TIBCO LogLogic® Log Management Intelligence

TIBCO LogLogic® Enterprise Virtual Appliance

TIBCO LogLogic® Enterprise Virtual Appliance - Container Edition

Configuration and Upgrade

Version 6.4.0
February 2022

Contents

Appliance Software Configuration

This section applies only to the TIBCO LogLogic® Log Management Intelligence appliance.

For instructions to set up TIBCO LogLogic® Enterprise Virtual Appliance, see *TIBCO LogLogic® Enterprise Virtual Appliance Quick Start*.

Setting up a new appliance

After you install the new TIBCO LogLogic® appliance in its rack and power it up, set up the appliance by using the GUI via a web browser, or by using the CLI via a console connection. For more information, see:

- Setting Up the Appliance by Using a Browser
- Setting up the Appliance by Using the Console

Upgrading an existing appliance

To upgrade an existing appliance, see Appliance Software Upgrade.

Specific configuration

After the appliance is running, you configure it for your specific needs. For more information, see:

- *TIBCO LogLogic® Log Management Intelligence User Guide*
- *TIBCO LogLogic® Log Management Intelligence Administration*

Reimaging an appliance

LogLogic LMI H4R1, H4R2, and H5 appliances come with an embedded SD card that contains an image of the appliance software. This feature facilitates reimaging the appliance in case of critical hardware or software failure. For instructions on how to use the backup image for recovery, contact TIBCO support through the online support portal at: TIBCO Support website or through email: support@tibco.com.

Note: By default on H4R1, H4R2, and H5 appliances, the labeled iDRAC network interface has an assigned default static address of `192.168.0.120`. By connecting the iDRAC network interface to a network infrastructure, the iDRAC web interface becomes available via HTTPS (`https://[<IPv6Address>]`) as well as via telnet and SSH to the same default IP.

Setting Up the Appliance by Using a Browser

You must follow a series of steps to set up a TIBCO LogLogic® appliance by using a browser.

1. Connecting the Appliance to a Network
2. Logging in to the Appliance
3. Configuring Network Settings
4. Setting the Time Zone and Time

Connecting the Appliance to a Network

Connect the appliance to a network where you can access a 10.0.0.x network address by using a class “C” subnet mask (255.255.255.0).

Note: The default IP address of the appliance is 10.0.0.11, which is assigned to the Eth0 port.

Logging in to the Appliance

Procedure

1. Open a browser on your workstation, and connect to the appliance by entering `https://10.0.0.11` in the browser address bar.
2. To accept the certificate, click **YES**.

3. On the login page, enter the default user name (admin) and password (admin).

   The End User License Agreement (EULA) is displayed.

4. Accept the EULA. You are prompted to change the password by entering the following information:
   - The current password
   - A new password, which must be at least six characters long and contain at least one number
   - The new password again for confirmation

   After changing the password, the login page is displayed.

Result

After logging in, a warning message might be displayed indicating that the time on the appliance is not set or synchronized. You can ignore this warning. For more information, see Setting the Time Zone and Time.

What to do next

It is good practice to also create a secondary administrative account. You can do this now or later.

- To customize the GUI theme, see the Theme section in *TIBCO LogLogic® Log Management Intelligence Administration*.
- To add more user accounts, see the Managing Users section in the *TIBCO LogLogic® Log Management Intelligence Administration*.
- To change the admin password later, see the User Preferences section in the *TIBCO LogLogic® Log Management Intelligence User Guide*.

Configuring Network Settings

For more information about network settings, see the Network Settings section in *TIBCO LogLogic® Log Management Intelligence Administration*.

Procedure

1. Go to **Administration > Network Settings**.
2. Type in the appropriate network information, and then click **Save**.

Setting the Time Zone and Time

From the **Administration > System Setting > Time** tab, you can modify the time for the appliance or configure a Network Time Protocol (NTP) server.

Note: This section is not applicable to LogLogic® EVA - Container Edition.

If you do not set the correct time for your appliance, the system does not function correctly.

When changing the system time of your appliance, ensure that the validity period of the certificates imported into the appliance matches the new system time.

Procedure

1. Go to **Administration > System Settings > Time**.
2. From the **Time Zone** list, select a time zone for your network.
3. To enable synchronizing your local time, select the **Update Time** check box. Then select how to update the appliance time in one of the following ways:
   - (Recommended) To synchronize your local time with that of an NTP server, select **NTP Server** and enter a host name or IP address for the NTP server.
     - If you have multiple appliances connected together, you must set up a common external NTP server for all appliances to ensure that the time on all appliances is synchronized. Ideally, this is the same NTP server used by the entire data center.
     - If you do not have access to a common external NTP server, you can use the appliance running as a Management Station as the common NTP server. The time settings of all appliances must be in sync.
     - It is important to have an NTP server set up for a single appliance, too.
   - To manually define the system time, select **Specify Time** and enter the system time (MMDDhhmmYY.ss).

     Note: When configuring LogLogic EVA on cloud platforms, a static time configuration is not supported. Use the **NTP Server** option instead.
4. To save your changes, click **Update**.

The appliance prompts you that an immediate reboot is required.

5. To let the appliance reboot for changes to take effect, click **OK**.

Setting up the Appliance by Using the Console

To set up a LogLogic appliance by using the console, you need the NULL modem cable shipped with the appliance, and compatible terminal software.

