

Packet Trace Guide

Technical Note

UPDATED: 28 July 2023

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

#1 Load Balancer in Price/Performance, 360 Central, 360 Vision, Chef, Chef (and design), Chef Habitat, Chef Infra, Code Can (and design), Compliance at Velocity, Corticon, Corticon.js, DataDirect (and design), DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Driving Network Visibility, Flowmon, Inspec, Ipswitch, iMacros, K (stylized), Kemp, Kemp (and design), Kendo UI, Kinvey, LoadMaster, MessageWay, MOVEit, NativeChat, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), Sitefinity Insight, SpeedScript, Stylized Design (Arrow/3D Box logo), Stylized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Workstation, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Classic, Fiddler Everywhere, Fiddler Jam, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, InstaRelinker, JustAssembly, JustDecompile, JustMock, KendoReact, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Any other marks contained herein may be trademarks of their respective owners.

Please refer to the NOTICE.txt or Release Notes – Third-Party Acknowledgements file applicable to a particular Progress product/hosted service offering release for any related required third-party acknowledgements.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Table of Contents

1 Introduction **4**

1.1 Document Purpose 4

1.2 Intended Audience 4

2 Perform a TCP Dump **5**

2.1 Perform a TCP Dump using the WUI 5

2.1.1 Perform a TCP Dump via the Console 6

2.1.1.1 Error during FTP Transfer 9

References **10**

Last Updated Date **11**

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

1 Introduction

One of the easiest ways to view the traffic traversing the Kemp LoadMaster is to perform a TCP dump. This simple command will capture all of the traffic (or just a specified subset) that is being transmitted and received by the LoadMaster. The results can be examined by analysing the .pcap file with Wireshark or another packet analyzer.

> When using the console to perform the TCP dump, an FTP server that can be reached by the LoadMaster is required in order to retrieve the packet capture files.

1.1 Document Purpose

The purpose of this document is to educate the reader on how to perform a TCP dump in the Kemp LoadMaster.

1.2 Intended Audience

This document is intended to be read by anyone who is interested in finding out how to perform a TCP dump in the LoadMaster.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

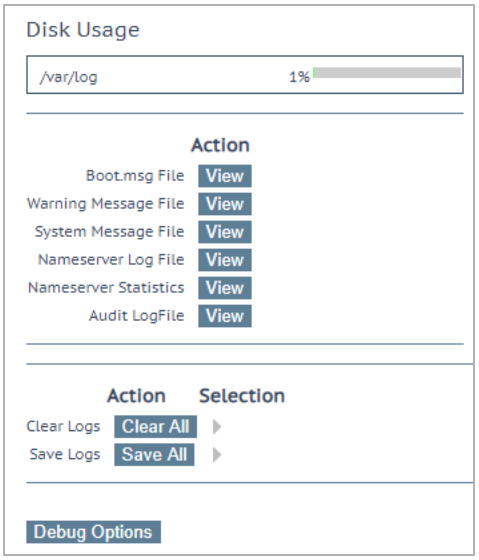
2 Perform a TCP Dump

There are two ways to perform a TCP dump in the LoadMaster – via the Web User Interface (WUI), or via the console. Refer to the relevant section below for steps.

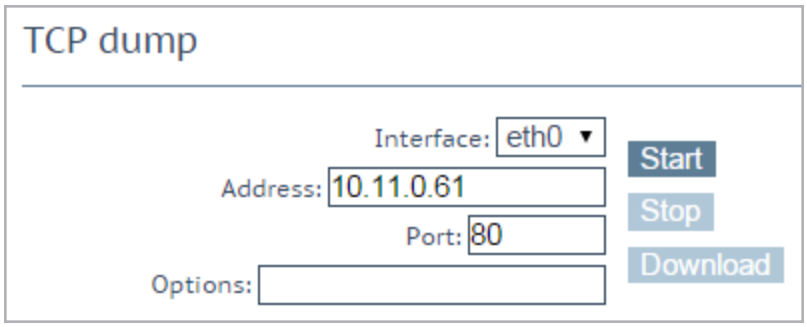
2.1 Perform a TCP Dump using the WUI

To perform a TCP dump using the WUI, follow the steps below:

1. In the main menu, select **System Configuration > Logging Options > System Log Files**.



2. Click **Debug Options**.



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3. A TCP dump can be captured either by one or all Ethernet ports. In the **TCP dump** section at the bottom of the screen, select the relevant **Interface** to run the TCP dump on, or select **All**.

