**OSSEC.LOG**

**root@WAZUH:/var/ossec/logs# tail -n 150 ossec.log**

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '92655'

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '92656'

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:225 at OS\_InsertRulesDB(): DEBUG: Reading rules file: 'ruleset/rules/0850-audit\_rules.xml'

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:161 at OS\_ReadXMLRules(): DEBUG: ruleset/rules/0850-audit\_rules.xml is the rulefile

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:162 at OS\_ReadXMLRules(): DEBUG: Not modifing the rule path

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:171 at OS\_ReadXMLRules(): DEBUG: Read xml for rule 'ruleset/rules/0850-audit\_rules.xml'.

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:179 at OS\_ReadXMLRules(): DEBUG: XML Variables applied.

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '92600'

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '92601'

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '92602'

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '92603'

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '92604'

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '92605'

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:225 at OS\_InsertRulesDB(): DEBUG: Reading rules file: 'ruleset/rules/0860-sysmon\_id\_13.xml'

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:161 at OS\_ReadXMLRules(): DEBUG: ruleset/rules/0860-sysmon\_id\_13.xml is the rulefile

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:162 at OS\_ReadXMLRules(): DEBUG: Not modifing the rule path

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:171 at OS\_ReadXMLRules(): DEBUG: Read xml for rule 'ruleset/rules/0860-sysmon\_id\_13.xml'.

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:179 at OS\_ReadXMLRules(): DEBUG: XML Variables applied.

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '92300'

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '92301'

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '92302'

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:225 at OS\_InsertRulesDB(): DEBUG: Reading rules file: 'ruleset/rules/0870-sysmon\_id\_8.xml'

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:161 at OS\_ReadXMLRules(): DEBUG: ruleset/rules/0870-sysmon\_id\_8.xml is the rulefile

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:162 at OS\_ReadXMLRules(): DEBUG: Not modifing the rule path

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:171 at OS\_ReadXMLRules(): DEBUG: Read xml for rule 'ruleset/rules/0870-sysmon\_id\_8.xml'.

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:179 at OS\_ReadXMLRules(): DEBUG: XML Variables applied.

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '92400'

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:225 at OS\_InsertRulesDB(): DEBUG: Reading rules file: 'ruleset/rules/0900-firewall\_rules.xml'

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:161 at OS\_ReadXMLRules(): DEBUG: ruleset/rules/0900-firewall\_rules.xml is the rulefile

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:162 at OS\_ReadXMLRules(): DEBUG: Not modifing the rule path

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:171 at OS\_ReadXMLRules(): DEBUG: Read xml for rule 'ruleset/rules/0900-firewall\_rules.xml'.

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:179 at OS\_ReadXMLRules(): DEBUG: XML Variables applied.

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:225 at OS\_InsertRulesDB(): DEBUG: Reading rules file: 'ruleset/rules/0905-cisco-ftd\_rules.xml'

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:161 at OS\_ReadXMLRules(): DEBUG: ruleset/rules/0905-cisco-ftd\_rules.xml is the rulefile

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:162 at OS\_ReadXMLRules(): DEBUG: Not modifing the rule path

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:171 at OS\_ReadXMLRules(): DEBUG: Read xml for rule 'ruleset/rules/0905-cisco-ftd\_rules.xml'.

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:179 at OS\_ReadXMLRules(): DEBUG: XML Variables applied.

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '91510'

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '91517'

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '91518'

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:41 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:42 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '91522'

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:42 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '91525'

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:225 at OS\_InsertRulesDB(): DEBUG: Reading rules file: 'ruleset/rules/0910-ms-exchange-proxylogon\_rules.xml'

2023/02/14 08:55:42 wazuh-dbd[264870] rules\_op.c:161 at OS\_ReadXMLRules(): DEBUG: ruleset/rules/0910-ms-exchange-proxylogon\_rules.xml is the rulefile

2023/02/14 08:55:42 wazuh-dbd[264870] rules\_op.c:162 at OS\_ReadXMLRules(): DEBUG: Not modifing the rule path

2023/02/14 08:55:42 wazuh-dbd[264870] rules\_op.c:171 at OS\_ReadXMLRules(): DEBUG: Read xml for rule 'ruleset/rules/0910-ms-exchange-proxylogon\_rules.xml'.

2023/02/14 08:55:42 wazuh-dbd[264870] rules\_op.c:179 at OS\_ReadXMLRules(): DEBUG: XML Variables applied.

