Technical Report

Logging in Clustered Data ONTAP

Defining and Examining Capabilities

Glenn Frye, NetApp
November 2014 | TR-4303

Abstract

This document is intended to serve as a guide to defining the different logs generated by the clustered Data ONTAP® system and the offered capabilities in viewing and accessing these logs. Definitions and context will be provided for the different types of logs in the clustered Data ONTAP system and how this has changed from 7-Mode. This document is intended for customers who require a deeper understanding of the logging mechanisms embedded in clustered Data ONTAP.

TABLE OF CONTENTS

1 Scope 3

2 Logging in Clustered Data ONTAP 3

2.1 Syslog 3

2.2 Event Management System 3

2.3 Audit Logs 4

2.4 AutoSupport 5

2.5 Other Logs 5

3 Collecting, Viewing, and Forwarding Logs in Clustered Data ONTAP 8

3.1 Viewing in CLI 9

3.2 Syslog Forwarding of EMS Events 9

3.3 EMS E-Mail Notifications 10

3.4 SNMP Traps 11

3.5 HTTP(S) to Pull Logs 11

3.6 AutoSupport 13

4 7-Mode to Clustered Data ONTAP Translation 13

References 14

Version History 14

LIST OF TABLES

Table 1) EMS severities. 4

Table 2) Log entry severities. 5

Table 3) Logs in /mroot/etc/log. 6

Table 4) Logs in /mroot/etc/log/mlog. 7

Table 5) 7-Mode and clustered Data ONTAP major differences. 13

LIST OF FIGURES

Figure 1) Webpage example. 13

1 Scope

This technical report details the logging capabilities of clustered Data ONTAP version 8.2. Logging in the clustered Data ONTAP operating system is instrumental to administrators seeking to monitor the status, health, and security of their environment; also, logs are the primary resource for NetApp® Support to pinpoint issues in clustered Data ONTAP behavior and configuration.

The purpose of this document is to make users aware of the different types of logs and their function and to detail the current capabilities of administrative auditing and the clustered Data ONTAP event management system, in conjunction with how administrators can leverage logs to monitor their cluster(s) with several mechanisms such as syslog forwarding. Definitions and context will be provided for the different types of logs in clustered Data ONTAP and how this has changed from 7-Mode.

2 Logging in Clustered Data ONTAP

Logs are event-triggered messages ranging in severity that are generated by the clustered Data ONTAP operating system and recorded in flat text files on the cluster. Logs are the primary resource for administrators, NetApp Support, and AutoSupport™ systems to determine and isolate root causes for a wide range of issues.

Logs can be collected, viewed, and forwarded using several different methods and will be discussed in the “Collecting, Viewing, and Forwarding Logs in the Clustered Data ONTAP operating system” section.

2.1 Syslog

Syslog is a defined standard for computer message logging. The standard is defined by the IETF in RFC 5424. Syslog defines how software formats and sends its messages so that administrators can properly monitor the software’s behavior and utilize tools that can receive and analyze the sent messages. Because this standard is universally recognized, administrators can monitor all assets that support syslog forwarding in real time.

Syslog messages are labeled with a facility code indicating the process or application that generated the message and assigned a severity. How the clustered Data ONTAP system defines the facilities and severities is discussed in the following section.

2.2 Event Management System

The event management system (EMS) is the clustered Data ONTAP messaging facility built on the syslog standard. EMS simplifies the management of clusterwide events and how the administrator chooses to be notified. EMS provides a cataloged logging mechanism, and every event has a formal definition. This allows EMS to provide services such as automatic spam management (such as message suppression), configurable notifications, assistance with translating low-level data into understandable text, NVRAM backing of messages, and automatic tagging of messages.

EMS contains thousands of predefined messages that are triggered on the corresponding event. The dot-separated, tree-style naming scheme of the messages provides significant accuracy pertaining to the messages’ origin and meaning. The formal event definition describes the meaning of the event in the context of the cluster. Each event contains a corrective action description, which can assist and accelerate the decisions the administrator has to make in response to the event. This standardization and accuracy also carry over to NetApp’s manageability tools, which utilize EMS data.