4. Optionally enter the IP **Address** and the **Port** to be monitored.

5. Enter any optional parameters as required in the **Options** text box.

> The maximum number of characters permitted in the **Options** field is **255**.

6. Click **Start**.

7. Make access from the client to the Virtual Server.

8. When appropriate, click **Stop**.

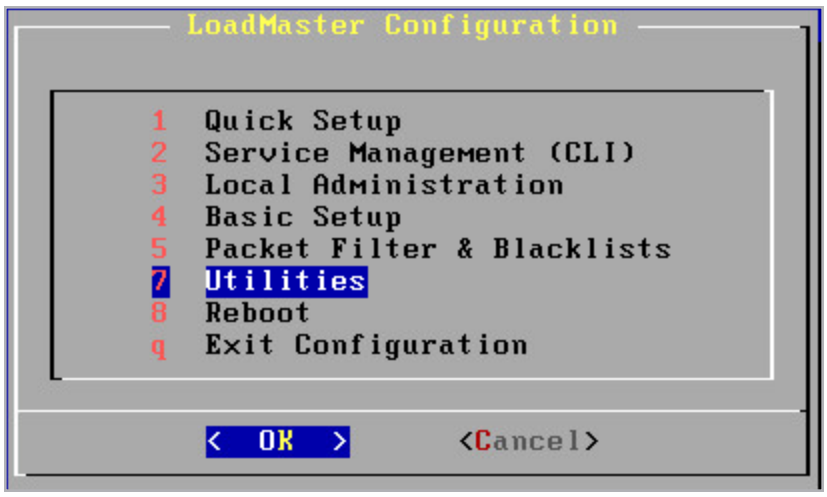
9. Click **Download**.

10. This downloads the results of the TCP dump in a .pcap file. This file can be analysed using a packet trace tool such as Wireshark.

2.1.1 Perform a TCP Dump via the Console

To perform a TCP dump via the console, follow the steps below:

1. Log in to the console.

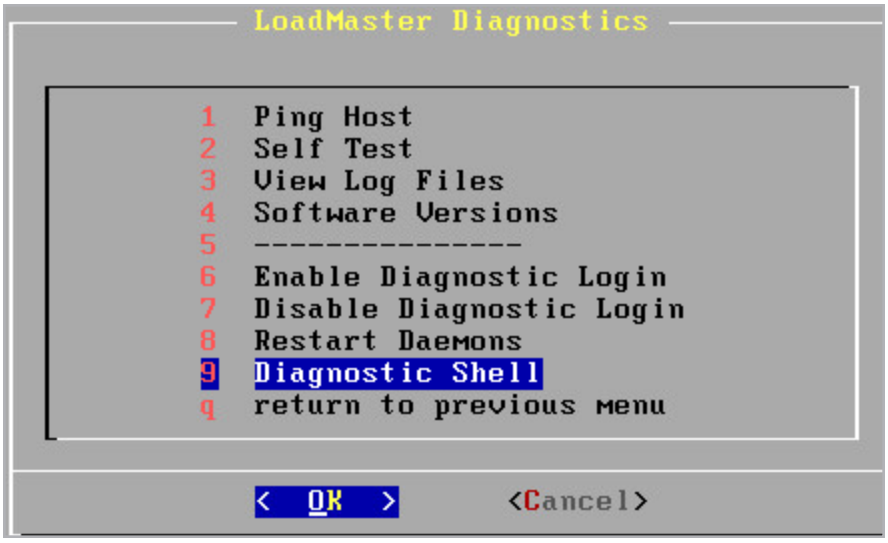


2. Select **Utilities**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



3. Select **Diagnostics**.



4. Select **Diagnostic Shell**.

5. Enter the relevant commands at the **%** prompt, for example:

tcpdump –s 1500 –c 10000 –i eth0 –w eth0.pcap FILTER0 &

> If performing a TCP dump on a two-armed device, ensure to enter the ampersand (**&**) at the end of the command and also use the command below.

