Wazuh Sorgu Dili (WQL) Kullanılarak Verilerin Filtrelenmesi

Wazuh API'sinin sorgularını kullanarak gelişmiş filtreleme mümkündür. Sorgular `q` parametre kullanılarak belirtilir. Bir sorgunun yapısı şu şekildedir:

- **Alan adı** : Filtrelenecek alan adı. Yanlış bir alan adı kullanılırsa, bir hata oluşacaktır.
- **Operatör** : Filtreleme yapılacak operatör:
    - `=`: eşitlik.
    - `!=`: eşitlik değil.
    - `<`: daha küçük.
    - `>`: daha büyük.
    - `~`: gibi.
    - `()`: gruplama operatörleri.
- **Değer** : Filtrelenecek değer.
- **Ayırıcı** : Birden fazla "sorguyu" birleştirmek için kullanılan operatör:
    - `,`: bir . temsil eder `OR`.
    - `;`: bir . temsil eder `AND`.

> Not: Ayrılmış karakterlerin, özellikle noktalı virgüllerin (`;` → `%3B`) yüzde kodlu olması gerekir . İşlemi kolaylaştırmak için cURL içinde `--data-urlencode` kullanabilirsiniz.

Örnekler

Örneğin, 18'den yüksek sürüme sahip Ubuntu aracılarını filtrelemek için aşağıdaki sorgu kullanılır. q parametresinin değerinin şu şekilde kodlandığını unutmayın `--data-urlencode`:

```
curl -G --data-urlencode "q=os.name=ubuntu;os.version>18" -k -X GET
"https://localhost:55000/agents?limit=500&pretty=true&select=id,name,os.name,os.version,os.codename,os.major" -H  "Authorization: Bearer $TOKEN"
```

Output


```
{
  "data": {
    "affected_items": [
      {
        "os": {
          "codename": "Bionic Beaver",
          "major": "18",
          "name": "Ubuntu",
          "version": "18.04.4 LTS"
        },
        "name": "wazuh-master",
        "id": "000"
      },
      {
        "os": {
          "codename": "Bionic Beaver",
          "major": "18",
          "name": "Ubuntu",
          "version": "18.04.4 LTS"
        },
        "name": "wazuh-agent4",
        "id": "004"
      },
      {
        "os": {
          "codename": "Bionic Beaver",
          "major": "18",
          "name": "Ubuntu",
          "version": "18.04.4 LTS"
        },
        "name": "wazuh-agent5",
        "id": "005"
      },
      {
        "os": {
          "codename": "Bionic Beaver",
          "major": "18",
          "name": "Ubuntu",
          "version": "18.04.4 LTS"
        },
        "name": "wazuh-agent6",
        "id": "006"
      },
      {
        "os": {
          "codename": "Bionic Beaver",
          "major": "18",
          "name": "Ubuntu",
          "version": "18.04.4 LTS"
        },
```

```
        "name": "wazuh-agent7",
        "id": "007"
      },
      {
        "os": {
          "codename": "Bionic Beaver",
          "major": "18",
          "name": "Ubuntu",
          "version": "18.04.4 LTS"
        },
        "name": "wazuh-agent8",
        "id": "008"
      },
      {
        "os": {
          "codename": "Bionic Beaver",
          "major": "18",
          "name": "Ubuntu",
          "version": "18.04.2 LTS"
        },
        "name": "wazuh-agent9",
        "id": "009"
      },
      {
        "os": {
          "codename": "Bionic Beaver",
          "major": "18",
          "name": "Ubuntu",
          "version": "18.04.2 LTS"
        },
        "name": "wazuh-agent10",
        "id": "010"
      }
    ],
    "total_affected_items": 8,
    "total_failed_items": 0,
    "failed_items": []
  },
  "message": "All selected agents information was returned",
  "error": 0
}
```


Daha doğru bir sonuç elde etmek için aynı alan birden fazla kez kullanılabilir. Örneğin, Ubuntu 18'den daha yüksek ancak Ubuntu 18.04.4'ten daha düşük bir sürüme sahip filtreleme ajanları:

```
curl -G --data-urlencode "q=os.name=ubuntu;os.version>18;os.version<18.04.4" -k -X GET "https://localhost:55000/agents?limit=500&pretty=true&select=id,name,os.name,os.version,os.codename,os.major" -H  "Authorization: Bearer $TOKEN"
```

