Helpful Hint: Blocking IPs in Elasticsearch

Jochen Kressin · 2020-11-12

In the second part of our "Helpful Hints" series, we'll examine how you can block specific IPs, or IP ranges from accessing Elasticsearch.

Search Guard provides TLS encryption and Role-Based Access Control (RBAC) to any data stored in Elasticsearch. This prevents unauthorized users from accessing data in your Elasticsearch cluster.

In some situations, you may want to limit access on a global level. For example, only allow access if the request comes from your internal network. To do that, you can use the IP blocking feature of Search Guard.

Global Blocks

Search Guard offers different types of blocks to control access to your Elasticsearch cluster on a global level.

You can allow or disallow access based on:

- usernames
- IPs
- netmasks

Blocks can be added and removed at runtime by:

- uploading the sg_blocks.yml configuration file using sgadmin

- using the Blocks REST API

A block consists of:

- a unique name
- a type (name, IP, netmask)
- a verdict (allow, disallow)
- a description (optional)

Whitelisting an IP range

We want to grant access to our Elasticsearch cluster from our internal IP network only, which in our case, can be any IP from 192.168.0.0 to 192.168.255.255.

For this we add a new block in blocks.yml and whitelist the IP range using a net mask:

```
allow_internal_network:
  type: "net_mask"
  verdict: "allow"
  value: ["192.168.0.0/16"]
  description: "Allow internal network"
```

After uploading the blocks.yml file by using sgadmin the changes take effect immediately. Access is now only possible from the internal network.

As an alternative, you can use the Blocks REST API like:

```
curl -u admin:admin \
  -XPUT "https://es.example.com:9200/_searchguard/api/blocks/internalnetwork" \
  -H 'Content-Type: application/json' \
  -d \
'    {
    "type" : "net_mask",
    "value" : [""192.168.0.0/16"],
    "verdict" : "allow",
    "description" : "Internal network only"
  }
'
```

Blacklisting individual IPs

In addition to whitelisting an IP or IP range, you can also use blacklisting. Search Guard will apply the whitelist first, and the blacklist second.

If you want to exclude one or more internal IPs from the allowed IP range we configured before, simply add a new block with the verdict disallow:

```
curl -u admin:admin \
  -XPUT "https://es.example.com:9200/_searchguard/api/blocks/internalnetwork_block_ips" \
  -H 'Content-Type: application/json' \
  -d \
'    {
    "type" : "ip",
    "value" : ["192.168.180.1"],
    "verdict" : "disallow",
    "description" : "Block specific internal IPs"
  }
'
```

Adding and removing blocks dynamically

As with all Search Guard configuration changes, any update to the blocks settings will take effect immediately. If you experience any current threats to your cluster, for example, brute-force attacks on user accounts or DOS attacks, you can add and remove blocks immediately.

Where to go next

- Read the Blocks documentation for more examples
- Check out the Blocks REST API documentation

Image: shutterstock / Dynamicfoto

This article was published on the Search Guard blog: https://search-guard.com/blog/elasticsearch-block-ips/