Oracle® Communications Messaging Server

Release Notes

Release 8.1.0

F15152-02

July 2020

This document provides release notes for Oracle Communications Messaging Server Release 8.1.0, consisting of the following sections:

New and Changed Features

This section lists the new features and feature enhancements released in Messaging Server 8.1 and patch sets.

- Additional Virtual Channel Support in MTA
- $< and $> Metacharacters Are Used in the AUTH_REWRITE Mapping
- Additional MTA Option
- Controlling the Prefix Generation on MTA-generated syslog Messages
- processnestedmessages and retainnestedmessages Options Have Been Added

Support for Storing BadGuy in Memcached Server (Patch Set 4)

Starting with Messaging Server 8.1.0.4.0, storing BadGuy details in memcached server is supported. You must install memcached server to store BadGuy details.

For more information, see *Messaging Server Security Guide*.

Additional Event Notification Types (Patch Set 2)

Starting with Messaging Server 8.1.0.2.0, the following Event Notification Types are supported along with the existing types:

- Copy
- ExpungeMsg
- MsgFlags
- AnnotateMsg

For more information, see *Messaging Server System Administrator's Guide*.

Migrating of Mailboxes from Microsoft Exchange Server to Oracle Messaging Server (Patch Set 2)

Starting with Messaging Server 8.1.0.2.0, a utility to migrate mailboxes from Microsoft Exchange Server to Oracle Communications Messaging Server is included.

For more information, see the discussion about migrating mailboxes from Microsoft Exchange Server to Oracle Communications Messaging Server (Doc ID 2632831.1) on the My Oracle Support Web site:

`https://support.oracle.com/portal/`

Support for Non-Root Users to Run Messaging Server on Linux (Patch Set 1)

Starting with Messaging Server 8.1.0.1.0, non-root users can run Messaging Server with RBAC privileges on Linux.

For more information, see *Messaging Server Security Guide*.

Support for Domain Keys Identified Mail (DKIM) (Patch Set 1)

Starting with Messaging Server 8.1.0.1.0, Domain Keys Identified Mail (DKIM) is supported. By using DKIM, email senders generate public and private key pairs. The public key is published to DNS records, and the matching private keys are stored in a sender's outbound email servers.

For more information, see the discussion about DKIM (Doc ID 2681977.1) on the My Oracle Support Web site: https://support.oracle.com/portal/.

Support for Solaris 11.4

Messaging Server now supports Solaris 11.4.

Support for Oracle Linux 7

Messaging Server now supports Oracle Linux 7 operating system.

Support for NSS 3.41

Messaging Server uses the open-source Mozilla Network Security Services library to provide SSL/TLS functionality. This release updates to Version 3.41.

Support for Packages Instead of commpkg

Starting with Messaging Server 8.1.0, **commpkg** is no longer used to install/uninstall the Messaging Server. Instead, Messaging Server is distributed as a package that can be directly installed or uninstalled with the **rpm** tool on Linux and the **pkgadd/pkgrm** tools on Solaris.

Note that legacy package commands like **pkginfo**, **pkgadd**, and **pkgrm** are not available in Solaris 11.4 OS. Please contact Oracle to install the necessary Oracle Solaris packages.

Store Transaction Logging

Store transaction logging is now enabled by default. To restore the previous default behavior, set the **messagetrace.activate** option to **no**.

Recipe-Based Initial Configuration Has Been Implemented

Starting with Messaging Server 8.1.0, the **init-config** command (also known as **configure**) supports recipe-based initial configuration. In this mode of operation, a minimal configuration is generated and then special **msconfig** recipe files are run to configure individual server roles. For more information on **init-config**, see the *Messaging Server Reference Guide*. The examples section gives example usage for common roles.

Routing-only MTA Initial Configuration (without LDAP) Has Been Implemented

Starting with Messaging Server 8.1.0, the **init-config** command can generate an initial configuration for a routing-only MTA that does not require use of LDAP. Although the MTA has always supported operation without LDAP, this makes it simpler to configure such an MTA. You can use the **init-config -r mta** command to generate an initial MTA configuration for this function.

JMS support for ENS

Messaging Server events can now use the bundled JMS ENS provider (**ens-jms.jar**). The Glassfish MQ JMS provider is no longer supported for use with Messaging Server.

Support for TLS 1.3

Messaging Server now supports TLS version 1.3 (RFC 8446) and is enabled by default.