Output

```
{
  "data": {
    "affected_items": [
      {
        "os": {
          "codename": "Bionic Beaver",
          "major": "18",
          "name": "Ubuntu",
          "version": "18.04.2 LTS"
        },
        "name": "wazuh-agent9",
        "id": "009"
      },
      {
        "os": {
          "codename": "Bionic Beaver",
          "major": "18",
          "name": "Ubuntu",
          "version": "18.04.2 LTS"
        },
        "name": "wazuh-agent10",
        "id": "010"
      }
    ],
    "total_affected_items": 2,
    "total_failed_items": 0,
    "failed_items": []
  },
  "message": "All selected agents information was returned",
  "error": 0
}
```


OR (,) operatörü ve LIKE AS (~) operatörünün kullanımına bir örnek, işletim sistemi adı *windows* veya *centos*içeren ajanları filtrelemek olabilir .

```
curl -G --data-urlencode "q=os.name~centos,os.name~windows" -k -X GET
"https://localhost:55000/agents?limit=500&pretty=true&select=id,name,os.name,os.version,os.codename,os.major" -H  "Authorization: Bearer $TOKEN"
```

Output


```
{
  "data": {
    "affected_items": [
      {
        "os": {
          "major": "6",
          "name": "Microsoft Windows 7 Ultimate Edition Professional Service Pack 1",
          "version": "6.1.7601"
        },
        "name": "jmv74211-PC",
```

```
        "id": "013"
      }
    ],
    "total_affected_items": 1,
    "total_failed_items": 0,
    "failed_items": []
  },
  "message": "All selected agents information was returned",
  "error": 0
}
```


Kimliği 0'dan farklı ve 4'ten küçük olan, adı alt dizeyi içeren `waz`ve ana sürümü 16 veya 18 olan Ubuntu ajanlarını elde etmek, aynı anda birden fazla operatörü içeren bir örnektir:

```
curl -G --data-urlencode "q=id!=0;id<4;name~waz;(os.major=16,os.major=18)" -k -X GET
"https://localhost:55000/agents?limit=500&pretty=true&select=id,name,os.name,os.version,os.codename,os.major" -H  "Authorization: Bearer $TOKEN"
```

Output


```
{
  "data": {
    "affected_items": [
      {
        "os": {
          "codename": "Xenial Xerus",
          "major": "16",
          "name": "Ubuntu",
          "version": "16.04.6 LTS"
        },
        "name": "wazuh-agent1",
        "id": "001"
      },
      {
        "os": {
          "codename": "Xenial Xerus",
          "major": "16",
          "name": "Ubuntu",
          "version": "16.04.6 LTS"
        },
        "name": "wazuh-agent2",
        "id": "002"
      },
      {
        "os": {
          "codename": "Xenial Xerus",
          "major": "16",
          "name": "Ubuntu",
          "version": "16.04.6 LTS"
        },
        "name": "wazuh-agent3",
```

```
        "id": "003"
      }
    ],
    "total_affected_items": 3,
    "total_failed_items": 0,
    "failed_items": []
  },
  "message": "All selected agents information was returned",
  "error": 0
}
```


Windows'ta`007` çalışan veya işletim sistemi ana sürümü 14 veya 18 olanlardan daha yüksek bir ID'ye sahip aracıları elde etmek :

```
curl -G --data-urlencode "q=id>007;(os.name~windows,(os.major=14,os.major=18))" -k -X GET
"https://localhost:55000/agents?limit=500&pretty=true&select=id,name,os.name,os.version,os.codename,os.m
ajor" -H  "Authorization: Bearer $TOKEN"
```

Output


```
{
  "data": {
    "affected_items": [
      {
        "os": {
          "codename": "Bionic Beaver",
          "major": "18",
          "name": "Ubuntu",
          "version": "18.04.4 LTS"
        },
        "name": "wazuh-agent8",
        "id": "008"
      },
      {
        "os": {
          "codename": "Bionic Beaver",
          "major": "18",
          "name": "Ubuntu",
          "version": "18.04.2 LTS"
        },
        "name": "wazuh-agent9",
        "id": "009"
      },
      {
        "os": {
          "codename": "Bionic Beaver",
          "major": "18",
          "name": "Ubuntu",
          "version": "18.04.2 LTS"
        },
        "name": "wazuh-agent10",
        "id": "010"
```

```
      },
      {
        "os": {
          "major": "6",
          "name": "Microsoft Windows 7 Ultimate Edition Professional Service Pack 1",
          "version": "6.1.7601"
        },
        "name": "jmv74211-PC",
        "id": "013"
      }
    ],
    "total_affected_items": 4,
    "total_failed_items": 0,
    "failed_items": []
  },
  "message": "All selected agents information was returned",
  "error": 0
}
```

Revision #2
Created 31 December 2024 13:30:46 by Ayşegül Sarıkaya
Updated 31 December 2024 13:35:37 by Ayşegül Sarıkaya