Note: For more information about CLI commands, see the Command Line Interface (CLI) section in *TIBCO LogLogic® Log Management Intelligence Administration* or type `help` at the command prompt.

Procedure

1. By using a laptop or other terminal device, connect the NULL modem cable to the serial port (**COM1**) located at the back of the appliance.
2. Open your terminal software. Use the following communication settings:

   `9600 baud, Null, 8 bit, 1 parity`
3. In the terminal program, log in as user `root` with password logapp.

   If you are setting up the appliance for the first time, set up the root-level accounts. See Setting up root-level accounts. Otherwise, continue on to step 4.
4. Configure the network settings:
   a. Set the appliance IP address and interface network settings:

   ```
   > set ip <ip address> <netmask> <gateway> <ifdev>
   ```

   If you are bonding two interfaces together, use *interface-name* to indicate `bond0` or `bond1`. For example:

   ```
   > set ip 10.9.3.250 255.255.255.0 10.9.3.1 eth0
   ```

   b. Set the DNS server IP address:

```
> set dns <ip address>
```

Example:

```
> set dns 10.1.1.5
```

Networking is restarted after this command.

5. Set the local time zone.

```
> set timezone <Enter>
```

From the displayed menu, select the time zone where this appliance is located.

6. Verify your settings:

```
> show changes
```

7. Save your changes:

```
> save
```

This updates the necessary files so that the network setting changes are permanent.

> ⚠ **Warning:** New settings do not go into effect until the appliance is restarted.

8. Select the network interface defaultgw.
9. Select the IP address to use to generate the Blue Coat certificate:

```
> 0
```

This generates the Blue Coat certificate for the interface configured above.

> **Note:** It is not necessary to select an interface for a Blue Coat certificate if you do not have any Blue Coat ProxySG devices in your network, or if you do have Blue Coat ProxySG devices but you do not use LogLogic LMI to collect the logs from those devices.

10. Verify the network settings by running the following command:

```
> show current
```

11. (Highly recommended) Set up an NTP server by using the IP address or DNS name of the NTP server:

```
> set ntpserver <ip address>
```

12. Type `exit` to exit the procedure.
13. When prompted whether to reboot the appliance, type `yes`.

> **Warning:**
> - Wait for a few minutes for the appliance to cease operation and then reboot the appliance.
> - When powering down the appliance it is important to follow any of the proper shutdown procedures:
>   - The system halt command
>   - The standard Linux shutdown procedure
>   - Reboot commands
>
> Failure to comply could cause a corrupted file system, loss of data, or a failure to boot the appliance.

Setting up root-level accounts

LogLogic® LMI requires at least two root-level accounts at the OS level (`root` and `toor`), and each has its own shell.

- The `root` account has a custom LogLogic LMI shell.

- The `toor` account is privileged (uid=0) and uses a standard Linux Bash shell for all general maintenance tasks and to access the appliance for troubleshooting. The `toor` account is disabled until you log in as `root`, and then set a password for `root` and `toor` accounts.

Procedure

1. Log in as the root user with password logapp.
2. When prompted to enter a new root password, re-enter the same password at the confirmation prompt.

   It is recommended to choose a suitable password based on the standard guidelines for strong password security, although the system accepts weak passwords.
3. When prompted, enter a new toor password, and then confirm your password.

   > **Warning:** Ensure that you make a note of your `root` and `toor` passwords and store them in a safe location. Lost passwords cannot be recovered.

Result

At this point the `toor` account becomes available.

Theme for Rebranding LogLogic LMI

From the **Administration > System Settings > General tab > Theme** section, you can configure the background colors of the header bars and font color of the header text.

Changing the theme includes setting the following colors on the GUI:

Field	Default value (hex)	Description
Primary Header Color	#0080cb	Color of the title bar
Secondary Header Color	#3498db	Color of the breadcrumb bar

Field	Default value (hex)	Description
Font Header Color	#aaeaff	Font color of the menu items and the text in the breadcrumb bar **Note:** The color of menu items changes only when you hover over the menu item.

You can change the theme immediately after upgrading or at any other time. Perform the following steps:

1. Select the color from the color palette or type the hexadecimal value of the color.
2. For the changes to take effect, either refresh the page, or log out and log in again.

Appliance Software Upgrade

You can upgrade directly from version 6.3.0 or 6.3.1 to version 6.4.0. This section is applicable to all editions - LogLogic LMI, LogLogic® EVA, and LogLogic® EVA - Container Edition.

For upgrade path and compatibility matrix, see TIBCO LogLogic® Log Management Intelligence Release Notes.

You can upgrade the appliance software in the following methods:

- Standard Upgrade
- Remote Upgrade

Upgrading the appliance software involves the following tasks:

Standard Upgrade	Remote Upgrade
1. Upgrade Considerations 2. Preparing to Upgrade the Appliance 3. Depending on the type of setup to upgrade, see the appropriate section: • Upgrading a Standalone Appliance • Upgrading in a High Availability Environment • Upgrading in an AWS Environment 4. Running the Postupgrade Script	1. Upgrade Considerations 2. Preparing to Upgrade the Appliance 3. Remote Upgrade

Upgrade Considerations

Read these considerations before you start the upgrade process. These considerations are applicable to both standalone and High Availability (HA) environments.

