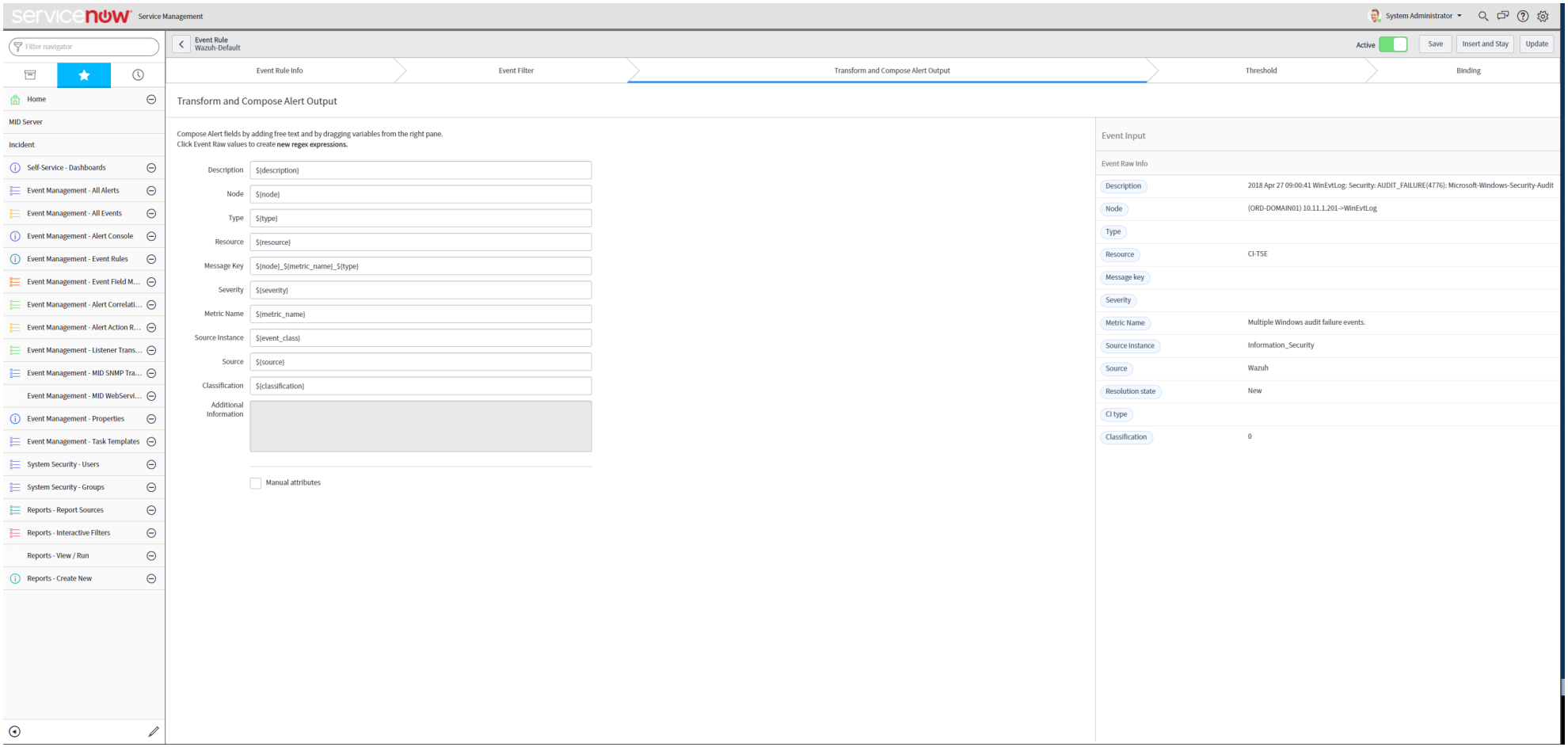
servicenow
Service Management
System Administrator
Filter navigator
Home
MID Server
Incident
Self-Service - Dashboards
Event Management - All Alerts
Event Management - All Events
Event Management - Alert Console
Event Management - Event Rules
Event Management - Event Field M...
Event Management - Alert Correlati...
Event Management - Alert Action R...
Event Management - Listener Trans...
Event Management - MID SNMP Tra...
Event Management - MID WebServi...
Event Management - Properties
Event Management - Task Templates
System Security - Users
System Security - Groups
Reports - Report Sources
Reports - Interactive Filters
Reports - View / Run
Reports - Create New
Event Rule
Wazuh-Default
Active
Save
Insert and Stay
Update
Event Rule Info
Event Filter
Transform and Compose Alert Output
Threshold
Binding
Transform and Compose Alert Output
Compose Alert fields by adding free text and by dragging variables from the right pane.
Click Event Raw values to create new regex expressions.
Description ${description}
Node ${node}
Type ${type}
Resource ${resource}
Message Key ${node}_${metric_name}_${type}
Severity ${severity}
Metric Name ${metric_name}
Source Instance ${event_class}
Source ${source}
Classification ${classification}
Additional Information
Manual attributes
Event Input
Event Raw Info
Description 2018 Apr 27 09:00:41 WinEvtLog: Security: AUDIT_FAILURE(4776): Microsoft-Windows-Security-Audit
Node (ORD-DOMAIN01) 10.11.1.201->WinEvtLog
Type
Resource CI-TSE
Message key
Severity
Metric Name Multiple Windows audit failure events.
Source instance Information_Security
Source Wazuh
Resolution state New
CI type
Classification 0