Platform LSF
Version 9 Release 1.2

Security

SC27-5303-02

Platform LSF
Version 9 Release 1.2

Security

SC27-5303-02

Note

Before using this information and the product it supports, read the information in “Notices” on page 9.

First edition

This edition applies to version 9, release 1 of IBM Platform LSF (product number 5725G82) and to all subsequent releases and modifications until otherwise indicated in new editions.

Significant changes or additions to the text and illustrations are indicated by a vertical line (|) to the left of the change.

If you find an error in any Platform Computing documentation, or you have a suggestion for improving it, please let us know. Send your suggestions, comments and questions to the following email address:

pccdoc@ca.ibm.com

Be sure include the publication title and order number, and, if applicable, the specific location of the information about which you have comments (for example, a page number or a browser URL). When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Chapter 1. Platform LSF security considerations 1
Communications between daemons and commands . 1
Transmission of Platform LSF commands for remote execution 1
Access to jobs belonging to other users 1
Accessing remote hosts 3
False requests 3
Authentication. 4

Chapter 2. Secure your Platform LSF cluster 5
Secure communications between daemons and commands 5
Encrypt transmission of LSF commands for remote execution and login 5
Restrict user access to remote hosts 6
Secure your cluster against false requests 6
Customize external authentication 7
Enable external authentication of LSF daemons . . . 7
Secure the cluster from root access for batch interactive jobs in pseudoterminals 7
Restrict user access to administration commands and log files 8

Notices 9
Trademarks 11
Privacy policy considerations 11

Chapter 1. Platform LSF security considerations

While the default LSF configuration is adequate for most clusters, you should consider the following issues if you want to increase the security of your LSF cluster.

Communications between daemons and commands

Communications between LSF daemons and between LSF commands and daemons are not encrypted. If your LSF clusters are running in an untrusted or unsecured environment, these communications may be susceptible to interception and spoofing attacks. You can enable strict checking of communications to deal with spoofing attacks.

Transmission of Platform LSF commands for remote execution

By default, the following LSF commands make use of remote shell (**rsh**) and remote login (**rlogin**):

- **badmin hstartup**
- **bpeek**
- **lsadmin limstartup**
- **lsadmin resstartup**
- **lsfrestart**
- **lsfshutdown**
- **lsfstartup**
- **lslogin**
- **lsrcp**

rsh and **rlogin** may not be suitable for transmission over an insecure network because it is not encrypted. You can configure these LSF commands to use secure shell (**ssh**), which provides encryption when transmitting commands for remote execution.

Access to jobs belonging to other users

All LSF jobs are run under the user ID of the user who submitted the job (unless you are using account mapping). LSF enforces restrictions on job access based on the user ID of the user who is running a command and the user ID associated with the submitted job.

All LSF users can view basic information on all jobs, including jobs submitted by other users, but can only view detailed information on or modify jobs submitted by their own user IDs. Only administrators can modify jobs submitted by other users.

User commands providing information on all jobs

Any LSF user can run the following commands to view basic information on any jobs running in the cluster, including jobs submitted by other users:

bjobs

displays information about LSF jobs. By default, **bjobs** displays information about your own pending, running, and suspended jobs. You can view information on jobs submitted by other users by using the **-u** option to specify a specific user, user group, or all users (using the all keyword).

bhist

displays historical information about LSF jobs. By default, **bhist** displays historical information about your own pending, running, and suspended jobs. You can view historical information on jobs submitted by other users by using the **-u** option to specify a specific user, user group, or all users (using the all keyword).

bhosts

displays information on hosts, including job state statistics and job slot limits. By default, you can view the number of jobs running on each host, including jobs submitted by other users; however, you only see the total number of jobs running on the host, not the specific users who submitted the jobs.

bqueues

displays information on queues, including job slot statistics and job state statistics. By default, the user can view the number of jobs running in each queue, including jobs submitted by other users; however, you only see the total number of jobs running in the queue, not the specific users who submitted the jobs.

