Oracle® Communications Messaging Server

Release Notes

Release 8.0.1

E63713-02

February 2016

This document provides release notes for Oracle Communications Messaging Server Release 8.0.1, consisting of the following sections:

New and Changed Features

The new features and feature enhancements in this release of Messaging Server are:

Message Store Automatic Failover

A message store replication group consists of one or more message store nodes. You can configure the message store nodes with one or more remote hosts. If remote hosts are configured, the message store contacts a remote host to retrieve the replication group data on start up. If a master has not been established in a group, an election is called. A priority value is assigned to a node. When an election is held, the node with the most up-to-date log record and the highest priority becomes the new master. A node with priority 0 cannot be elected.

When the master fails, the replicas will automatically hold an election to select a new master. The automatic failover facility will redirect incoming connections to a new master.

Support for LMTP Client and Server to Detect and Respond to Certain Conditions

We have added LMTP client and server support to detect and respond to the condition where a given host's LMTP server is responding but is not associated with the master store replica. When this happens the LMTP server produces a banner or **MAIL FROM** response.

Support for Oracle Clusterware

Messaging Server High Availability now supports Oracle Clusterware High Availability software.

MMP counterutil Monitoring (Connection and Login Counters for IMAP and POP)

Counters added to the MMP for the IMAP and POP proxies are similar to those implemented in **IMAPD** and **POPD**. **mmpstat** is the name of the newly introduced **counterobject**. You can infer the individual counters' meanings from their IMAP and POP counterparts. As with IMAP and POP, the counters are enabled by default (and are not configurable), and you can read/reset their values using the **counterutil** command.

MTA Prefix/Suffix Text Addition Facilities Support the Addition of Both HTML and Plain Text

The MTA prefix/suffix text addition facilities now support the addition of both HTML and plain text as well as the insertion of prefix/suffix text into text/html parts.

You indicate HTML in a prefix/suffix addition by enclosing it in <html></html> tags, which are removed from the addition.

You place additions to text/html parts immediately after the <body> tag (prefix text) and immediately before the </body> tag (suffix text).

You precede plain text additions to text/html by
<pre> and follow them by </pre>
. HTML additions to text/plain parts remove all HTML tags and convert all entities to corresponding characters.

As part of this change, we have increased the maximum size of additions from 1024 to 4096 characters.

There are no options associated with this capability.

msprobe Provides Per-Service Support for Monitoring

We have added an **-r** option to **msprobe** to report status to **stdout** in csv (comma-separated value) format and a *server* option to specify one server.

Disable TLS 1.0 with Option

TLS 1.0 is now disabled by default. If you have trouble with clients connecting, you can enable it by setting the **base.tlsminversion** option to TLS1.0.

Bundled NSS Upgraded to NSS 3.19.2

This release of Messaging Server upgrades NSS to version 3.19.2.

Bundled ICU Upgraded to 55.1

This release of Messaging Server upgrades ICU to 55.1.

Berkeley Database Upgraded to 6.1.26

Berkeley Database has been upgraded to version 6.1.26.

New QUARANTINE_ACTION Milter Plug-in

A new **QUARANTINE_ACTION** option has been added to the milter plug-in. If this option is set it specifies the Sieve action to use when a milter quarantine message modifier is engaged. For additional information, see the *Messaging Server Reference*.

J Records Contain Recipient Information

J records produced in response to DATA and BDAT command failures will now contain recipient information if there was a single valid message recipient. Note that the information logged is whatever was passed in the **RCPT TO** command; not the output of alias processing.

$+% Metacharacter in *_ACCESS Mappings

The **$+%** metacharacter, when set in a **FROM_ACCESS**, **SEND_ACCESS**, **ORIG_SEND_ACCESS**, **MAIL_ACCESS**, or **ORIG_MAIL_ACCESS** mapping, acts in a fashion similar to **$N**: A string is read from the mapping result and returned as an error. The difference with **$+%** is that the error is deferred to the DATA phase of the transaction. Note that **$X** does not presently work with **$%X** as it does with **$N**.

Also note that the effect of **$+%** can be observed in **imsimta test -rewrite**; an "Ending address list failed:" will be noted in the output.

New refusenotary Restricted Channel Option

The **refusenotary** restricted channel option has been added. If set, this option causes the SMTP server to not offer the DSN extension and the SMTP/LMTP client to not attempt to use the DSN extension even if it's available.

