Lustre Capabilities Security Level

Fan Yong

2008-06-20

1 Introduction

Lustre introduces MDS/OSS capabilities to enhance lustre system security on HEAD branch. In this document, we define lustre capabilities security level to match kinds of security requirement. It also describes how the lustre system runs under different capabilities security levels, including interoperability between 1.8.x client and 2.0 server, remote clients, and so on.

2 Nomenclature

- 1.8.x client: it is 1.6 code based which does not support MDS/OSS capabilities.
- 2.0 server: it is HEAD code based which supports MDS/OSS capabilities, such feature can be switched by some proc interface(s) or mount option(s).
- Remote client: it is HEAD code based, which means the client is in different kerberos domain against server, and is regarded as untrusted one. The contrary case is local client, which is in the same kerberos domain as server. A local client can claim to be remote one, but the inverted case is forbidden. Both remote client and local client are 2.0 client, and support MDS/OSS capabilities.

3 specification

Generally, there are four security levels for lustre capabilities as following:

- Level 0: disable MDS/OSS capabilities for all clients.

  This is the default capabilities security level for HEAD branch now. MDS/OSS capabilities are neither generated nor verified. It is for some very closed (all clients are trusted) and high performance lustre environment. On the other hand, if 1.8.x client wants to talk with 2.0 server, the system must run under such capabilities security level. So it is for interoperability between 1.8.x client and 2.0 server also.

- Level 1: enable MDS/OSS capabilities on remote client.

  It is for an open lustre environment with both local client and remote client. Under such level, the MDS/OSS capabilities will be enabled automatically for remote client, but disabled for local client.

- Level 2: enable MDS/OSS capabilities on selected client(s).

  Under this level, the lustre administrator can configure the system to enable MDS/OSS capabilities for some local client also. That means, except the remote client is untrusted, some local client maybe untrusted also, the lustre administrator can configure the system to verity their behavior as needed. Supporting MDS/OSS capabilities for selected client(s) is a planing feature which maybe done in 2.x release or later.

- Level 3: enable MDS/OSS capabilities on all clients.

  It is the highest capabilities security level up to now. All the clients behavior (both local client and remote one) are need to be verified. Since signing capabilities is time-consuming work, under such level, the performance maybe some affected.

According to the description above, we have the following rules:

- If the lustre system contains 1.8.x client and 2.0 server, for the interoperability between them, the system only can run under level 0, otherwise, the 1.8.x client will be refused when connects to 2.0 server.

- If the lustre system will enable remote client,the system should run under level 1 or other higher level. Otherwise, the remote client will be refused when connects to server.

4 Feature control

We will support mount option for MDS/OSS to allow configure lustre capabilities security level when mount.

Currently, HEAD branch supplies two proc interfaces to control MDS/OSS capabilities independently. But I think the MDS/OSS capabilities should be enable/disable on the same time, only enable MDS or OSS capabilities on some clients make little sense for lustre security. Since a client is untrusted, all of its behavior both on MDS and on OSS should be verified. So I suggest to merge such control proc interfaces into one. When capabilities security level is changed on-line (for server), the clients should remount to match the new security level.