Note: EMS does not contain command history or administrative auditing. That is discussed in the next section.

Table 1 shows how EMS defines the severity of events.

Table 1) EMS severities.

Severity Number	Severity Type	Description
0	NODE_FAULT	A data corruption has been detected, or the node is unable to provide client service.
1	SVC_FAULT	A temporary loss of service has been detected, typically a transient software fault.
2	NODE_ERROR	A hardware error has been detected that is not immediately fatal.
3	SVC_ERROR	A software error has been detected that is not immediately fatal.
4	WARNING	A high-priority message; does not indicate a fault.
5	NOTICE	A normal-priority message; does not indicate a fault.
6	INFO	A low-priority message; does not indicate a fault.
7	DEBUG	A debugging message, typically suppressed from customer.
N/A	VAR	Message has variable severity, selected at runtime.

The equivalent of a syslog "facility" in EMS is the origin of the event. In the CLI output in the following example, `kern` is the "facility" with dot-separated `uptime.filer` to pinpoint the exact event within `kern`. The description contains the cluster-specific information, in this case, the count of operations.

```
cluster::> event log show
Time                Node              Severity      Event
------------------- ----------------- ------------- ---------------------------
3/18/2014 13:00:04  cluster-01
                                      INFORMATIONAL kern.uptime.filer:   1:00pm up 20:17 0 NFS
ops, 0 CIFS ops, 0 HTTP ops, 0 FCP ops, 0 iSCSI ops
```

2.3 Audit Logs

Audit logging is essential for the administrative security of the clustered Data ONTAP system. The audit log records the commands sent to the cluster, the user who is sending them, and the success or failure of the command. This applies to command line interface (CLI), Data ONTAP API (ONTAPI®) calls (such as commands from NetApp manageability tools), and HTTP requests.

Note: In clustered Data ONTAP, the audit log is stored in `/mroot/etc/log/mlog/command-history.log`. Command history can also be viewed in the MGWD log, located in `/mroot/etc/log/mlog/mgwd.log`.

Commands from CLI, ONTAPI, and HTTP fall under two categories: set and get. Set requests are commands that modify the cluster, such as `volume <create|modify|delete>`. Get requests are commands that simply query information about the cluster, such as `show` commands.

By default, set requests are recorded in `command-history.log` and `mgwd.log`, but get requests are not. To view or modify this setting, perform the `security audit` CLI operations:

```
cluster::> security audit show
               Auditing State for              Auditing State for
               Set Requests:                   Get Requests:
               ------------------              ------------------
    CLI:       on                              off
    HTTP:      on                              off
    ONTAPI:    on                              off

cluster::> security audit modify -cliset <on|off> -httpset <on|off> -ontapiset <on|off> -cliget
<on|off> -httpget <on|off> -ontapiget <on|off>
```


Note: Auditing is never fully off; set requests are always recorded in `command-history.log`, regardless of the `security audit` settings. If set requests are turned off, then they are just not recorded in `mgwd.log`.

This topic is also covered in the Clustered Data ONTAP 8.2 System Administration Guide for Cluster Administrators.

2.4 AutoSupport

The AutoSupport (ASUP™) system is the clustered Data ONTAP automated health-monitoring facility that enables error reporting and, in some instances, can generate a NetApp Support case. Reporting might be triggered by an error condition using an EMS event or by schedule. ASUP alerts can be sent to the administrator's internal IT organization using e-mail and/or to NetApp Support for automated analysis. The ASUP message contains important log data from EMS and other user space applications. Exactly which logs ASUP collects is discussed in the next section.

2.5 Other Logs

EMS events follow the syslog standard because they have the ability to be forwarded to a syslog server for real-time monitoring and because EMS events are the most relevant events to an administrator. The rest of the logs generated by the clustered Data ONTAP operating system are generated from user space applications that are constantly logging their activity. These logs are lower level and not targeted for administrators, but are mostly utilized by NetApp Support, development, and QA.

