What's New in the LISTSERV® Version 16.0-2017a Level Set

28 February 2017

THE 2017a LEVEL SET

The LISTSERV 16.0-2017a level set includes all known fixes and patches and between-release enhancements up to 28 February 2017. There are a number of bug fixes and enhancements in LISTSERV itself, and there are also changes and fixes to the WA CGI for the web interface and to the default web templates (default.wwwtpl) to support the WA changes.

<div style="border:1px solid red">

IMPORTANT: LISTSERV 16.0 requires a valid version 16.0 LAK!
This Level Set also requires valid Maintenance expiring on 28 Feb 2017 or later!

You must obtain and install a LISTSERV version 16.0 product LAK and (for sites with perpetual licensing) an appropriate maintenance LAK, or LISTSERV will not start after the upgrade.

[More information](#)

</div>

Table of Contents

LISTSERV 16.0-2017a Level Set Changes for LISTSERV

Since the release of LISTSERV 16.0-2014b in May 2014, the following improvements and bug fixes have been made.

Security, Usability: DKIM replaces DomainKeys

Perhaps the most significant change in this level set release is the replacement of the now-deprecated DomainKeys email authentication system with the DKIM (DomainKeys Identified Mail) system. For most LISTSERV sites already using DomainKeys authentication, this is a transparent change requiring no adjustment to your current settings.

> Please note, however, that sites that have used the LISTSERV DomainKeys feature since it was originally released should take this opportunity to review their key pair, as key lengths which were sufficient for DomainKeys may be too short for DKIM. Per RFC 6376 "DomainKeys Identified Mail (DKIM) Signatures", Section 3.3.3, "Signers MUST use RSA keys of at least 1024 bits for long-lived keys", whereas many DomainKeys sites may be using keys of 512 or 768 bits.

For more general information about DKIM, please see http://www.dkim.org/ .

Extensibility, Usability: RSS abstract encoding made more robust

LISTSERV now more robustly encodes plain-text abstracts to avoid feed validation errors. HTML abstracts are presumed to have been correctly generated and are left alone.

> To complete the implementation of this change for plain-text RSS abstracts, you MUST also rebuild all web archive indexes with the REINDEX command after upgrading LISTSERV. While logged in as a LISTSERV maintainer, issue the command
>
> ```
>                 REINDEX WWW ALL
> ```
>
> either by using the "LISTSERV command" menu item under Server Configuration in the web interface, or by sending it in the body (not the subject) of an email addressed to the LISTSERV@ command address for your server.

Usability: Misc-Options= NEW_MESSAGE_ID

The option NEW_MESSAGE_ID has been added to the Misc-Options= list header keyword. When specified, this causes LISTSERV to generate a new RFC822 Message-ID: field for outbound messages. This solves a problem with email providers that bounce messages with duplicate Message-ID: fields. Specifically, it solves the problem experienced by Gmail subscribers who are set to the REPRO option, and currently do not receive the copy of their own mail sent to them by the server after it is processed.

Setting this option may cause idiosyncratic issues with the way Gmail presents the mail in its indexes. The REPRO copy of the mail will show up in both the Sent folder and the Inbox folder, as part of a single thread. This is cosmetic only; the links are to the same message, and if one is marked as read, the other will also be marked as read.

Additionally, if the Gmail user's subscription is set to SUBJECTHDR, the Gmail interface will not display "[LISTNAME]" as part of the subject of the REPRO copy. This could lead to the erroneous conclusion that the original message and the REPRO copy are duplicates, except for small differences in the timestamp. The only useful way to show the difference is to use Gmail's "Show original" feature to inspect the headers thus revealed.

It should be noted that systematically changing message IDs does not follow relevant Internet standards for mail, and could promote mailing loops. Consider carefully whether or not the benefits of viewing REPRO mail in Gmail outweigh the potential problems engendered by changing message IDs before adding this setting to your list(s).

Extensibility, Usability: TRACE_DNS debug flag assists in debugging DMARC errors

The new TRACE_DNS debug flag is useful for debugging problems with DMARC lookups from LISTSERV, as in conjunction with the "DEBUG QUERY TXT *hostname*" command, it can show you exactly what information LISTSERV is receiving (or not receiving) from its DNS servers.