- After upgrading, if you try to access the appliance from the Mozilla Firefox browser, the `Secure Connection Failed` error message might be displayed. See the Mozilla Firefox support site for tips on troubleshooting security error codes.
- In case of a Management Station cluster or a High Availability cluster, ensure that all appliances have the same LogLogic LMI and LogLogic LSP versions (the hot fix versions need not match). For more information about HA upgrade, see *TIBCO LogLogic® Log Management Intelligence Administration*.
- If the LogLogic LMI appliance uses LogLogic TCP as the message routing protocol, ensure that the source and destination appliances have the same LogLogic LMI version, for best compatibility.
- To properly forward Check Point data, you must update both your sender and receiver LogLogic LMI appliances to the same LogLogic LMI version.
- Even if you disable the **SSH Daemon at Startup** option before upgrading to version 6.3.0 or later, the SSH daemon runs at startup after the upgrade is completed, although the option is displayed as disabled on the **Administration > System Settings > General** tab. You must disable the option again after the upgrade.

Advanced Feature Artifacts

In versions 6.3.x, groups were available only in the Advanced Dashboards. In other Advanced Features (Bloks, Data Models, Aggregation Rules, and Enrichment Lists), the corresponding artifacts were displayed on the main page of the feature.

After upgrading to LogLogic LMI 6.4.0, the artifacts from versions 6.3.x are stored in different groups, depending on whether the artifacts are built-in or how they are related to LogLogic LSP.

The main pages in version 6.3.x are now named with 'All'. For example, All Dashboards, All Bloks, and so on. For more information about types of groups and managing groups, see Groups in *TIBCO LogLogic® Log Management Intelligence User Guide*.

Artifact	Before version 6.4.0	In version 6.4.0
Any user-created artifacts	On the main page. No groups.	User group

Artifact	Before version 6.4.0	In version 6.4.0
Any system-created artifacts	On the main page. No groups.	System group
LogLogic LSP data models	On the Data Models page. No groups.	• LSP > <*dataModelName*> group or • LSP > <*deviceManufacturerName*> group For example: • The LSP > Cisco group contains all Cisco data models • The LSP > Blue_Coat_Syslog group contains only the Blue_Coat_Syslog data model
LogLogic LSP aggregation rules	On the main Rules page. No groups.	• LSP > <*dataModelName*> group or • LSP > <*deviceManufacturerName*> group
LogLogic LSP dashboards	All Dashboards, System, User, LSP groups - as applicable	All Dashboards, System, User groups: as before Dashboards of LSP group: • LSP > <*dataModelName*> group or • LSP > <*deviceManufacturerName*> group
LogLogic LSP	On the main	• LSP > <*dataModelName*> group

Artifact	Before version 6.4.0	In version 6.4.0
enrichment lists	Enrichment Lists page. No groups.	or • LSP > *<deviceManufacturerName>* group
Compliance Suite aggregation rules and filter Bloks	Not applicable	• ComplianceSuite > *<dataModelName>* group or • ComplianceSuite > *<deviceManufacturerName>* group
Compliance Suite dashboards	ComplianceSuite group	ComplianceSuite > GDPR group

Preparing to Upgrade the Appliance

Before starting the upgrade process, ensure that you have met the following requirements. These requirements are applicable to both standalone and High Availability (HA) environments.

Note: In an HA environment, perform the checks on each appliance.

- Fulfill software and hardware requirements
- Verify disk space requirements
- Back up the appliance data
- Apply Hotfixes
- Configure Parameters
- Disable the file system checks
- Download and extract the upgrade package

- Extract and run the health check script

Fulfill software and hardware requirements

Ensure that you fulfill the following requirements:

- Software download access to the TIBCO eDelivery website or TIBCO Support website.

  If you do not have access, register at TIBCO Support website or contact Technical Support by email.

- Check which TIBCO LogLogic® Log Source Packages versions are compatible with LogLogic LMI. If your appliance is using an earlier version of LogLogic® LSP, you must first upgrade to one of the supported LogLogic LSP versions of the LogLogic LMI release to which you want to upgrade. See "LogLogic LMI-LogLogic LSP Upgrade Matrix" in TIBCO LogLogic® Log Management IntelligenceRelease Notes.

  The LogLogic LSP documentation is available on the TIBCO eDelivery website or TIBCO Support website after logging in.

- A null modem cable (if connecting to the appliance by using a console)

Verify disk space requirements

Verify that the appliance has sufficient disk space available for the upgrade:

1. Log in to the appliance via SSH and run the following command:

   ```
   df -h
   ```

2. In the **Available** column, the disk space required for the partitions must be as follows:

Partition	Upgrade path	Disk space
/	All	100 MB

Partition	Upgrade path	Disk space
`/loglogic`	From LogLogic LMI and LogLogic EVA version 6.3.0 or 6.3.1 to 6.4.0	4 GB

3. Ensure that the maximum used space of the `/loglogic` directory, excluding the `/loglogic/data` and `/loglogic/update` subdirectories, is up to 9 GB. Run the following command::

```
$du -sh --exclude=/loglogic/data --exclude=/loglogic/update
/loglogic
```

Back up the appliance data

It is strongly recommended that you back up your data on the appliance before performing an upgrade.

Just after a software upgrade, you must wait at least one day to back up the appliance data, otherwise the backed up log data is inconsistent with the platform software.

For more information, see the Backup and Restore section in *TIBCO LogLogic® Log Management Intelligence Administration*.

Apply Hotfixes

Apply the appropriate hotfixes.
For more information about a hotfix, see the corresponding hotfix Readme file.

