Oracle Flash Storage System and Oracle MaxRep for SAN Security Guide

Part Number E56029-01
Oracle Flash Storage System, release 6.1
Oracle MaxRep for SAN, release 3.0
2014 October

ORACLE

Contents

Preface

This guide will help you understand the security features of an Oracle Flash Storage System and Oracle MaxRep for SAN.

Related Documentation

- *Oracle Flash Storage System Administrator's Guide*
- *Oracle FS1-2 Flash Storage Installation Guide (Racked)*
- *Oracle FS1-2 Flash Storage Installation Guide (Not Racked)*
- *Oracle MaxRep for SAN User's Guide*
- *Oracle MaxRep for SAN Hardware Guide*
- *Oracle Flash Storage System Glossary*

Oracle Contacts

Table 1 Oracle resources

For help with...	Contact...
Support	*http://www.oracle.com/support* (www.oracle.com/support)
Training	*https://education.oracle.com* (https://education.oracle.com)
Documentation	• *Oracle Technology Network Documentation* (http://docs.oracle.com) • From Oracle FS System Manager (GUI): **Help** > **Documentation** • From the Oracle FS System web server: (http://*system-name-ip*/, where *system-name-ip* is the name or the public IP address of your system)
Documentation feedback	*http://www.oracle.com/goto/docfeedback* (http://www.oracle.com/goto/docfeedback)
Contact Oracle	*http://www.oracle.com/us/corporate/contact/index.html* (http://www.oracle.com/us/corporate/contact/index.html)

Product Overview

This section provides an overview of the Oracle FS System and Oracle MaxRep for SAN.

Oracle FS System

An Oracle FS System is an integrated, full-featured network storage system. The system combines many industry-leading features, including:

- Flash optimized design of a hybrid (SSD and HDD) storage array
- QoS tools to manage the storage resources (capacity, CPU, and cache) across multiple workloads that are based on the requirements or conditions of your business
- QoS Plus Auto Tiering to optimize dynamically the finely-grained storage allocations
- Scalability in capacity, in connectivity, and in performance
- Enterprise-grade RAS (reliability, availability, and serviceability)
- Engineered for Oracle databases and Oracle applications

For detailed instructions about managing and administering the Oracle FS System, refer to *Oracle Flash Storage System Administrator's Guide*.

Oracle MaxRep for SAN

Oracle MaxRep for SAN uses one or more Replication Engines to replicate Oracle FS System data in a storage area network (SAN) environment. The Replication Engine is a 2U server that manages and monitors the replication and recovery process.

In SAN replication, pairs of LUNs that are made up of source and target LUNs, are called replication pairs. The LUNs can reside on two Oracle FS Systems in a single location or on separate remotely distributed Oracle FS Systems, designated as primary and secondary.

The transfer of data takes place automatically as the data on the source LUN changes. Those changes are replicated to the target LUN. The replication pair updates continuously as long as the integrity of both LUNs persists and the communication link between the LUN locations is maintained. Oracle MaxRep for SAN can replicate between Oracle FS Systems that reside in the same data center, or

are geographically distributed between remote locations. The Oracle MaxRep Replication Engines use communication links between the two sites to replicate changes.

For details about Oracle MaxRep for SAN Replication Engines, refer to *Oracle MaxRep for SAN Hardware Guide.*

Secure Installation and Configuration

Initial Installation

The Oracle FS System includes a default account name and password that is used for initial installation and configuration of the system. After the first login, the system prompts you to enter a new password.

> **Note**: Oracle requires that you change the default passwords for security purposes. Be sure that the Primary Administrator also obtains this password. Keep the password secure.

For more information about installing and configuring the system, refer to *Oracle FS1-2 Flash Storage Installation Guide.*

Physical Security

To control access to your system, you must maintain the physical security of your computing environment. For example, a system that is logged in and left unattended is vulnerable to unauthorized access. The computer's surroundings and the computer hardware must be physically protected from unauthorized access at all times.

The Oracle FS System and Oracle MaxRep Replication Engine are intended for restricted access whereby access is controlled through the use of a means of physical security (for example, key, lock, tool, badge access) and personnel authorized for access have been instructed on the reasons for the restrictions and any precautions that need to be taken.

