LoadRunner

Security Guide

Document Release Date: February 2018

Software Release Date: February 2018

Contents

Welcome to This Guide

Introduction

Welcome to the LoadRunner Security Guide.
This guide provides information for working with LoadRunner in a secure environment.

Secure Implementation and Deployment

This section provides information on implementing and deploying LoadRunner in a secure manner with the help of digital certificates.

A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a Certification Authority (CA). It contains the IP address of the machine for which it was issued, a validation date, and the digital signature of the certificate-issuing authority.

Certificates created by LoadRunner utilities have following attributes:

- Signature hash algorithm: sha256
- Encryption algorithm: RSA (2048 Bits)

Generating Certificates

LoadRunner provides the command line utilities: **gen_ca_cert**, and **gen_cert** for generating certificates.
For details, search for “**gen_ca_cert**” utility in the LoadRunner Help Center.

Installing Certificates

Using the LoadRunner Controller’s Authentication Settings dialog box, **Controller > Tools > Authentication Settings**, you specify the certificates required for the scenario run on the Controller. This dialog box lets you generate a certificate or select one created earlier.

To install certificates on a load generator machine, you can use the Certificate Authentication commands provided with the Network and Security Manager command line tool. For details, search for “**Network and Security Manager command line tool**” in the LoadRunner Help Center.

Network and Communication Security

This section provides information on network and communication security.

Securing Communication using SSL Certificates

The LoadRunner Controller’s Agent Configuration Settings dialog box enables you to define the relevant settings for enabling the LoadRunner agent on Windows machines.

To access this dialog box, select **Start > All Programs > HPE Software > HPE LoadRunner > Advanced Settings > Agent Configuration** and press the **Settings** button.

This dialog box allows you to:

- Turn on security (Use Secure Connection – SSL)
- Validate server certificates
- Validate client certificate

For server certificates, you can specify a level:

- **None**: do not check server certificates
- **Medium**: verify that the server certificate is signed by a trusted Certification Authority
- **High**: verify that the sender IP matches the certificate information.

You can also use the Network and Security Manager command line tool to specify certificates. For details, search for “**Network and Security Manager command line tool**” in the LoadRunner Help Center.

Setting a Load Generator as Secure (Checking the Client Certificate)

Using the Network and Security Manager command line tool’s **check_client_cert** flag, you can instruct the load generator or MI Listener to check the client certificates of the Controller that is trying to connect to it.

For details, see the following sections in the LoadRunner Help Center:

- “MI Listener” and “Monitor Over Firewall” sections to determine which machine is the server and which is the client.
- “Network and Security Manager - Command Line Tool”

When working over firewall, only folders that are marked as secure can be used.

Files can be transferred to and from a directory when security mode is enabled (i.e Over Firewall) only if this directory is a sub-folder of the Operating System temporary folder, or any directory that is listed in the configuration file **mft_settings.ini**.

To add a secure folder on the load generator machines:

1. Create a file called **mft_settings.ini** in the folder <**installation_folder>\dat\**
   (if the file exist then add the below)
2. Open the file and add a **[general]** section,
3. Under the **[general]** section, add a single attribute called **SecureDirectories=<path>**
   For example:
   [general]
   SecureDirectories=C:\MyFolder

Securing Communication using Secured Channels (to be deprecated)

Secure communication can be established between the Controller and load generator hosts using a security key. Each host in the system must be set up with an identical security key. If security keys on the hosts do not match, secure communication cannot be established.

Note: In future versions of LoadRunner, this option may not be supported. Keep this in mind if you employ this option for the current version.

APIs and References

This section provides information related to user authentication.

APIs for Over Firewall Mode

To prevent misuse of LoadRunner by outside sources, LoadRunner maintains a list of the functions that are allowed to be executed on a load generator for each supported protocol.

The lists are stored in files with the **.asl** extension under **<installation_folder>\merc_asl\*.asl** where ***** indicates the relevant protocol.

To add a new function to the lists of allowed functions for a load generator, add a new line to the relevant protocol list file containing the function name with an appended "=" character as follows:

<function_name>=

For general LoadRunner (lr) or C functions, add the function to the end of the file, **lrun_api.asl**.

