TIBCO Enterprise Message Service™ Appliance Release Notes

Software Release 3.1.0
December 2019

Important Information

THIS SOFTWARE MAY BE AVAILABLE ON MULTIPLE OPERATING SYSTEMS. HOWEVER, NOT ALL OPERATING SYSTEM PLATFORMS FOR A SPECIFIC SOFTWARE VERSION ARE RELEASED AT THE SAME TIME. SEE THE README FILE FOR THE AVAILABILITY OF THIS SOFTWARE VERSION ON A SPECIFIC OPERATING SYSTEM PLATFORM.

THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. TIBCO SOFTWARE INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.

THE CONTENTS OF THIS DOCUMENT MAY BE MODIFIED AND/OR QUALIFIED, DIRECTLY OR INDIRECTLY, BY OTHER DOCUMENTATION WHICH ACCOMPANIES THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY RELEASE NOTES AND "READ ME" FILES.

The following information is for FCC compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radiofrequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without Pluribus Networks' written authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Pluribus Networks equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.

- Move the equipment to one side or the other of the television or radio.

- Move the equipment farther away from the television or radio.

- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Pluribus Networks, Inc. could void the FCC approval and negate your authority to operate the product.

Contents

TIBCO Documentation and Support Services 5

New Features 7

Release 3.1.0 7

Release 3.0.3 7

Release 3.0.2 7

Release 3.0.1 7

Changes in Functionality 8

Release 3.1.0 8

Release 3.0.3 8

Release 3.0.2 8

Release 3.0.1 8

Deprecated and Removed Features 9

Deprecated Features 9

Removed Features 9

Migration and Compatibility 10

upgrade-software Command 10

Refreshing Servers in Central Administration 11

Upgrading Disaster Recovery Configurations 11

Reviewing Uplink Port Configuration 11

Closed Issues 12

Known Issues 16

TIBCO Documentation and Support Services

TIBCO is proud to announce the latest release of TIBCO Enterprise Message Service ™ Appliance software. This release is the latest in a long history of TIBCO products that leverage the power of the Information Bus® technology to enable truly event-driven IT environments. To find out more about how TIBCO Enterprise Message Service Appliance software and other TIBCO products are powered by TIB® technology, visit us at www.tibco.com.

How to Access TIBCO Documentation

Documentation for TIBCO products is available on the TIBCO Product Documentation website, mainly in HTML and PDF formats.

The TIBCO Product Documentation website is updated frequently and is more current than any other documentation included with the product. To access the latest documentation, visit https://docs.tibco.com.

TIBCO Enterprise Message Service Appliance Documentation

The following documents for this product can be found on the TIBCO Documentation site:

- *TIBCO Enterprise Message Service Appliance Installation and Reference*
- *TIBCO Enterprise Message Service Appliance Release Notes*
- *Rack Mounting Your TIBCO Chassis With Included Rail Kit*

TIBCO Enterprise Message Service Documentation

The following documents form the TIBCO Enterprise Message Service documentation set:

- *TIBCO Enterprise Message Service User's Guide*
- *TIBCO Enterprise Message Service Central Administration*
- *TIBCO Enterprise Message Service Installation*
- *TIBCO Enterprise Message Service C and COBOL Reference*
- *TIBCO Enterprise Message Service Java and .NET API Reference*
- *TIBCO Enterprise Message Service Release Notes*

Other TIBCO Product Documentation

You may find it useful to read the documentation for the following TIBCO products:

- TIBCO EMS® Client for z/OS (CICS)
- TIBCO EMS® Client for z/OS (MVS)
- TIBCO EMS® Client for IBM i

Third-Party Documentation

- Java™ Message Service specification, available through http://www.oracle.com/technetwork/java/jms/index.html.
- *Java™ Message Service* by Richard Monson-Haefel and David A. Chappell, O'Reilly and Associates, Sebastopol, California, 2001.