To use the feature, issue the LISTSERV maintainer command "DEBUG FLAGS +TRACE_DNS". For instance (the interesting parts are highlighted in light grey):

```
Paused - enter a command:
debug flags +trace_dns
1 Feb 2017 15:10:05 From LISTSERV@LISTSERV.EXAMPLE.COM: debug flags +trace_dns
* Debug flags for this session: 00000200
*
00000001 TRACE_DIST        [Trace DISTRIBUTE processing - OFF]
00000002 TRACE_MIME        [Trace MIME parser - OFF]
00000004 TRACE_LISTS       [Trace (a few) list-related functions - OFF]
00000008 TRACE_SPAM        [Trace spam filter calls - OFF]
00000010 TRACE_EMM         [Trace Embedded Mail-Merge processor - OFF]
00000020 TRACE_DEV         [Temporary ad hoc tracing for development use - OFF]
00000040 TRACE_FSAV        [Trace FSAV calls - OFF]
00000080 TRACE_LDAP_CALLS [Trace LDAP library calls - OFF]
00000100 TRACE_LDAP_DATA  [Trace data obtained from LDAP - OFF]
00000200 TRACE_DNS          Trace DNS lookups
08000000 HOLD_DISTBG       [Do not process background DISTRIBUTE jobs - OFF]
10000000 HOLD_XB64         [Hold X-B64 jobs instead of processing them - OFF]
20000000 KEEP_JOBFILES     [Keep successfully processed job files - OFF]
40000000 TRACE_TCPGUI      [Additional TCPGUI tracing - OFF]
```

Next, enter the command "DEBUG QUERY TXT hostname" with whatever hostname is configured in DNS with the DMARC TXT record LISTSERV should be referencing.

```
Paused - enter a command:
debug query txt _dmarc.yahoo.com
1 Feb 2017 15:10:43 From LISTSERV@LISTSERV.EXAMPLE.COM: debug query txt
_dmarc.yahoo.com
1 Feb 2017 15:10:43 DBG> Looking up TXT records for _DMARC.YAHOO.COM
1 Feb 2017 15:10:43 DBG> Trying 8.8.8.4
1 Feb 2017 15:10:43 DBG> One record found
* _DMARC.YAHOO.COM IN TXT "v=DMARC1; p=reject; pct=100; rua=mailto:dmarc_y_rua@y
ahoo.com;"
```

If there is no DMARC record for the hostname you specify, the response will be different:

```
1 Feb 2017 15:21:37 DBG> Looking up TXT records for _DMARC.EXAMPLE.COM
```

```
1 Feb 2017 15:21:37 DBG> Trying 8.8.8.4
1 Feb 2017 15:21:37 DBG> No record found
* DNS query for _DMARC.EXAMPLE.COM returned no TXT record.
```

Finally, turn off the debug flag:

```
Paused - enter a command:
debug flags -trace_dns
1 Feb 2017 15:11:00 From LISTSERV@LISTSERV.EXAMPLE.COM: debug flags -trace_dns
* Debug flags for this session: 00000000
*
* 00000001 TRACE_DIST       [Trace DISTRIBUTE processing - OFF]
* 00000002 TRACE_MIME       [Trace MIME parser - OFF]
* 00000004 TRACE_LISTS      [Trace (a few) list-related functions - OFF]
* 00000008 TRACE_SPAM       [Trace spam filter calls - OFF]
* 00000010 TRACE_EMM        [Trace Embedded Mail-Merge processor - OFF]
* 00000020 TRACE_DEV        [Temporary ad hoc tracing for development use - OFF]
* 00000040 TRACE_FSAV       [Trace FSAV calls - OFF]
* 00000080 TRACE_LDAP_CALLS [Trace LDAP library calls - OFF]
* 00000100 TRACE_LDAP_DATA  [Trace data obtained from LDAP - OFF]
* 00000200 TRACE_DNS        [Trace DNS lookups - OFF]
* 08000000 HOLD_DISTBG      [Do not process background DISTRIBUTE jobs - OFF]
* 10000000 HOLD_XB64        [Hold X-B64 jobs instead of processing them - OFF]
* 20000000 KEEP_JOBFILES    [Keep successfully processed job files - OFF]
* 40000000 TRACE_TCPGUI     [Additional TCPGUI tracing - OFF]
```

These example commands were issued from the LISTSERV command line; note that the commands may also be issued by email or through the web interface's "LISTSERV command" pages.

