



Lenovo Dynamic System Analysis Installation and User Guide



Version 10.5

Note

Before using this information and the product it supports, read the information in Appendix D “Notices” on page 73.

(April 2019)

© Copyright Lenovo 2014, 2019.

LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant to a General Services Administration (GSA) contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925.

Contents

About this publicationiii	Transferring collected data to the customer inventory repository	24
Conventions and terminology	iii		
New in this release.	v	Chapter 8. Copying data and logs.	25
Chapter 1. Technical overview	1	Chapter 9. Supporting Dynamic System Analysis Features on Demand	27
Chapter 2. Installing Lenovo Dynamic System Analysis	3	Using Features on Demand for Portable Dynamic System Analysis	27
Hardware and software requirements	3	Downloading the FoD key and installing with the key file	27
Hardware requirements	3	Using the FoD Key on an IMM for a portable target system	28
Supported hardware	3	Using the FoD Key on a CMM for a portable target system	29
Software requirements	10	Using the FoD Key on an IOM/Switch for a portable target system	31
Supported operating systems	11	Using the Features on Demand GUI support for CD-based Preboot DSA	32
Installing Dynamic System Analysis on removable media.	12	Using Features on Demand GUI support for Embedded Preboot DSA	35
Chapter 3. Running diagnostic tests on a local system	13	Chapter 10. Troubleshooting and support.	39
Chapter 4. Collecting system information.	15	Known limitations, problems, and workarounds	39
Collecting system information on a local system using the Preboot Edition	15	Dynamic System Analysis event log	50
Collecting system information on a local system using removable media	16	Dynamic System Analysis core dump file	51
Collecting system information on a remote system running VMware ESXi	16	Getting help and technical assistance	51
Collecting IMM information from a remote system	17	Before you call	52
Converting collected data on a local system.	17	Using the documentation	52
Chapter 5. Comparing system information.	19	Getting help from the World Wide Web	52
Comparing firmware versions on a local system with the latest versions	19	Software service and support	53
Comparing current system information to previously collected data	19	Hardware service and support	53
Comparing multiple system information files	20	Appendix A. Accessibility features for Dynamic System Analysis	55
Chapter 6. Viewing collected system information.	21	Appendix B. Dynamic System Analysis commands	57
Chapter 7. Transferring data and logs.	23	Appendix C. Environment variables	71
Transferring collected data to a remote system	23	Appendix D. Notices.	73
		Index	75

About this publication

This publication provides information about how to download and use Dynamic System Analysis.

Conventions and terminology

Paragraphs that start with a Note, Important, or Attention in bold have specific meanings to highlight key information:

Note: These notices provide important tips, guidance, or advice.

Important: These notices provide information or advice that might help you avoid inconvenient or difficult situations.

Attention: These notices indicate possible damage to programs, devices, or data. An attention notice appears before the instruction or situation in which damage can occur.

In this book, when you are instructed to enter a command, type the command and press Enter.

New in this release

Enhancement

- Support Microsoft Windows 2016 (except Nano)
- Resolved CVE-2016-2183: SWEET32 Attack on 3DES and Blowfish
- Resolved CVE-2016-8624: invalid URL parsing with “#”
- Support TLS 1.2 by default and disable TLS 1.0/1.1 by default
- Resolved the issue that logging in to systems through DSA may disclose passwords to local users

Chapter 1. Technical overview

Lenovo Dynamic System Analysis (DSA) is a system information collection and analysis tool that is used by System x Service and Support personnel to aid in the diagnosis of system problems. This software can be used while the operating system is running.

Two editions of Dynamic Systems Analysis are available:

Preboot Edition

The Preboot edition of Dynamic System Analysis runs as an embedded Preboot image or from the boot menu.

You can create bootable media such as CD, DVD, ISO, USB or PXE using Lenovo ToolsCenter Bootable Media Creator (BoMC) or download the Windows/Linux update package for Preboot DSA to flash an embedded Preboot image. Reboot the system from the image you created or enter the boot menu to enter Preboot DSA.

For more information, see [Lenovo Bootable Media Creator \(BoMC\) Users Guide](#).

Portable Edition

This edition of Dynamic System Analysis runs from a command-line interface as a self-extracting executable file.

DSA creates a temporary directory called `/tmp` on Linux or `%TEMP%` on Windows, and extracts all of the Dynamic System Analysis files to that directory. DSA then runs the command. When the command has finished executing all actions, the temporary directory and all of the Dynamic System Analysis files are deleted from the local system.

You can download the Portable Edition from the Web site and install it on removable media, such as CD, DVD, or a USB flash drive.

Dynamic System Analysis collects information about the following aspects of a system, if applicable:

- Drive Health Information
- Event logs for the operating system, ServeRAID controllers, and service processors
- Event logs for the system including Chassis Event log and IPMI Event log
- FoD Activation key information
- Hardware inventory, including PCI and USB information
- IBM LightPath status
- Installed packages
- Kernel Modules
- LSI RAID and controller configuration
- Network interfaces and settings
- Option cards for firmware and driver information:
 - Broadcom
 - Brocade Adapter
 - Diablo FlashDimm
 - Emulex
 - LSI Controller
 - Mellanox Adapter
 - Qlogic
- Performance data and details for running processes

- ServeRAID configuration
- Service Processor status and configuration
- System configuration
- System environmental information
- Vital product data, firmware, and basic input/output system (BIOS) information

System information is collected into a compressed XML file that can be sent to Lenovo Service and Support. You can view the system information using an optionally generated HTML Web pages or text files.