Support for New Indexing and Search Engine

Messaging Server now supports Elasticsearch as an index and search service for use with the Classic message store and Cassandra message store.

Monitoring Using msstatbot Tool

Messaging Server now uses **msstatbot** tool to perform basic administrative tasks, and monitor cluster health. See *Messaging Server System Administrator's Guide* for more information on the **msstatbot** tool.

Login User Name and Password Normalization

Login user names and passwords are now normalized to Unicode normalization form C. This is a conservative subset of the behavior recommended in RFC 8265. In addition, login user names containing a domain with an IDN A-label (RFC 5890) are canonicalized to IDN U-labels. As a result, non-ASCII user and domain names in LDAP must be provisioned in Network Unicode (RFC 5198). If user or domain names were previously provisioned in decomposed Unicode or IDN A-labels, the LDAP directory must be updated prior to deploying this release.

Enhanced "foreverypart" Sieve Extension

It is now possible to control whether or not the "foreverypart" Sieve extension looks inside of nested messages or treats them as leaf parts. The ":processnestedmesssages" argument tells "foreverypart" to look inside and is the default. The ":retainnestedmessages" argument causes nested messages to be treated as leaf parts.

Alarm Submit Default Port Has Been Changed

Starting with Messaging Server 8.1.0, the default value of the **alarm.noticeport** option has been changed to **587**.

IMAP Email Address Internationalization

The IMAP server now advertises and implements IMAP Support for UTF-8 (RFC 6855). This means that email messages conforming to RFC 6532 can now be delivered to the message store if permitted by use of the utf8negotiate, utf8header, or utf8strict channel keyword.

However, once these messages are in the message store they will be presented undamaged to legacy IMAP and POP clients (note that this behavior is not fully compliant with RFC 6855 but we believe this behavior is least likely to cause problems in the long run). It's possible legacy clients will have problems displaying these messages and likely legacy clients will be unable to reply to these messages. Sites choosing to allow EAI may wish to either create support materials explaining the issue or wait until significant clients have been upgraded.

Note that IMAP APPEND has no restrictions on use of UTF-8 header mail messages. This is necessary to avoid surprises when migrating mail from other systems to our message store.

The behavior of IMAP APPEND has changed with this feature: any line containing 8-bit characters in an email header that does not conform to either RFC 2047 or RFC 6855 will cause a blank line to be insertted prior to that line so it is treated as part of the message body.

Support for UTF-8 User Names, email addresses, and Domains

Messaging Server now supports use of UTF-8 in user names, email addresses, and domains. When provisioning UTF-8 domains, be sure to store the U-label form in LDAP as described in RFC 5890. While Messaging Server supports this type of internationalization, be aware that supporting systems outside of Messaging Server (e.g., identity services, provisioning services, monitoring, and logging services) may not provide a similar level of support. Customers are encouraged to consider the consequences of deploying fully internationalized user and domain identifiers on systems external to Messaging Server prior to doing so. Reading the discussion of the provisioning considerations related to such identifiers in section 3.2 of RFC 5894 is recommended.

Note that use of Net Unicode as described in RFC 5198 is required for these identifiers. In particular, this requires use of Unicode normalization form C when transmitting Unicode text on the Internet and applies to these identifiers in LDAP, IMAP, and SMTP.

New IMAP Capabilities Have Been Added

The IMAP server now supports URL-PARTIAL (RFC 5550) and STATUS=SIZE (RFC 8438) capabilities. See Supported Standards for a full list of IMAP capabilities.

New Milter Actions Added to the MILTER_ACTIONS Mapping

The **ADDHEADER** and **INSHEADER** milter modification actions has been added to the **MILTER_ACTIONS** mapping table.

Support for File Carbon Copy

The File Carbon Copy (Fcc) is now supported for sieve extension.

include_retries MTA Option Added to the Mapping

A **include_retries** MTA option has been added which provides the means to include message retry information in various mappings.

Sieve Vacation Extension Has Been Enhanced

A **:noheadercheck** nonpositional parameter has been added to the Sieve vacation extension. If specified, it suppresses the checks for List-*: intended to prevent vacation replies from being sent to mailing lists.

Mapping Template Has Been Enhanced

A construct of the form $?a,b,c,... can now be used in a mapping template to perform random value selection.

DEQUEUE_ACCESS Mapping Has Been Implemented

A DEQUEUE_ACCESS mapping has been implemented.

