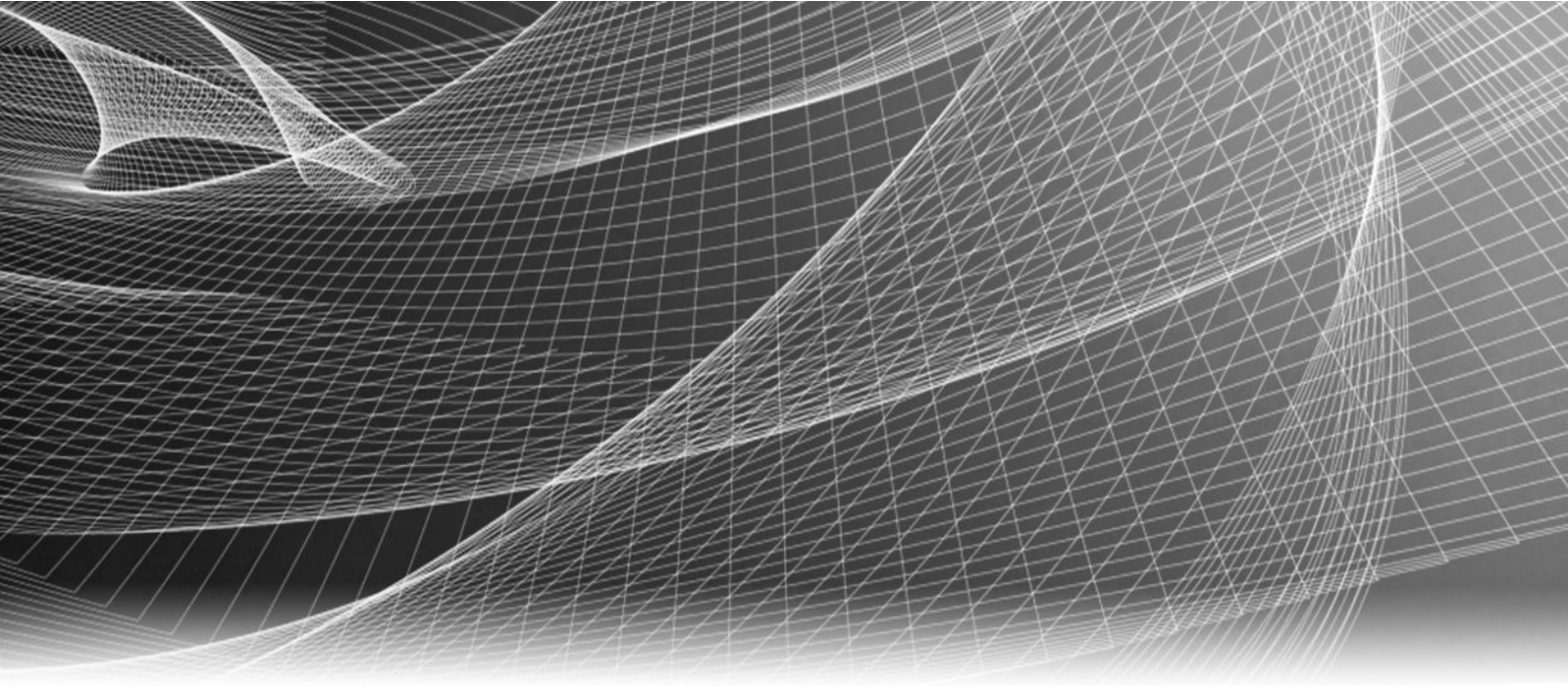

Isilon OneFS

Version 7.2.1.0 - 7.2.1.2

Release Notes

EMC²

Networking

New and changed in OneFS 7.2.1.2	ID
A new kernel driver for the QLogic (formerly Broadcom) NetXtreme Ethernet (BXE) 10 GigE NIC, 1.78.79.ISILON.01, was integrated into OneFS 7.2.1.2.	164251

Logging to the `ec_logstore_recover_file` log file was improved as follows:
• The default logging level for the endurant cache logstore recovery process changed from `NOTICE` to `INFO`.
• The number of files that are successfully recovered following the recovery process is recorded in the log file.
In the following example of the log file output, 10 files were recovered:
`Logstore 1:0007:0013: 10 files to recover data for (error 0)`
`10/10 files were successfully recovered from logstore`
	158951

OneFS web administration interface

New and changed in OneFS 7.2.1.2	ID
The time zone database that OneFS relies on—when you configure the time zone for the cluster—was updated to Time Zone Data v.2015g. This database is made available by the Internet Assigned Numbers Authority (IANA). For more information about the changes to this version of the time zone database, see the IANA website.	162441