You can use Dynamic System Analysis to create a merged log that includes events from all collected logs and to compare the firmware configurations on a server to those from UpdateXpress.

Important:

- To install or use Dynamic System Analysis, you must be logged in to the local system using a user ID that has administrator or root privileges. On a Linux system, you must log in using the **root** user name and privilege.
- On Linux systems, run Dynamic System Analysis from a journaling file system (such as ext3 or ReiserFS). You cannot run these commands from a virtual machine file system (VMFS).

Chapter 2. Installing Lenovo Dynamic System Analysis

This section provides information about hardware and software requirements and instructions for downloading and installing Dynamic System Analysis on removable media.

Hardware and software requirements

Dynamic System Analysis has specific requirements for hardware and software. These requirements include support for certain supported operating systems and hardware requirements for running Dynamic System Analysis.

Hardware requirements

To successfully run Dynamic System Analysis, the system on which you install Dynamic System Analysis must meet certain hardware requirements.

Disk space requirements

To install Dynamic System Analysis, the system must have 100 MB of disk space.

Memory requirements

It is recommended that DSA Preboot Edition run on a system with more than 1 GB physical memory.

The amount of memory required for running Dynamic System Analysis depends on the size of the logs being collected from a system and viewed. To display the DSA data, systems must have 30 MB to 100 MB of available memory.

The following list provides minimum physical memory requirements based on the operating system:

- Microsoft Windows requires 256 MB or more
- Linux requires 512 MB or more

ServeRAID requirements

Dynamic System Analysis can collect ServeRAID log information from ServeRAID Manager 6.10 and later. Dynamic System Analysis cannot collect information from the following ServeRAID controllers unless ServeRAID Manager is installed:

- ServeRAID-7t SATA RAID
- ServeRAID-8i
- ServeRAID-8k
- ServeRAID-8k-l
- ServeRAID-8s

Service processor requirements

Environmental data is available only on System x servers that have either an Integrated System Management Processor (ISMP), a Remote Supervisor Adapter (RSA) series service processor, or an Integrated Management Module (IMM).

Supported hardware

Use this information to identify various systems and storage products that are supported by Dynamic System Analysis.

Supported Intel and AMD processor-based systems

You can run diagnostic tests and collect system information for the following Intel and AMD processor-based systems using Dynamic System Analysis:

Table 1. Supported systems

Server	Machine type
IBM BladeCenter HS23	1929, 7875
IBM BladeCenter HS23E	8038, 8039
IBM Flex System x220 Compute Node	2585, 7906
IBM Flex System x222 Compute Node	7916
IBM Flex System x240 Compute Node	7863, 8737, 8738, 8956
IBM Flex System x280 X6/x480 X6/x880 X6	4259, 7903
IBM Flex System x440	7917
IBM iDataPlex dx360 M4 server	7912, 7913
IBM iDataPlex dx360 M4 Water Cooled server	7918, 7919
IBM NeXtScale nx360 M4	5455, 5465
IBM System x3100 M4	2582
IBM System x3100 M5	5457
IBM System x3250 M4	2583
IBM System x3250 M5	5458
IBM System x3300 M4	7382
IBM System x3500 M4	7383
IBM System x3530 M4	7160
IBM System x3550 M4	7914,
IBM System x3630 M4	7158, 7159
IBM System x3650 M4	7915
IBM System x3650 M4 BD	5466
IBM System x3650 M4 HD	5460
IBM System x3750 M4	8718, 8722, 8733, 8752
IBM System x3850 X6/x3950 X6	3837, 3839

The systems listed in the above table are supported by Portable DSA.

Supported storage

DSA does not run directly on an external storage device. DSA collects system information and runs diagnostic tests on the following storage devices:

- IBM System StorageDS4000 family
- IBM System StorageDS8000 family

Supported server options

• Ethernet adapters

- Broadcom 1 Gb 4 port Mezzanine Card Tier 1
- Broadcom 1 Gb Ethernet CFFh Expansion Card
- Broadcom 1 Gb 2-port Ethernet Mezzanine Card
- Broadcom 10 Gb Ethernet CFFh Expansion Card for IBM BladeCenter
- Broadcom Dual Port 10 GB SFP + Adapter
- Broadcom Dual Port 10 GB SFP + Ethernet Card
- Broadcom Dual Port 10 GbE SFP+ Embedded Adapter
- Broadcom Dualrunner/Quadrunner NetXtreme I
- Broadcom NetXtreme II
- Broadcom NetXtreme Dual_Port 10 GbE BaseT Adapter for IBM System x
- Emulex 2-Port 10 Gb Multi-function IO Adapter (CFFh) for IBM BladeCenter (vNIC)
- Emulex 2+2 10 Gb (CFFh) for IBM BladeCenter (vNIC)
- Emulex 10 GbE vNIC w/ BE3 Chipset
- Emulex Dual Port 10 GBase-T Embedded Adapter for IBM System x
- Emulex Dual Port 10 GbE SFP+ Embedded Adapter for IBM System x
- Emulex Dual Port 10 GbE SFP+ Embedded Adapter BE3R for IBM System x
- Emulex Dual Port 10 GbE SFP+ VFA II for IBM BladeCenter HS23
- Emulex Dual Port 10 GbE SFP+ VFA III for IBM System x
- Emulex x ITE-Blacktip onboard NIC for Flex
- Flex System 4-port 10 GB Ethernet Adapter
- Flex System CN4024 4-port 10 Gb Ethernet Adapter
- Flex System CN4054 10 Gb Virtual Fabric Adapter
- Flex System CN4058 Virtual Fabric Adapter FCoE Upgrade
- Flex System EN4052 2-port 10 Gbit Ethernet Adapter
- Flex System EN4172 2-port 10 Gb Ethernet Adapter
- IBM NetXtreme II 1000 Express Ethernet Adapter
- Intel 10 GB SFP+ NIC
- Intel I350-T2 Dual Port GbE Adapter
- Intel I350-T4 Dual Port GbE Adapter
- Intel I350-F1 Single Port Fiber GbE Adapter
- Intel P3600 2.5 PCIe NVMe SSD Flash Drive (400G/800G/1.6T/2T)
- Intel S3500 Wolfsville 1.2 / 1.6TB SSDs
- Intel X520-DA2 Dual Port 10 GbE SFP+ Adapter for IBM System x
- Intel X520 Dual Port 10 GbE SFP+ Embedded Adapter
- Intel X540 Dual Port 10 GBaseT Embedded Adapter
- Intel X710 2x10GbE SFP+ Adapter for IBM System x
- Intel X710 ML2 4x10GbE SFP+ Adapter for IBM System x
- Intel Xeon Phi 3120A
- Intel Xeon Phi 5110P
- Intel Xeon Phi 7120A
- Intel Xeon Phi 7120P
- Mellanox 2x 10 GbE SFP+ ConnectX-2LowLatency, RDMA
- Mellanox 2xFDR10 ConnectX3 Adapter
- Mellanox 2-port 40 Gb Ethernet Adapter for Flex System EN6132
- Mellanox 2-port FRD Infiniband Adapter for Flex System IB6132 (Malaya-x)
- Mellanox 10 Gb 2-port Ethernet Adapter for Flex System EN4132
- Mellanox 10 Gb 2-port Ethernet Expansion Card
- Mellanox 10 GB Ethernet Mezzanine Card (x-only) Tier 2 (Malaya-xnet)
- Mellanox ConnectX-3 10 GbE Adapter
- Mellanox ConnectX-2 Dual Port 10 GbE Adapter
- Mellanox ConnectX-2 Dual Port 10 GbE Adapter for IBM System x
- Mellanox ConnectX-3 Dual Port 40 GbE Adapter
- Mellanox ConnectX-3 Dual Port PCI-E 2.0 Mezzanine

- Mellanox ConnectX-3 Dual Port QSFP FDR 10 IB Adapter
- Mellanox ConnectX-3 Dual Port QDR/FDR10 Mezzanine Card
- Mellanox ConnectX-3 FDR VPI IB/E Adapter
- Mellanox ConnectX-3 FDR14 Mezzanine Card
- Mellanox ConnectX-3 Pro ML2 VPI FDR/10G/40G
- Mellanox FDR FDR IB Dual Port
- Mellanox QDR/FDR Mezzanine Card (x-only) Tier 2 (Malaya-x)
- QLogic 16 Gb FC HBA

Note: Mellanox options are only supported by portable DSA, not by preboot Dynamic System Analysis.

- **Graphics Processing units**

- NVIDIA Gemini Kepler GPU (K10)
- NVIDIA Quadro 2000, 4000, 5000, 6000, 600, 5000 update
- NVIDIA Telsa K8
- NVIDIA Telsa K10
- NVIDIA Tesla K80 (Stella Duo) GPU Accelerator
- NVIDIA Tesla K20, K20C, K20X
- NVIDIA Tesla K40m
- NVIDIA Quadro K420, K620
- NVIDIA Quadro K600, K2000, K4000, K5000, 6000
- NVIDIA Quadro K2200, K4200, K5200
- NVIDIA Tesla M2090, M2090 update, X2090, X2090 update
- NVIDIA Tesla Stella Duo GPU Accelerator
- NVIDIA VGX K1, K2