Latent Preprocessing Facility

The latent preprocessing facility supported by the sieve/recipe language interpreter has been activated for use in recipes. A complete list of the directives that are supported can be found in the Recipe language discussion in the *Messaging Server Reference*.

msconfig Run Command Now Allows Arguments

The **msconfig run** command now allows arguments to be specified. Arguments can then be retrieved using the new functions **argc** and **argv**, which work in the usual way.

For example, the following simple recipe prints out the values of **argc** and **argv**:

```
print "argc = " . argc . "\n";
j = 0;
loop {
  exitif ++j > argc;
  print "argv(" . j . ") = \"" . argv(j) . "\"\n";
}
```

official_host_name for a Channel Now Defaults to the Channel Name with ".hostname" Appended if Omitted

If omitted in a Unified Configuration, the *official_host_name* for a channel now defaults to the channel name with ".hostname" appended. This has the effect of making the *official_host_name* optional in Unified Configurations.

Setting Deleted Options in Sieve Script Returns Warning

Attempts to set deleted options in the recipe language now cause a warning to be issued rather than causing the script to fail with an error.

BANNER_REVERSE_HOST TCP/IP Channel-Specific Option

A new **BANNER_REVERSE_HOST** TCP/IP channel-specific option has been added. This boolean option, if set to a nonzero value, causes a reverse DNS lookup to be performed on the local host's IP addresses for each incoming connection. If the lookup succeeds, the resulting value replaces the value of the **BANNER_HOST** TCP/IP channel-specific option for the connection.

MTA Can Now Associate Prefix/Suffix Text Additions with Domain Entries in LDAP

The MTA can now associate prefix/suffix text additions with domain entries in LDAP. This text will be inserted into messages submitted by any authenticated user associated with the domain.

The default LDAP attributes associated with this capability are **mailDomainPrefixText** and **mailDomainSuffixText**. These default attributes can be overridden with the new MTA options **ldap_domain_attr_prefix_text** and **ldap_domain_attr_suffix_text**.

Associate Sieve Scripts with Authenticated Users and an Authenticated User's Domain

We have added the ability to associate Sieve scripts with authenticated users and an authenticated user's domain. These are system-level scripts designed to implement filtering functions based on the message sender; they are not intended for end-user use.

The sender domain and user Sieves are evaluated immediately after source channel Sieves and before the system Sieve.

Exchange Journal Format Archiving for IMAP APPEND with LDAP Attributes

We have added support to the archiving library to produce Microsoft Exchange Journal format archive messages. Note that this support extends to store compliance archiving of IMAP APPENDs as well as the archiving plugin.

ENS SSL Support

We have added SSL support to ENS in a separate default port 8997. We have added new options to support this feature.

ENS Support for Password-Based Authentication

We have added Messaging Server options to support password-based authentication to the ENS server. Table 1 describes the options.

Table 1 Options for Password Based Authentication to ENS

Unified Configuration Option	Legacy Configuration Option	Description
ens.mustauthenticate	**local.ens.mustauthenticate**	Enable/Disable authentication
ens.secret	**local.ens.secret**	Change the secret for authentication
notifytarget:*target-name***.ensuser**	**local.store.notifyplugin.***target-name***.ensuser**	Specify username for the ENS **notifytarget/notifyplugin**
notifytarget:*target-name***.enspwd**	**local.store.notifyplugin.***target-name***.enspwd**	Specify password for the ENS **notifytarget/notifyplugin**

Enabling and Disabling Password Based Authentication

To enable password based authentication, run the following command in Unified Configuration:

```
msconfig set ens.mustauthenticate 1
```

or in legacy configuration:

```
configutil -o local.ens.mustauthenticate -v 1
```

To disable password based authentication, run the following command in Unified Configuration:

```
msconfig set ens.mustauthenticate 0
```

or in legacy configuration:

```
configutil -o local.ens.mustauthenticate -v 0
```

This option enables or disables whether authentication is required by the ENS broker. The default value of the **ens.mustauthenticate** option is **0**.

If **mustauthenticate** option is set, authentication is required by the ENS broker in both SSL and non-SSL ports.

Changing the Secret for Authentication

To change the secret for authentication, run the following command in Unified Configuration:

```
msconfig
set ens.secret secret text
write
```

or in legacy configuration:

```
configutil -o local.ens.secret -v "secret text"
```

There is no default value for **ens.secret**.