2023/02/14 08:55:42 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '91000'

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:42 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '91001'

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:42 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '91002'

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:189 at \_Rules\_ReadInsertDB(): DEBUG: Entering \_Rules\_ReadInsertDB()

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:111 at \_Groups\_ReadInsertDB(): DEBUG: Entering \_Groups\_ReadInsertDB

2023/02/14 08:55:42 wazuh-dbd[264870] rules\_op.c:1019 at OS\_ReadXMLRules(): DEBUG: You are using a deprecated Mitre format in rule '91003'

2023/02/14 08:55:42 wazuh-dbd[264870] rules\_op.c:1152 at OS\_ReadXMLRules(): ERROR: (1450): Syntax error on regex: 'Set-.+VirtualDirectory.+?Url.+\<\w+.\*\>.\*?\<\/\w+\>.+?VirtualDirectory': 6.

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:228 at OS\_InsertRulesDB(): ERROR: (1220): Error loading the rules: 'ruleset/rules/0910-ms-exchange-proxylogon\_rules.xml'.

2023/02/14 08:55:42 wazuh-dbd[264870] main.c:256 at main(): CRITICAL: (1202): Configuration error at 'etc/ossec.conf'.

2023/02/14 09:11:52 wazuh-modulesd:syscollector: INFO: Starting evaluation.

2023/02/14 09:11:53 wazuh-modulesd:syscollector: INFO: Evaluation finished.

root@WAZUH:/var/ossec/logs#

**root@WAZUH:/var/ossec/logs# cat ossec.log | grep -i -E "error|critical|warning|fatal"**

2023/02/14 08:55:34 wazuh-dbd[264870] db\_op.c:214 at mysql\_osdb\_query\_insert(): ERROR: (5203): Error executing query 'INSERT INTO category(cat\_name) VALUES ('git\_dependabot\_security\_updates\_new\_repos')'. Error: 'Data too long for column 'cat\_name' at row 1'.

2023/02/14 08:55:34 wazuh-dbd[264870] db\_op.c:118 at osdb\_checkerror(): INFO: (5210): Attempting to reconnect to database.

2023/02/14 08:55:34 wazuh-dbd[264870] db\_op.c:140 at osdb\_checkerror(): INFO: Connected to database 'Alerts\_DB1' at '127.0.0.1'.

2023/02/14 08:55:34 wazuh-dbd[264870] rules.c:60 at \_\_Groups\_InsertGroup(): ERROR: (5204): Database error. Unable to run query.

2023/02/14 08:55:34 wazuh-dbd[264870] db\_op.c:214 at mysql\_osdb\_query\_insert(): ERROR: (5203): Error executing query 'INSERT INTO category(cat\_name) VALUES ('git\_dependabot\_security\_updates\_new\_repos')'. Error: 'Data too long for column 'cat\_name' at row 1'.

2023/02/14 08:55:34 wazuh-dbd[264870] db\_op.c:118 at osdb\_checkerror(): INFO: (5210): Attempting to reconnect to database.

2023/02/14 08:55:34 wazuh-dbd[264870] db\_op.c:140 at osdb\_checkerror(): INFO: Connected to database 'Alerts\_DB1' at '127.0.0.1'.

2023/02/14 08:55:34 wazuh-dbd[264870] rules.c:60 at \_\_Groups\_InsertGroup(): ERROR: (5204): Database error. Unable to run query.

2023/02/14 08:55:34 wazuh-dbd[264870] db\_op.c:214 at mysql\_osdb\_query\_insert(): ERROR: (5203): Error executing query 'INSERT INTO category(cat\_name) VALUES ('git\_dependabot\_security\_updates\_new\_repos')'. Error: 'Data too long for column 'cat\_name' at row 1'.

2023/02/14 08:55:34 wazuh-dbd[264870] db\_op.c:118 at osdb\_checkerror(): INFO: (5210): Attempting to reconnect to database.

2023/02/14 08:55:34 wazuh-dbd[264870] db\_op.c:140 at osdb\_checkerror(): INFO: Connected to database 'Alerts\_DB1' at '127.0.0.1'.

2023/02/14 08:55:34 wazuh-dbd[264870] rules.c:60 at \_\_Groups\_InsertGroup(): ERROR: (5204): Database error. Unable to run query.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:214 at mysql\_osdb\_query\_insert(): ERROR: (5203): Error executing query 'INSERT INTO category(cat\_name) VALUES ('git\_repository\_vulnerability\_alert')'. Error: 'Data too long for column 'cat\_name' at row 1'.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:118 at osdb\_checkerror(): INFO: (5210): Attempting to reconnect to database.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:140 at osdb\_checkerror(): INFO: Connected to database 'Alerts\_DB1' at '127.0.0.1'.

2023/02/14 08:55:37 wazuh-dbd[264870] rules.c:60 at \_\_Groups\_InsertGroup(): ERROR: (5204): Database error. Unable to run query.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:214 at mysql\_osdb\_query\_insert(): ERROR: (5203): Error executing query 'INSERT INTO category(cat\_name) VALUES ('git\_repository\_vulnerability\_alert')'. Error: 'Data too long for column 'cat\_name' at row 1'.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:118 at osdb\_checkerror(): INFO: (5210): Attempting to reconnect to database.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:140 at osdb\_checkerror(): INFO: Connected to database 'Alerts\_DB1' at '127.0.0.1'.