- **Fibre Channel adapters**

- Brocade 4 Gb FC Dual-port HBA
- Brocade 4 Gb FC Single-port HBA
- Brocade 8 Gb FC Dual-port HBA
- Brocade 8 Gb FC Single-port HBA
- Brocade 10 Gb CNA
- Brocade 16 Gb FC Dual-port Mezz
- Brocade 16 Gb FC Quad Port
- Brocade 16 Gb FC Single/Dual-port HBA
- Diablo IBM 200 GB SATA MLC Flash DIMM 00FE001
- Diablo IBM 400 GB SATA MLC Flash DIMM 00FE005
- Emulex 2-Port 10 Gb Multi-function IO Adapter
- Emulex 2-port 16 Gb FC Adapter for Flex System FC5052
- Emulex 4-port 16 Gb FC Adapter for Flex System FC5054
- Emulex 4G FC exp. card
- Emulex 4 Gb/s FC PCI Express HBA (lpe11000/lpe11002)
- Emulex 4 Gb/s FC PCI-X 2.0 HBA (lp11000/lp11002)
- Emulex 4G SFF FC exp
- Emulex 8 Gb FC Dual-port HBA for IBM System x
- Emulex 8 Gb FC Mezz card
- Emulex 8 Gb FC Single-port HBA for IBM System x
- Emulex 10 Gb/s Fibre Channel over Ethernet Dual Channel Converged Network Adapter
- Emulex 10 Gb 4-port Mezz card w/ Fcoe/iSCSI key (Wildcat) for System X Tier 1
- Emulex 10 Gb Dual Port Ethernet Mezzanine Card
- Emulex 10 GbE Virtual Fabric Adapter 5 Adv with Fcoe/iSCSI enabled
- Emulex 10 GbE Virtual Fabric Adapter 5 Lite for IBM System x
- Emulex 10 GbE Virtual Fabric Adapter 5 Plus for IBM System x
- Emulex 10 GbE Virtual Fabric Adapter 5 Standard for IBM System x
- Emulex 16 Gb Fibre Channel Single/Dual-port HBA
- Emulex Dual Port 10 GbE SFP+ Embedded Adapter for IBM System x
- Emulex x ITE-Blacktip onboard NIC for Flex
- Emulex Nantahala onboard NIC OCI14104-U2-X
- Emulex PCI-e Gen 2.0 Dual Port 10 Gb NIC
- Endeavor III/Endeavor III Lite (vNIC2) using IBM FoD for FCoE Upgrade
- Flex System CN4058S 8-port 10Gb Virtual Fabric Adapter
- IBM SAS HBA controller

- Intel I350-F1 1xGbE Fiber Adapter for IBM System x
 - Intel I350-T2 2xGbE BaseT Adapter for IBM System x
 - Intel I350-T4 4xGbE BaseT Adapter for IBM System x
 - LSI 1068 SAS HBA
 - LSI 12Gb RoMB
 - LSI N2115 SAS/SATA HBA
 - LSI N2125 SAS/SATA HBA
 - LSI N2126 SAS/SATA HBA
 - LSI N2215 SAS/SATA HBA
 - QLogic 2-Gbps Fibre Channel HBA
 - QLogic 2-port 16 Gb FC Adapter for Flex System FC5172
 - QLogic 4G/8G FC CFF exp. card
 - QLogic 4G/8G FC dual port HBA
 - QLogic 4G/8G FC single port HBA
 - QLogic 4G/8G SFF FC exp. card
 - Qlogic 8 Gb FC 2 port Mezzanine card Tier 1 for Flex
 - QLogic 10 Gb ASIC Update
 - Qlogic 10 GbE CFFh DC
 - QLogic 10 Gb ASIC Update
 - Qlogic 10 Gb FCoE Dual Port
 - QLogic 16 Gb FC HBA
 - Qlogic 16 Gb Dual port FC Adapter for Flex System
 - Qlogic 8200 Dual Port 10GbE SFP+ Adapter
 - QLogic Dual Port 10 GbE SFP+ Embedded Adapter for IBM System x
 - QLogic iSCSI PCIe dual port HBA
 - QLogic iSCSI PCIe HBA
- **Network adapters**
 - IBM 10 GbE PCIe SR Server Adapter
 - IBM NetXtreme II 10 GigE Express Fiber SR Adapter
 - Intel PRO/1000 PT Dual Port Server Adapter (no diagnostic support)
 - Intel PRO/1000 PT Quad Port Server Adapter (no diagnostic support)
 - Intel PRO/1000 PF Server Adapter (no diagnostic support)
- **RAID adapters**
 - Adaptec IBM ServeRAID 6m
 - Adaptec IBM ServeRAID 6i +
 - Adaptec IBM ServeRAID 7k
 - Adaptec IBM ServeRAID 7t
 - Adaptec IBM ServeRAID 8i, 8k, 8k-l, and 8s
 - LSI BBC 6 Gb SAS RAID card
 - LSI Feature-on-Demand M1100 Upgrade
 - LSI IR 1078, 1064, 1064e, and 1068e
 - LSI M5016
 - LSI M5100 Feature-on-Demand RAID 5 cacheless, RAID 6
 - LSI M5100 Upgrades - Battery
 - LSI M5100 Upgrades - 1 GB Flash
 - LSI M5100 Upgrades - RAID 5 cacheless
 - LSI MegaRAID 8480
 - LSI MR 10is
 - LSI ServeRAID 0//10 FDE SAS-2 6 GB
 - LSI ServeRAID B5015
 - LSI ServeRAID C105
 - LSI ServeRAID F5110-200/800GB SAS/SATA Controller for IBM System x
 - LSI ServeRaid H1135 Controller
 - LSI ServeRAID M1015, M5014, M5015 and M5025