How to Contact TIBCO Support

You can contact TIBCO Support in the following ways:

- For an overview of TIBCO Support, visit http://www.tibco.com/services/support.
- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the TIBCO Support portal at https://support.tibco.com.
- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to https://support.tibco.com. If you do not have a user name, you can request one by clicking Register on the website.

How to Join TIBCO Community

TIBCO Community is the official channel for TIBCO customers, partners, and employee subject matter experts to share and access their collective experience. TIBCO Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from TIBCO products. In addition, users can submit and vote on feature requests from within the TIBCO Ideas Portal. For a free registration, go to https://community.tibco.com.

New Features

This section lists features added since the last major release of this product.

Release 3.1.0

The following new feature was added in version 3.1.0 of TIBCO Enterprise Message Service Appliance.

health-check-config

The optional **`health-check-config`** command can enable an EMS status port for external entities such as a load balancer, to easily check on EMS server readiness using a standard http interface.

Release 3.0.3

No new features have been added in version 3.0.3 of TIBCO Enterprise Message Service Appliance.

Release 3.0.2

No new features have been added in version 3.0.2 of TIBCO Enterprise Message Service Appliance.

Release 3.0.1

The following new features have been added in version 3.0.1 of TIBCO Enterprise Message Service Appliance.

Export a Single Log File

The **`export`** command now supports the ability to export a single log file.

A New Command to Restart the Management Zone and Export Zone Log Files

Added a new diagnostics command to either reboot the management zone or export the management zone log files.

The `zone-admin restart` can be used to restart management zones without hindering EMS server traffic.

The `zone-admin get-logs` command can be used to export zone log files.

Changes in Functionality

This section lists the changes in functionality in this release of the product.

Release 3.1.0

No change in functionality.

Release 3.0.3

No change in functionality.

Release 3.0.2

No change in functionality.

Release 3.0.1

The show <instance> logs Command Improved to Display File Size

With this release of the product, the **`show <instance> logs`** command prints a column with information on the size of each file. The size is in bytes and is only displayed for log files.

Deprecated and Removed Features

The following tables list any features that have been deprecated or removed for the current version of TIBCO Enterprise Message Service Appliance.

Deprecated Features

For deprecated features, if relevant, useful alternatives are listed. Any use of a deprecated feature should be discontinued because it might be removed in a future release. To avoid becoming dependent on deprecated features, ensure that you become familiar with the suggested alternative features.

Affected Component	Description	Affected Release
CLI Commands	The **`key-accept`** command is deprecated and may be removed in a future release. This command is no longer necessary. DR members automatically publish public data for other DR members to use during **`key-join`**. During **`key-join`**, DR members automatically request an update from the DR leader so they can finish the join sequence.	2.5.1

Removed Features

No features are removed in this release of TIBCO Enterprise Message Service Appliance.

Migration and Compatibility

The following are instructions on how to migrate from a previous release to version 3.1.0 of TIBCO Enterprise Message Service Appliance.

- Upgrades to EMSA 3.1.0 and later are only supported from EMSA 2.5.1 and higher. You must upgrade to EMSA 2.5.1 before upgrading to EMSA 3.1.0.
- If you are running a Disaster Recovery (DR) quad you must first upgrade the backup sites.

Upon upgrading to a newer version of the EMS appliance, we also recommend that you upgrade the Central Administration server and EMS clients to the latest version available. Upgrade and restart your EMS installations in the following order:

1. Upgrade and restart the Central Administration server.
2. Upgrade and restart all EMS appliance instances.
3. Upgrade and restart EMS clients.

Verify Existing Software Version

Before beginning your upgrade, verify the software version on the appliance:

1. On the CLI, issue the version-show command.
2. Note the version number given for the EMS appliance.

- If the version number is lower than 2.5.1, first upgrade to version 2.5.1 before proceeding with the instructions below.
- If you are upgrading from a release prior to 2.2.0, contact TIBCO Support for assistance.

upgrade-software Command

If you are migrating from release 2.5.1 and later, update the software using the **`upgrade-software`** command. See the command reference in the *TIBCO Enterprise Message Service Appliance Installation and Reference*.