Support for New Parameters Added to the XCLIENT SMTP Command

Support has been added for the **DESTADDR** and **DESTPORT** parameters to the **XCLIENT SMTP** command.

Support for Statefile Added to msconfig Utility

Statefile support has been added to the msconfig utility, consisting of:

- A **--statefile** switch on the msconfig command line which is used to specify the path to the statefile to be read/updated. All statefile support is disabled if **--statefile** is not specified.
- The **read** function in the recipe language now accepts a third string paramater specifying the name of a statefile variable. The variable will be used if present or will be updated with any value that's entered.
- Three new recipe language functions have been added: **exists_statefile**, **get_statefile**, **set_statefile**, and **delete_statefile**. These functions can be used to get, set, and delete statefile variables, respectively.
- The **msconfig write** command has been extended to update the statefile in addition to writing out any new configuration information.

nextif Added to the Sieve and Recipe Language

A **nextif** statement has been added to the **Sieve** and **Recipe** language loop facility.

get_msconfig_info Added to the Recipe Language

A new function, **get_msconfig_info**, has been added to the **Recipe** language. It can be used to return various pieces of information about the **msconfig** utility itself.

SHA-2 Hash Functions Added to the Recipe Language

Support for the SHA-2 family hash functions SHA-256 and SHA-512 has been added to the **hash** and **hash_hmac** functions in the **Recipe** and **Sieve** languages.

msconfig SET Command Enhanced

The **msconfig SET** command now allows the C-style backslash sequences \r (carriage return), \n (line feed), \t (tab), and \uNNNN (Unicode character, must specify exactly 4 hexadecimal digits) in option values.

Support for XCONVTAG SMTP Extension

The **flagtransfer** channel option now enables the use of a new **XCONVTAG SMTP** extension. This extension is used to pass along conversion tag information.

New Flags Added to the AUTH_ACCESS Mapping

In this release, following new flags have been added to the AUTH_ACCESS mapping:

- A **$S** flag is set on input in the **AUTH_ACCESS** mapping if a connection to the destination for this message is already open and is going to be reused.
- A **$+R** flag can now be used in the **AUTH_ACCESS** mapping to specify an alternate **ALLOW_TRANSACTIONS_PER_SESSION** TCP/IP channel-specific option value for the current message. Note that using the value to force the current session to terminate will cause the setting to return to the default **ALLOW_ TRANSACTIONS_PER_SESSION** value.
- A **$V** flag can now be used in the **AUTH_ACCESS** to specify a skip count to be encoded in the queue file name of the current message. This flag is specifically intended for use by **smartsendauth_access** callout.
- A **$+.** flag can now be used in the **AUTH_ACCESS** mapping to specify the host name to use in any **HELO**, **EHLO**, or **LHDO** commands that are issued.
- A **$n** flag can now be used in the **AUTH_ACCESS** mapping to signal a temporary failure for the current message and cause it to be tried again later. Note that **$N** is used to permanently fail the current recipient.
- A **$(** flag can now be used in the **AUTH_ACCESS** mapping to provide a value overriding the **MAX_MX_RECORDS TCP/IP-channel-specific** option.
- A **$+%** flag can now be used in the **AUTH_ACCESS** mapping to specify an override backoff time that will be used if the delivery attempt fails.

Activating Spam Filter Has Been Enhanced

Previously the **$+R** sequence in **FROM_ACCESS** and recipient access mappings was only capable of activating a single spam filter, using the syntax "$+Rnumber | optin-string". It now accepts an additional syntax, "$+Rn1,s1,n2,s2..." that can be used to activate multiple spam filters (n1, n2 ...), each with an associated option string (s1, s2 ...).

REPROCESS_TIMEOUT and REPROCESS_CONNECT_TIMEOUT Options Added to Milter Configuration Files

Two new options, **REPROCESS_TIMEOUT** and **REPROCESS_CONNECT_ TIMEOUT**, have been added to milter configuration files. These option allow a different and usually longer timeout to be set when the milter is invoked during a reprocessing operation (and thus no SMTP/SUBMIT client is present).

A "$S Flag Is Used in the LOG_ACTION Mapping

The "$S" input flag is now set for the **LOG_ACTION** mapping if the current log entry is going to be written to the log file, and clear if it is not.

Enabling the XBCC SUBMIT Extension

The new **bccserver** channel option, when placed on a SUBMIT server channel, enables the **XBCC SUBMIT** extension which can be used by clients to generate separate blind carbon responses with a single transaction. By default, the **nobccserver** option is disabled.

