

[ANNOUNCE] DSFS Network Forensic File System for Linux Patches

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2005-08/7995.html>

From: Jeff V. Merkey (jmerkey_at_soleranetworks.com)

Date: 08/31/05

Date: Wed, 31 Aug 2005 10:33:43 -0600
To: linux <linux-kernel@vger.kernel.org>

The Solera Networks DS File System kernel patches have been posted at <ftp.soleranetworks.com> and can be downloaded via anonymous ftp access.

These patches are for the 2.4.29, and 2.6.9 kernels. These patches includes all kernel changes made to the Linux kernel and GPL code that allows multiple gigabit capture and stream to disk capability. These patches are being provided as required by the terms of the GNU Public License. Also included with this announcement are white papers which can be located at www.soleranetworks.com describing the appliance features and characteristics of the DSFS file system.

The Core File System code is a separate proprietary module and is not released under the GPL and is shipped on the Solera Networks DS 1U, 2U, and 3U appliances. DS Appliances support gigabit ethernet and 10Ge Ethernet via the Intel e1000/ixgb adapter drivers.

Current Capture rates sustained with a 2U appliance with DSFS on Linux 2.6.X and 2.4.X kernels are:

975,000 pps @ 72 byte packets x 2 interfaces = 120 MB/S stream to disk
445,000 pps @ 256 byte packets x 2 interfaces = 226 MB/S stream to disk
208,000 pps @ 576 byte packets x 2 interfaces = 240 MB/S stream to disk
119,000 pps @ 1024 byte packets x 2 interfaces = 245 MB/S stream to disk
82,000 pps @ 1500 byte packets x 2 interfaces = 247 MB/S stream to disk

Current Capture rates sustained with a 1U appliance with DSFS on Linux 2.6.X and 2.4.X kernels are:

975,000 pps @ 72 byte packets x 1 interfaces = 60 MB/S stream to disk
445,000 pps @ 256 byte packets x 1 interfaces = 113 MB/S stream to disk
208,000 pps @ 576 byte packets x 1 interfaces = 119 MB/S stream to disk

Linux–Kernel: [ANNOUNCE] DSFS Network Forensic File System for Linux Patches

119,000 pps @ 1024 byte packets x 1 interfaces = 122 MB/S stream to disk
82,000 pps @ 1500 byte packets x 1 interfaces = 123 MB/S stream to disk

Current Capture rates sustained with a 3U appliance with dual disk controllers with DSFS on Linux 2.6.X and 2.4.X kernels are:

975,000 pps @ 72 byte packets x 3 interfaces = 180 MB/S stream to disk
445,000 pps @ 256 byte packets x 3 interfaces = 339 MB/S stream to disk
208,000 pps @ 576 byte packets x 3 interfaces = 360 MB/S stream to disk
119,000 pps @ 1024 byte packets x 3 interfaces = 365 MB/S stream to disk
82,000 pps @ 1500 byte packets x 3 interfaces = 370 MB/S stream to disk

The DSFS file system supports over 300 open source applications with high performance stream to disk network forensic storage capability and also supports SPAN, Optical Splitter, and Asymmetric Routed configurations. DSFS performs stream merging and also exposes the captured data as native LIBPCAP files and virtual network interfaces which allow seamless integration with Snort, tEthereal, and hundreds of open source Network Forensic and Network Management tools on Linux and Windows. DSFS is the culmination of 2 years of intense development efforts by Solera Networks to create a powerful platform infrastructure for the development of high performance network forensic open source applications on the Linux Operating System.

DSFS is fully SMP enabled and supports Hyperthreaded architectures as well as native SMP.

Jeff V. Merkey
Solera Networks
www.soleranetworks.com

–

To unsubscribe from this list: send the line "unsubscribe linux–kernel" in the body of a message to majordomo@vger.kernel.org
More majordomo info at <http://vger.kernel.org/majordomo–info.html>
Please read the FAQ at <http://www.tux.org/lkml/>