Network Security

Install the Oracle FS System and the Oracle MaxRep Replication Engine behind a firewall and connected to a secure customer management network. Firewalls provide assurance that access to the system is restricted to a known network route, which can be monitored and restricted, if necessary.

Enable only the network services that you know are required by connected servers.

If there are any firewalls located between the Pilot and the source or destination of a service, the ports must be open for that service to function.

The following table lists all of the software ports that are used by the Pilot for communicating with other components within the Oracle FS System and with services running on the network.

Table 2 Pilot TCP ports

Port number	Application	Description
22	Application SSH	This port may be opened only in rare situations if it is needed for service purposes. In those situations, the administrator is notified by Oracle Support that this port needs to be opened. This port is disabled by default.
25	Simple Mail Transfer Protocol (SMTP)	Used by the Oracle FS System for email notifications that are sent by the Oracle FS System and for account password recovery. This port is only used for outbound communication to a configured email server.
53	DNS	Used by the Oracle FS System to resolve the address of the Oracle ASR server and to locate mail servers for sending password recovery instructions.
80	HTTP	Used by the Oracle FS System for status monitoring and the download from the Pilot of documentation and various applications, such as Oracle FS System Manager (GUI).
123	Network Time Protocol (NTP)	Used by the Oracle FS System to synchronize the system time with an external time service provider.
161	Simple Network Management Protocol (SNMP)	Used by a host SNMP Management Server to monitor the Oracle FS System.
162	SNMP traps	Used by the Oracle FS System to transmit SNMP traps to an external management application or by UPS devices to send notifications to an Oracle FS System. For example, used by compliant UPS devices to warn the Oracle FS System that the UPS device is running on battery power.
443	HTTPS	Used by the HTTPS Call-Home option on the Pilot. This port must be open on all three Pilot ports to the Oracle Call-Home server. Also used by HTTPS for checking status and alerts, using a web browser.
8083	Oracle WebCLI service	Used by the Oracle FS System for the FSCLI interface and for application integration.
8085	REST interface	Used by the Oracle FS System for application integration with a REST-based management application. This port is disabled by default.
10000	Network Data Management Protocol (NDMP)	Used by the Oracle FS System to provide backup and restore access to all file systems on the Oracle FS System.

26012	Oracle FS System Manager	Used by the Oracle FS System Manager (GUI) and Oracle FS Path Manager (FSPM) to communicate with the Oracle FS System.

The following table lists all of the software ports that are used by the MaxRep Replication Engine for communicating with storage arrays, application hosts, and other replication Engines running on the network:

Purpose	Replication Engine	Primary LUN	Secondary LUN
User Interface	Inbound HTTP		
Default: TCP Port 80	N/A	N/A	N/A
Configuration	Inbound HTTP		
Default: TCP Port 80	N/A	N/A	N/A
Or TCP (21 + configured passive port range	N/A	N/A	N/A
Or TCP (20 + 21)	Outbound FTP or (>1024)	Outbound FTP or (>1024)	N/A
Data resync	Inbound TCP Port 873	N/A	N/A
FX data (Push)	N/A	N/A	N/A
FX data (Pull)	N/A	N/A	N/A

Software and Firmware Updates

The Oracle FS System and the Oracle MaxRep for SAN software and firmware are updated on a regular basis.

Download the latest software and firmware updates from My Oracle Support (MOS) to ensure that your Oracle FS System is up to date. You can download general availability releases, as well as patches specific to your system, from MOS.

In addition to software updates that you perform, the Oracle FS System performs automatic updates to hardware components using firmware already stored in the system.

For example, when replacement hardware is installed and the replacement hardware is at a lower firmware version than the current system version, the firmware in the new hardware is automatically updated. Automatic updates also occur during a system, Controller, or Drive Enclosure restart where a system software update contains non-critical hardware firmware updates and the update

has been purposely ignored by the system during non-disruptive updates due to the additional time needed for installation.

Drive firmware updates are never installed on a system restart unless an administrator specifies that the drive firmware is to be updated.