AUTH_DEACCESS Mapping Has Been Implemented

A new **AUTH_DEACCESSS** mapping table has been implemented. This mapping forms a pair with the **AUTH_ACCESS** mapping table and is intended to be used to release resources allocated by the **AUTH_ACCESS** mapping. More specifically, **AUTH_ACCESS** can now be used to allocate some connection-related resource, which can then be used by one or more connections used to deliver the current and possibly subsequent messages. The **AUTH_DEACCESSS** mapping is called when the last connection is finally closed. The mappings communicate through the use of a **deaccess** parameter string, which is set by the new "$," flag in the AUTH_ACCESS mapping.

ALIAS_DESCRIPTION Alias Option Has Been Added

An **alias_description** alias option has been added so that aliases can have a description attached that shows up in unified configuration. This option has no effect on alias expansion.

New Options for SMTP and LMTP Channels Has Been Implemented

You can now use the following options for SMTP and LMTP channels:

- A new **TIMEOUT_MULTIPLIER TCP/IP channel-specific** option has been implemented for SMTP and LMTP channels. This option is used to change the units of the various timeout parameters from the default of minutes to seconds, allowing for shorter timeouts with finer granularity.
- A new **BANNER_RECEIVE_TIME TCP/IP-channel-specific** option has been added. This new option specifies the amount of time the SMTP/LMTP client will wait to receive the initial banner from the SMTP/LMTP server. The default value for this option is **2 minutes**. Prior to this option being available, the timeout to receive the banner was controlled by the **STATUS_MAIL_RECEIVE_TIME TCP/IP-channel-specific** option, which defaulted to **10 minutes**.

--dryrun Option Has Been Added to msconfig Command

You can now specify **--dryrun** on the **msconfig** command line to turn off automatic configuration writes and if the configuration has been modified will cause **msconfig** to exit with an error (EX_CONFIG).

log_remote_option Has Been Added

You can use the **log_remote_mta** option to control the generation of a separate logging field for remote MTA information.

Support for the JSON Format

MTA connection and transaction logs can now be written in JSON format. JSON format is enabled by setting the **log_format** MTA option to **5**. When the setting is done, each line of the resulting log file consists of a single, separate JSON object.

include_domain Option Has Been Added to msconfig Command

A bit-encoded **include_domain** MTA option has been added. At present only one bit (0, value 1) is defined, which if set causes destination domain information to be included in CONVERSIONS mapping probes.

id MTA Option Has Been Added

An **id MTA** option has been added. This option can be used to specify an identifier for a particular MTA or group of MTAs that share a common network setup. Currently, this option is only used by the smartsend plugin in its probes for IP address lists.

interfaceaddress Source Channel Option Has Been Enhanced

The **interfaceaddress** source channel option has been extended to allow specification of two different addresses, one used for logging and the other as the actual TCP/IP source address. Normally the same address is used for both purposes. When two addresses are specified they must be separated by a sharp sign with the logging address appears first, such as, "logging-address#bind-address".

New Option Has Been Added

A new **TLS_NEGOTIATION_TIME** TCP/IP-channel-specific option has been added. This new option specifies the amount of time the SMTP/LMTP client will wait for the opposite end of the connection during TLS negotiations. The default value for this option is **1 minute**. Prior to this option being available, the timeout for TLS negotiation in the SMTP server was controlled by the **STATUS_TRANSMIT_TIME** TCP/IP-channel-specific option and the timeout for the TLS negotiation option in the SMTP client was controlled by the **STATUS_RECEIVE_TIME** TCP/IP-channel-specific option, both of which defaulted to **10 minutes**.

Additional Bit Flag Has Been Implemented for MTA

The **log_filename**, **log_envelope_id**, **log_tracking**, **log_message_id**, **log_auth, log_filter**, **log_reason**, **log_diagnostics**, **log_remote_mta**, l**og_isc_status**, l**og_uid**, l**og_mailbox_uid**, l**og_conversion_tag,** and **log_transactionlog** MTA all accept an additional bit flag, position 2, value 4. If set along with bit 0 (value 1), this bit causes the attribute to appear unconditionally in XML and JSON log entries even if it is blank. The **log_times**, **log_intermediate**, and **log_username** use different bits to provide similar controls. See the option descriptions for details.