Specifying the Username for the ENS

To specify the username for the ENS, run the following command in Unified Configuration:

```
msconfig set notifytarget:target-name.ensuser username
```

or in legacy configuration:

```
configutil -o local.store.notifyplugin.target-name.ensuser -v username
```

The default value of the option **ensuser** is **guest**.

Specifying the Password for the ENS

To specify the password for the ENS, run the following command in Unified Configuration:

```
msconfig set notifytarget:target-name.enspwd password
```

or in legacy configuration:

```
configutil -o local.store.notifyplugin.target-name.enspwd -v password
```

The default value of the option **enspwd** is **NULL**. The value of the **enspwd** option will be equal to the value of **ens.secret** if one of the following conditions is met:

- The **notifytarget** is **ms-internal**.
- The value of **notifytarget:***target-name***.enshost** is not set.
- The value of **notifytarget:***target-name***.enshost** is equal to the value of **service.listenaddr**.
- The value of **notifytarget:***target-name***.enshost** is the loopback address, "127.0.0.1" or "::1".

If you provide the **ensuser** and **enspwd**, then the **notifytarget** figures out whether or not the ENS broker that it connects to requires password based authentication. If the ENS broker requires a password, then the password provided will be used or if it does not require a password, it will not be used.

With the newer version of the ENS broker that uses authentication with **ens.mustauthenticate** set to 1, you must set a password using the **ens.secret** option. Otherwise all connections to the ENS broker will fail. If authentication is disabled with **ens.mustauthenticate** set to 0, the older version of the ENS broker which does not have authentication will be used. By default, authentication is disabled.

New Client API ens_sopen

We have added a new client API, **ens_sopen**, that creates a secure connection to the ENS Broker that supports authentication and TLS/SSL.

Increase in Buffer Size for Data: URLs

The buffer size and associated logic for data: URLs has been changed to accommodate URLs up to 4096 characters long primarily to accommodate the much longer verdict strings that Symantec Brightmail returns. It will also make it possible to do more with Sieve prefixes and suffixes on milter verdicts.

Milter spamfilter Plugin Enhanced to Use Context-Sensitive editheader Operations

We have enhanced the milter spamfilter plugin to use context-sensitive **editheader** operations. For example, in the generated Sieves the header fields being modified are selected on the basis of content, not position. This change provides a closer semantic match, especially in cases where multiple milters simultaneously modify the same header field.

The use of context-sensitive editing is controlled by the new milter option **CONTEXT_EDITS**. If set to 1 context-sensitive editing is enabled. If you set the option to 0, it is disabled. 1 is the default.

Note that context-sensitive editing requires that the milter plugin maintain a separate copy of the message header, which may increase overhead.

The milter plugin already makes use of the nonstandard **replaceheader** action, which was originally part of the **editheader** draft but was dropped prior to standardization. This change required an additional nonstandard editheader enhancement: A **:count** argument has been added to **deleteheader**, which specifies the maximum number of fields that **deleteheader** will delete.

New Options Added to the Milter spamfilter Plugin

Normally, messages are transferred to the milter server as they are presented to the MTA. Setting **DEFER_MESSAGE_TRANSFER** (integer; default is 0) to a non-zero value defers the transfer until after the preceding spamfilter plugin has completed its actions, at which point the message header and body are transferred to the milter server from the MTA's internal storage areas. Normally this option is used in conjunction with setting the **IMMEDIATE_HEADER_MODIFICATIONS** option on a previous milter spamfilter plugin, which results in the modifications made by the previous milter being visible to the current milter.

By default the milter interface converts milter header modification actions to Sieve actions. Setting **IMMEDIATE_HEADER_MODIFICATIONS** (integer, default 0) to a non-zero value will cause the plugin to modify the MTA's internal copy of the message header directly. No Sieve actions will be generated.

Note: This option should ONLY be used with plugins enabled on the basis of the source channel. Use with plugins enabled on destination channels will cause inconsistent results.