The log entries define their severity similar to the syslog standard. Table 2 lists those severities.

Table 2) Log entry severities.

Severity Number	Severity Type	Description
0	EMERGENCY	Panic condition that causes a disruption of normal service
1	ALERT	Condition that should be corrected immediately, such as a failed disk
2	CRITICAL	Critical conditions, such as disk errors
3	ERROR	Errors, such as those caused by a bad configuration file
4	WARNING	Conditions that might become errors if not corrected
5	NOTICE	Normal but significant conditions that are not errors, but might require special handling
6	INFORMATIONAL	Information, such as the hourly uptime message
7	DEBUG	Used for diagnostic purposes

All logs are stored in `/mroot/etc/log` and `/mroot/etc/log/mlog`, including EMS, audit logs, and user space application logs. Table 3 and Table 4 list the different logs in `/mroot/etc/log` and `/mroot/etc/log/mlog`, respectively, along with the purpose of the log.

Note: Logs in `/mroot/etc/log` rotate once per week, with a maximum of five rotations before the oldest log is deleted.

Table 3) Logs in /mroot/etc/log.

Logs in `/mroot/etc/log`	Description
acp/	• Sent to ASUP • Shelf Alternate Control Path Management (ACP) logs
auditlog.log	• The 7-Mode audit log • Clustered Data ONTAP equivalent is `command-history.log` • Still logs node shell commands (i.e., `node run` commands) • Sent to ASUP starting in clustered Data ONTAP 8.2.2
autosupport/	• Directory for the compressed archives containing the log files to be sent to ASUP
backup.log	• Log for NDMP backup procedures such as SMTape
clone.log	• Logs LUN cloning
ems.log	• The file that contains EMS events • Sent to ASUP • The file that gets read in CLI on `event log show` commands
ems_persist	• Binary formatted file, used by NetApp Support in certain circumstances
hm/	• Job queuing and process information
leak_data, leak_data_filtered	• Memory information, pertinent mostly for debugging purposes
messages.log	• The 7-Mode messages log • Clustered Data ONTAP equivalent is `/mroot/etc/log/mlog/messages.log` • In clustered Data ONTAP, may contain some node-level logs
mlog/	• Contents of this directory are sent to ASUP • Contains management component application logs
snapmirror.log, snapmirror_audit.log, snapmirror_error.log	• SnapMirror® logs
nbu_snapvault.log	• SnapVault® logs
ndvm.log	• DataMotion™ logs
playlist_diag	• Logs absent FileIDs from the WAFL® playlist
plxcoeff/	• Contains PLX PCI-E switch logs • Sent to ASUP starting in clustered Data ONTAP 8.2.1

Logs in `/mroot/etc/log`	Description
repl_vbm_logs/	• Logs any SnapMirror corruptions
servprocd/	• Service processor logs
shelflog/	• Shelf logs
sis.log	• Deduplication logs
ssram/	• System scratchpad RAM log
stats/	• Performance-related logs
treecompare.log	• Logs for the treecompare process that compare data integrities in volumes and/or qtrees using Snapshot® copies
vfiler_trans_migrate_cmds_log.log, vfiler_trans_migrate_log.log	• 7-Mode StorageMotion logs
volread.log	• Logs for the volread engine used by SnapMirror

Note: All logs in `mlog` are sent to ASUP. Also, these logs rotate once per day, with a maximum of 35 rotations before the oldest log is deleted.

Table 4) Logs in /mroot/etc/log/mlog.