Upgrade path	Hotfix to be applied
From version 6.3.0 to 6.4.0	• LogLogic LMI 6.3.0 HF-1 • LogLogic LMI 6.3.0 HF-2
From version 6.3.1 to 6.4.0	None

Configure parameters

Before upgrading, configure the following parameters as applicable:

- CPU and memory configuration
- Active Directory
- Data vault

CPU and memory configuration

Before upgrading to LogLogic LMI 6.1.0 or later, the CPU and memory of TIBCO LogLogic® Enterprise Virtual Appliance must be changed to match the minimum hardware requirements of LogLogic LMI. For more information, see Minimum Hardware Requirements in *TIBCO LogLogic® Enterprise Virtual Appliance Quick Start*.

Active Directory

If you are setting up Active Directory (AD), after adding the certificate to the truststore, in the `/loglogic/tomcat/bin/setenv.sh` file, disable endpoint verification by setting the JAVA option:

```
JAVA_OPTS="$JAVA_OPTS -
Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true"
```

Note: If a different value of `JAVA_OPTS` is already configured in the file, add this line in the file after the existing line. You must restart Tomcat for the settings to take effect.

Data vault

If you are upgrading from 6.3.0 and if the data vault feature is enabled, you must enable the automatic unlocking of the data vault by running the following command:

```
system data_vault enable_auto_unlock
```

Disable file system checks

Disable file system checks by performing the following steps:

1. Before starting the upgrade process, run the CLI command `> system fsck disable` to prevent running a file system check during upgrade.
2. After the upgrade process is complete, run the CLI command `> system fsck enable` to reenable the check if needed.

For more information about the `system fsck` command, see the system Command section in *TIBCO LogLogic® Log Management Intelligence Administration*.

Download and extract the upgrade package

Log in to the TIBCO eDelivery website or TIBCO Support website and download the latest software update that you want to apply to the appliance.

1. Download the update package (in `.tar` format), `TIB_loglmi_<version>_fileupgrade.tar`

   The package contains the following files. The `bz2` and `bz2.sig` files are required to perform the file update process.

File name	Description
`bz2`	The update file
`bz2.sig`	The signature file for the upgrade file
`healthcheck.tar.gz`	The health check utility tool

2. Connect to the appliance from the shell login as the `toor` user and the password that was created during Setting up the Appliance by Using the Console. Use the command line through the serial port with a null modem cable or by using SSH. It is recommended to use the serial port; by using SSH, the connection is lost after the final reboot but only temporarily.
3. Extract all files into the destination directory (`/loglogic/update`) on the appliance by running the following command:

```
$ tar xf <filepath_update_package> -C /loglogic/update
```

4. Clean up the directories by running the following command:

```
$ rm -f <filepath_update_package>
```

Extract and run the health check script

The health check package includes the following files:

- `TIB_loglmi_<version>_healthcheck.tar.gz`
- `healthcheck.sh`

1. Extract the health check package contents by running the following command:

   ```
   $ tar zxvf <filepath_healthcheck_package> -C /loglogic/update
   ```

   where: `<filepath_healthcheck_package>` is the file path. For example:

   ```
   /loglogic/update/healthcheck/healthcheck.tar.gz
   ```

2. (Only for TIBCO LogLogic® LX1025R1 Appliance) Run the following command to bypass the swap file check:

   ```
   $ touch /loglogic/update/flag_skip_for_LX1025R1
   ```

3. Run the health check script:

   ```
   $ /loglogic/update/healthcheck/healthcheck.sh
   ```

Warning: Do not install the health check package under the `/loglogic/tmp` folder.

Health Check - Failure Scenarios

Scenarios when the health check script might fail and the workaround in each scenario are as follows:

Items checked	Failure scenario
`/` and `/loglogic` partitions	The script checks the minimum disk space available on the appliance, otherwise the upgrade might fail. See Verify disk space requirements. If the disk space is lesser, the error message `check FAILED` is displayed. For example: `/ free 100 MB check FAILED` If you need help to reduce disk space usage, contact TIBCO Support.
RAID health	The script checks if the RAID status is optimal. The script fails if the disks are bad or missing, and the upgrade process fails. In case of failure, contact TIBCO Support. **Note:** Applicable only to hardware models
Platform model	The script checks to ensure that the system product name and platform model from `/etc/platform` matches the output from the `dmidecode` command. The script also checks if the appliance model is supported in the current release. In case of failure, contact TIBCO Support. **Note:** Applicable only to hardware models
Resource requirements	**For LogLogic EVA:** The script verifies the minimum CPU frequency, number of cores, and minimum memory requirements. See the Minimum Hardware Requirements section in *TIBCO LogLogic® Enterprise Virtual Appliance Quick Start*. **For hardware appliances:** The script verifies the memory requirement when Advanced Features are enabled. A warning is displayed if the minimum memory requirement of 32 GB is not satisfied. **Note:** 64 GB if you are using Advanced Features; 128 GB in a heavy production deployment
LogLogic LMI	The script verifies that the correct hotfix version is installed.