2023/02/14 08:55:37 wazuh-dbd[264870] rules.c:60 at \_\_Groups\_InsertGroup(): ERROR: (5204): Database error. Unable to run query.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:214 at mysql\_osdb\_query\_insert(): ERROR: (5203): Error executing query 'INSERT INTO category(cat\_name) VALUES ('git\_repository\_vulnerability\_alert')'. Error: 'Data too long for column 'cat\_name' at row 1'.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:118 at osdb\_checkerror(): INFO: (5210): Attempting to reconnect to database.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:140 at osdb\_checkerror(): INFO: Connected to database 'Alerts\_DB1' at '127.0.0.1'.

2023/02/14 08:55:37 wazuh-dbd[264870] rules.c:60 at \_\_Groups\_InsertGroup(): ERROR: (5204): Database error. Unable to run query.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:214 at mysql\_osdb\_query\_insert(): ERROR: (5203): Error executing query 'INSERT INTO category(cat\_name) VALUES ('git\_repository\_vulnerability\_alert')'. Error: 'Data too long for column 'cat\_name' at row 1'.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:118 at osdb\_checkerror(): INFO: (5210): Attempting to reconnect to database.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:140 at osdb\_checkerror(): INFO: Connected to database 'Alerts\_DB1' at '127.0.0.1'.

2023/02/14 08:55:37 wazuh-dbd[264870] rules.c:60 at \_\_Groups\_InsertGroup(): ERROR: (5204): Database error. Unable to run query.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:214 at mysql\_osdb\_query\_insert(): ERROR: (5203): Error executing query 'INSERT INTO category(cat\_name) VALUES ('git\_repository\_vulnerability\_alerts')'. Error: 'Data too long for column 'cat\_name' at row 1'.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:118 at osdb\_checkerror(): INFO: (5210): Attempting to reconnect to database.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:140 at osdb\_checkerror(): INFO: Connected to database 'Alerts\_DB1' at '127.0.0.1'.

2023/02/14 08:55:37 wazuh-dbd[264870] rules.c:60 at \_\_Groups\_InsertGroup(): ERROR: (5204): Database error. Unable to run query.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:214 at mysql\_osdb\_query\_insert(): ERROR: (5203): Error executing query 'INSERT INTO category(cat\_name) VALUES ('git\_repository\_vulnerability\_alerts')'. Error: 'Data too long for column 'cat\_name' at row 1'.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:118 at osdb\_checkerror(): INFO: (5210): Attempting to reconnect to database.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:140 at osdb\_checkerror(): INFO: Connected to database 'Alerts\_DB1' at '127.0.0.1'.

2023/02/14 08:55:37 wazuh-dbd[264870] rules.c:60 at \_\_Groups\_InsertGroup(): ERROR: (5204): Database error. Unable to run query.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:214 at mysql\_osdb\_query\_insert(): ERROR: (5203): Error executing query 'INSERT INTO category(cat\_name) VALUES ('git\_repository\_vulnerability\_alerts')'. Error: 'Data too long for column 'cat\_name' at row 1'.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:118 at osdb\_checkerror(): INFO: (5210): Attempting to reconnect to database.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:140 at osdb\_checkerror(): INFO: Connected to database 'Alerts\_DB1' at '127.0.0.1'.

2023/02/14 08:55:37 wazuh-dbd[264870] rules.c:60 at \_\_Groups\_InsertGroup(): ERROR: (5204): Database error. Unable to run query.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:214 at mysql\_osdb\_query\_insert(): ERROR: (5203): Error executing query 'INSERT INTO category(cat\_name) VALUES ('git\_repository\_vulnerability\_alerts')'. Error: 'Data too long for column 'cat\_name' at row 1'.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:118 at osdb\_checkerror(): INFO: (5210): Attempting to reconnect to database.

2023/02/14 08:55:37 wazuh-dbd[264870] db\_op.c:140 at osdb\_checkerror(): INFO: Connected to database 'Alerts\_DB1' at '127.0.0.1'.

2023/02/14 08:55:37 wazuh-dbd[264870] rules.c:60 at \_\_Groups\_InsertGroup(): ERROR: (5204): Database error. Unable to run query.

2023/02/14 08:55:38 wazuh-dbd[264870] db\_op.c:214 at mysql\_osdb\_query\_insert(): ERROR: (5203): Error executing query 'INSERT INTO category(cat\_name) VALUES ('SecurityComplianceCenterEOPCmdlet')'. Error: 'Data too long for column 'cat\_name' at row 1'.