New Attributes Added to dssetup

There are new schema items for Messaging Server added to dssetup 6.4.0.28.0:

- mailDomainPrefixText
- mailDomainSuffixText
- mailDomainSenderSieve
- mailSenderSieve
- mailDomainCaptureAddress
- mailCaptureAddress

mailDomainPrefixText

Syntax: 1.3.6.1.4.1.1466.115.121.1.15 (UTF-8)

MAY for inetDomain and sunManagedOrganization

single valued

Definition: Attribute for domain based header.

attributeTypes: (2.16.840.1.113894.1009.1.101.0.1192.1.1 NAME 'mailDomainPrefixText' DESC 'domain based email header' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE)

mailDomainSuffixText

Syntax: 1.3.6.1.4.1.1466.115.121.1.15 (UTF-8)

MAY for inetDomain and sunManagedOrganization

single valued

Definition: Attribute for domain based footer.

attributeTypes: (2.16.840.1.113894.1009.1.101.0.1193.1.1 NAME 'mailDomainSuffixText' DESC 'domain based email footer' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE)

mailDomainSenderSieve

Syntax: 1.3.6.1.4.1.1466.115.121.1.15 (UTF-8)

MAY for inetDomain and sunManagedOrganization

multi-valued

Definition: Domain based Sieve for outgoing mail.

attributeTypes: (2.16.840.1.113894.1009.1.101.0.1194.1.1 NAME 'mailDomainSenderSieve' DESC 'domain based sieve for outgoing mail' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15)

mailSenderSieve

Syntax: 1.3.6.1.4.1.1466.115.121.1.15 (UTF-8)

MAY for inetMailGroup inetMailUser inetManagedGroup

multi-valued

Definition: User level Sieve for outgoing mail.

attributeTypes: (2.16.840.1.113894.1009.1.101.0.1195.1.1 NAME 'mailSenderSieve' DESC 'user level sieve for outgoing mail' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15)

mailDomainCaptureAddress

Syntax: 1.3.6.1.4.1.1466.115.121.1.15 (UTF-8)

MAY for inetDomain and sunManagedOrganization

multi-valued

Definition: Domain based journal archive address.

attributeTypes: (2.16.840.1.113894.1009.1.101.0.1196.1.1 NAME 'mailDomainCaptureAddress' DESC 'domain journal archive address' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15)

mailCaptureAddress

Syntax: 1.3.6.1.4.1.1466.115.121.1.15 (UTF-8)

MAY for inetMailGroup inetMailUser inetManagedGroup

multi-valued

Definition: User level journal archive address.

attributeTypes: (2.16.840.1.113894.1009.1.101.0.1198.1.1 NAME 'mailCaptureAddress' DESC 'user journal archive address' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15)

Snapshot Changes

The following snapshot changes or recommendations have been implemented.

- The initial **snapshotverify** schedule has been changed to every 10 minutes.
- **imdbverify** keeps all the snapshots current.
- Do not set **store.snapshotdirs** to more than 3.

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 AXS-One and Operational Archiving Removed
- imarchive -s Feature Is Deprecated
- Legacy Initial Configuration Is Deprecated
- msgtrace Log Format Is Deprecated
- Oracle GlassFish Message Queue Is Deprecated
- MMP Legacy Configuration Support Is Deprecated
- readership Command Is Deprecated
- MTA BDB Databases Are Deprecated
- Support for Sparse Zones Is Deprecated
- Enabling POP Before SMTP Is Deprecated
- native, unix, and file mailDeliveryOption Settings Are Deprecated
- Support for TLS Features Described as "must not" or "should not" in TLS Best Practices Is Deprecated

Support for AXS-One and Operational Archiving Removed

AXS-One and Operational Archiving are no longer supported.

imarchive -s Feature Is Deprecated

This feature is deprecated and may be removed in a later release.

Legacy Initial Configuration Is Deprecated

The **configure** tool can presently generate a legacy initial configuration. This facility may be removed in a later release to encourage use of Unified Configuration for new deployments.

msgtrace Log Format Is Deprecated

The store **msgtrace** log format is deprecated in favor of the store action log format. The store action log (when **msgtrace.active** is set to **transactlog**) has similar capability but uses an easy to parse format (XML) that is equivalent to the MTA XML transaction log format. The **msgtrace** log format may be removed in a later release.

Oracle GlassFish Message Queue Is Deprecated

The Oracle Glassfish MQ C SDK (also known as OpenMQ and JMQ) and JMQ JMS provider are not recommended. They have been deprecated and their support may be removed in a later release. Instead, use Java JMS (presently with the Oracle Glassfish MQ provider) and the ENS C API. Note that we do not support use of JMQ with anything running in web containers other than Glassfish.