Logs in `/mroot/etc/log/mlog`	Description
.last_rotate.log	• Records history of log rotations
apache_access.log	• Logs history of access to the apache server • Contains history of GET requests for log files over HTTP(S)
apache_error.log	• Logs apache errors
bcomd.log	• Logs for the BCOM daemon, which handles SAN interaction between the management component and SCSI blade
command-history.log	• Audit log for clustered Data ONTAP • Records commands from CLI, ONTAPI, HTTP • Always records set requests, but can toggle recording of get requests
debug.log	• Logs at the DEBUG severity level
fpolicy.log	• Logs for FPolicy®, which is a notification mechanism to enable partner software-based solutions to work in conjunction with clustered Data ONTAP
hashd.log	• Logs for the BranchCache hash daemon
jm-restart.log	• Contains list of jobs that the job manager has restarted

Logs in `/mroot/etc/log/mlog`	Description
memsnap-*.log (asterisk is a wildcard, because there are several types of memsnap logs)	• Contains memory information
messages.log	• The messages log in clustered Data ONTAP • Contains important logs throughout cluster • Some overlap with EMS, but no EMS features such as suppression
mgwd.log	• Contains logs from the management component • Records set requests by default, but can be toggled • See Audit Logs section
ndmpd.log	• Contains logs for the NDMP daemon
notifyd.log	• Contains logs for the NOTIFY daemon, which handles ASUP
php.log	• Contains logs for the PHP process • Contains history of syncing logs across nodes in the cluster
secd.log	• Contains logs for the SecD daemon, which handles various authentication tasks, such as NAS authentication
servprocd.log	• Contains logs on the service processor daemon
sktlog/	• Debug-level logs for the main kernel
sktlogd.log	• Debug-level log for the main kernel
spdebug.log	• Contains logs related to abnormal events from the service processor
spmd.log	• Contains logs on the service process manager daemon, which monitors user space applications to make sure they are healthy and running
vifmgr.log	• Contains logs related to interfaces and networking
vldb.log	• Contains logs on the volume location database application

3 Collecting, Viewing, and Forwarding Logs in the Clustered Data ONTAP operating system

The administrator can view logs on the cluster using several different methods. EMS events can be forwarded, and the administrator can determine which events to forward, along with the forwarding mechanism. These methods will be discussed in the following section.

Note: Another reference for managing EMS can be found in Managing event messages in the Clustered Data ONTAP 8.2 System Administration Guide for Cluster Administrators.

3.1 Viewing in CLI

The `event` commands will query EMS and display events that match the supplied parameters. In the following example, a query is issued for the entire cluster for ERROR and WARNING events.

```
cluster::> event log show -node cluster* -severity ERROR,WARNING
Time                Node             Severity      Event
------------------- ---------------- ------------- ---------------------------
3/20/2014 16:02:08  cluster-02
                                     ERROR         asup.post.drop: AutoSupport message (HA Group
Notification from cluster-02 (REBOOT (after giveback)) INFO) for host (0) was not posted to
NetApp. The system will drop the message.
3/20/2014 16:00:04  cluster-01
                                     WARNING       wackiron.near.hour.limit: aggr0: Hours since
wafliron was last run is approaching its limit. Hours remaining: 20.
```

The administrator can also query EMS by the type of event. In the following example, a query is issued for the entire cluster to return any authentication event.

```
cluster::> event log show -node cluster* -event *auth*
Time                Node             Severity      Event
------------------- ---------------- ------------- ---------------------------
3/21/2014 09:36:26  cluster-01
                                     WARNING       login.auth.loginDenied: message="1 login
failure from localhost, diag"
3/20/2014 15:29:55  cluster-01
                                     WARNING       sshd.auth.loginDenied: message="Failed
keyboard-interactive/pam for admin from 10.62.195.80 port 55666 ssh2"
3/20/2014 13:37:22  cluster-01
                                     WARNING       sshd.auth.loginDenied: message="Failed
keyboard-interactive/pam for admin from 10.62.195.80 port 53523 ssh2"
3 entries were displayed.
```

Note: Utilizing delimiters such as commas and asterisks in commands can greatly customize the output of the command and limit unneeded output. As an example, refer to the CLI command earlier where `cluster*` is used for the `–node` field and `*auth*` is used for the `–event` field. By ending the node name with a wildcard asterisk, this selects all nodes in the cluster. And by encapsulating `auth` with wildcard asterisks, a complete output for EMS authentication events on the cluster is provided.