- LSI ServeRAID M1110
- LSI ServeRAID M1115 RAID SAS-2 6 Gb PCIe
- LSI ServeRAID M1200 Series Zero Cache/RAID 5 Upgrade for IBM Systems-FoD
- LSI ServeRAID M1215 SAS/SATA Controller for IBM System x+SPY
- LSI ServeRAID M5100 Performance Accelerator for IBM System x
- LSI ServeRAID M5100 Upgrade
- LSI ServeRAID M5100 Upgrade - 512MB Flash (P/N 81Y4484/81Y4484)
- LSI ServeRAID M5100 Upgrade - 512MB Flash (P/N 81Y4484/81Y4487)
- LSI ServeRAID M5110 RAID SAS-2.5 6 Gb
- LSI ServeRAID M5110e RAID SAS-2.5 6 Gb
- LSI ServeRAID M5115 SAS/SAT Controller
- LSI ServeRAID M5120 RAID SAS-2.5 6 Gb PCIe
- LSI ServeRaid M5200 4GB Flas/RAID 5 Upgrade for IBM System x
- LSI ServeRAID M5210 SAS/SATA Controller for IBM System x
- LSI ServeRAID MR 10i, 10ie, 10is, 10k and 10m
- LSI N2225 SAS/SATA HBA for IBM System x
- LSI N2226 SAS/SATA HBA for IBM System x
- LSI Shikra NGP Storage Mezzanine Expansion for Flex System
- LSI x ITE-Blacktip onboard RAID (LSI 2004) for Flex
- LSI x ITE-Nantahala - onboard RAID (LSI 3004)
- ServeRAID M5215 with 2B Flash Enablement
- ServeRAID M5225 SAS/SATA Controller for IBM System x
- **HDD**
 - 3.5' 7.2K SATA/SAS (NL 512E)
 - 2.5' 10K/15K/7.2K SATA/SAS (4KN/512E)
 - High Availability SD Daughter Card
 - Hitachi Sunset Cove +, 12Gbps SAS Gen3 HS & SS
 - Intel S3500 1.2TB/1.6TB SATA 2.5" MLC HS/SS/G3HS/G3SS EnterpriseValue SSD for IBM System x
- **Optical Storage**
 - IBM 8x 1.8" HS 12Gb SAS HDD Backplane
 - IBM 4x 2.5" HS 12Gb SAS HDD Backplane
- **Storage adapters**
 - Fusion IO 1.2TB High IOPS MLC Duo
 - Fusion IO 2.4TB High IOPS MLC Duo
 - Fusion IO 365 GB High IOPS MLC Mono Adapter
 - Fusion IO 640 GB High IOPS MLC Duo
 - Fusion IO 785 GB High IOPS MLC Mono Adapter
 - Hitachi 12Gbps SAS and SAS Self-Encrypting SSDs in 2.5" G3 Hot Swap and G3 Simple Swap Trays
 - IBM 12 Small Form Factor Disk Storage Module for BladeCenter S
 - IBM 200 GB SATA MLC Flash DIMM
 - LSI 300 GB MLC Option Bulk
 - LSI 300 GB SLC Option Bulk
 - LSI 600 GB MLC Option Bulk
 - LSI 800 GB MLC Option Bulk
- **Tape drives**
 - IBM DDS5 36/72 SATA

- IBM DDS5 36/72 SCSI
 - IBM DDS5 36/72 USB
 - IBM DDS6 80/160 USB
 - IBM External Tape Drive HH SAS LTO 6
 - IBM GoVault tape drive
 - IBM LTO2 FH 200/400 SCSI
 - IBM LTO2 HH 200/400 SCSI
 - IBM LTO3 FH 400/800 SCSI
 - IBM LTO3 HH 400/800 SAS
 - IBM LTO4 HH 400/800 SAS
 - IBM LTO5 HH 400/800 SAS
 - IBM HH LTO 6 SAS Tape Drive
 - IBM VS160 tape drive
 - Pompano: RDX USB 3.0 Docks
- **Daughter cards**
 - BPE-4
 - cKVM Daughter Card for IBM BladeCenter
 - Emulex Dual Port 10 GB SPF Ethernet Daughter Card
 - Intel Dual Port 10 GB-T Ethernet Daughter Card
 - LSI BR10i, BR10ie, BR10il
 - Quad Port 1G-T Ethernet Daughter Card

Software requirements

The information in this section describes the required software and supported Web browsers for Dynamic System Analysis.

Required device drivers

It is strongly recommended to have the appropriate service processor device drivers installed and running before running Dynamic System Analysis. This provides access to additional problem determination information, including the hardware event logs.

For systems equipped with a Baseboard Management Controller (BMC), the appropriate drivers are on the IPMI device driver and mapping layer. If the machine has a Remote Supervisor Adapter II (RSA II), use the Remote Supervisor Adapter Daemon. For all supported service processors including the older Remote Supervisor Adapter (RSA) or Integrated Systems Management Processor, you can download drivers from the [Lenovo Support website](http://datacentersupport.lenovo.com) page on the Web site at <http://datacentersupport.lenovo.com>.

The following list provides information about collecting device drivers, firmware level, and log data.