User commands that restrict information on jobs submitted by other users

Any LSF user can run the following command to provide detailed information on jobs running in the cluster, but not on jobs submitted by other users:

bpeek

displays standard output and standard error output that have been produced by unfinished jobs. This command displays detailed information on the progress of a job, but you can only view jobs that belong to your own user ID.

Queue and administrator commands that modify all jobs

Queue administrators and LSF administrators can run the following commands to modify jobs submitted by any user. LSF users can also run these commands, but only to modify their own jobs with certain restrictions:

bbot

moves a pending job relative to the last job in the queue.

btop

moves a pending job relative to the first job in the queue.

LSF administrator commands that modify all jobs

LSF administrators can run the following commands to modify jobs submitted by any user. LSF users can also run these commands, but only to modify or control their own jobs with certain restrictions:

bchkpnt

Checkpoints one or more checkpointable jobs. LSF administrators can checkpoint jobs submitted by any user.

bkill

Sends a signal to kill unfinished jobs.

bmod

Modifies job submission options of a job.

brestart

Restarts checkpointed jobs.

bresume

Resumes a suspended job.

bstop

Suspends unfinished jobs.

Job data files

Jobs running in the LSF cluster inherit the environment from the user that submitted the job. Work files and output files are created based on the file permissions environment of the user (such as **umask** in POSIX environments). LSF does not provide additional security to these files. Therefore, to increase the security of work and output data, you need update the security of your hosts and file system according to the operating systems on your hosts.

Accessing remote hosts

By default, LSF provides commands for running tasks on remote hosts using LSF daemons (**lim** and **res**) and LSF ports (LSF_LIM_PORT and LSF_RES_PORT) for communication. Therefore, even if your cluster restricts users from directly logging into or running commands on remote hosts (therefore restricting your users to using LSF batch commands to access remote hosts), users can still run the following commands to run tasks on remote systems under certain circumstances.

lsrun

runs an interactive task on a remote host through LSF. You can run a single task on a single remote host.

lsgrun

runs a task on a set of remote hosts through LSF. You can run a single task on multiple remote hosts.

ch

changes the host on which subsequent commands are to be executed. You can change tasks to run on a selected remote host.

False requests

LSF clusters may be vulnerable to large-scale denial of service (DOS) attacks. If one of the LSF daemons becomes overloaded with false requests, it may not be able to respond to valid requests.

By default, LSF refuses to accept client requests from hosts not listed in `lsf.cluster.`*`cluster_name`*. If LSF daemons are started on the unlisted host, the daemons will continue to retry the connection. The LSF master host rejects these requests, but if there are many unlisted hosts doing the same thing, it may become overloaded and be unable to respond to valid requests.

Since LSF can handle large clusters (several thousand hosts in a cluster) and is designed to be resistant to this type of attack, a malicious attack needs to simulate a larger scale of false hosts in order to be successful, but LSF still remains potentially vulnerable to a very large-scale attack.

Authentication

In LSF, authentication can come by means of external authentication using the LSF **eauth** executable, or by means of identification daemons (**identd**). External authentication provides the highest level of security and is the default method of authentication in LSF. It is installed in the directory specified by the **LSF_SERVERDIR** parameter in the `lsf.conf` file.

By default, **eauth** uses an internal key to encrypt authentication data, but you may use a customized external key to improve security. You can also write your own **eauth** executable to meet the security requirements of your cluster, using the default **eauth** as a demonstration of the **eauth** protocol.

Chapter 2. Secure your Platform LSF cluster

Perform the following tasks to secure your LSF cluster.

Note: If you are running LSF in a mixed cluster, you must make sure that `lsf.conf` parameters set on UNIX and Linux match any corresponding parameters in the local `lsf.conf` files on your Windows hosts. Therefore, when you need to edit the `lsf.conf` file, be sure to specify the same parameters for UNIX, Linux, and Windows hosts.

Secure communications between daemons and commands

To deal with spoofing attacks in your cluster, enable strict checking of communications between LSF daemons and between LSF commands and daemons.