SMB

New and changed in OneFS 7.2.1.2	ID
New control: A OneFS registry key was added to the `gconfig` file, MaxSMB2DialectVersion. This key provides the ability to control the highest SMB2 dialect of the SMB2 protocol. The valid options and the effect of setting each option are as follows: • `2.02` • This option enables the SMB 2.02 dialect and disables the SMB 2.10 and 3.0 dialects. • `2.10` • This option enables the SMB 2.02 and 2.10 dialects and disables the SMB 3.0 dialect. • `3.00` • This option enables all three SMB dialects.	158080

New and changed in OneFS 7.2.1.2	ID
Note The default setting is option `3.00`. If an invalid option is selected, a message similar to the following appears in the `lwiod.log` file: `INFO: Invalid SMB2 protocol max dialect configuration. MaxSmb2DialectVersion is not in allowed list (2.02, 2.10, 3.00). Default MaxSmb2DialectVersion value is in use.` **Note** This option was added to enable support to troubleshoot issues that might be related to differences between the supported SMB2 dialects.	

New and changed in OneFS 7.2.1.1

Authentication

New and changed in OneFS 7.2.1.1	ID
A user that attempts to connect to the cluster over SSH, through the OneFS API, or through a serial cable, can no longer be authenticated on clusters running in compliance mode if any of the following identifiers are assigned to the user as either the user's primary ID or as a supplemental ID: • UID: 0 • SID: S-1-22-1-0 For more information, see ESA-2015-148 on the EMC Online Support site.	156328
The message that is logged in the `/var/log/lsassd.log` file when a trusted Active Directory domain is offline now includes the name of the domain that cannot be reached. In the example below, *‹domain_name›* is the name of the domain that is offline: `[lsass] Domain '<domain_name>' is offline`	155805

Backup, recovery, and snapshots

New and changed in OneFS 7.2.1.1	ID
If you run the `stat` command to view information about a file, the Snapshot ID of the file is now included in the output. This information appears in the st_snapid field.	154833
Reduces lock contention by changing the lock type used by the SyncIQ coordinator when reading the `siqpolicies.gc` file coordinator from an exclusive lock to a shared lock.	151757

Resolved in OneFS 7.2.1.2

Authentication

Authentication issues resolved in OneFS 7.2.1.2	ID
OneFS did not cache the user group membership information that was returned by an LDAP provider when a user was authenticated to the cluster over Pluggable Authentication Module (PAM)-based protocols such as SSH and FTP. As a result, OneFS repeatedly queried the LDAP provider for this information. In some environments, this issue might have overloaded the LDAP provider and caused it to become unavailable. If this issue occurred, users could not be authenticated to the cluster until the issue was resolved.	163735
The `/usr/bin/isi_hwtools/isi_hdfw_update` command was added to the `sudoers` file. The `sudoers` file defines the commands that a user with sudo privileges is permitted to run. This addition allows you to run the `/usr/bin/isi_hwtools/isi_hdfw_update` command on compliance mode clusters. Before to this fix, drive firmware could not be updated on compliance mode clusters.	163612
OneFS did not cache the user group membership information that was returned by an LDAP provider when a user was authenticated to the cluster over SMB. As a result, OneFS repeatedly queried the LDAP provider for this information. In some environments, this issue might have overloaded the LDAP provider and caused it to become unavailable. If this issue occurred, users could not be authenticated to the cluster until the issue was resolved.	163607
If the selective authentication setting was enabled for a Windows trusted domain, and if a user was assigned to a group in that domain to which the ISI_PRIV_LOGIN_SSH role-based access privilege was assigned, and if the user attempted to log in through an SSH connection, the user was denied access to the cluster. This issue occurred because the selective authentication setting prevented OneFS from resolving the user's group membership.	161272
If a cluster could not contact a writable Windows 2008 R2 or later domain controller (DC), attempts to fail over to a read-only domain controller were unsuccessful, and a `KRB_AP_ERR_BAD_INTEGRITY` error was returned to the cluster. This issue occurred because the name-type that was sent in the Kerberos Ticket-Granting Ticket request was not KRB5-NT-SRV-INST, which is the required name-type for compatibility in this environment. As a result, clients that were connected to the cluster might have experienced intermittent authentication issues.	160417

If the `sudoers` file contained role-based access control (RBAC) role names with spaces or hyphens, the `sudoers` file was invalid. As a result, `sudo` commands could not be run on the cluster. If this issue occurred on a cluster running in compliance mode, commands that required the `sudo` command—that is, commands that require root-level access—could not be run. This included `sudo` commands executed by the compadmin user. If any user attempted to run a `sudo` command, messages similar to the following appeared on the console:
`sudo: >>> /usr/local/etc/sudoers:syntax error near line 162 <<<`
`sudo: >>> /usr/local/etc/sudoers:syntax error near line 165 <<<`
`sudo: parse error in /usr/local/etc/sudoers near line 162`
	159518