Additional Virtual Channel Support in MTA

Bit 3 (value 8) of the **log_conversion_tag** MTA option, if set, will cause the first conversion tag associated with each message recipient, if present, to be treated as an additional "virtual channel" by the MTA counter subsystem. This "channel" will then appear in counter output along with all the other channels. Note that no attempt is made to distinguish these virtual channels from normal channels; use of unique names must be dealt with by appropriate configuration.

$< and $> Metacharacters Are Used in the AUTH_REWRITE Mapping

The $< and $> metacharacters can now be used in AUTH_REWRITE mappings to send messages to syslog. The semantics are the same as in other access mappings, e.g, SEND_ACCESS.

Additional MTA Option

The new **authrewrite_extra_headers** MTA can be to include the content of additional header fields in AUTH_REWRITE mapping table probes.

Controlling the Prefix Generation on MTA-generated syslog Messages

The prefix used on syslog messages generated by the **log_connections_syslog** and **log_messages_syslog** MTA options is now controlled by the **log_syslog_prefix** MTA option.

> **Note:** In Messaging Sever 8.1, the default value of **sndopr_prefix** is **IMTA-W-**.

The "IMTA-W-" prefix used on MTA-generated syslog messages is now controlled by the **sndopr_prefix** MTA option. Note that setting the option to the empty string eliminates the prefix entirely.

processnestedmessages and retainnestedmessages Options Have Been Added

The **processnestedmessages** and **retainnestedmessages** options have been added. You can use thes options to control whether or not the conversion channel "looks inside" of nested message parts (processnestedmessages, the default) or treats them as leaf parts (retainnestedmessages).

Documentation Updates

The documentation set for Messaging Server 8.1.0 includes the following new guide:

- *Unifed Communications Suite Schema Reference*: Provides information on LDAP Schema.

Deprecated and Removed Features

Support for the following features may be eliminated in a later release, may be already removed in this release, or removed in a previous release:

- Support for Solaris 10, Oracle Linux 6, Red Hat Enterprise Linux 6 Deprecated
- Support for Index and Search Service (ISS) Removed
- Support for Cassandra Store Indexed Search Removed
- Support for Oracle Glassfish Message Queue Removed
- Support for Sun Cluster and Veritas Cluster Agents Removed
- Support for Delegated Administrator Tool Removed
- MMP Submission Proxy and MMP Legacy Config Support Removed
- Support for SSL server certificate validation for MMP connections Removed
- Support for SSL server certificate validation Removed
- TLS Version 1.1 Disabled by Default
- Support for Legacy Store msgtrace Logging Removed
- capability_x_unauthenticate Option Removed
- Support for IDN A-labels in LDAP Deprecated
- Support for SSL version 2 CLIENT-HELLO Removed

Support for Solaris 10, Oracle Linux 6, Red Hat Enterprise Linux 6 Deprecated

Messaging Server no longer supports Solaris 10, Red Hat Enterprise Linux 6, and Oracle Linux 6 operating system.

Support for Index and Search Service (ISS) Removed

Starting with this release of Messaging Server, Messaging Server no longer ships with the ISS component. Use of the old version of ISS with this version of Messaging Server is only supported for migration of search indexes from ISS to Elasticsearch.

Support for Cassandra Store Indexed Search Removed

This version requires use of Elasticsearch with Cassandra Store for Indexed Search. Use of Datastax Max with Solr integration is no longer supported starting with Messaging Server 8.1.0.

Support for Oracle Glassfish Message Queue Removed

This version no longer supports use of Glassfish Message Queue (also known as OpenMQ and Java Message Queue), except for the purpose of migrating from ISS to Elasticsearch. A warning will be generated in the log if Glassfish MQ support is enabled without Elasticsearch migration. Customers wishing to use JMS can use the ENS JMS provider (**ens-jms.jar**) to subscribe to Messaging Server events.

Support for Sun Cluster and Veritas Cluster Agents Removed

The Sun Cluster and Veritas Cluster Agents have been removed and are no longer supported. Oracle Clusterware, Automatic Failover, and Cassandra Store continue to be supported as HA options. The **ha_ip_config** tool has been removed; you can use **msconfig** to run **HAConfig.rcp** to configure the IP address for Oracle Clusterware HA.

Oracle Clusterware HA certification is not completed in Messaging Server 8.1.0 release.

Support for Delegated Administrator Tool Removed

Starting with Messaging Server 8.1.0, the Oracle Communications Delegated Administrator tool is no longer provided with Messaging Server. The **inetuser** utility is included in the Messaging Server package and can be used as a basic limited provisioning tool. Users may also develop their own provisioning tools based on the information in the *Oracle Communications Schema Guide*.