You need to shut down all hosts in the LSF cluster to enable strict checking.

If you are running a Platform MultiCluster environment, you must enable strict checking in all clusters.

1. Shut down all hosts in the LSF cluster.
   ```
   lsfshutdown
   ```
2. Edit the `lsf.conf` file.
3. Enable strict checking by specifying the **`LSF_STRICT_CHECKING`** parameter.

   Add the following line to `lsf.conf`:
   ```
   LSF_STRICT_CHECKING=Y
   ```
4. Start up all hosts in the LSF cluster.
   ```
   lsfstartup
   ```

Your LSF cluster now requires an LSF-generated checksum for all communications.

Encrypt transmission of LSF commands for remote execution and login

By default, certain LSF commands use **`rsh`** for remote execution and **`rlogin`** for remote login, both of which are not encrypted. To secure these LSF commands, enable the use of **`ssh`** for remote execution, because **`ssh`** provides encryption when transmitting LSF commands.

The following LSF commands are covered by this change:

- **`badmin hstartup`**
- **`bpeek`**
- **`lsadmin limstartup`**
- **`lsadmin resstartup`**
- **`lsfrestart`**
- **`lsfshutdown`**
- **`lsfstartup`**
- **`lslogin`**
- **`lsrcp`**

1. Edit the `lsf.conf` file.
2. Change the remote execution shell from **rsh** to **ssh** by specifying the **LSF_RSH** parameter.

   For example,

   ```
   LSF_RSH="ssh -o 'PasswordAuthentication no' -o 'StrictHostKeyChecking
   no'"
   ```
3. Change the remote login shell by specifying the **LSF_LSLOGIN_SSH** parameter.

   ```
   LSF_LSLOGIN_SSH=yes
   ```
4. Reconfigure LIM and restart **mbatchd** on the master host to activate these changes.

   ```
   lsadmin reconfig
   ```

   ```
   badmin mbdrestart
   ```

The affected LSF commands now use **ssh** for remote execution and remote login.

Restrict user access to remote hosts

Even if your cluster restricts users from directly accessing remote hosts, they can still use **lsrun**, **lsgrun**, and **ch** to run tasks on specific remote hosts.

To prevent users from accessing specific remote hosts and let LSF control which remote hosts are being used, restrict access to the **lsrun**, **lsgrun**, and **ch** commands.

1. Edit the `lsf.conf` file.
2. Restrict user access to the **lsrun** and **lsgrun** commands by specifying the **LSF_DISABLE_LSRUN** parameter.

   ```
   LSF_DISABLE_LSRUN=Y
   ```

   LSF administrators still have access to **lsrun** and **lsgrun**.
3. Reconfigure LIM and restart **mbatchd** on the master host to activate these changes.

   ```
   lsadmin reconfig
   ```

   ```
   badmin mbdrestart
   ```
4. Restrict access to the **ch** commands by restricting the execution permissions of the **ch** binary in the LSF binary directories to the LSF administrators.

Only LSF administrators can run **lsrun** and **lsgrun** to launch tasks in remote hosts, and only LSF administrators can run **ch** to change the remote hosts on which a task runs.

Secure your cluster against false requests

To secure your cluster against false requests sent from unlisted hosts, restrict access to the LSF master host and master candidates.

The parameters you set to restrict access depend on whether your cluster allows dynamic hosts.

1. Edit the `lsf.conf` file.
2. Limit the number of master candidates in your cluster that are specified by the **LSF_MASTER_LIST** parameter.
3. If your cluster does not allow dynamic hosts, prevent unlisted hosts from sending requests by specifying the **LSF_REJECT_NONLSFHOST** parameter.