Adding `–instance` to the command will output more information about the event and the corrective action that should be taken.

```
cluster::> event log show -messagename wackiron.past.hour.limit -instance

             Node: cluster-02
        Sequence#: 7054
             Time: 3/25/2014 09:00:04
         Severity: WARNING
           Source: statd
     Message Name: wackiron.past.hour.limit
            Event: wackiron.past.hour.limit: aggr0_cluster_02_0: Number of hours since wafliron
was last run on the specified volume is past its limit. Run 'wafliron' as soon as possible.
      Corrective Action: Run wafliron on the affected volume. From the boot menu, run 'wafliron'.
From the dblade CLI, run 'aggr wafliron start [aggr-name]'.
      Description: This message occurs when the number of hours since wafliron was last run on
the specified volume is past its limit. Because the limit was passed, if the bootarg
'wackiron_enforce_panic' is true, the system will panic on the next boot.
```

3.2 Syslog Forwarding of EMS Events

Currently, only EMS events can be forwarded to a syslog server. The entire EMS catalog can be forwarded, or just individual or categorical events. First, an event destination must be created; then the events to be forwarded to the destination must be selected. In the following example, a syslog destination

named `test_auth_forward` is created with the corresponding IP address of the server to receive the syslog packets. Then the EMS events to be forwarded (in this case, all authentication events) are selected with the `event route add-destinations` command.

Note: An EMS event can have more than one destination.

```
cluster::> event destination create -name test_auth_forward -hide-parameters false -syslog
10.228.225.243 -syslog-facility default

cluster::> event route add-destinations -messagename auth* -destinations test_auth_forward
33 entries were acted on.
```

3.3 EMS E-Mail Notifications

Like syslog forwarding, only EMS events can be sent using SMTP (e-mail). It's important to make sure the correct host names are set in `event config` to make sure of proper SMTP traffic. Refer to the following example. In the first command, the proper SMTP server name is set along with the source e-mail address. In the second command, the event destination created in the last section is modified to enable it to send e-mail notifications to the given e-mail address (while still doing syslog forwarding). In the third command, `sshd.auth.loginDenied` is added to that event destination. Therefore, if a user is denied login to the cluster using SSH, an e-mail notification will be sent to the supplied e-mail address.

```
cluster::> event config modify -mailfrom admin@mycluster.netapp.com -mailserver smtp.netapp.com

cluster::> event destination modify -name test_auth_forward -mail smtpdest@netapp.com

cluster::> event route add-destinations -messagename sshd.auth.loginDenied -destinations
test_auth_forward
```

Here's an example of what that e-mail notification would contain:

"Filer: cluster-01

Time: Mon, Mar 24 14:55:44 2014 -0500

Severity: LOG_WARNING

Message: sshd.auth.loginDenied: message="Failed keyboard-interactive/pam for admin from 10.62.195.80 port 52976 ssh2"

Description: This event is issued when sshd refuses a login attempt due to authentication failure.

Action: Use a valid username/password combination to login.

Source: sshd

Index: 16251"

The history of e-mail notifications can be viewed as well.

```
cluster::> event mailhistory show
Time                Node        Seq#  Message Name           Address
------------------- ----------- ----- ---------------------- -----------------
3/24/2014 14:55:44  cluster-01  1     sshd.auth.loginDenied  smtpdest@netapp.com
```

Another useful configuration for EMS alerting involves assigning events to a destination based on the event severity. This simplifies the configuration process so administrators can get the most severe events pushed to syslog, SMTP, and optionally SNMP (if the event supports SNMP). In the following example, a new event destination will be created, and all events with the severities of EMERGENCY, ALERT, and CRITICAL will be added. To specify all events with those severities, it necessary to use a query in the `event route add-destinations` command. This syntax for queries is understood by enclosed curly brackets, {…}.

```
cluster1::> event destination create -name important_events -hide-parameters false -syslog
10.228.225.243 -syslog-facility default -mail smtpdest@netapp.com
```



```
cluster1::> event route add-destinations {-severity EMERGENCY,ALERT,CRITICAL} -destinations
important_events
687 entries were acted on.
```

Now any event that occurs within those severities will be pushed to syslog and SMTP.