Items checked	Failure scenario
hotfix version	

Database schema	If the health check script finds any database schema inconsistencies, the console displays the message:
	`Ignore the inconsistency?[yes/no]:`
	Type **no** to stop the process and go back and fix the issue before you proceed. You can run the health check command multiple times until you fix all inconsistencies. If you type **yes**, all inconsistencies are ignored and you can proceed. It is good practice to contact TIBCO Support for advice about whether it is safe to ignore the inconsistencies.
	If the health check fails with the error:
	`Schema consistency checking failed`
	go through the schema log files, and if required, run the following commands in MySQL as a workaround:
	`use logappconfig`
	`alter table oddsfieldtags drop FOREIGN KEY oddsfieldtags_ibfk_1;`
	`alter table oddsfieldtags drop index msgPatternId;`
	`alter table oddsfieldtags add index oddsfieldtags_ibfk_1 (msgPatternId);`
	`alter table oddsfieldtags add constraint oddsfieldtags_ibfk_1 FOREIGN KEY (msgPatternId) REFERENCES oddsmessagepattern(uuid) ON DELETE CASCADE;`
	If you applied these specific schema changes in the past, there is no need to do them again. Contact TIBCO Support for assistance and provide the following log file:`/loglogic/tmp/_schemaChecking/schemaChecking.log`

Report data	The following message might be displayed to warn you about unconverted report data from the previous upgrade process: `There is report data on the system that was not converted after the last upgrade. Do you want to convert this data`

Items checked	Failure scenario
	`now? [yes/no]:` • Type **yes** to exit the health check command at this point and run the `rundbm` command to complete the postupgrade process from the previous upgrade. • Type **no** to ignore this warning and proceed. The data left over from the last upgrade is deleted, the current upgrade causes a new set of data to be created. The new set of data needs to be converted. **Caution:** After choosing **no**, you cannot go back later to run the `rundbm` command for the same data.

Data vault	The health check might fail and the following error might be displayed:
	
	`Data Vault is turned on but auto-unlock is not enabled.`
	
	If this error occurs, enable the automatic unlocking of the data vault by running the following command:
	
	`system data_vault enable_auto_unlock`

Advanced Features	The health check might fail and the following warning might be displayed: `WARNING: Advanced Features may not perform correctly with the current memory configuration on LMI 6.2.0 and above! Do you want to continue upgrade? [yes/no]` This is because Advanced Features is enabled on the appliance but the configured memory is less than 64 GB. If this occurs, type yes to continue, or disable the Advanced Features, or configure more memory on the appliance. **Note:** Minimum requirement in a heavy production deployment: 128 GB
High availability	The health check might fail if the Advanced Features option is already enabled and in any of the following situations:

Items checked	Failure scenario
	• The appliance is in an HA environment when upgrading • The appliance was in an HA environment and you disabled HA before upgrading The following message is displayed: `Please turn off Advanced Features before proceeding with the upgrade.` If this error message is displayed, disable Advanced Features and run the health check script again. **Note:** Applicable only when Advanced Features is enabled.

What to do next

After the health check is successful, the appliance is ready for an upgrade. See the relevant section:

- Upgrading a Standalone Appliance
- Upgrading in a High Availability Environment
- Upgrading in an AWS Environment

Standard Upgrade

The standard upgrade procedure is performed directly on the LogLogic LMI appliance. Depending on the type of setup to upgrade, see the appropriate section:

- Upgrading a Standalone Appliance
- Upgrading in a High Availability Environment
- Upgrading in an AWS Environment

Upgrading a Standalone Appliance

This section describes the procedure to upgrade a standalone appliance.

For upgrading appliances in high availability setup, see Upgrading in a High Availability Environment.

Before you begin

Ensure that you have:

- Read Upgrade Considerations
- Performed all tasks mentioned in Preparing to Upgrade the Appliance

To upgrade from the GUI

1. Log in to the appliance GUI. You must log in as a user with administrator privileges.
2. Click **Administration > File Update**.

   The **File Update** page is displayed.
3. From the **Select File** list, select the appropriate software update, for example, `update-<timestamp>-full.tar.bz2`.

   If you do not see any files in the list, verify that the update files are added to the `/loglogic/update` directory.
4. Click **Update**.

   You might need to wait about 30 - 40 minutes for the update to complete. You can watch the progress on the **File Update** page.
5. (Optional) To update the SSL signature algorithm to `sha2`, run the script:

   ```
   /loglogic/tomcat/conf/cert_utils/certgen.sh
   ```

Result

A message displayed on the webpage informs you that the update is in progress. When the process completes, you are redirected to the login page. The new software release number is displayed at the bottom of the login page and after logging in, on the top right corner of the GUI.

What to do next

After upgrading the appliance, perform the following tasks:

- (Only for TIBCO LogLogic® LX1025 Appliance) Enable the swap file by performing the following steps:
  1. Log in to the appliance through SSH as `toor` user.
  2. Run the following command:

     ```
     $ /loglogic/scripts/enable_12g_swap_file.sh
     ```
- Run the post upgrade script on the appliance. See Running the Postupgrade Script.

Upgrading in a High Availability Environment

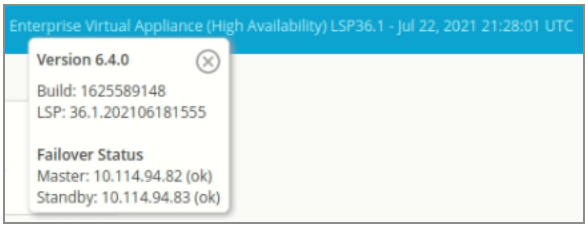
This section describes the procedure to upgrade appliances in high availability setup.

- For upgrading a standalone appliance, see Upgrading a Standalone Appliance.
- For detailed information about HA, see Failover *TIBCO LogLogic® Log Management Intelligence Administration*.

Before you begin

The following prerequisites must be met before starting the upgrade process on your HA appliances.