- To collect SCSI and USB device information (including diagnostics), the `sg` driver must be loaded. Run **lsmod** and verify that the `sg` driver is loaded before running Dynamic System Analysis. If it is not loaded, run **modprobe sg**.
- To collect Broadcom Ethernet firmware levels, the Broadcom NetXtreme Gigabit Ethernet drivers must be installed. The `tg3` driver that is provided by default in current Linux distributions does not export this information. These drivers are available for download from the support Web site at <http://www.lenovo.com/support>.
- To collect LSI Logic 1020/1030 SCSI Controller and RAID information, the `mptctl` driver must be loaded. Run **lsmod** and verify that the `mptctl` driver is loaded before running Dynamic System Analysis. If it is not loaded, run **modprobe mptctl**.
- To collect Emulex HBA information from a Linux system, the `emulex` driver and utility (`corekit`) must be installed. Run **lsmod** and verify that `lpfc` and `lpfcdfc` are loaded before running Dynamic System Analysis.

- To collect Service Processor logs, configuration, and environmental data, the appropriate Service Processor driver must be installed. These drivers are available for download from the support Web site at <http://www.lenovo.com/support>.
- (Linux only) To collect ServeRAID information for ServeRAID controller 7t, 8i, 8k-l, 8k, 8s on systems running Red Hat 5, libstdc++.so.5 must be installed.
- To collect Emulex FC HBA data, the Emulex utility (HBACmd) must be installed.
- To transfer data collections to the support site using sFTP (by default) or FTP, libcurl must be installed.
- To use the UpdateXpress comparison analysis feature, the system on which the analysis is performed must have an Internet connection. UpdateXpress versions 4.02 and later are supported.

Supported Network Virtual Teaming software

Dynamic System Analysis is supported for use with the following Network Virtual Teaming software:

- Linux Bonding version 2.6.1
- Linux Bonding version 2.6.0
- Linux Bonding version 2.4.1

Supported Web browsers

To view the information that is collected by DSA, you must use one of the following Web browsers.

- Internet Explorer 6.0 Service Pack 1 or later
- Mozilla 1.4.0 or later
- Firefox 1.04 or later

Supported operating systems

Dynamic System Analysis supports the following operating systems.

Microsoft Windows Server 2016 (except Nano)

Microsoft Windows Server 2012 Edition

Windows Server 2012
Windows Server 2012 R2

Microsoft Windows Server 2011 Editions

Windows Small Business Server 2011
Windows Small Business Server 2011 Essential

Microsoft Windows Server 2008 Editions

Windows Server 2008, Datacenter Edition (x86, x64)
Windows Server 2008, Enterprise Edition (x86, x64)
Windows Server 2008 Foundation
Windows Server 2008 HPC Edition
Windows Server 2008 R2
Windows Server 2008 R2 HPC Edition (x64, ROK)
Windows Server 2008 R2 SP1
Windows Server 2008, Standard Edition (x86, x64)
Windows Server 2008, Web Edition (x86, x64)
Windows Essential Business Server 2008 Premium Edition
Windows Essential Business Server 2008 Standard Edition

Microsoft Windows Preinstallation Environment

Windows Preinstallation Environment 3.0
Windows Preinstallation Environment 2.1

Red Hat Enterprise Linux

- Red Hat Enterprise Linux 7 Server (SP1) (x86 & x64)
- Red Hat Enterprise Linux 6 (Up to SP7) (x86, x64)
- Red Hat Enterprise Linux 5 (Up to SP10) (x86, x64)
- Red Hat Enterprise Linux 5 (Up to SP9) with Xen (x86, x64)
- Red Hat Enterprise Linux 4 (Up to SP9) (x86, x64)

SUSE Linux

- SUSE Linux Enterprise Server 12 (x64)
- SUSE Linux Enterprise Server 12 with Xen (x64)
- SUSE Linux Enterprise Server 11 (Up to SP4) (x86/x64)
- SUSE Linux Enterprise Server 11 with Xen (Up to SP4) (x86/x64)
- SUSE Linux Enterprise Server 10 (Up to SP4) (x86/x64)
- SUSE Linux Enterprise Server 10 with Xen (Up to SP4) (x86/x64)
- SUSE Linux Enterprise Real Time 10 (Up to SP4) (AMD64/EM64T)

VMware

- VMware vSphere 6.0 custom image
- VMware vSphere Hypervisor 5.5 (Up to U2)
- VMware vSphere 5.1 (Up to U3) custom image
- VMware vSphere Hypervisor 5.0 (ESX5) (Up to U3) is supported only through use of the --vmware-esxi option
- VMware ESX Server, 4.1 (Up to U3)
- IBM Customized Image 4.1 (Up to 4.1 U3) is supported only through use of the --vmware-esxi option
- VMware ESX Server 4.0 (Up to U3)
- IBM Customized Image 4.1 (Up to 4.0 U3) is supported only through use of the --vmware-esxi option

Installing Dynamic System Analysis on removable media

You can install Dynamic System Analysis on removable media, such as a CD, DVD, or a USB flash drive.

Important: Ensure that the removable media has enough free space available to contain Dynamic System Analysis. To view the hardware requirements for Dynamic System Analysis, refer to “Hardware requirements” on page 3.