Note: New EMS events may be included in future clustered Data ONTAP upgrades, so it is strongly recommended to rerun the `event route add-destinations` command to enable new EMS events to be associated with the existing event destinations after an upgrade.

3.4 SNMP Traps

A subset of the EMS events supports triggering SNMP traps. In a similar fashion to setting up e-mail notifications, an SNMP receiver can simply be added to a new event destination or an existing one.

Note: Because only a subset of EMS events supports SNMP, it is recommended that a separate event destination be created solely for SNMP traps, because an existing event destination mapped to EMS events that do not support SNMP traps will not allow an SNMP receiver to be added until the events are unmapped.

To view the EMS events that support SNMP, simply query the EMS catalog and leverage the `snmp-support` flag. In the following example, a query is sent for EMS volume events that support SNMP traps.

```
cluster::> event route show -snmp-support true -messagename *vvol*
                                                          Freq    Time
Message                          Severity       Destinations   Threshd Threshd
-------------------------------- -------------- -------------- ------- -------
wafl.vvol.offline                INFORMATIONAL  -              0       0
wafl.vvol.online                 INFORMATIONAL  -              0       0
wafl.vvol.restrict               INFORMATIONAL  -              0       0
3 entries were displayed.
```

In the following example, an event destination, `volume_trap`, is created, and an SNMP receiver will be added to it, along with the volume events.

Note: The default SNMP community string is `public`.

```
cluster::> event destination create -name volume_trap -snmp 10.228.225.242

cluster::> event route add-destinations -messagename
wafl.vvol.offline,wafl.vvol.online,wafl.vvol.restrict -destinations volume_trap
3 entries were acted on.
```

Now the SNMP receiver will receive traps on those events if they occur.

The history of SNMP traps can be viewed similarly to e-mail notification history:

```
cluster::> event snmphistory show
Time                Node         Seq#  Message Name           Address
------------------- ------------ ----- ---------------------- -----------------
3/25/2014 10:56:14  cluster-01   2     wafl.vvol.online       10.228.225.242/
                                                              public
3/25/2014 10:40:37  cluster-01   1     wafl.vvol.offline      10.228.225.242/
                                                              public
2 entries were displayed.
```

3.5 HTTP(S) to Pull Logs

Administrators can access the two directories mentioned in section 2.5 using HTTP or HTTPS to download log files.

1. To access the logs using HTTP(S), first verify that the cluster management LIF is up.

```
cluster::> network interface show
            Logical    Status     Network            Current       Current Is
```



```
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
cluster     cluster_mgmt up/up    10.63.24.180/18    cluster-01    e0c     true
```

2. Then verify that the web protocol engine supports HTTP (for HTTPS access, you must also enable SSL and install a digital certificate, which is outside the scope of this document, but instruction are located in the Clustered Data ONTAP 8.2 System Administration Guide for Cluster Administrators).

```
cluster::> system services web show
External Web Services: true
              Status: online
   HTTP Protocol Port: 80
  HTTPs Protocol Port: 443
        TLSv1 Enabled: true
        SSLv3 Enabled: true
        SSLv2 Enabled: false
```

The status shows online.

3. The next step is to add HTTP(S) to the existing firewall policy, if firewall is enabled. This will allow web access requests to pass through the firewall.

```
cluster::> system services firewall policy show -policy mgmt -service http,https
Policy           Service    Action IP-List
---------------- ---------- ------ --------------------
mgmt
                 http       allow  0.0.0.0/0
                 https      allow  0.0.0.0/0
2 entries were displayed.
```

HTTP(S) shows as allowed for the `mgmt` firewall policy.

4. Next, the service processor infrastructure web service must be enabled. It is denoted by the acronym `spi`.

```
cluster::> vserver services web show –vserver cluster -name spi

                     Vserver: cluster
                Service Name: spi
              Type of Vserver: admin
        Version of Web Service: 1.2.0
     Description of Web Service: Service Processor Infrastructure
Long Description of Web Service: This service offers HTTP/HTTPs access to applications running on
the Service Processor. Log and core files from all nodes in the cluster will be exposed for
Service Processor retrieval.
           Service Requirements: ontapi=1.0.0, index>1.0.0
       Default Authorized Roles: admin
                        Enabled: true
                       SSL Only: false
```

Near the bottom of the output, the SPI shows `Enabled: true`. Also, the default authorized role is the administrator.