The Delegated Administrator tool included with previous versions of Messaging Server might still work since there are no incompatible schema changes. However, since that tool is not actively updated, users should limit access to that tool to trusted administrators on a trusted network.

MMP Submission Proxy and MMP Legacy Config Support Removed

The MMP mail submission SMTP proxy has been removed from this release. Configurations including the **submitproxy** will generate a warning and be ignored. The MMP requires use of unified configuration starting with this release. Use the **configtoxml** utility to convert a legacy configuration to a unified configuration.

Support for SSL server certificate validation for MMP connections Removed

Starting with Messaging Server 8.1.0, the IMAP/POP, immonitor-access, and mshttpd POP collect services will fail connections if the server certificate can not be fully validated (previous releases ignored invalid certificates for these services). Server administrators relying on these services should verify necessary certificates are properly issued and can be validated prior to upgrading to Messaging Server 8.1.0.

Support for SSL server certificate validation Removed

The **base.ldapcheckcert** option has been deleted in Messaging Server 8.1.0. LDAP SSL connections will fail unless the server certificate is valid. This option previously defaulted to **1** so there will not be a behavior change unless this had been explicitly set to **0**.

TLS Version 1.1 Disabled by Default

Messaging Server 8.1.0 now disables TLS 1.1 by default. In addition, it supports TLS version 1.3 and enables that version by default. The new **base.tlsv13enable** option can be used to disable TLS 1.3. The **base.tlsminversion** option can be used to re-enable TLS 1.0 or TLS 1.1 if required for compatibility with legacy clients. The **sslv3enable** option has been deleted; this version no longer supports SSL version 3.

Support for Legacy Store msgtrace Logging Removed

The legacy msgtrace log format has been removed with this release. Store Transaction logging will be generated instead of the legacy format. Note that store transaction logging does not include the Message-ID header value by default; see the **messagetrace.actionattributes** option for information on enabling Message-ID header value logging.

capability_x_unauthenticate Option Removed

With the publication of RFC 8437, there is now a standards-track UNAUTHENTICATE extension to IMAP. The **imap.capability_unauthenticate** option is now used to turn on the standard extension. The pre-standard option, **imap.capability_x_unauthenticate** now has no effect except to advertise the X-UNAUTHENTICATE capability. The new option must be used to enable the extension.

Support for IDN A-labels in LDAP Deprecated

Previous releases didn't process IDN A-labels (RFC 5890) present in a fully qualified user login identity. As a result it was possible to provision non-ASCII domain names to LDAP in their A-label form as long as the A-label form was always used. This release now decodes IDN A-labels in login user domains, so domains in LDAP must be provisioned in U-label rather than A-label form. This change is expected to improve readability of logs and improve end-user experience for non-ASCII domains.

Support for SSL version 2 CLIENT-HELLO Removed

Messaging Server no longer supports SSL clients that violate RFC 6176. Such clients will timeout during the SSL negotiation as the server will no longer interpret the prohibited SSL version 2 CLIENT-HELLO message.

Fixes in This Release

This section lists the fixed issues in this release of Messaging Server.

Note: For the list of bugs that have been fixed in 8.1 patch sets, refer to the patch Readme documents on My Oracle Support (MOS).

Table 1 Fixes in Messaging Server 8.1.0

Bug Number	Customer SR	Notes
29311176	N/A	Default value of the **addrsperfile** channel option would be set only when no **addrsperfile** is in effect.
29282512	N/A	The log verify option for EXPN and VRFY operations has been added on SMTP.
29048156	N/A	Distributed shared folders are now properly working.
29046607	N/A	When the **local.service.http.usesentdate** option is set, the **mbox.mjs** command in mshttpd would list the message sent date and not the internal date.
28997503	N/A	Support has been added in Messaging Server for sending text to syslog from the **AUTH_REWRITE** mapping table.
28890357	N/A	The **imsconnutil** utility will move the status of user to **CLOSING** if the user is performing a transaction and could not be killed immediately.
28873176	N/A	The **CasAccessTier.rcp** file now correctly sets the **store.dbtype** value.
28869023	N/A	**--isc** switch has been removed from the **configure** tool usage.
28763997	N/A	Network File System (NFS) support is added for the MTA logs.
28755906	N/A	ESTALE error on nslog are handled now.
28746104	N/A	Invalid **bs** entry in transaction logs for search, sort or thread mailbox events is fixed now.
28734043	N/A	The reporting of certain TLS errors by SMTP/LMTP clients has been fixed.
28695393	N/A	Issue in A-labels decoding In intermediate addresses is fixed now.
28685895	N/A	Issues caused due to the incompatible change introduced due to **Solaris 11.4 b64_decode** api is fixed now.
28680934	N/A	A problem has been fixed with imap append code using the wrong extension for relinker file **- *amsg**.
28577594	N/A	A problem has been fixed so that refreshing does not crash MMP With Adminpolicy Group.
28512469	N/A	A problem has been fixed with the uninitialized use of **as=** in the MTA log
28506353	N/A	Two new options, **TIMEOUT** and **CONNECT_ TIMEOUT**, have been added to milter configuration files.