Account Management

For more information about managing accounts, refer to *Oracle Flash Storage System Administrator's Guide*.

Administrator Account Types

Administrator accounts have certain privileges, which depend on the role of the account. To administer an Oracle FS System, you must log in using an administrator account. Every account performs a specific role that defines system privileges. The following table describes the privileges for each administrator role for the Oracle FS System.

Table 3 Administrator privileges by role

Administrator role	Privileges
Primary Administrator	Performs all configuration, management, and monitoring tasks, including the ability to modify all other accounts. This account cannot be deleted or disabled.
Administrator 1	Performs all configuration, management, and monitoring tasks except for running the Drive Enclosure console.
Administrator 2	Performs all tasks except for the following caveats: • Cannot create and manage File Servers and administrator accounts. • Cannot modify global system settings or settings for Small Network Management (SNMP) and Network Data Management Protocol (NDMP) settings. • Cannot modify software configurations or hardware configurations. • Cannot shut down the system. • Cannot run the Drive Enclosure console.
Monitor	Displays system information only; cannot modify the configuration. Can modify the account attributes of their account.
Oracle Support	Performs limited customer service-only functions; cannot modify the configuration. This account cannot be deleted or disabled. **Note**: Only the Oracle Support personnel can use this account. For the complete list of command options that this role is authorized to perform, see the PARAMETERS section in a specific Oracle FS CLI command.
Support	Performs limited customer service-only functions; cannot modify the configuration. For the complete list of command options that this role is authorized to perform, see the PARAMETERS section in a specific Oracle FS CLI command.

The following table describes the privileges for each administrator role for the Oracle MaxRep Replication Engine.

User Type	Privileges
Primary Administrator	Performs all configuration, management, and monitoring tasks, including the ability to modify all other accounts. This account cannot be deleted or disabled.
Admin Access	Performs all configuration, management, and monitoring tasks .
Non-admin Access	Performs monitoring tasks, and can manage account settings for the user only.

Disable Accounts

You can disable administrator accounts for the Oracle FS System. When you disable an account, that account cannot establish a new login to the system using the GUI or FSCLI.

Note: You cannot disable the Primary Administrator account.

NDMP Account

The NDMP account on the Oracle FS System uses the same password validation rules and routines as the other system accounts.

Password Protection

The following sections describe how the Oracle FS System protects account passwords. For complete details about password protection and password security requirements, refer to *Oracle Flash Storage System Administrator's Guide*.

Password Strength

Passwords for the Oracle FS System must adhere to the following security policy:

- Must be eight characters to 16 characters in length
- Cannot contain dictionary words
- Cannot be any of the last 50 passwords

Note: The system retains recent passwords for one year.

- Must contain at least one uppercase letter, one lowercase letter, one numeric character, and one special character

- Can have a default duration of up to 180 days

Password Expiration

- When a password expires, the system notifies the user at login. The system directs the user to the Account Settings page in Oracle FS System Manager (GUI) or provides a prompt in the Oracle FSCLI to reset the password. The user will not be able to login again until after they reset the password.
- You can configure the duration in which a password is set to expire from 1 to 180 days for each account that you create.

> **Note**: Refer to your company's policy on password expiration to determine the duration you should set.

- The system displays a system alert 10 days and again one day before the password is set to expire. The alert notifies the user about the expiration date and reminds the user to change the password.
- The system retains up to 50 used passwords for each account, and does not allow the user to reuse old passwords.

> **Note**: The system does permit a password from one account to be the same as a previously used password of a different account.

Password Repository

It is your responsibility to maintain a repository of system passwords, including those used by Oracle Support. You must also be prepared to provide the required password access to Oracle Support when Oracle Support requires access.

Password Recovery

The Oracle FS System allows the ability for users to reset forgotten passwords for the Oracle FS System. An email server must be set up and the user must have a valid email address associated with the user account.

For security auditing, the system generates an event that specifies the account that reports the forgotten password.