Security, Anti-Spam: MAX_CONSECUTIVE_SUBS now applied to X-CONFIRM command

It was discovered that LISTSERV list signup pages could be exploited to flood targets with bogus subscription confirmation requests by invoking the X-CONFIRM command over and over for individual addresses to multiple lists on the server. This could happen either accidentally (broken external script) or by malicious intent. The original exploit would result in a further flooding several days later when the bogus subscription requests expired. Because X-CONFIRM is not a SUBSCRIBE command, it was not limited by the MAX_CONSECUTIVE_SUBS setting

To mitigate this problem, LISTSERV's internal X-CONFIRM function was modified to honor MAX_CONSECUTIVE_SUBS, and will reject consecutive X-CONFIRM commands from the same user once that limit is reached. The rejection message is displayed in the web interface and is not sent to the targeted address.

Usability: SPOOL_CLEANUP feature added

A new site configuration keyword, SPOOL_CLEANUP, has been added to help automate clearing old files from the spool that should not be kept indefinitely. The keyword takes a single integer value denoting the number of days between cleanups, and setting it to 0 disables it. The default is 30 days. Examples:

```
    VM:   SPOOL_CLEANUP = 7
    Unix: SPOOL_CLEANUP=7
          export SPOOL_CLEANUP
    Win:  SPOOL_CLEANUP=7
```

The keyword is not explicitly editable in the web administration interface, but can be added by using the "Find or Add Configuration Variable" search box at the top of the Site Configuration page. Once added, the keyword becomes available and editable in the My Configuration tab.

Alternately, the keyword can be set in LISTSERV's main site configuration file as usual.

In LISTSERV 16.0-2017a, enabling the feature targets only .ERROR files found in the spool directory. In future versions, the feature may target other types of files.

LISTSERV 16.0-2017a Level Set Changes for WA

The current WA version at level-set release is "16.5 (Build Date: 28 Feb 2017 18:01:23)".

WA has been greatly streamlined since the release of LISTSERV 16.0-2014b which contained WA 2.4.1 r4239. A number of functions have been optimized and old unused code removed. In addition, a number of XSS and other vulnerabilities have been quashed. Because these issues remain exploitable in older versions of WA, L-Soft will not discuss the specific changes made in this regard, other than to state that all those vulnerabilities that have been found during the course of a comprehensive code review have been fixed in the current release of WA.

For LISTSERV running under Microsoft Windows: A file named WA.SYM has been added to the web interface, along with WA.EXE. This file is required to be present in order for WA to produce meaningful error reports under Microsoft Windows. The installer will place the file in the CGI/scripts directory with WA.EXE.

If WA.EXE crashes, files with names similar to WA-20170209-155115-007.CRASH will be written into the web interface's UPLOAD directory. These files can be then used by L-Soft Support to assist in diagnosing the crash.

WA.SYM is not needed for LISTSERV running under unix, as the usual core files will be created and backtraces can be generated from them for diagnosis by support.

LISTSERV 16.0-2017a Level Set Changes for Web Templates

Improvements

- Obsolete syntax has been replaced throughout.
- All mentions of DomainKeys have been replaced with DKIM, and a few outdated links have been updated.
- The Admin Dashboard can now compare LISTSERV and WA build dates when checking for latest version. This will help insure compatibility between your installed versions of LISTSERV and WA.
- Archive search has been improved.
- More accurate error messages are displayed when no archives exist, or when a list is private.

Fixes

- Input field content is now encoded with &+HTMLENCODE(); as a security measure.
- Changelog settings no longer include the unsupported DAILY option.