Table 1 (Cont.) Fixes in Messaging Server 8.1.0

Bug Number	Customer SR	Notes
28502370	N/A	A problem has been fixed with "B" records were not being logged.
28498985	N/A	Oracle Convergence now generates separate messages for each bcc recipient with an explicit "bcc:" header value.
28495718	N/A	Support has been added to enable / disable multiple spam filter slots in the **FROM_ACCESS** mapping table.
28475802	N/A	The DNS Realtime Blackhole List check for incoming POP and IMAP connections is now properly working when MMP's are under production load.
28468607	N/A	Support has been added to pass conversion tag information from SMTP client to SMTP server.
28460700	N/A	HELO without an argument should clear system name even though none was specified.
28445114	N/A	LDAP SSL connection error seen during **mboxutil -r** is fixed now.
28428519	N/A	Support has been added to the **imsbackup** utility to track single copy in classic store.
28417187	N/A	Flag update scan has been optimized to reduce high CPU issues.
28368078	N/A	Check should be performed on musttlsserver for the **IGNORE_BAD_CERT** option.
28314804	N/A	**-s** option has been added to the **imexpire** command to exclude "**0 expired messages**" on mailboxes which has no expiration messages.
28314561	N/A	Support has been added to turn on resolver client debugging for MMP DNS RBL lookups.
28266407	N/A	The memory leak occurs when a message is viewed in webmail and then the message headers are re-fetched for the same message. This memory leak has been fixed.
28265138	N/A	Empty local part string is allowed now before rebuilding the address for rewriting.
28256387	N/A	A problem has been fixed with the **imexpire** command to not duplicate tasks.
28256382	N/A	A problem has been fixed where the **store.searchengine** should not be restricted
28249856	N/A	A problem has been fixed where autocreate **check_ mailuserstatus** function is not checking the **defer** status set by **rehostuser**.
28214925	N/A	Issues with vacation response when **List-Id** is present in the email header is fixed.
28167630	N/A	Milter **ADDHEADER** and I**NSHEADER** actions now call the **MILTER_ACTIONS** mappings.
28122046	N/A	A problem has been fixed where the Imapd is crashed in the **Index_fetchreply**.

Table 1 (Cont.) Fixes in Messaging Server 8.1.0

Bug Number	Customer SR	Notes
28063769	N/A	Problem caused by attempting to optimize MIME scanning across sieve and conversion operations has been fixed.
27560645	N/A	**imexpire -f** command should load the rule file specified by the **-f** option only. It should not load the **store.expirerule** files under the store partitions.
27485647	N/A	Folder names in expirerule should be in MUTF-7 format.
27357808	N/A	Problem has ben fixed where Mshttpd was crashed due to heap corruption.
26108389	N/A	Rehostuser should pass **-oBatchMode=yes** when running ssh.

Known Problems

This section lists the known problems in this release of Messaging Server.

Note: For the most recent known problems with Messaging Server 8.1, refer to the patch Readme documents on MOS.

Indexed Search Convertor Warning While Converting PDF File

SR Number: N/A

Bug Number: 26226239

In Cassandra message store, the Indexed Search Convertor might fail to convert a large PDF file.

Cassandra Store Cannot Be Stopped When Other Message Store Processes Are Running

SR Number: N/A

Bug Number: 26187893

Indexed Search Converter Should Limit the Queue Size

SR Number: N/A

Bug Number: 26122176

During bursts of high traffic, the Indexed Search Convertor (ISC) does not currently limit the queue size and return a busy error to the client when the queue is full, enabling the client to fail over to another ISC.

