Oracle ACFS Security and Encryption

An Oracle White Paper
April, 2011

ORACLE

EXECUTIVE OVERVIEW

Oracle Automatic Storage Management Cluster File System (ACFS) is a major component of the Oracle Cloud File System, which is designed to help organizations to deploy their applications, databases and storage in private clouds.

Oracle ACFS security and encryption are part of ACFS integrated data services. Other ACFS data services include snapshots, tagging, and replication.

The combined capabilities of Oracle ACFS security and encryption provide the security foundation for ACFS and the Oracle Cloud File System.

ORACLE ACFS SECURITY

Oracle ACFS security provides realm-based security for Oracle ACFS file systems, enabling users to create realms and specify security policies for users and groups to control access to file system objects. This security feature provides a fine-grained access control on top of the access control provided by the operating system.

Oracle ACFS security uses realms, rules, rule sets, and command rules to enforce security policies.

- An Oracle ACFS realm is a virtual container of files and directories; access is defined by security filters (command rules and rule sets)
- Oracle security rules are Boolean expressions based on system parameters such as: time, user name, host name, IP address and application rules; they enable multi-factor authorization for realm secured files and directories
- Rule set is a set of one or more security rules
- Command rules are associations of file system operations such as open, create, read, write, close etc.; they enable fine-grained access control

An ACFS security administrator manages security for all ACFS file systems in a cluster and has a security administration password that is different from his/her OS password. The security administration password is stored in an Oracle

Wallet for additional security, and all security commands are protected by this password.

ACFS security has feature-rich Command Line Interface (CLI) that supports

- Creation and destruction of realms
- Addition and deletion of users, groups, rule sets, and command rules to realms.
- Creation, modification, and destruction of rules and rule sets
- Backup and restore of ACFS security policies
- Batch command that supports executing several commands at once
- Info commands that display details about all aspects of ACFS security

ASM Configuration Assistant (ASMCA) GUI tool also provides basic configuration of ACFS security.

Oracle ACFS security can utilize the encryption feature to protect the contents of realm-secured files stored in Oracle ACFS file systems.

Oracle ACFS Security Rule Set and Rules

It is important to understand the concept of security rule set and rules to take full advantage of the ACFS security feature. The security rule set option is either ALL_TRUE or ANY_TRUE, and the default is ALL_TRUE.

ALL_TRUE means that all the rules in the rule set must be evaluated to grant access or access is denied.

ANY_TRUE means any one of the rules in the rule set must be evaluated to grant access or access is denied.

The security rule option is either ALLOW or DENY (access), and the default is DENY. There are four rule types: username, time, host, and applications.

Below are two examples of using rule set and rules.

Example 1: only allow application "gedit" to edit a configuration file between 9-11am.

Rule set option = ALL_TRUE

Rules	Rule Option
1. Application=gedit	Allow
2. Time=9-11am	Allow

If another application like "vi" tries to edit the configuration file between 9-11am, it will fail rule 1, so no access to the file is allowed.

Example 2: allow user to access files in two different time windows: 8-10am and 2-4pm.

Rule set option = ANY_TRUE

Rules	Rule Option
1. Time=8-10am	Allow
2. Time=2-4pm	Allow

Access to files outside of the two time windows will not work because it will fail both rules 1 and 2.

Basic ACFS Security Steps:

Cluster wide commands

Command	User	Function
acfsutil sec init	Root	Initialize ACFS security for the cluster
acfsutil sec admin add/delete	Security Administrator	Add/remove an ACFS security administrator
acfsutil sec admin password	Security Administrator	Change the password of an existing ACFS security administrator

Only a security administrator can run the following commands.

Command	Function
acfsutil sec prepare	Prepare an ACFS file system for ACFS security (per file system)
acfsutil sec realm create/destroy	Create/destroy an ACFS security realm
acfsutil sec realm add/delete	Add/delete objects in an ACFS security realm
acfsutil sec rule create	Create an ACFS security rule
acfsutil sec ruleset create	Create an ACFS security ruleset
acfsutil sec info	Display ACFS security information (Realms, Rules, Rulesets, Realm properties of files)

Examples

Accessing Medical Records

To setup a system so that only designated person (MedHistAdmin2) can access medical records between 10pm and 2am.

1. Initialize Oracle ACFS security

```
# /sbin/acfsutil sec init –u SecAdmin –g SecAdminGrp
; Designate an OS user as the first security administrator
$ /sbin/acfsutil sec admin passwd
$ /sbin/acfsutil sec admin add SecAdmin2     ; Add additional security admin
```

2. Prepare and enable an ACFS file system for security
$ /sbin/acfsutil sec prepare –m /acfsmounts/acfs1

3. Create a security realm on the file system
$ /sbin/acfsutil sec realm create MedHistRealm –m /acfsmounts/acfs1 –e on –a AES –k 128
-d "Realm for Medical History information"

4. Create security rules
$ /sbin/acfsutil sec rule create MedHistRule1a –m /acfsmounts/acfs1 –t time 22:00:00, 02:00:00 –o ALLOW

5. Create security rule set
$ /sbin/acfsutil sec ruleset create MedRuleSet1 –m /acfsmounts/acfs1

6. Add rules to rule sets
$ /sbin/acfsutil sec ruleset edit MedRulesSet1 –m /acfsmounts/acfs1 –a MedHistRule1a

7. Add objects to a security realm
$ /sbin/acfsutil sec realm add MedHistRealm –m /acfsmounts/acfs1 –l ALL:MedRuleSet1
-f –r /acfsmounts/acfs1/medicalrecords

A simple way to test this is try to access (as SecAdmin2) the medical record both inside and outside of the 10pm-2am window.