Failed Login Attempts

You can set the number of consecutive failed login attempts that the Oracle FS System allows. When the threshold is exceeded, the system disables the account and writes an entry in the event log. Only a Primary Administrator or an Administrator 1 can re-enable the account. After the account is reenabled, the system resets the counter upon a successful login. The failed login attempts value must be between 1 and 20 (the default is 10 attempts).

Session Time-Out Settings

The customer can set the session time-out so that the Oracle FS System terminates a session after a given period of inactivity. The session time-out value must be between 1 and 999 minutes (the default is 20 minutes).

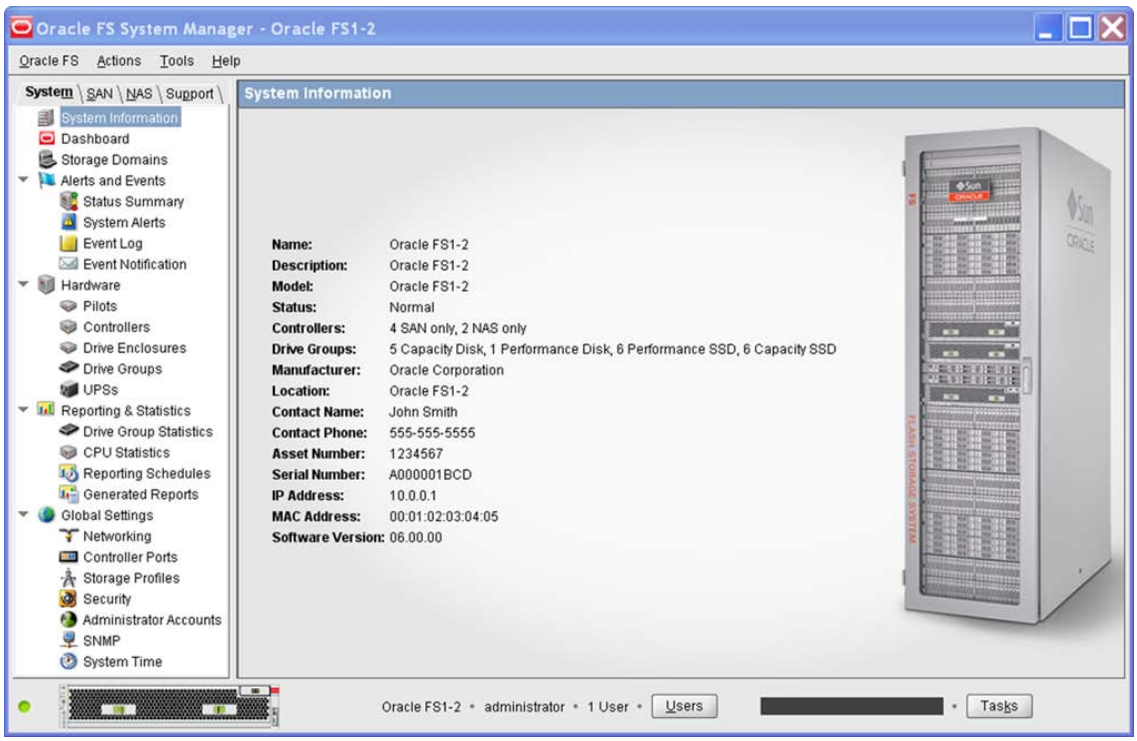
Oracle FS System Access

The Oracle Flash Storage System is managed by using the Oracle FS System Manager (GUI) or the Oracle FS CLI (FSCLI). These interfaces are described in the following sections. For more information about using the interfaces, refer to *Oracle Flash Storage System Administrator's Guide*.

Oracle FS System Manager Access

Use Oracle FS System Manager (GUI) to deploy, provision, manage, and maintain an Oracle FS System.

