# KIP-993: Allow restricting files accessed by File and Directory ConfigProviders



## Status

**Current state**: Accepted

**Discussion thread**: *here*

**JIRA**: *here*

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

## Motivation

Currently, the built in file and directory configuration providers used have unrestricted access to files specified by the caller. In security-sensitive environments, the ability to limit the files accessible to these providers when used with Kafka Connect would be beneficial. For example:

```
config.providers=directory

config.providers.directory.class=org.apache.kafka.connect.configs.DirectoryConfigProvider

config.providers.directory.param.allowed.paths=/var/run,var/configs
```

If a caller tries to access another path, for example:

```
ssl.keystore.password=${directory:/etc/passwd:keystore-password}
```

it will return an error that prompts the user to specify the correct paths.

## Public Interfaces

The implementations, DirectoryConfigProvider and FileConfigProvider of the interface org.apache.kafka.common.config.provider.ConfigProvider**,** will be updated to introduce a configuration that limits the provider's access exclusively to the designated file or directory path.

Affected components:

- org/apache/kafka/common

Name: allowed.paths
Type: List
Documentation: Comma separated designated paths that this configuration provider has permission to access files from. If not set, all paths are allowed.
Default: empty

## Proposed Changes

Classes DirectoryConfigProvider and FileConfigProvider that implements the **ConfigProvider** interface will be updated. In the `configure()` method of the classes, the newly added configuration will be retrieved. Their `get()` method will then verify whether the file it is attempting to access resides within the designated paths and recursive access to directories will be allowed. If the file is not within any of the designated paths, an empty string will be returned for the value. This behaviour is consistent with how EnvVarConfigProvider handles when user attempts to access environment variables that are not allowed. When using FileConfigProvider, users can also specify files in the allowed.paths to limit access to specific files so that other files in the same directory are not accessible.

In cases where no path is specified, the configuration providers will retain their previous unrestricted access to any file.

This feature will not be useful when using a ConfigProvider in server.properties or in Kafka clients because providers are set in runtime only when used with Kafka Connect.

## Compatibility, Deprecation, and Migration Plan

There are no compatibility concerns since this update introduces a new configuration. In the absence of this configuration, the behaviour remains unchanged, allowing the configuration providers to access any files, ensuring seamless compatibility.

## Test Plan

New unit tests and integration testing with a client (producer/consumer) will be added.

## Rejected Alternatives

None.