Inotify v1 Goals and Design

Please see inotify-intro.[latest].pdf for background and a longer-term vision for the system.

Overview

In the current design, clients must have superuser privileges. They keep track of the highest transaction ID TX_MAX for which they have received events. They pull new events from the NameNode by issuing an RPC with TX_MAX, and the NN responds with events that reflect transactions with IDs greater than TX_MAX. We send events that reflect the state changes we believe clients would be most interested in; not all FSEditLogOps have a corresponding inotify event. In particular, we use the following events:

```plaintext
enum INodeType {
    FILE = 0x0;
    DIRECTORY = 0x1;
    SYMLINK = 0x2;
}

message CreateEventProto {
    required INodeType type = 1;
    required string path = 2;
    required int64 ctime = 3;
    required int32 replication = 4;
    required string ownerName = 5;
    required string groupName = 6;
    optional string symlinkTarget = 7;
    repeated AclEntryProto acls = 8;
}

message CloseEventProto {
    required string path = 1;
}

message ReOpenEventProto {
    required string path = 1;
}

message RenameEventProto {
    required string srcPath = 1;
    required string destPath = 2;
}

message MetadataUpdateEventProto {
    required string path = 1;
    optional int64 mtime = 2;
    optional int64 atime = 3;
}
```
The NN calls FSEditLog.selectInputStreams to read transactions with IDs greater than the client's specified TX_MAX from its journals and converts them to the above events. We will recommend settings for dfs.namenode.num.extra.edits.retained and dfs.namenode.num.extra.edits.segments.retained so that under reasonable conditions edits are never deleted before a client has a chance to pull them.

**Justifications**

A. Why a pull model as opposed to push?

The first reason is simplicity. We can leverage Hadoop RPC and don't have to design our own communication protocol or manage an extra set of open sockets on the NameNode. The second is that even if we adopted the push model, we would still need build a system that pulls from journals (or use a much more complex, stateful per-client queuing system, discussed in B) for the cases where 1) a client crashes and misses some edits and 2) there is a NameNode failover and some edits are logged to the new primary before clients can connect to it. So we might as well rely solely on the pull model for now, and if efficiency concerns emerge, we can look again into the push model.

It is certainly somewhat inefficient to fetch edits from the Quorum Journal or other journals on every client pull (although this shouldn't impact NameNode CPU time much), but it should not be difficult to build an edit (or event) cache on the NameNode so that several client requests for the same events do not all result in journal reads. Additionally, if the the NameNode stores edits in a local journal in addition to a remote journal, we can read from the local journal whenever possible.

B. Why superuser-only?

If we allowed unprivileged users to become inotify clients, a reasonable security model might be to allow them to read events for directories and files for which they have read access. The issue then is that with our pull-based system, in order to know whether an unprivileged client has permissions to read an event based on a transaction X, we need to know what permissions the client had when transactions up to X and nothing more had been applied to the namesystem. This is exceedingly difficult, since we would essentially need to reconstruct the namesystem at that earlier point in time. So the only way to support unprivileged users would be to adopt a push-based system where we determine which clients to send an event to right when it occurs, requiring only a lookup of the current namesystem state. But as discussed in A, it is much harder to build a push-based system than a pull-based one. In addition, while we can handle client failures and namenode failovers by falling back to the pull model for superusers (as discussed again in A), for unprivileged users (since pull is infeasible) we would need to maintain some sort of queue of unread events on the NameNode that is preserved in
the event of a failover. Or we would have to loosen our guarantees to unprivileged clients – events missed in such situations are permanently lost and clients must use an ls -R or something similar to resynchronize their view of the filesystem state. In sum, adding support for unprivileged users introduces complexity that does not seem justified for the first version of inotify.

**Future Work**

1. Support running the inotify logic in a separate, reduced-functionality NameNode so that the load on the primary NameNode is reduced.
2. Allow clients to watch events from specific directories rather than from the entirety of HDFS. We will need to decide whether undesired events should be filtered out on the NameNode or client side.
3. Possibly support a inotify-specific security model (e.g. path-based security) that is separate from HDFS permissions and eliminates the complexities discussed in part B of the previous section.