Users with a multiple appliance installation, such as fault tolerant or disaster recovery configurations, must update all appliances in the installation to software release 2.5.1 or greater prior to beginning the upgrade to software release 3.1.0.

Note that, during the system startup that follows the reboot triggered by an **`upgrade-software`** command, additional upgrade tasks take place. If you log in to the CLI before all the upgrade and startup tasks have completed, the CLI displays progress information until the system is fully ready.

⚠ Software release 3.1.0 is a large upgrade package, including both TIBCO Enterprise Message Service and significant operating system upgrades. Upgrading the appliance requires between 30 minutes to 1 hour to complete and should not be interrupted. Additionally, the process can trigger multiple reboots of the appliance. Because the appliance system may be unavailable for some time, please plan accordingly. Failure to carefully follow upgrade instructions may result in complications, including the loss of data. Please contact TIBCO Support if you have any questions regarding upgrading to 3.1.0.

If additional user actions are required to complete the upgrade, these actions are also noted in the CLI. These actions can include additional reboots of the appliance. This is normal; you can log back in following the reboot to continue monitoring the upgrade progress.

When a software upgrade package is applied, the file is renamed during the upgrade process with the suffix `.aquila`. This indicates that the package has been applied. If needed, the renamed package can also be used for software upgrade; there is no need to re-upload a new package.

All additional upgrade tasks are described in this document.

Refreshing Servers in Central Administration

Refresh the EMS server instances in Central Administration after migrating the EMS appliance to the current release, and before making any configuration change or deployment.

Upgrading Disaster Recovery Configurations

When migrating the EMS appliances in a disaster recovery quad to the most recent release, you must upgrade all four appliances before issuing the **`dr-config`**, **`dr-recover`**, or **`dr-restore`** commands to change the active site. If the quad is only partially upgraded, these commands will not work as expected. Contact TIBCO Support if it is necessary to do a recover or restore on a partially upgraded quad.

For best results, follow this sequence:

1. Upgrade the software on each appliance at the backup site, as described in the reference for the **`upgrade-software`** command.
2. From the CLI of each appliance at the backup site, disable EMS services: **`services all disable perm`**.
3. Upgrade the software on the appliances at the production site.

Reviewing Uplink Port Configuration

When you upgrade from an earlier release to software release 2.5.1, the port uplink configuration is reset to enable a single port when the appliance restarts. That is, when the appliance boots after the upgrade, only port 41 is enabled. After the upgrade, verify that the LACP trunk is functioning normally before changing the default behavior.

If you have performed this step after upgrading to 2.5.1, you do not need to repeat these steps after upgrading to software release 3.1.0.

Issue the command **`port-show uplink`** to review the status of the appliance ports. The output is similar to the following:

```
===== PORT-SHOW =====
port ip mac vlan  hostname   status                nnnconfig   trunk
---- --- --- ---- --------   ---------------------- -------- ---------
30 ... ... EMSAPP9 up,PN-switch,PN-other,LLDP,trunk,vlan-up  ... crosslink
31 ... ... EMSAPP9 up,PN-switch,PN-other,LLDP,trunk,vlan-up  ... crosslink
32 ... ... EMSAPP9 up,PN-switch,PN-other,LLDP,trunk,vlan-up  ... crosslink
41 ... ... 441     up,host,LACP-fallback,vlan-up             ...
41 ... ...         up,host
            . . . More hosts . . .
42                  disabled,trunk                           ... uplink
65 ... ... 1 EMSAPP8 up,PN-internal,stp-edge-port,vlan-up    ...
66 ... ... 441       p,host,stp-edge-port,vlan-up            ...
```

In the above example, the note the line containing Port 41 information. The `LACP-fallback` status implies that the appliance did *not* negotiate a successful LACP trunk with the network switch. In this case, it is not safe to enable both ports 41 and 42 until this situation is corrected.