- Both HA appliances must have the same hardware model and software version.
- Ensure that you have read Upgrade Considerations and have performed all tasks mentioned in Preparing to Upgrade the Appliance on each appliance.
- Ensure that your HA environment is synchronized, by viewing the cluster status on the build details on the top navigation bar. Ensure that there are no warning messages.



- If currently enabled in your HA environment, disable the following features on the active appliance:
    - Archiving:

      Note down all the archive configuration settings to help you when you reenable the archiving feature.
    - Advanced Features:

      Must be disabled from the CLI. Disabling Advanced Features automatically disables the Monthly Index, Advanced Aggregation, and Monitoring Console features.

This HA upgrade procedure uses the following example appliance information:

Appliance	Appliance type	IP address
Appliance A	HA active	19.0.2.44
Appliance B	HA standby	19.0.2.45
Public	HA public	19.0.2.46
	Network mask	255.255.255.0
	Network broadcast	19.0.2.255

Important Considerations

The process of upgrading an HA pair involves disabling HA on the standby appliance (appliance B) and then on the active appliance (appliance A). After upgrading the appliance software on each appliance, you enable HA on appliance B and then on appliance A. Thus, after upgrade, the active and standby appliances are interchanged.

- Forcing failovers for the purpose of keeping one particular appliance “active” is not recommended, because it has no particular benefit and any failover event causes some loss of data - even if for a few seconds. To force a failover, you must wait until the postupgrade process is complete.
- The log data collected on appliance A after disabling HA is ignored while setting up HA on appliance A during initialization and syncing.

Note: The terms "active" and "standby" might suggest that these appliances are not equivalent in every respect. In fact, they must have identical capabilities for High Availability pairing to work. Therefore, for clarity during the upgrade process below, the original active appliance is referred to as "appliance A" and the original standby appliance is referred to as "appliance B" (even though their roles reverse and then revert).

Procedure

Disable HA on appliance B (standby):

1. From the CLI, disable the HA configuration:
   a. From a command prompt, log in as the `root` user, and type the password.
   b. Run the following command to disable HA:

      ```
      set failover disable
      ```

   c. When the prompt displays the message CHANGES HAVE NOT BEEN SAVED!, type `save` and then press Enter.
2. Install the correct version of LogLogic LSP.
3. Perform the GUI upgrade steps.
4. After the appliance reboots, run the postupgrade script as described in Running the Postupgrade Script.

Disable HA on appliance A (active):

5. From the CLI, disable the HA configuration:
   a. From a command prompt, log in as the `root` user, and type the password.
   b. Run the following command to disable HA:

      ```
      set failover disable
      ```

   c. When the prompt displays the message CHANGES HAVE NOT BEEN SAVED!, type `save` and then press Enter.

Configure appliance B as the active appliance:

6. Set up HA configuration:
   a. From a command prompt, log in as the root user, and type the password.

b. Run the following command to set up HA:

```
set failover configure
```

c. Enter the IP addresses of the cluster: `<HA_public_IP_address> <network_mask> <network_broadcast> bond0`.

For example:

```
19.0.2.46 255.255.255.0 19.0.2.255 bond0
```

d. When prompted about this appliance being the destination of automatic migration:

Enter N.

Type the IP address of the peer appliance (appliance A): `19.0.2.44`

e. Follow the prompts. Ensure that you type save when prompted.

Wait until `done` is displayed on the CLI, indicating that the HA setup is successful on the appliance.

At this point, appliance B has become the active appliance. As appliance A is no longer part of the HA pair, it is reported as "out of cluster" by appliance B.

Configure appliance A as the standby appliance:

7. Install the correct version of LogLogic LSP.
8. Perform the GUI upgrade steps.
9. After the appliance reboots, run the postupgrade script as described in Running the Postupgrade Script.
10. After the upgrade process completes successfully, set up the HA configuration:
    a. From a command prompt, log in as the root user, and type the password.
    b. Run the following command to set up HA:

```
set failover configure
```

    c. Enter the IP addresses of the cluster: `<HA_public_IP_address> <network_mask> <network_broadcast> bond0`.

    For example:

```
19.0.2.46 255.255.255.0 19.0.2.255 bond0
```

d. When prompted about this appliance being the destination of automatic migration:

   Enter Y.

   Type the IP address of the peer appliance (appliance B):
   `19.0.2.45`

e. Follow the prompts. Ensure that you type save when prompted.

   Wait until `done` is displayed on the CLI, indicating that the HA setup is successful on the appliance. Appliance A has become the standby appliance.

Result

The upgrade is complete. Appliance B is active and appliance A is standby.

What to do next

After upgrade is successful, perform the following tasks:

- (Only for TIBCO LogLogic® LX1025 Appliance) Enable the swap file by performing the following steps:
  1. Log in to the appliance through SSH as `toor` user.
  2. Run the following command:

     ```
     $ /loglogic/scripts/enable_12g_swap_file.sh
     ```

- Reenable the following features if you had disabled them before starting the upgrade process:
  - **Archiving**

    Important: Do not change any settings in the archive configuration while re-enabling the archive feature.

  - **Advanced Features**

    After enabling Advanced Features, you can explicitly enable the Monthly Index, Advanced Aggregation, and Monitoring Console - as applicable. In an HA environment, you can enable the Advanced Features, Advanced Aggregation,

and Monitoring Console only from the CLI on the active appliance.

