### matchsig

Checks whether the string value of the field is included in the specified pattern group and outputs the result.

#### Syntax

matchsig [invert=BOOL] [verify=BOOL] guid=SIG\_GUID field=FIELD

Required Parameter

**guid=SIG\_GUID**

Pattern group GUID

**field=FIELD**

Target field name. The value of the target field must be a string, and any other key value is considered a search failure.

Optional Parameter

**invert=BOOL**

Option to invert the result of matching the value specified by the field option against the parttern group (default: f).

* t: Returns the result only if the value of the target field is not included in the pattern group.
* f: Returns the result if the string value of the target field matches at least one of the patterns in the specified pattern group.

**verify=BOOL**

Option to activate the validation for the port group at the query parsing stage (default: t).

* t: validates the pattern group at the query parsing stage.
* f: NOT validate the pattern group at the query parsing stage. This option prevents the system from issuing syntax errors at the policy synchronization stage.

#### Description

The pattern group uses the Aho-Corasick algorithm to test thousands of keywords or more simultaneously, like network intrusion detection devices. By first matching all keywords belonging to the pattern group against the input string at once and then executing the filter expression of the selected patterns sequentially, the command eventually returns the rule name that matches the pattern.

**Example of patterns**

|  |  |  |
| --- | --- | --- |
| expr (required) | expr2 (optional) | rule (required) |
| Keyword pattern: Primary high-speed detection | Boolean expression: Secondary filtering | Pattern name |
| "addextendedproc" and "xp\_cmdshell" |  | xp\_cmdshell |
| "REMOTE\_ADDR" and ("fputs" or "fwrite") | path == "lib.php" | zb now\_connect |

For example, if you set pattern "REMOTE\_ADDR" and ("fputs" or "fwrite"), filter expression path == "lib.php", rule zb now connect, the command checks whether the REMOTE\_ADDR string and the fputs or fwirte string are searched at the same time in the target field value, and then checks whether the path field value matches the lib.php string.