Alternatively, if the port 41 status was instead `LACP-PDUs`, then the appliance did successfully establish an LACP uplink connection to the network switch.

Once you've verified that the LACP connection was successfully established, you can use the **`uplink-config`** command to change the uplink configuration to enable both ports 41 and 42 on boot.

The default uplink configuration is compatible with most networks. Should your installation require a custom uplink configuration, verify that everything else is working properly before modifying the uplink.

Closed Issues

The following are the issues closed in the listed release of TIBCO Enterprise Message Service Appliance.

Closed in Release	Key	Description
Issues Closed in Release 3.1.0		
3.1.0	EMS-7699	Fixed a defect where Central Administration would expose the **Health Check Listen** property for a server running in an EMS Appliance. On EMSA the feature is administered using the CLI command "health_check_config" and not by using the server "Health Check Listen property."
3.1.0	EMS-7160	Fixed an issue that could cause a memory leak every time a standby fault tolerant peer disconnected.
3.1.0	EMS-6748	When using fault tolerance with a pair of appliances, the order in which either EMS server in an fault tolerant pair was started could affect whether certain state replication performance optimizations were enabled. This would also affect the behavior of store compaction. This has been fixed.
3.1.0	EMS-6725	The EMS server could leak sockets when an incoming connection failed (for example, because of a network failure). Incoming connection handshakes are now subject to a timeout that is the larger of server_timeout_server_connection and server_timeout_client_connection, if either is specified. Otherwise, the timeout is handshake_timeout, if specified. If none of these are specified, the timeout on the incoming connection handshake defaults to 3 seconds.
3.1.0	EMS-6686	Previously, when EMS clients used certificates with an extended key usage extension, they were required to include the client authentication flag. Now, client certificates will be considered valid with either the client authentication flag or the server authentication flag, or both.
3.1.0	EMS-6616	The EMS server could leak sockets when an incoming connection failed (for example, because of a network failure). Incoming connection handshakes are now subject to a timeout that is the larger of server_timeout_server_connection and server_timeout_client_connection, if either is specified. Otherwise, the timeout is handshake_timeout, if specified. If none of these are specified, the timeout on the incoming connection handshake defaults to 3 seconds.
Issues Closed in Release 3.0.3		
3.0.3	EMSA-2033	Improved EMSA syslog reporting to report detected disk IO errors.

Closed in Release	Key	Description
3.0.3	EMSA-2032	Fixed an issue cause a memory leak every time a standby fault tolerant peer disconnected. where a corrupted `statelog.txt` file could prevent failover.
3.0.3	EMSA-2015	Fixed an issue that could cause a kernel panic in the IP module under heavy a workload.
3.0.3	EMSA-1992	The NTP package has been updated.
3.0.3	EMS-7160	Fixed an issue that could cause a memory leak every time a standby fault tolerant peer disconnected.
3.0.3	EMS-6748	When using fault tolerance with a pair of appliances, the order in which either EMS server in an fault tolerant pair was started could affect whether certain state replication performance optimizations were enabled. This would also affect the behavior of store compaction. This has been fixed.
Issues Closed in Release 3.0.2		
3.0.2	EMS-7425	Fixed a defect in which the separate counts for client and admin connections reported by the EMS server since release EMS 3.0.0 could be incorrect when using LDAP authentication if the LDAP server was slow.
3.0.2	EMS-7424	Reverted a storefile change introduced in release EMSA 3.0.1, due to a risk of store corruption.
3.0.2	EMS-7397	Fixed a defect in which the detection of a duplicate message sent within a transaction could cause the server to crash if `track_message_ids` was enabled. In such a situation, the server will now trace the message and roll back the corresponding transaction.
3.0.2	EMS-7379	Fixed a defect in which very large server trace statements would be missing their line break.
Issues Closed in Release 3.0.1		
3.0.1	EMSA-1888	Fixed an issue where the standby server would not start automatically when the active server became unresponsive.
3.0.1	EMSA-1881	Fixed an issue where failure to create a mgmt-zone would cause the ems-gateway to not activate on boot.
3.0.1	EMS-7358	In servers configured using a JSON file, fixed a defect in which deleting a static destination could erroneously clear permissions from other destinations.
3.0.1	EMS-7356	Fixed a defect which could stop communication between the EMS server and an LDAP server.