5. Next, verify the proper cluster user account roles are mapped to the HTTP application.

```
cluster::> security login show -application http

Vserver: cluster
                            Authentication                 Acct
UserName         Application Method         Role Name        Locked
---------------- ----------- -------------- ---------------- ------
admin            http        password       admin            no
```

By default, the administrator already has access to the HTTP application.

Note: A user must be in an administrative role to access the HTTP application.

6. Finally, verification must be made that the user or administrator has access to the web service.

```
cluster::> vserver services web access show -name spi
Vserver         Type     Service Name     Role
--------------- -------- ---------------- ----------------
cluster         admin    spi              admin
```

Now the administrator can access the web service. To access it, the following address must be entered into a web browser: `(http:// or https://)<cluster-mgmt-ip>/spi/<node-name>/etc/log/.`

After the administrator logs in, the log files in the directory will show, and they can be downloaded. For navigation to `/mroot/etc/log/mlog` where the user application logs are stored, simply append `mlog` to the preceding web address.

Note: Starting in clustered Data ONTAP 8.2.1, steps 2 through 6 are already completed by default.

Figure 1 shows a portion of what the web browser should display.

Figure 1) Webpage example.

Name	Last Modified	Size
Parent Directory/	Mon Mar 24 13:29:21 America/New_York 2014	-
.last_rotate	Mon Mar 24 16:22:56 America/New_York 2014	30
.spin.039b8eb9.0299.4	Mon Mar 24 16:22:49 America/New_York 2014	755684
apache_access.log	Mon Mar 24 17:43:19 America/New_York 2014	23058242
apache_access.log.0000000001	Mon Mar 24 17:43:19 America/New_York 2014	23058242
apache_error.log	Mon Mar 24 17:25:29 America/New_York 2014	35079
apache_error.log.0000000001	Mon Mar 24 17:25:29 America/New_York 2014	35079
bcomd.log	Mon Mar 24 16:22:56 America/New_York 2014	0
bcomd.log.0000000001	Wed Feb 26 12:12:51 America/New_York 2014	35992
bcomd.log.0000000002	Thu Feb 27 11:10:41 America/New_York 2014	0
bcomd.log.0000000003	Fri Feb 28 11:10:41 America/New_York 2014	0

This is also covered in the Clustered Data ONTAP 8.2 System Administration Guide for Cluster Administrators.

3.6 AutoSupport

For information about managing AutoSupport, see Managing AutoSupport in the Clustered Data ONTAP 8.2 System Administration Guide for Cluster Administrators.

4 7-Mode to Clustered Data ONTAP Translation

There are some differences when moving from 7-Mode to clustered Data ONTAP. Among the major benefits are the enhancement and expansion of EMS. Table 5 outlines the major differences that should be noted between them.

Table 5) 7-Mode and clustered Data ONTAP major differences.

7-Mode	Clustered Data ONTAP
`/etc/syslog.conf` file	Replaced by the `event` and `event config` commands

7-Mode	Clustered Data ONTAP
`/etc/log/auditlog` files	`/mroot/etc/log/mlog/command-history.log` log files **Note:** The 7-Mode files are present and still capture node-level commands.
The messages file, `etc/log/messages.log`	Now in `/mroot/etc/log/mlog/`

References

The following references were used:

- Data ONTAP 8.2 System Administration Guide for 7-Mode https://library.netapp.com/ecmdocs/ECMP1155684/html/frameset.html
- Clustered Data ONTAP 8.2 System Administration Guide for Cluster Administrators https://library.netapp.com/ecmdocs/ECMP1196798/html/frameset.html

Version History

Version	Date	Document Version History
Version 1.0	November 2014	Initial documentation for clustered Data ONTAP version 8.2

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.