Protecting TDE Wallet

To protect Oracle Transparent Data Encryption (TDE) wallet on the ACFS file system (by allowing only Oracle binary to access the wallet.)

The file system mounted on /u01/app/oracle/acfsmounts/data_tdevolume for security

1. Create a realm
$ /sbin/acfsutil sec realm create TDEWalletRealm -m /u01/app/oracle/acfsmounts/data_tdevolume -d "Realm to secure the TDE Wallet" -e off

2. Create a rule
$ /sbin/acfsutil sec rule create allowOracleAppRule –m /u01/app/oracle/acfsmounts/data_tdevolume –t application /path_to/oraclebinary –o ALLOW

3. Create a ruleset
$ /sbin/acfsutil sec ruleset create TDEWalletRuleSet –m /u01/app/oracle/acfsmounts/data_tdevolume

4. Add the rule in the ruleset

$ /sbin/acfsutil sec ruleset edit TDEWalletRuleSet –m /u01/app/oracle/acfsmounts/data_tdevolume -a allowOracleAppRule -o ALL_TRUE

5. Specify option ALL for the ruleset
$ /sbin/acfsutil sec realm add TDEWalletRealm –m /u01/app/oracle/acfsmounts/data_tdevolume -u oracle -l ALL:TDEWalletRuleSet –f -r /u01/app/oracle/acfsmounts/data_tdevolume/data_wallet

A simple way to test this is try to access (ls, vi, cat, etc.) the TDE wallet as root or security administrator, and it should fail.

ORACLE ACFS ENCRYPTION

Oracle ACFS encryption enables users to encrypt data stored on disk (data-at-rest). The encryption feature protects data in an Oracle ACFS file system and prevents unauthorized use of data in the case of data loss or theft.

ACFS encryption can be applied to the entire file system or just individual files and directories. It is completely transparent to authorized users, and applications work unchanged with encrypted files. Encrypted and unencrypted files can co-exist on the same file system.

System administrators and Oracle ACFS security administrators can initiate encryption operations. Also, users can encrypt and decrypt files they own.

Each file is protected by two keys, the file encryption key (FEK) and the volume encryption key (VEK). File data is encrypted using a unique FEK; the FEK is stored on disk, and is encrypted using a VEK.

Volume encryption keys are stored in an Oracle Wallet, which can be password protected, in the OCR.

Data is encrypted when flushed to disk and decrypted when read from disk. Encryption performance varies depending on the workload, and there's minimal overhead when working with cached data.

An Oracle ACFS security administrator can manage encryption parameters on a per-realm basis.

The dual key (VEK and FEK) implementation enhances data protection and allows fast VEK rekeying. By using a separate master VEK, only FEK of each file needs to be re-encrypted instead of all of the file data.

Basic ACFS Encryption Steps:

Command Tool Example	Function
acfsutil encr init	Initialize the cluster for encryption, and creates the OCR encryption key store for storing volume encryption keys
acfsutil encr set	Sets encryption parameters on a particular file system
acfsutil encr on/off	Turns on/off encryption, this can be done for the entire file system or for individual files or directories
acfsutil encr rekey	Create a new FEK or VEK

Example

Below is an usage example:

1. create storage for encryption keys
/sbin/acfsutil encr init

2. Set encryption parameters
/sbin/acfsutil encr set -a AES -k 256 -m /u01/app/acfsmounts/myacfs

3. Encrypt an ACFS file system
/sbin/acfsutil encr on -m /u01/app/acfsmounts/myacfs

4. Turn off encryption
/sbin/acfsutil encr off -m /u01/app/acfsmounts/myacfs

One way to check the encryption is to dd the file after it is encrypted, and examines the file to ensure it's not readable.

CONCLUSION

Oracle ACFS security provides realm-based security for Oracle ACFS file systems, and it provides a fine-grained access control on top of the access control provided by the operating system.

Oracle ACFS encryption enables users to encrypt data stored on disk, and it protects data in an Oracle ACFS file system and prevents unauthorized use of data in the case of data loss or theft.

Together Oracle ACFS security and encryption provide a robust security foundation for ACFS as well the Oracle Cloud File System.

ACFS Security and Encryption
April, 2011
Author: Paul Tsien
Contributing Authors: Balaji Pagadala, Harsha Sabbineni, Samarjeet Tomar

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
www.oracle.com

Copyright © 2003, Oracle. All rights reserved.
This document is provided for information purposes only
and the contents hereof are subject to change without notice.
This document is not warranted to be error-free, nor subject to
any other warranties or conditions, whether expressed orally
or implied in law, including implied warranties and conditions of
merchantability or fitness for a particular purpose. We specifically
disclaim any liability with respect to this document and no
contractual obligations are formed either directly or indirectly
by this document. This document may not be reproduced or
transmitted in any form or by any means, electronic or mechanical,
for any purpose, without our prior written permission.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective owners.