Closed in Release	Key	Description
3.0.1	EMS-7296	Fixed a defect in which slow operations could interfere with the heartbeat protocol between the EMS server and clients, resulting in client disconnect. This defect affected Releases 2.4.0 to 3.0.0.
3.0.1	EMS-7155	Fixed a defect in which the store files of an EMS server in standby-replicating state could grow much larger than the corresponding store files of the active-replicating server.
Issues Closed in Release 3.0.0		
3.0.0	EMSA-1835	Fixed an issue where appliance arp optimizations could intermittently interfere with uplink network performance.
3.0.0	EMSA-1828	Fixed an issue that caused the file timestamp of exported log files to be changed.
3.0.0	EMSA-1825	Fixed an issue that could cause the standby server to activate during a **dr-restore** command if the servers were not stopped before the **dr-restore** was issued.
3.0.0	EMSA-1806	Fixed an issue that could cause the EMS servers on a DR backup site to activate following an upgrade even though the production site was already active.
3.0.0	EMSA-1764	Fixed an issue where if a DR snapshot send lost its TCP connection to the backup site at the wrong time, it could cause a significant delay before the next snapshot was sent.
3.0.0	EMSA-1744	Fixed an issue that could cause the EMS Appliance health check to incorrectly report an error while checking for degraded PCI devices.
3.0.0	EMSA-1739	Fixed an issue where a misconfigured customer network switch could cause the internal uplink and crosslink trunking to become corrupted.
3.0.0	EMSA-1731	Fixed and issue that could cause the tibfile user authorization for SFTP access to be lost.
3.0.0	EMSA-1643	An EMS server instance would encounter startup problems if LDAP authorization was enabled and the LDAP server was unreachable during server startup. This has been fixed.
3.0.0	EMSA-1609	In some situations, the monitoring agent would lose LINK heartbeats. In addition to causing peer agents to temporarily lose communication with each other, this condition could also trigger an unnecessary fault tolerant failover. To correct this issue, the monitoring agent now postpones all failover decisions until "down" conditions can be confirmed.
3.0.0	EMSA-1533	Fixed an issue that could cause appliance log files to grow to over 1GB.

Closed in Release	Key	Description
3.0.0	EMS-6829	When message swapping was disabled in a fault-tolerant configuration, persistent messages that had been sent to an EMS instance before a failover could be delivered to consumers with an empty body after the failover. This has been fixed.
3.0.0	EMS-7160	Fixed an issue that could cause a memory leak every time a standby fault tolerant peer disconnected.

Known Issues

The table lists the known issues of TIBCO Enterprise Message Service Appliance.