Figure 1 Oracle FS System Manager (GUI)



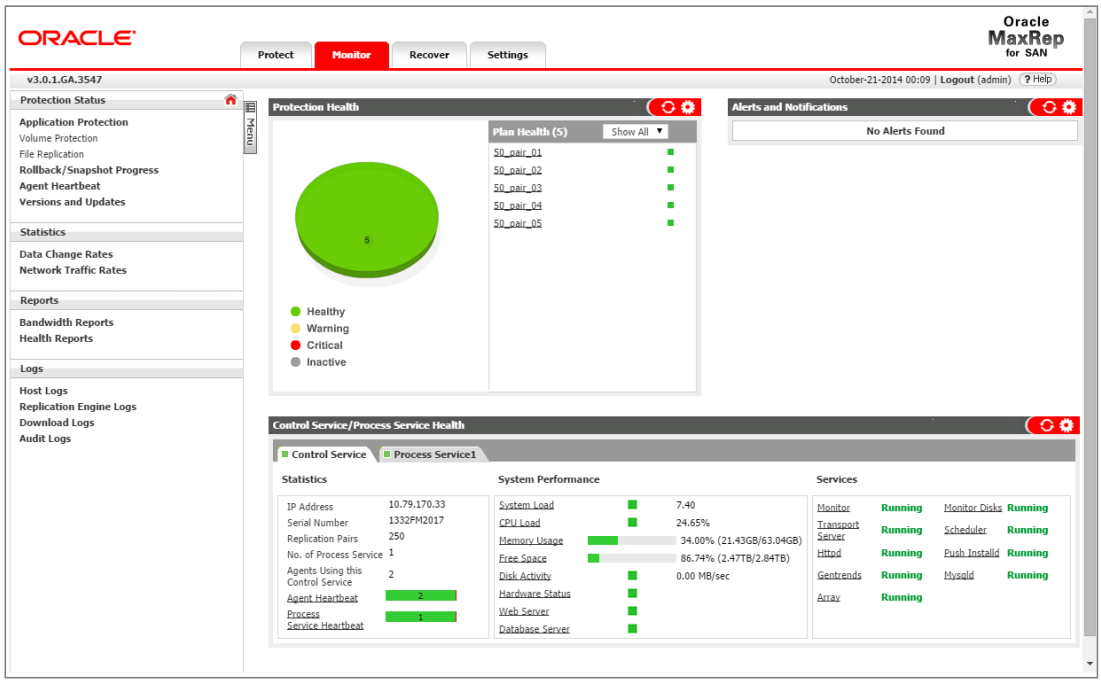
The GUI eliminates the complexity of provisioning tiered storage. For example, you can select the appropriate application storage profile to provision and to tune the storage easily by preselecting the appropriate QoS parameters. Using the storage attributes that you provide through the GUI, the system implements predictive application performance characteristics before it physically provisions the storage. This feature puts you in control of resource allocation.

The Pilot runs the management interface for the Oracle FS System. The GUI, along with the other software that is implemented in the Oracle FS System, enables policy-based provisioning.

Oracle MaxRep for SAN GUI Access

Use the Oracle MaxRep for SAN GUI to configure, monitor, and manage the replication policies for the Oracle FS System. The Oracle MaxRep for SAN GUI accesses the MaxRep Replication Engines through an Internet browser.

Figure 2 Oracle MaxRep for SAN GUI



For more information about using the Oracle MaxRep for SAN GUI, refer to *Oracle MaxRep for SAN User's Guide.*

Oracle FS System CLI Access

The Oracle FS CLI is the command-line interface for configuring, operating, and monitoring an Oracle FS System. The Oracle FS CLI provides the same capabilities as the Oracle FS System Manager (GUI), allowing configuration and management of the Oracle FS System performed from the command line or through custom scripts.

The following features are available with Oracle FS CLI:

