationships, and anomalies across multiple events over time. LogZilla provides both simple trigger-based correlation and advanced stateful correlation through SEC (Simple Event Correlator).

Correlation Methods

Stateless Correlation (Triggers)

LogZilla Triggers provide immediate, single-event correlation:

- Real-time event matching against defined filters
- Instant action execution when conditions are met
- Simple alerting and notification scenarios
- Managed through the web interface or API

Stateful Correlation (SEC)

Simple Event Correlator enables complex, multi-event correlation:

- Maintains state across events over time
- Supports event pairs, thresholds, and time windows
- Handles scenarios requiring memory of past events
- Processes events through the Script Server architecture

Common Correlation Scenarios

Network Infrastructure

- **Interface flapping**: Detect rapid link up/down cycles
- **Device reload monitoring**: Correlate planned vs. unplanned restarts
- **Service dependency tracking**: Monitor cascading service failures
- **Security incident detection**: Identify attack patterns across devices

System Monitoring

- **Threshold-based alerting**: Count events within time windows
- **Service availability**: Track service start/stop sequences
- **Performance degradation**: Correlate resource exhaustion indicators
- **Capacity planning**: Identify usage pattern trends

Security Analysis

- **Brute force detection**: Count failed login attempts
- **Privilege escalation**: Correlate authentication and authorization events
- **Data exfiltration**: Monitor unusual file access patterns
- **Audit trail integrity**: Detect log tampering attempts

Windows Environment

- **Event ID correlation**: Leverage Windows Event ID patterns
- **Security event monitoring**: Track critical Windows security events
- **Service monitoring**: Correlate Windows service state changes
- **System integrity**: Monitor audit log and system file changes

Getting Started

Basic Correlation

Identify patterns: Determine which events need correlation
Choose method: Select triggers for simple cases, SEC for complex scenarios
Create rules: Define correlation logic and actions
Test thoroughly: Verify rules work with sample events
Monitor performance: Ensure correlation processing scales appropriately

Advanced Correlation

Design SEC instances: Organize rules by function or system type
Configure forwarders: Route specific events to appropriate SEC instances
Implement time windows: Define appropriate correlation timeframes
Set up alerting: Configure actions for correlation matches
Monitor and tune: Adjust rules based on operational experience

Architecture Overview

Event correlation in LogZilla follows this processing flow:

Event ingestion: Syslog-ng receives and forwards events
Parsing and enrichment: Events are normalized and tagged
Trigger evaluation: Stateless triggers match individual events
SEC processing: Complex correlation via Script Server and SEC instances
Action execution: Correlated events trigger alerts and responses

Best Practices

Rule Design

- Start with simple correlation scenarios
- Use specific patterns to avoid false positives
- Set appropriate time windows for event relationships
- Test rules thoroughly before production deployment

Performance Considerations

- Filter events before sending to SEC instances
- Use multiple SEC instances for different correlation types
- Monitor SEC process resource usage
- Implement correlation rule lifecycle management

Operational Management

- Document correlation rules and their purposes
- Implement version control for SEC rule files
- Monitor correlation effectiveness and tune as needed
- Plan for correlation rule maintenance and updates

Additional Capabilities

LogZilla's event correlation extends beyond basic pattern matching to provide enterprise-grade operational intelligence:

Business Process Monitoring

- **Revenue pipeline tracking**: Monitor e-commerce workflows end-to-end
- **Service level correlation**: Correlate technical metrics with business KPIs
- **Compliance automation**: Automate SOX, PCI, and regulatory monitoring

Advanced Security Detection

- **APT correlation**: Detect multi-stage advanced persistent threats
- **Lateral movement tracking**: Identify sophisticated attack progressions
- **Behavioral analysis**: Correlate user and system behavior patterns

Infrastructure Intelligence

- **Cascading failure prediction**: Prevent widespread outages through early detection
- **Capacity planning automation**: Predict resource exhaustion before impact
- **Multi-cloud correlation**: Unified monitoring across cloud providers

DevOps Integration

- **CI/CD pipeline correlation**: Track deployment success across environments
- **Performance regression detection**: Correlate code changes with performance impact
- **Automated remediation**: Trigger corrective actions based on correlation results

Related Topics

- Advanced Event Correlation Walkthrough (https://www.logzilla.ai/docs/event-correlation/advanced-event-correlation-walkthrough)
- SOAR Security Orchestration (https://www.logzilla.ai/docs/event-correlation/soar-security-orchestration)
- Creating Triggers (https://www.logzilla.ai/docs/creating-triggers/)
- Data Transforms (https://www.logzilla.ai/docs/data-transforms/rewrite-rules)
- Windows Event Forwarding (https://www.logzilla.ai/docs/receiving-data/windows-event-forwarding)
- Syslog Settings (https://www.logzilla.ai/docs/administration/syslog-settings)