Upgrading in an AWS Environment

In an AWS environment, you can upgrade LogLogic EVA from version 6.3.0 or 6.3.1 to version 6.4.0 by running a cross-version migration script.

Before you begin

Before you start the upgrade procedure, you must meet the following requirements:

1. Deploy a new instance of LogLogic EVA 6.4.0 in AWS. LogLogic LSP 36.1.0 is automatically installed with it.

   For instructions, see the Deploying LogLogic EVA on AWS section in *TIBCO LogLogic® Enterprise Virtual Appliance Quick Start*.

2. The status of the following Advanced Features options (enabled or disabled) on the source instance and the new 6.4.0 instance must be identical:

   - Advanced Features
   - Advanced Aggregation
   - Monitoring Console

3. The version of LogLogic LSP on both LogLogic EVA instances must be identical. Therefore, on your existing LogLogic EVA instance, you must upgrade the LogLogic LSP to version 36.1.0, because LogLogic EVA 6.4.0 is compatible with LogLogic LSP 36.1.0.

   For instructions about upgrading LogLogic LSP, see TIBCO LogLogic® Log Source Packages 36.1.0 Installation and Upgrade.

Perform the following procedure on the source LogLogic EVA instance (version 6.3.0 or 6.3.1) and the destination LogLogic EVA (6.4.0) instance - as indicated.

Procedure

1. On the destination instance:

   a. Log in as the `toor` user.

   b. Extract the SSH public key from the file `/root/.ssh/id_rsa.pub` and display it

on the console by running the following command:

```
$ cat /root/.ssh/id_rsa.pub
```

c. Copy the SSH public key displayed on the console.

2. On the source instance:

a. Log in as the `toor` user.

b. Ensure that the file `/root/.ssh/authorized_keys` exists. If not, create the file by running the following commands:

```
$ touch /root/.ssh/authorized_keys
$ chmod 600 /root/.ssh/authorized_keys
```

c. Insert the SSH public key of the destination instance (from step 1b) into the `/root/.ssh/authorized_keys` file by running the following command:

```
$ echo 'SSH_public_key' >> /root/.ssh/authorized_keys
```

where *SSH_public_key* is the SSH public key from step 1b.

d. Insert the SSH public key of the source instance into the `/root/.ssh/authorized_keys` file by running the following command:

```
$ cat /root/.ssh/id_rsa.pub >> /root/.ssh/authorized_keys
```

3. On the destination instance:

a. Log in as the `toor` user.

b. Run the following migration script:

```
$ /loglogic/scripts/crossversion_migration/migrate.sh -v <source_version> -s <IP_address_source_instance>
```

where:

- <*source_version*> can be either `v630` or `v631`.
- <*IP_address_source_instance*> must be the IP address of the source

instance.

For example:

```
$ /loglogic/scripts/crossversion_migration/migrate.sh -v v631
-s 192.0.2.4
```

c. After the destination appliance reboots, remove the old finger print of the destination instance by running the following command:

```
$ ssh-keygen -f ~/.ssh/known_hosts -R <address_to_destination_instance>
```

d. Log in as the `toor` user.

Result

All data and configuration settings from the source instance are migrated to the LogLogic EVA 6.4.0 destination instance.

The password of the 6.4.0 appliance GUI is set identical to the password of the source appliance. However, the password of the `toor` user remains unchanged after migration.

Remote Upgrade

You can remotely upgrade the appliance software on a LogLogic LMI appliance or a LogLogic EVA instance from a computer with Windows, Linux, or macOS platform. This method is applicable in the following scenarios:

Category	Applicable to	Not applicable to
Number of appliances	One appliance at a time	Multiple appliances at a time
Setup	• LogLogic LMI hardware appliances • LogLogic EVA on VMware	LogLogic EVA on cloud and container platforms: • Microsoft Azure • AWS

Category	Applicable to	Not applicable to
		• KVM • Docker

Before you begin

On the computer where you invoke the upgrade procedure, ensure that the following requirements are met:

- The computer can access the target appliance remotely via SSH, and must not have any settings that might interrupt the process, such as sleep mode or battery-saver mode.
- Python version 3 and the supported Paramiko library must be installed on the computer.
- Continuous power supply and network connectivity must be available till the process completes.

Procedure

1. Log in to the computer from where you want to perform the upgrade.
2. (Optional) To perform a dry run of the command before actually performing the upgrade, add the --dry-run option with the command:

   ```
   $> ./remote_upgrade.py --host <IP_address_of_LMI_appliance> --upgrade-file <filename_of_tar_file> --dry-run
   ```

   The dry run does not start the upgrade process; it checks the SSH connection to the target appliance and retrieves the versions of LogLogic LMI and LogLogic LSP on the target appliance.
3. Run the upgrade command in the following format:

   ```
   $> ./remote_upgrade.py --host <IP_address_of_LMI_appliance> --upgrade-file <filename_of_tar_file>
   ```

   For example:

```
$> ./remote_upgrade.py --host 192.0.2.81 --upgrade-file loglogic-
lmi-6.4.0-fileupgrade.tar
```

Note: To upgrade an HA pair, provide the public IP address of the pair. If the IP address is not a public address, the upgrade process stops.

The remote upgrade script performs the following tasks:

a. Uploads the `.tar` file to the LogLogic LMI appliance or LogLogic EVA instance. If the `.tar` file exists on the appliance, then this step is skipped.

b. Runs the health check script. If any check fails, the upgrade process stops.

c. Performs the software upgrade on the LogLogic LMI appliance or LogLogic EVA instance.