Workaround:

Perform one of the following:

1. Increase the active thread limit (**isc.msgprocessor.maxthreads** option).
2. Add more ISC instances to the deployment.

Cassandra Message Store Quota Root Usage Updates Can Overwrite Each Other

SR Number: N/A

Bug Number: 25667309

Cassandra message store quota root usage updates can overwrite each other, so, quota usage can be inaccurate.

Cassandra Store Search Should Normalize Queries to NFC Format

SR Number: N/A

Bug Number: 25506348

Some iOS clients send search requests in the non-standard NFD format, which produce incorrect results when the backing index is in the standard NFC format.

imap lsub Command Does Not Display Subscribed Shared Folders

SR Number: N/A

Bug Number: 25345931

Because Cassandra message store does not currently support shared folders, subscribed folders are not displayed when a user with access rights and subscribed to a shared folder lists the subscribed folders.

Event Notification Service Times Out Under Stress

SR Number: N/A

Bug Number: 25205101

Occasionally, the Event Notification Service (ENS) times out when under stress.

Workaround:

If an overload condition causes ENS to time out, add additional store affinity groups to the deployment.

Cassandra Message Store Is Missing Annotation Search

SR Number: N/A

Bug Number: 25177871

Currently, the Cassandra message store does not advertise ANNOTATE-EXPERIMENT-1 because it does not implement annotation search yet.

Cassandra Store msgindex Table Partition Assignment Can Be Inaccurate

SR Number: NA

Bug Number: 25130372

The Cassandra store **msgindex** table partition assignment can be inaccurate when multiple threads are updating the quota record of a user at the same time. The **msgindex** partition can become very large and impact performance.

Workaround: Limit the total message count per user to less than 1 million messages.

imsrestore Command Does Not Restore Annotations and Shared Folders in Cassandra Message Store

SR Number: N/A

Bug Number: 24755752

Currently, in Cassandra message store, the **imsrestore** command does not restore annotations and shared folders because these features are not yet supported.

Internal date Time Zone Information Is Lost During Backup and Restore

SR Number: N/A

Bug Number: 24462739

Resource Consumption Grows in Cassandra Store as Number of Messages Inbox Increases

SR Number: N/A

Bug Number: 24462049

The amount of CPU, RAM, and network resources consumed by **imapd** when in Cassandra message store mode grows as the number of messages in a mailbox increases.

imsbackup -x Command Does Not Back Up Expunged Messages

SR Number: 3-14371431171, 3-14313694321

Bug Number: 24406306

Running the **imsbackup -x** command does not back up expunged messages.

Mail Deletion Fails When Deleted by a User Subscribed to the Mailbox (Cassandra Message Store Only)

SR Number: N/A

Bug Number: 24302912

This problem occurs only when a user having access to a shared folder performs expunge operations on the shared folder.

Unable to Copy Email Messages to Shared Folders (Cassandra Message Store Only)

SR Number: N/A

25325977

Because Cassandra message store does not currently support shared folders, copying email messages to shared folders does not work.

configure Script Does Not Always Disable sendmail

SR Number: N/A

Bug Number: 23070490

Disabling **sendmail** through the **configure** script is not always successful.

Shared Folders Are Not Supported (Cassandra Message Store Only)

SR Number: N/A

Bug Number: N/A

Currently, the Cassandra message store does not support shared folders.

Deleting and Moving Email Messages on iOS Is Not Successful

SR Number: N/A

Bug Numbers: 24389385, 24384152, and 24382296

There is an issue on iOS where deleting all email messages, or moving all email messages into a folder, might not be successful.

Store ENS Event Feature Parity with Glassfish MQ Store Events

SR Number: N/A

Bug Number: 26290829

The events and event attributes available for ENS need to have feature parity with the events and event attributes that are available for Oracle Glassfish Message Queue events.

Messaging Server Now Requires High Level of TLS Security

SR Number: NA

Bug Number: 21626085

Messaging Server 8.0.1 and greater requires a high level of TLS security that legacy clients may not support. If legacy clients are unable to connect to Messaging Server, then the tlsminversion options can be used to reduce server security requirements thus allowing legacy clients to connect.

Workaround:

Run the following command in a Unified Configuration before starting Messaging Server to avoid a start up failure after upgrading:

```
msconfig set base.tlsminversion TLS1.0
```

or in a legacy configuration:

```
configutil -o local.tlsminversion -v TLS1.0
```

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Oracle Communications Messaging Server Release Notes, Release 8.1.0
F15152-02