Key	Summary/ Workaround
EMSA-2057	**Summary**: TIBCO Enterprise Message Service Appliance appliances with NVMe fast storage may report a spurious hard error on boot up. **Workaround**:This error can be safely ignored if additional errors are not reported.
EMSA-1966	**Summary**: In rare cases it is observed that the **`upgrade-software`** command can timeout before performing the software upgrade. **Workaround**: Open a new CLI window, and run the **`upgrade-software`** command again.
EMSA-1801	**Summary**: Low level system utilities may report that a zpool upgrade is required. It is NOT required and not recommended at this time. **Workaround**: None. Do not upgrade the zpool.
EMSA-1730	**Summary**: Some newer transceivers supplied by TIBCO may erroneously be reported as "unsupported" in the **`port-show`** command output, even though they are in fact supported. **Workaround**: None.
EMSA-1693	**Summary**: Following repeated issuances, the command `export` *`instance`* `logs` may fail with a memory fault error. Following the error, some exported log files may have incorrect ownership or permissions. The permissions are corrected by subsequent exports. **Workaround**: Use `log-show -f` *`instance`* `emsd.log` to monitor raw EMS server logs rather than periodic exports.
EMSA-1666	**Summary**: The appliance operating system may report status transitions between ok and n/a (unavailable) as warnings. These are only informational messages, not warnings that must be acted on. **Workaround**: None. Warnings with an `n/a` for the changes to/from value can be ignored.
EMSA-1656	**Summary**: Making multiple setup modifications that include changes to the hostname or Mgmt-IP information can cause a session disconnect if an EMS Gateway is set up during the same **`config-apply`** session. As a result of the disconnect, changes made are not fully processed. **Workaround**: There are two available workarounds: • Disable the EMS Gateway using the **`ems-gateway disable`** command before making changes. • Make and apply the Mgmt-IP (and hostname) changes and apply them before making other changes.

Key	Summary/ Workaround
EMSA-1651	**Summary**: The **`log-rotate`** command may renumber `emsd.log` log rotation files in a way that is inconsistent with the EMS server log file rotation comments. **Workaround**: After using the **`log-rotate`** command, use `export` *`instance`* `logs` to export all the log rotations so that the correct sequence for old logs may be determined.
EMSA-1638	**Summary**: Because of changes to SSL behavior introduced in version 2.5 of the TIBCO Enterprise Message Service Appliance, you should not use Central Administration 8.3 to administer the appliance if it is on version 2.4 or earlier. **Workaround**: Use Central Administration version 8.2 to administer an appliance that is on version 2.4 or below.
EMSA-1553	**Summary**: The EMS Appliance does not correctly handle the UTF-8 extended character set in server configuration files. UTF-8 extended characters are converted to their ASCII escape sequence. **Workaround**: Restrict server configurations to the legal ASCII character set.
EMSA-1375 EMSA-1374	**Summary**: If the EMS server `listen` URLs are modified in Central Administration and the default TCP `listen` URL is removed or changed to SSL, the local `call-tibemsadmin` command will no longer work, and the listen URL displayed by the info command will no longer be valid. **Workaround**: Use Central Administration to restore the expected default TCP listen URL, or use an external tibemsadmin client to connect.
EMSA-780	**Summary**: When an appliance is configured with a remote syslog collector IP address, the collector might receive unwanted `INFO` level operating system log messages. **Workaround**: Configure the syslog collector to ignore messages from the appliance that are below the `notice` priority level. In general, the syslog collector should also be configured to only collect messages on the facilities that come from the appliance, including `local5`, `daemon`, and `kernel`.

Key	Summary/ Workaround
EMSA-520	**Summary**: The Appliance offers two choices for Console I/O to the appliance: a serial port, or a keyboard and monitor connected directly to the appliance (VGA). However, by default output goes only to the serial console port once booted. You must modify the default behavior using the boot menu in order to use the VGA console port. **Workaround**: Configure the appliance as follows: 1. If it is powered on, power off the Appliance. 2. Attach the VGA Monitor and keyboard (or serial console cable, if desired) to the console port on the back of the appliance. 3. Power on the appliance. 4. Press the space bar when the boot menu displays. This pauses the boot, and allows time to pick a display option. 5. Use the arrow keys to select the desired console connection. Select **Monitor** to enable the VGA port, or Serial to select the default console port. 6. Press **Enter** to commence booting with selected option.
EMS-6501	**Summary**: Upon issuing the forcestart or forcestart-instance CLI commands, you may see the following type of warning in the corresponding EMS server log file: `WARNING: [admin@hostname]: create sender failed: invalid temporary queue [$TMP$.instx.xxx.n].` **Workaround**: This is harmless. You can safely ignore this warning.