Actifio Radically Simple

Actifio Tech Brief

Incremental Login Delay

The password authentication process during login to AGM has been enhanced to safeguard against brute force attacks. An incremental delay between login failures now ensures we can fulfill the security requirements for our customers. Incremental delay between login failures is supported for local database authentication as well as LDAP authentication. Incremental login delay will be disabled by default. Users will have to enable the functionality using the CLI. The Actifio CLI is fully documented in the ***Actifio CLI Reference***.

Although this feature will greatly reduce the risk of brute-force attack, it will not guarantee protection against all attacks.

Feature details

AGM users will get incremental login delay when they keep providing wrong passwords. When a user successfully logs in, the login failure delay is reset for that user. It is also reset if there are no login attempts for a user for more than one hour.

CLI Changes

A new parameter, `login.rate.control`,is available for the `setparameter` and `getparameter` commands. Incremental login delay feature will be disabled by default.

Use the `setparameter` command to enable or disable incremental delay for failed logins during authentication.

```
udstask setparameter -param login.rate.control -value true|false
```

Use the `getparameter` command to check whether the functionality is enabled. For example:

```
udsinfo getparameter -param login.rate.control
```