tcpdump –s 1500 –c 10000 –i eth1 –w eth1.pcap FILTER1

6. Please select the appropriate filter for **FILTER0** and **FILTER1**:

   a) Host 1.2.3.4

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

b) Port 1234

c) Host 1.2.3.4 and port 1234

7. For example, a complete TCP dump command might look like this:

tcpdump –s 1500 –c 10000 –i eth0 –w eth0.pcap host 1.2.3.4 and port 80

8. This will capture all traffic to or from IP 1.2.3.4 with a source or destination port of 80.

> As the example command above is set to quit after 10,000 packets, the capture may need to be restarted if the situation in question does not occur within the first 10,000 packets captured, i.e. in the case of heavy load.

9. Make access from the client to the Virtual Server to produce the error.

10. Return to the diagnostic shell.

11. Stop the packet capture by holding **Ctrl** on the keyboard and pressing **C**.

12. If running a TCP dump on a two-armed setup, enter the command **fg**. The second trace will appear. Stop the second packet capture by holding **Ctrl** on the keyboard and pressing **C**.

13. Connect to the FTP server and send the file by entering the command:

ftp <FTP IP address>

14. Enter credentials (this depends on the FTP server).

15. Then, enter the following commands:

binary

put eth0.pcap

put eth1.pcap (if running a packet tract on a two-armed configuration)

bye

16. It is now possible to retrieve the packet capture files from the FTP server and analyse them in the application of choice, for example Wireshark.

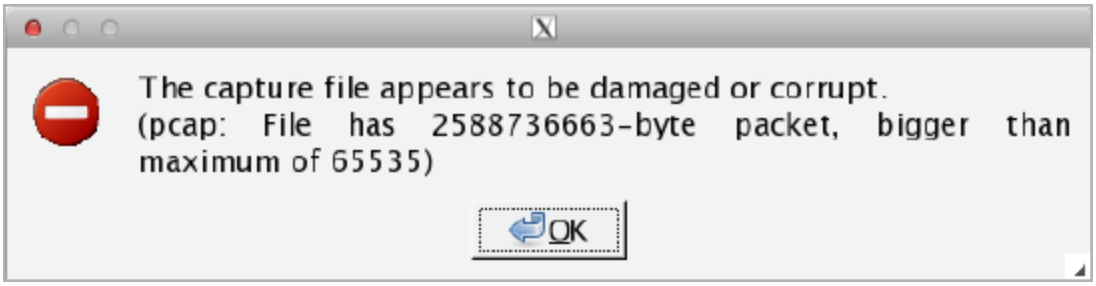
17. Use the **exit** command to exit the Diagnostic Shell.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

If instructed by a Kemp Support Engineer, you can send them the packet trace file for analysis. Before sending the packet capture, please open it using a relevant tool, for example Wireshark, to ensure both the quality of the data and the integrity of the file.

> Please keep in mind any security implications of sending the packet capture.

2.1.1.1 Error during FTP Transfer



If an error occurs which notifies of a damaged or corrupt file, it is likely that the file was not transferred in binary mode. Repeat **Step 13** in the **Perform a TCP Dump via the Console** section and ensure to issue the **binary** command before transferring.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

References

Unless otherwise specified, the following documents can be found at http://www.kemptechnologies.com/documentation.

Web User Interface (WUI), Configuration Guide

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Last Updated Date

This document was last updated on 28 July 2023.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.