Important: F-Secure Anti-Virus Support

LISTSERV Classic and LISTSERV Classic HPO sites running F-Secure Anti-Virus or F-Secure Linux Security should note carefully the following:

F-Secure Server Security 11.x/12.x and Linux Server Security 10.x/11.x Support

These versions of F-Secure's products are certified for use with LISTSERV 16.0-2014b and following. However, **L-Soft STRONGLY RECOMMENDS that these products be used only with LISTSERV 16.0-2017a and following.** This is due to backward-incompatible changes introduced in the 11.x versions of the F-Secure products. The incompatibility may result in occasional spurious reports from LISTSERV of out-of-date anti-virus signatures. *We have taken account of this incompatibility in LISTSERV version 16.0-2017a.* To ensure that you have at least LISTSERV version 16.0-2017a, issue a SHOW LICENSE to your LISTSERV server. The build date reported should be 28 Feb 2017 or later.

Integration documentation and information about where to download F-Secure installers and hotfixes can be found at http://www.lsoft.com/resources/manuals-download.asp?id=301&format=PDF .

Applying LISTSERV 16.0-2017a

IMPORTANT: Install (or ensure that it is installed) your LISTSERV 16.0 product LAK before upgrading! A valid product LAK (License Activation Key) with "REL=16.0" must be installed before upgrading or LISTSERV will not start after the upgrade. Also, **a valid maintenance LAK expiring no earlier than 28 Feb 2017 is required** in order to apply this level set release.

If you have not received a LISTSERV 16.0 product LAK, please contact your sales representative or SALES@LSOFT.COM before upgrading!

To find out if you can upgrade to LISTSERV 16.0 with your current license key, please issue a SHOW LICENSE command to LISTSERV and examine the response. It will be similar to this:

```
License type:        Permanent
Expiration date:     None - perpetual license
Maintenance until:   26 May 2017, serial number MNT-XYZ-1
Capacity:            Unlimited
Version:             16.0
Serial number:       XYZ-1
Build date:          28 Feb 2017
```

Your license key will be valid for the 16.0 upgrade if your current product LAK is for version 16.0 or higher, and your maintenance LAK is valid until at least 28 Feb 2017.

Sites running LISTSERV 14.4 or later may use the LAK input tool in the Web Administration interface to apply and check their new LAK before upgrading.

The installation kits found on L-Soft's web site can be used either to install a new copy of LISTSERV or to upgrade an existing installation. To download LISTSERV 16.0-2017a, simply go to L-Soft's Web site and

download an evaluation copy of LISTSERV or LISTSERV Lite, then follow the installation instructions for your operating system. The kits can be found at:

http://www.lsoft.com/download/listserv.asp

http://www.lsoft.com/download/listservlite.asp

Current Supported Operating Systems

LISTSERV for Microsoft Windows	Windows 7 (64-bit only)
	Windows 8.x (64-bit only)
	Windows 10 (64-bit only)
	Windows Server 2008 R2
	Windows Server 2012
	Windows Server 2012 R2
	Windows Server 2016
LISTSERV for Unix	AIX 4.3 (PowerPC) and later
	Linux 2.6 and later (64-bit)
	Linux 2.6 and later (RH6 64-bit)
	Linux 2.4.2 or later (S/390)
	Solaris 10 and later (SPARC)
	Solaris 10 and later (x64)
LISTSERV for MacOS	MacOS X (x86)
LISTSERV for VM/ESA, z/VM	(LISTSERV 15.5 only)

Support for 32-bit Windows and Linux has been withdrawn as of the release of LISTSERV 16.0-2017a.

Please note that support has also been withdrawn for OpenVMS as of this level set release.

SPECIAL NOTES

1. This document does not include upgrade instructions. Please see the installation guide specific to your OS platform for upgrade instructions. Installation guides are available at http://www.lsoft.com/resources/manuals.asp#2 .

2. LISTSERV version 16.0-2017a is available only for operating systems currently supported by L-Soft. L-Soft no longer has development systems for unsupported operating systems and is not in a position to compile LISTSERV 16.0-2017a for those systems.

end of file