

# KIP-753: ACL authentication, Host field support IP network segment

- [Status](#)
- [Motivation](#)
- [Public Interfaces](#)
- [Proposed Changes](#)
  - [Command line code changes](#)
  - [Server code changes](#)
- [Compatibility, Deprecation, and Migration Plan](#)

*This page is meant as a template for writing a [KIP](#). To create a KIP choose Tools->Copy on this page and modify with your content and replace the heading with the next KIP number and a description of your issue. Replace anything in italics with your own description.*

## Status

**Current state:** *"Under Discussion"*

**Discussion thread:** <https://lists.apache.org/thread.html/r865d6bdcba7bb77758dc42b5a8888f9b38d814b0d97635e0cf03a586%40%3Cdev.kafka.apache.org%3E>

JIRA:

 Unable to render Jira issues macro, execution error.

Please keep the discussion on the mailing list rather than commenting on the wiki (wiki discussions get unwieldy fast).

## Motivation

Currently, kafka-acls.sh adds the ACL rule, and the --allow-host field only supports IP and \* options. If a user wants to set up authentication for a batch of IPs, multiple ACL rules need to be added. These IPs are usually in a network segment. I want to allow the network segment to be set in the host field of the ACL to authenticate. Any IP that allows a segment of the network will allow/deny access to the topic.

## Public Interfaces

The public interface changes are mainly divided into two parts: command-line tools and server-side interfaces. The KIP interface changes are mainly on the command line. The bin/kafka-acls.sh:

LITERAL type ACL:

- bin/kafka-acls.sh --bootstrap-server 10.0.0.92:9092 --add --allow-principal User:test1 --allow-host 192.0.1.2 --producer --topic topic
- bin/kafka-acls.sh --bootstrap-server 10.0.0.92:9092 --add --allow-principal User:test1 --allow-host 192.0.1.2/21 --producer --topic topic

PREFIXED type ACL:

- bin/kafka-acls.sh --bootstrap-server 10.0.0.92:9092 --add --allow-principal User:test1 --allow-host 192.0.1.1 --producer --topic topic --resource-pattern-type prefixed
- bin/kafka-acls.sh --bootstrap-server 10.0.0.92:9092 --add --allow-principal User:test1 --allow-host 127.0.0.1/22 --producer --topic topic --resource-pattern-type prefixed

Command line parameter specification change:

Option	Description (old)	Description(new)
--------	-------------------	------------------

<code>--allow-host</code> <String: <code>allow-host</code> >	Host from which principals listed in <code>--allow-principal</code> will have access. If you have specified <code>--allow-principal</code> then the default for this option will be set to <code>*</code> which allows access from all hosts.	Host from which principals listed in <code>--allow-principal</code> will have access. Host supports both IP and network segment formats. Eg: 192.0.0.1 or 192.0.0.1/20. If you have specified <code>--allow-principal</code> then the default for this option will be set to <code>*</code> which allows access from all hosts.
--	---	---

## Proposed Changes

### Command line code changes

None

### Server code changes

In the `matchingACLExists` method of `AclAuthorizer`, the determination of host is modified to support network segments

```
private def matchingAclExists(operation: AclOperation,
                             resource: ResourcePattern,
                             principal: KafkaPrincipal,
                             host: String,
                             permissionType: AclPermissionType,
                             acls: AclSeqs): Boolean = {
  .....
  (acl.host == host || acl.host == AclEntry.WildcardHost)
  .....
}
```

## Compatibility, Deprecation, and Migration Plan

None

## Rejected Alternatives

None