Perform these steps to install Dynamic System Analysis on removable media:

- Step 1. Download the appropriate portable-edition package for the local operating system from the [Lenovo ToolsCenter DSA website](http://support.lenovo.com/us/en/documents/LNVO-DSA) Web site at: <http://support.lenovo.com/us/en/documents/LNVO-DSA>:
- `Invgy_utl_dsa_dsa_dsalxxx-10.x_portable_platform.exe` for Windows systems
 - `Invgy_utl_dsa_dsa_dsalxxx-10.x_portable_platform.bin` for Linux systems

where *installation_directory* is the path to the extracted installation files and *platform* is the supported operating system.

Step 2. Insert or mount the removable medium.

Step 3. Copy the portable-edition package to the removable media.

Chapter 3. Running diagnostic tests on a local system

The following steps describes how to run diagnostic tests on a local system using the Preboot Dynamic System Analysis GUI, the Preboot Edition command-line interface, and Dynamic System Analysis on removable media.

Select a diagnostic option and complete the steps for that option.

Preboot Edition GUI

1. Boot to the Dynamic System Analysis, either by booting to removable media or, for preinstalled Dynamic System Analysis, pressing **F2** to interrupt the boot sequence.
2. Select **Quit to DSA** to exit the standalone memory diagnostic program.

Note: After you exit the standalone memory diagnostic environment, you must restart the system before you can access this environment again.
3. Enter **gui** or select **Click here to start diagnostics (GUI)** to launch the Dynamic System Analysis graphical environment.
4. Click **I Accept** to accept the Preboot license.
5. Click **Customized Inventory Collection and Diagnosis**.
6. Select the desired Diagnostic items.
7. Click the cell in the **Test Loop** column to set loop counts for each individual test.
8. Click **OK** to start Diagnostics.
9. When the Diagnostics are finished, to display the Diagnostic details, click the button located under Diagnostic Tests in the navigation pane on the left.

Preboot Edition CLI

1. Boot to the Dynamic System Analysis, either by booting to removable media or, for preinstalled Dynamic System Analysis, pressing **F2** to interrupt the boot sequence.
2. Enter **cmd** or select **Click here to start diagnostics (CLI)** to launch the Dynamic System Analysis command environment.
3. From the menu to enter the interactive diagnostics environment, select **Diagnostics**. The options in this environment are:

Execute Diagnostic Tests

Executes the selected tests.

Get Diagnostic Extended Results

Displays the extended results of diagnostics tests that have already run.

4. When the tests are complete, enter **:x** to exit the menu.
5. Select the completed tests to view the results.

Dynamic System Analysis on removable media

1. Insert the media into the system, and if necessary, mount the removable media.
2. From a command line, change to the directory for the removable media.
3. Enter the following command to collect system information:
`lnvgy_utl_dsa_dsa_dsalxxx-10.x__portable_plaform -diags`
where the platform is the supported Linux distribution.

Chapter 4. Collecting system information

The topics in this section describe how to use Lenovo Dynamic System Analysis to collect system information and how to convert the collected data to another format.

Collecting system information on a local system using the Preboot Edition

The following procedure describes how to collect system information on a local system using the Preboot Dynamic System Analysis graphical user interface (GUI) and the Preboot Edition command-line interface (CLI).

Select a collection option and complete the steps for that option.

- **Preboot Edition GUI:**

1. Boot to the Dynamic System Analysis, either by booting to removable media or, for preinstalled Dynamic System Analysis, pressing **F2** to interrupt the boot sequence.
2. Select **Quit to DSA** to exit the standalone memory diagnostic program.

Note: After you exit the standalone memory diagnostic environment, you must restart the system before you can access this environment again.

3. Select **Click here to start diagnostics (GUI)** or enter **gui** from the command line to start the graphical user interface.
4. Click **I Accept** to accept the Preboot License.
5. Click **Full Inventory Collection and Diagnosis**.
6. By default inventory and diagnostic tests are performed. If you want to run only one of the two tests, you can deselect one. At least one test must be selected.
7. Select the actions to be performed after the data collection. If an Internet connection is available, you can choose to send the results to the IBM Web site. If you have the removable media available, you can choose to save the result to the removable media.
 - By default, diagnostic tests are performed. To skip the diagnostic tests, deselect **Run Diagnostic Test** and click **OK** to begin the collection process.
 - When the inventory is finished, the chosen actions will be performed automatically. To display the Inventory details, in the navigation pane, click **Full inventory file**.

- **Preboot Edition CLI:**

1. Boot to the Dynamic System Analysis, either by booting to removable media or, for preinstalled Dynamic System Analysis, press **F2** to interrupt the boot sequence.
2. Select **Diagnostics** from the navigation pane.
3. Click **Click here to start diagnostics (CLI)** or enter **cmd** from the command line to start the command-line interface.
4. Select the **Data Collection** option to open the data collection menu.
5. When the collection is finished, click **View collection results** to display the results.
6. When you are done, enter **:q** to exit the viewer.

Collecting system information on a local system using removable media

The following procedure describes how to collect system information on a local system using removable media.