MMP Legacy Configuration Support Is Deprecated

MMP support for legacy configuration is deprecated and may be removed in a later release.

readership Command Is Deprecated

Support for the **readership** command is deprecated and may be removed in a later release.

MTA BDB Databases Are Deprecated

MTA access to database files and the **imsimta** tools to manipulate MTA database files are deprecated and may be removed in a later release. MTA text databases continue to be supported.

Support for Sparse Zones Is Deprecated

Sparse zone support is deprecated and may be removed in a later release.

Enabling POP Before SMTP Is Deprecated

SMTP Authentication, or SMTP Auth (RFC 2554), is the preferred method of providing SMTP relay server security. SMTP Auth allows only authenticated users to send mail through the MTA. The legacy MMP POP before SMTP feature is deprecated and may be removed in a later release.

native, unix, and file mailDeliveryOption Settings Are Deprecated

The **native**, **unix** and **file mailDeliveryOption** settings are deprecated and may be removed in a later release.

If you actively depend on these features please contact Oracle support.

The initial Unified Configuration will no longer include a channel block and channel class for the **native** channel. The **native** and **file** delivery options will not work by default. There is no expected impact to customers using an existing configuration that is upgraded at this time.

Support for TLS Features Described as "must not" or "should not" in TLS Best Practices Is Deprecated

Support is deprecated for all TLS features mentioned as "must not" or "should not" in RFC 7525 at http://tools.ietf.org/html/rfc7525 and may be removed in a later release.

Fixes in This Release

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

Table 2 Fixes in Messaging Server 8.0.1

Bug Number	Customer SR	Notes
20778318	3-10480785151	After transaction limit, new session does not use **auth** as first session did.
20816084	Not Applicable	**mshttpd** not interpreting meta charset tag in html body when no charset in **C-t**.
20816136	Not Applicable	**reconstruct** removes too many annotations.
21418554	3-11026432331	**immonitor-access** does not retrieve the message when using **-I** (IMAP).
21486770	Not Applicable	**imapd** core forceoff -> **mboxname_owner**, but ctx->**imapd_mailbox** is null.
21659748	Not Applicable	IMAP search on date range returning results from ISS as **AFTER** not **SINCE**.
21779362	Not Applicable	**rehostuser** logs error about LDAP connection which was successfully reconnected.

Known Problems

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

Messaging Server Now Requires High Level of TLS Security

SR Number: NA

Bug Number: 21626085

Messaging Server 8.0.1 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
```

Starting Messaging Server Can Fail After Upgrade in HA

SR Number: NA

Bug Number: 21785994

Starting Messaging Server can fail after you upgrade from version 7U4 P27 to 8.0.1 or from 7U4 P27 to 7.0.5.28 (or higher) then to 8.0.1 in an HA environment.

Workaround:

After upgrading to Messaging Server 8.0.1.0 in HA, run **start-msg** before running any other command.

SNMP Issues

The SNMP support in Messaging Server depends on operating system APIs that are unstable across major OS releases. Due to this issue, the SNMP feature works best on the oldest supported version of a given operating system and may have problems on newer operating systems. For Solaris 11, you can get SNMP working by doing the following.

1. Create a soft link to the **madmand** library.

   ```
   cd /opt/sun/comms/messaging64/lib
   ln -s madmand madmand9
   ```

2. Install the Solaris10 Packages.

   ```
   pkgadd SUNWsmagt SUNWsmcmd
   ```

3. Configure Messaging Server to run the SNMP Agent in stand-alone mode.

   ```
   msconfig
   set role.snmp.enable = 1
   set role.snmp.listenaddr = externally visible IP address
   set role.snmp.standalone = 1
   write
   ```

Documentation Updates

Messaging Server documentation is now available in book form on the Oracle Help Center website instead of the Oracle Wikis website. The documentation set includes:

- *Messaging Server Installation and Configuration Guide*
- *Messaging Server Reference*
- *Messaging Server Release Notes*
- *Messaging Server Security Guide*
- *Messaging Server System Administrator's Guide*

Document Revision History

The following table lists the revision history for this document:

Version	Date	Description
E63713-02	February 2016	Minor formatting and text changes.
E63713-01	September 2015	Initial release.

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 8.0.1
E63713-02