Result

After the upgrade is completed:

- The appliance restarts.
- A log file is saved at the same location where the script is run.
- The state of Advanced Features before the upgrade are retained on the appliance after the upgrade.

What to do next

For more information about the upgrade events, see the log file.

Running the Postupgrade Script

After you upgrade an appliance to a new software release and the appliance reboots, you must run the postupgrade script on the appliance.

Upgrade scenario	When to run the script
Standalone	After the Upgrading a Standalone Appliance procedure.

Upgrade scenario	When to run the script
upgrade	
HA environment	After the GUI upgrade steps on the active appliance (Disable HA on appliance A (active):) and on the standby appliance (Disable HA on appliance A (active):).
Remote upgrade	Not applicable to remote upgrades.

Note: If the postupgrade script is not run during the upgrade procedure, some of the parsed reports data might be lost. The affected report types are different from one LogLogic LMI version to another.

Procedure

1. Log in to the appliance via SSH, by using the `toor` user.
2. Go to the CLI scripts directory:

   ```
   $ cd /loglogic/bin
   ```

3. Run the postupgrade script:

   ```
   $ ./rundbm
   ```

   The configuration menu appears, as follows:

   ```
   Configuration Menu:
   1) Modify the above configuration
   2) Start the Post Upgrade Process
   3) Help
   4) Exit the Post Upgrade Process

   Enter choice:
   ```

4. Type 1 and the modify configuration menu appears. The menu items vary based on the appliance configuration.

For example:

```
1) module_<version>_wwwlog
2) module_<version>_i5OSAudit
3) module_<version>_stats
4) module_<version>_ids
5) Return to Configuration Menu
6) Help
Enter 1-6:
```

If there is no data to be converted, the menu might appear as follows:

```
1) Return to Configuration Menu
2) Help
Enter 1-2:
```

5. For each option in the modify configuration menu, change the number of days to preserve for any of these logs that should not be set to seven days. For example, for Blue Coat:
   a. Type 1.
   b. Specify if you want to change the default value. If you type y, enter the amount of preexisting BlueCoat/wwwlog data (in days) that you want accessible on the appliance after the upgrade. For example, if you want access to the past month's Blue Coat data, enter 31. The default setting is 7, which converts the previous week. The higher the number of days you enter, the longer the postupgrade process takes to complete. To preserve the ability to search on all log data collected from Blue Coat log sources, input a number of days to include the first collection of Blue Coat log information. After entering the number of days, the module configuration menu appears again.
6. Type 5 to go back to Configuration Menu.
7. Type 2 to start the postupgrade process.

   The conversion time for the postupgrade process depends on the amount of data to be migrated.
8. After typing 2 to start the postupgrade process, the configuration menu is displayed immediately, with the additional option, 5) Monitor the Post Upgrade Process. Type 5 to monitor the postupgrade process.

```
1) Modify the above configuration
2) Start the Post Upgrade Process
3) Help
4) Exit the Post Upgrade Process
5) Monitor the Post Upgrade Process
```

Press Ctrl+C to exit.

The configuration menu is displayed again. A message is displayed indicating that the postupgrade process has been completed.

```
2019-02-11 20:10:37,818 - dbmLogger - INFO: ** All migrations
complete!
```

9. Type 4 to exit the postupgrade script.

TIBCO Documentation and Support Services

For information about this product, you can read the documentation, contact TIBCO Support, and join TIBCO Community.

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.

Product-Specific Documentation

The following documentation for this product is available on the TIBCO LogLogic® Log Management Intelligence Product Documentation page.

- *TIBCO LogLogic® Log Management Intelligence Release Notes*
- *TIBCO LogLogic® Log Management Intelligence Administration*
- *TIBCO LogLogic® Log Management Intelligence Configuration and Upgrade*
- *TIBCO LogLogic® Log Management Intelligence Hardware Installation Guide*
- *TIBCO LogLogic® Log Management Intelligence Log Source Report Mapping*
- *TIBCO LogLogic® Log Management Intelligence Security Guidelines*
- *TIBCO LogLogic® Log Management Intelligence SSD Hardware Field Installation*
- *TIBCO LogLogic® Log Management Intelligence Syslog Alert Message Format Quick Reference*
- *TIBCO LogLogic® Log Management Intelligence User Guide*
- *TIBCO LogLogic® Log Management Intelligence XML Import/Export Entities Reference*
- *TIBCO LogLogic® Enterprise Virtual Appliance Quick Start*

Other TIBCO Product Documentation

The following documents for TIBCO LogLogic® Log Source Packages are available on the TIBCO eDelivery website or TIBCO Support website after logging in.

- *TIBCO LogLogic® Log Source Packages Release Notes*
- *TIBCO LogLogic® Log Source Packages Installation and Upgrade*
- *TIBCO LogLogic® Log Source Packages Log Configuration Guides*
- *TIBCO LogLogic® Log Source Packages Log Collector Guides*

How to Contact TIBCO Support

Get an overview of TIBCO Support. You can contact TIBCO Support in the following ways:

- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the TIBCO Support website.
- 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 TIBCO Support website. 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 TIBCO Community.

Legal and Third-Party Notices

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.

This and other products of TIBCO Software Inc. may be covered by registered patents. Please refer to TIBCO's Virtual Patent Marking document (https://www.tibco.com/patents) for details.