



Cloud Data Management Interface Extension: Expiring ACEs

Version 1.0b

"Publication of this Working Draft for review and comment has been approved by the Cloud Storage Technical Working Group. This draft represents a "best effort" attempt by the Cloud Storage Technical Working Group to reach preliminary consensus, and it may be updated, replaced, or made obsolete at any time. This document should not be used as reference material or cited as other than a 'work in progress.' Suggestion for revision should be directed to <http://snia.org/feedback>."

Working Draft

Revision History

Date	Version	By	Comments
1/22/12	1.0a	John Eastman, Mezeo Software James Perry, Mezeo Software	Initial Creation
1/23/12	1.0b	Marie McMinn	Performed technical edit.

The SNIA hereby grants permission for individuals to use this document for personal use only, and for corporations and other business entities to use this document for internal use only (including internal copying, distribution, and display) provided that:

- Any text, diagram, chart, table, or definition reproduced shall be reproduced in its entirety with no alteration, and,
- Any document, printed or electronic, in which material from this document (or any portion hereof) is reproduced shall acknowledge the SNIA copyright on that material, and shall credit the SNIA for granting permission for its reuse.

Other than as explicitly provided above, you may not make any commercial use of this document, sell any excerpt or this entire document, or distribute this document to third parties. All rights not explicitly granted are expressly reserved to SNIA.

Permission to use this document for purposes other than those enumerated above may be requested by e-mailing tcmd@snia.org. Please include the identity of the requesting individual and/or company and a brief description of the purpose, nature, and scope of the requested use.

Copyright © 2012 Storage Networking Industry Association.

Expiring ACEs CDMI Extension

Overview

A common trait of cloud storage services is the ability to 'share' an object with other clients for a limited time. This extension proposes an additional attribute of ACEs used in ACLs that imposes a time limit (expiration) on the ACE. Once the expiration has passed, the ACE would no longer be valid and is no longer included in the authorization calculation for the object.

Modifications to the current CDMI spec:

1) Insert into Clause 16.1.6 – ACL Evaluation:

After the bullet item:

- ACEs that do not refer to the principal P requesting the operation are ignored.

Insert bullet:

- ACEs that have an expiration value less than the current time are ignored.

2) Change 16.1.6 Clause – ACL Evaluation:

Original text:

```
ACE = { acetype , identifier , aceflags , acemask , acetime }
```

Revised text:

```
ACE = { acetype , identifier , aceflags , acemask , acetime, expiration }
```

3) Insert into 16.1.6 Clause after “acemask = uint_t | acemaskstring”:

```
expiration = uint_t
```

4) Insert into 16.1.6 Clause after “When ACE masks...”:

When ACE expiration is presented in string format, it shall, at all times, be specified in ISO-8601 point-in-time format, as described in 5.14.

5) Insert New Clause 16.1.? – ACE Expiration:

An ACE may have an optional expiration associated with it. The expiration is a point-in-time value, in ISO-8601 point-in-time format, as described in 5.14, which specifies that the ACE is no longer valid and shall be ignored after the time specified.