- Runs as a command-line interface

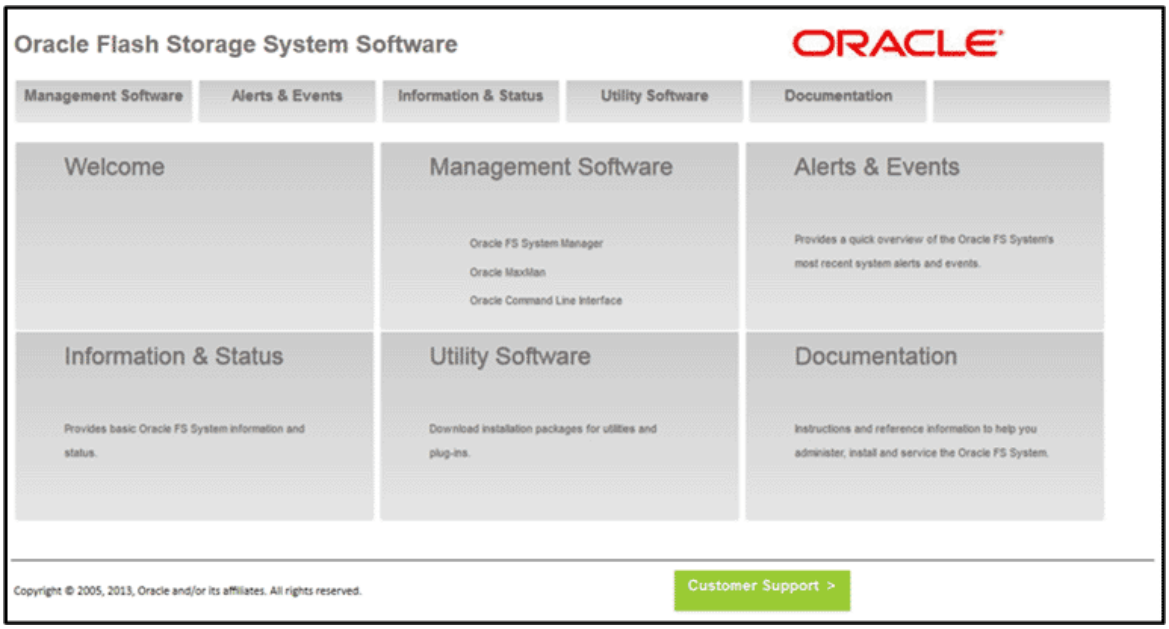
- Communicates from the host system to the Oracle FS System Pilot
- Uses familiar conventions for parameters and options, and provides reasonable default values where possible
- Checks for required sets of parameters and displays error messages if the required values are missing
- Supports automation through custom scripts using common scripting languages
- Provides help for each of its commands and subcommands

Web Access

You can access and download the Oracle FS System applications using the Pilot web client. Applications include the Oracle FS System Manager (GUI), Oracle MaxMan, Oracle FSCLI (FSCLI), and various other utilities. In addition, the Pilot web client provides some information about the status of the Oracle FS System and links to technical documentation.

A username and password are not required to access the web pages that contain the Management Software, Utilities, and Documentation sections. This does not pose a security risk because the use of the downloaded software does require a valid Oracle FS System login.

Figure 3 Oracle FS System web client



A username and password are required to access Alerts & Events and Information & Status pages. Access to these pages adheres to the following guidelines:

- The system prompts the user for a valid username and password before access to these pages is granted.
- The username and password must be a valid Oracle FS System login with appropriate rights to allow access to alerts, events, and system status.
- The login is only valid in the current browser session and only for a maximum of 60 minutes. The system timeouts the session after 10 minutes of non-use.

Log Files

Log files adhere to the following rules:

- Only authorized users are capable of viewing and extracting logs from the system.
- Logs do not contain passwords of any accounts.
- The system logs failed login attempts and logs the username (but not the password) of the attempted login.

For more information about managing log files, refer to *Oracle Flash Storage System Administrator's Guide*.

System Log Bundles

If a significant system event occurs, the Oracle FS System automatically collects the appropriate logs. Log files can be sent to Oracle Support automatically (if Call-Home is enabled) or manually (you can download the logs and attach them to a MOS Service Request). Both Call-Home and MOS provide secure encrypted log transfers. If you transfer the logs to Oracle Support using any other method, the security of the configuration information is your responsibility.

System information can be collected from the following sources and placed into the system log bundle:

- Pilot hardware component
- Controller hardware components
- Drive Enclosure hardware components
- Hosts
- Statistics
- Replication appliances
- System configuration

> **Note**: These log files do not contain customer data.

Client Logs

The Oracle FS System maintains client logs that contain a history of the Oracle FS System Manager (GUI) and Oracle FS CLI (FSCLI) activities that have been performed on the system.