Audit Trail Log

Overview

From version 5.9, Artifactory maintains an Audit Trail Log which registers all operations related to users, groups and permissions to allow auditing and tracking capabilities that allow you to enforce security policies in your organization. Operations that will be registered in the log include:

- Creation, update and deletion of users
- Creation, update and deletion of groups
- Creation, update and deletion of permission targets
- Creation, update and deletion of access tokens

The Audit Trail Log is located under `$JFROG_HOME/artifactory/var/log/access-security-audit.log`

Page Contents

Enabling and Disabling

Logging audit trail events is enabled by default. It can be disabled and re-enabled using the following REST API endpoint:

This is a REST API endpoint of the Access Service

Enabling or disabling the audit trail log is a feature of the Access Service. Therefore, this call is to the Access Service whose default port is 8040.

Audit Trail Logging

Description: Enables or disables Audit Trail Logging
Since: 5.9.0
Security: Requires a user with Admin privileges to the Access service
Usage: PATCH /api/v1/config
Consumes: application/json

```
PATCH /api/v1/config
{
 "config" : "---\nsecurity:\n  audit:\n    enabled: <true | false>\n"
}
```

Sample usage showing how to disable Audit Trail Logging:

```
curl -H "Content-Type:application/json" -X PATCH -u access-admin:password http://localhost:8040/access/api/v1
/config -d '{"config" : "---\nsecurity:\n  audit:\n    enabled: false\n"}'
```

Log File Format

An entry in the Audit Trail Log has the following format:

```
Date | User IP | User | Logged Principal | Entity Name | Event Type | Event | Data Changed
```

where:

Date	A date and time stamp for the log entry formatted: yyyy-MM-dd'T'HH:mm:ss.SSSZ
User IP	The IP address of the user that performed the operation in Artifactory
User	The username of the user that performed the operation in Artifactory
Logged Principal	The login information of the Artifactory service that performed the operation against Access

Entity Name	The security entity that the operation modified. For example, permission target name, group name, username etc.
Event Type	The type of operation performed where: C = Create, U = Update, D = Delete
Event	The security entity on which the operation was performed where: USR = user, GRP = Group, PRM = Permission, TKN = Token

Data Changed	A JSON describing the data that was changed
	The following describes a map that specifies permissions when creating or updating a permission target:
	r = Read
	t = Annotate
	w = Deploy/Cache
	d = Delete/Overwrite
	m = Manage

Example 1

An admin user named **admin** created a user named **bob** and added him to 3 groups named: **dev-team**, **code-reviewers**, **rnd-team-leaders**.

```
2018-02-18T11:57:05.282+0200|10.0.0.132|admin|jf-artifactory@a64971e1-3c3c-4069-a769-dfb473dc8a67|bob|C|USR|
{
   "added":{
      "customData.updatable_profile":"true",
      "password":"*",
      "groups.dev-team":"UserGroupImpl(name=dev-team, realm=internal)",
      "groups.code-reviewers":"UserGroupImpl(name=code-reviewers, realm=internal)",
      "allowedIps":"[*]",
      "groups.rnd-team-leaders":"UserGroupImpl(name=rnd-team-leaders, realm=internal)",
      "realm":"internal",
      "email":"bob@company.com",
      "status":"enabled",
      "username":"bob"
   }
}
```

Example 2

An admin user named **devops-admin** added a user named **dylan** to a permission target named **nodejs-developers** with read, annotate, deploy and delete permissions.

```
2018-02-18T13:19:51.644+0200|10.0.0.132|devops-admin|jf-artifactory@a64971e1-3c3c-4069-a769-dfb473dc8a67|jf-artifactory@a64971e1-3c3c-4069-a769-dfb473dc8a67:nodejs-developers|U|PRM|{
   "added":{
      "actions.dylan(USER):w":"dylan(USER):w",
      "actions.dylan(USER):d":"dylan(USER):d",
      "actions.dylan(USER):r":"dylan(USER):r",
      "actions.dylan(USER):n":"dylan(USER):n"
   }
}
```

Managing Log File Size

The Audit Trail Log size is managed as a series of a files which are configured with a maximal size. By default, this log is limited to a size of 1GB split into 10 files each of which is up to 100MB in size.

To change the number of files or their maximal size, change the following tags of the `SECURITY.AUDIT` log appender in *`$JFROG_HOME/artifactory/var/etc/access/logback.xml:`*

Maximum number of files: <`maxIndex`>

Maximum size of each file: <`MaxFileSize`>