2023/02/14 08:55:38 wazuh-dbd[264870] db\_op.c:118 at osdb\_checkerror(): INFO: (5210): Attempting to reconnect to database.

2023/02/14 08:55:38 wazuh-dbd[264870] db\_op.c:140 at osdb\_checkerror(): INFO: Connected to database 'Alerts\_DB1' at '127.0.0.1'.

2023/02/14 08:55:38 wazuh-dbd[264870] rules.c:60 at \_\_Groups\_InsertGroup(): ERROR: (5204): Database error. Unable to run query.

2023/02/14 08:55:38 wazuh-dbd[264870] db\_op.c:214 at mysql\_osdb\_query\_insert(): ERROR: (5203): Error executing query 'INSERT INTO category(cat\_name) VALUES ('ComplianceDLPSharePointClassification')'. Error: 'Data too long for column 'cat\_name' at row 1'.

2023/02/14 08:55:38 wazuh-dbd[264870] db\_op.c:118 at osdb\_checkerror(): INFO: (5210): Attempting to reconnect to database.

2023/02/14 08:55:38 wazuh-dbd[264870] db\_op.c:140 at osdb\_checkerror(): INFO: Connected to database 'Alerts\_DB1' at '127.0.0.1'.

2023/02/14 08:55:38 wazuh-dbd[264870] rules.c:60 at \_\_Groups\_InsertGroup(): ERROR: (5204): Database error. Unable to run query.

2023/02/14 08:55:38 wazuh-dbd[264870] db\_op.c:214 at mysql\_osdb\_query\_insert(): ERROR: (5203): Error executing query 'INSERT INTO category(cat\_name) VALUES ('InformationBarrierPolicyApplication')'. Error: 'Data too long for column 'cat\_name' at row 1'.

2023/02/14 08:55:38 wazuh-dbd[264870] db\_op.c:118 at osdb\_checkerror(): INFO: (5210): Attempting to reconnect to database.

2023/02/14 08:55:38 wazuh-dbd[264870] db\_op.c:140 at osdb\_checkerror(): INFO: Connected to database 'Alerts\_DB1' at '127.0.0.1'.

2023/02/14 08:55:38 wazuh-dbd[264870] rules.c:60 at \_\_Groups\_InsertGroup(): ERROR: (5204): Database error. Unable to run query.

2023/02/14 08:55:39 wazuh-dbd[264870] db\_op.c:214 at mysql\_osdb\_query\_insert(): ERROR: (5203): Error executing query 'INSERT INTO category(cat\_name) VALUES ('MipAutoLabelSharePointPolicyLocation')'. Error: 'Data too long for column 'cat\_name' at row 1'.

2023/02/14 08:55:39 wazuh-dbd[264870] db\_op.c:118 at osdb\_checkerror(): INFO: (5210): Attempting to reconnect to database.

2023/02/14 08:55:39 wazuh-dbd[264870] db\_op.c:140 at osdb\_checkerror(): INFO: Connected to database 'Alerts\_DB1' at '127.0.0.1'.

2023/02/14 08:55:39 wazuh-dbd[264870] rules.c:60 at \_\_Groups\_InsertGroup(): ERROR: (5204): Database error. Unable to run query.

2023/02/14 08:55:40 wazuh-dbd[264870] db\_op.c:214 at mysql\_osdb\_query\_insert(): ERROR: (5203): Error executing query 'INSERT INTO category(cat\_name) VALUES ('ComplianceDLPExchangeClassification')'. Error: 'Data too long for column 'cat\_name' at row 1'.

2023/02/14 08:55:40 wazuh-dbd[264870] db\_op.c:118 at osdb\_checkerror(): INFO: (5210): Attempting to reconnect to database.

2023/02/14 08:55:40 wazuh-dbd[264870] db\_op.c:140 at osdb\_checkerror(): INFO: Connected to database 'Alerts\_DB1' at '127.0.0.1'.

2023/02/14 08:55:40 wazuh-dbd[264870] rules.c:60 at \_\_Groups\_InsertGroup(): ERROR: (5204): Database error. Unable to run query.

2023/02/14 08:55:42 wazuh-dbd[264870] rules\_op.c:1152 at OS\_ReadXMLRules(): ERROR: (1450): Syntax error on regex: 'Set-.+VirtualDirectory.+?Url.+\<\w+.\*\>.\*?\<\/\w+\>.+?VirtualDirectory': 6.

2023/02/14 08:55:42 wazuh-dbd[264870] rules.c:228 at OS\_InsertRulesDB(): ERROR: (1220): Error loading the rules: 'ruleset/rules/0910-ms-exchange-proxylogon\_rules.xml'.

2023/02/14 08:55:42 wazuh-dbd[264870] main.c:256 at main(): CRITICAL: (1202): Configuration error at 'etc/ossec.conf'.

root@WAZUH:/var/ossec/logs#