   ```
   LSF_REJECT_NONLSFHOST=yes
   ```

4. Edit the `lsf.cluster.`*`cluster_name`* file.
5. Limit or remove the range of IP addresses that are allowed to be dynamic LSF hosts by editing or deleting the **`LSF_HOST_ADDR_RANGE`** parameter.
   - If your cluster allows dynamic hosts, limit the range of IP addresses that are specified by the **`LSF_HOST_ADDR_RANGE`** parameter.
   - If your cluster does not allow dynamic hosts, ensure that the **`LSF_HOST_ADDR_RANGE`** parameter is not specified.
6. Reconfigure LIM and restart **`mbatchd`** on the master host to activate these changes.

   ```
   lsadmin reconfig
   ```

   ```
   badmin mbdrestart
   ```

Customize external authentication

By default, **`eauth`** uses an internal key to encrypt authentication data, but you may whish to use your own external key to further improve security.

You can also write your own external authentication application to meet the security requirements of your cluster.

1. Edit the `lsf.sudoers` file.
2. Use a custom external key by specifying the **`LSF_EAUTH_KEY`** parameter.

   ```
   LSF_EAUTH_KEY=key
   ```
3. Restart the cluster to activate this change.

   ```
   lsfrestart
   ```

Enable external authentication of LSF daemons

You can increase LSF daemon security in your cluster by enabling LSF daemon authentication.

1. Edit the `lsf.sudoers` file.
2. Enable LSF daemon authentication by specifying the **`LSF_AUTH_DAEMONS`** parameter.

   ```
   LSF_AUTH_DAEMONS=Y
   ```
3. Reconfigure the master host to activate this change.

   ```
   badmin reconfig
   ```

Secure the cluster from root access for batch interactive jobs in pseudoterminals

Batch interactive jobs in pseudoterminals (that is, jobs submitted using **`bsub -Is`** and **`bsub -Ip`** commands) could obtain root privileges to your cluster due to environment variables (**`LD_PRELOAD`** and **`LD_LIBRARY_PATH`**) contained in the jobs.

To enhance security against users obtaining root privileges using batch interactive jobs in pseudoterminals, enable the cluster remove these environment variables from batch interactive jobs during job initialization. These environment variables are put back before the job runs.

1. Edit the `lsf.conf` file.
2. Enable the cluster to remove the **`LS_PRELOAD`** and **`LD_LIBRARY_PATH`** environment variables from jobs submitted using **`bsub -Is`** and **`bsub -Ip`** commands during job initialization by specifying the **`LSF_LD_SECURITY`** parameter.

```
LSF_LD_SECURITY=y
```

3. Reconfigure LIM and restart **mbatchd** on the master host to activate these changes.

   ```
   lsadmin reconfig
   ```

   ```
   badmin mbdrestart
   ```

In jobs submitted using **bsub -Is** and **bsub -Ip** commands, the **LD_PRELOAD** and **LD_LIBRARY_PATH** environment variables are moved to the **LSF_LD_PRELOAD** and **LSF_LD_LIBRARY_PATH** environment variables and are moved back before the job runs.

Restrict user access to administration commands and log files

Log files may contain sensitive cluster information that need to be restricted to LSF administrators only. To restrict access to the LSF cluster log files, restrict the read/write permissions to all files in the `log` directory.

Cluster administrative tools (**badmin** and **lsadmin**) can only be used by LSF administrators. To provide an additional layer of security to prevent unauthorized administrator access to your LSF cluster, restrict the execution permissions for these commands.

1. Restrict access to the LSF cluster log files by restricting the read/write permissions of the **log** directory to the LSF administrators.
2. Restrict access to the administrative tools by restricting the execution permissions of the **badmin** and **lsadmin** binaries in the LSF binary directories to the LSF administrators.

   Tip:

   You can also restrict access to other LSF commands by restricting the execution permissions of their respective binary files.

Only LSF administrators can read the contents of the log directory or run cluster administration commands (**badmin** and **lsadmin**).

Notices

This information was developed for products and services offered in the U.S.A.

IBM® may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Intellectual Property Law
Mail Station P300
2455 South Road,
Poughkeepsie, NY 12601-5400
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

LSF®, Platform, and Platform Computing are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software

Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Printed in USA

SC27-5303-02