Example: To add a function called **fopen**, add the following to the end of the file **lrun_api.asl**:

fopen=

When adding a new function to the file, ensure that the new line ends with a carriage return (CR/LF). Otherwise, the new function will not be read properly.

Ensure that the relevant protocol **.asl** files are updated as required on all affected load generators.

Allowed Applications for Over Firewall Mode

To prevent misuse of LoadRunner by outside sources, LoadRunner maintains a list of the applications that are allowed to be executed on a load generator.

The list is stored in: **<installation_folder>\launch_service\merc_asl\process.asl**

To add a new application to the list of allowed applications for a load generator, add a new line to the application list file containing the application (process) name with an appended "=" character.

Example: To add an application called **mspaint.exe**, add the following to the end of the **process.asl** file

mspaint.exe=

When adding a new application to the file, ensure that the new line ends with a carriage return (CR/LF). Otherwise, the new application will not be read properly.

Ensure that the **process.asl** file is updated as required on all affected load generators.

Personal information masking Model

LoadRunner Masking

LoadRunner provides several built in mechanisms for masking customer data.

Password Masking in Scripts (VuGen)

You can mask text within your script to protect your passwords and other confidential text strings. You can perform masking from the user interface or through programming.

You can restore the string at any time to determine its original value. When you mask a string, it appears in the script as a coded string. VuGen uses 32-bit encryption.

In order for the script to use the masked string, it must be unmasked with **lr_unmask**.

lr_start_transaction(lr_unmask("38620da61ca1093e7aa7ec"));

For details, see the LoadRunner Function Reference.

Masking Model FAQs

Question
Does LoadRunner transmit account passwords in an approved encrypted format?
Answer
Account passwords can be transmitted securely when SSL is enabled in LoadRunner.

Question
Does LoadRunner store account passwords in approved encrypted format?
Answer
User passwords are not stored at all, only the hash; but internal system passwords are stored in AES 256.

Question
Is SAML v 2.0 supported for performing authentication?
Answer
No.

Logs

This section provides information related to logs.

Log and Trace Model

There are several types of logs provided within LoadRunner:

- Vuser logs
- Scenario logs
- Custom logs

You can control the level of detail in the VuGen logs through the runtime setting's Log node.

Recommendations:

- Pay attention to the log level and do not leave the level at Debug.
- Restrict access to the log directory.
- If log archiving is needed, create your own archiving policy.

Log and Trace Security Administration and Features

Sensitive data will only appear in logs if the LoadRunner scripts write sensitive data to the logs as per a user's discretion. It is the user's responsibility not to insert unprotected sensitive data into regular LoadRunner entity fields.

The extent of the data provided in log files depends on the runtime setting's log level.

It is always recommended to store passwords in an encrypted format.

Logs FAQ

Question
Does LoadRunner audit access to need-to-know information and key application events?
Answer

Yes, through the application log files.
Question
Does LoadRunner support the creation of transaction logs for access and changes to the data?

Answer
The information can be found in the logs based on the log level. For details, see the LoadRunner Help Center.

General Questions

Question
How can I report security issues?
Answer
Report security issues using the following link: https://www.microfocus.com/support-and-services/report-security/

Question
Where can customers obtain the latest information regarding security vulnerabilities in LoadRunner?
Answer
You can obtain the latest information regarding security vulnerabilities via this webpage:
https://support.microfocus.com/security/

Legal Notices

Disclaimer

Certain versions of software and/or documents (“Material”) accessible here may contain branding from Hewlett-Packard Company (now HP Inc.) and Hewlett Packard Enterprise Company. As of September 1, 2017, the Material is now offered by Micro Focus, a separately owned and operated company. Any reference to the HP and Hewlett Packard Enterprise/HPE marks is historical in nature, and the HP and Hewlett Packard Enterprise/HPE marks are the property of their respective owners.

Warranty

The only warranties for Seattle SpinCo, Inc. and its subsidiaries (“Seattle”) products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Seattle shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated, valid license from Seattle required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Micro Focus Trademark Information

Company Details

Company name: Micro Focus International plc
Place of registration: England and Wales
Registered number: 5134647
Registered address: The Lawn, 22-30 Old Bath Road, Berkshire, RG14 1Q