- Step 1. Insert the media into the system, and if necessary, mount the removable media.
- Step 2. On a command line, change to the directory for the removable media.
- Step 3. Enter the following command to collect system information:
`lnvgy_utl_dsa__dsalxxx-10.x_portable_platform [-x] [-v] [-text]`

where the platform is the supported operating system.

This command creates compressed CIM-XML output by default. You can also create HTML output by specifying the `-v` option and ASCII text output by specifying the `-text` option. If you specify the `-x` option, compressed CIM-XML output is not created, and you must specify the `-v` or `-text` option, or both.

Collecting system information on a remote system running VMware ESXi

The following procedure describes how to collect system information on a remote system that is running the VMWare embedded hypervisor using removable media.

- The remote system running VMware must be accessible to the system running DSA.
- The system running DSA must have port 5989 open.

- Step 1. Download the latest release of the DSA tool for Windows or Linux, or copy the latest DSA tool to the media.
- Step 2. Boot the system.
- Step 3. Select **DHCP** or configure the IP address manually following VMWare instructions.
- Step 4. Complete these steps:
 - a. Insert the media into the system, and if necessary, mount the removable media.
 - b. From a command line, change to the directory for the latest version of the DSA tool.
 - c. Enter the following command to collect system information:
`lnvgy_utl_dsa__dsalxxx-10.x_portable_platform --vmware-esxi user_id:password@ip_address`

where the `user_id:password@ip_address` specifies the user ID, IP address, and port number to use for authentication with the hypervisor.

Note: Not all information is available using this method. Certain raw data, such as: LSI RAID, Emulex, and SSD raw data cannot be collected through ESXi. In this case, you have to reboot and use the built-in preboot DSA tool.

Collecting IMM information from a remote system

The following procedure describes how to collect Intelligent Management Module (IMM) information (IMM Configuration, xFW information, Environmental, Chassis Event Log, Lightpath, and IPMI Event log) from a remote system using out-of-band (OOB) mode with removable media.

- Step 1. Insert the media into the system, and if necessary, mount the removable media.
- Step 2. From a command line, change to the directory for the removable media.
- Step 3. Enter the following command to collect system information:
`lnvgy_utl_dsa_dsalxxx-10.x_portable_plaform --ipmi-lan system`

where *platform* is the supported operating system, and *system* is the remote system to which you want to collect IMM-related information. Specify the system using the following format: *user_id:password@ip_address[:port]*.

Converting collected data on a local system

The following procedure describes how to convert data collected on the local system to another format using removable media.

- Step 1. Insert the media into the system, and if necessary, mount the removable media.
- Step 2. On a command line, change to the directory for the removable media.
- Step 3. Enter the following command to collect system information:
`lnvgy_utl_dsa_dsalxxx-10.x_portable_platformdata_file [-v | -text]`

where:

- *platform* is the supported operating system
- *data_file* is the fully-qualified name of the compressed CIM-XML data file that you want to convert

Specify `-v` to convert the data to HTML format. Specify `-text` to convert the data to ASCII text format.

Chapter 5. Comparing system information

The topics in this section describe how you can use Dynamic System Analysis to compare collected system information.

Comparing firmware versions on a local system with the latest versions

The following procedure describes how to perform a comparison of the installed firmware versions on a local system to the latest versions of firmware available on the Web using removable media.

The local system must have Internet access.

Step 1. Insert the removable media into the system, and if necessary, mount the removable media.

Step 2. On a command line, change to the directory for the removable media.

Step 3. Enter the following command to collect system information:
`lnvgy_utl_dsa_dsa/xxx-10.x_portable_platform -ux [-x] [-v] [-text]`

where the platform is the supported operating system.

When the comparison is finished, the analysis is written to a compressed CIM-XML output file by default. You can also create HTML output by specifying the `-v` option and ASCII text output by specifying the `-text` option. If you specify the `-x` option, compressed CIM-XML output is not created, and you must specify the `-v` or `-text` option, or both.

Note: Internet access is required for the `-ux` option.

Comparing current system information to previously collected data

The following procedure describes how to collect system information a local system and then compare the current system information to one or more system information files that were previously collected.

Important: You can only compare system information that was collected using the same version of Dynamic System Analysis.

Step 1. Insert the media into the system, and if necessary, mount the removable media.

Step 2. From a command line, change to the directory for the removable media.

Step 3. Enter the following command to collect system information:
`lnvgy_utl_dsa_dsa/xxx-10.x_portable_plaform -r data_file -v`

where the platform is the supported operating system, and where *data_file* is the fully-qualified name of the system information file that you want to compare. Separate multiple data files using a space.

Comparing multiple system information files

The following procedure describes how to compare two or more system information files that were previously collected.

- Step 1. Insert the media into the system, and if necessary, mount the removable media.
- Step 2. From a command line, change to the directory for the removable media.
- Step 3. Enter the following command to compare system information:
`lnvgy_utl_dsa__dsalxxx-10.x_portable_platform -r data_file -v`

where the *platform* is the supported operating system, and where *data_file* is the fully-qualified name of the system information file that you want to compare. Separate multiple data files using a space.

If you specify the `-i` option, this command compares the specified data file against the data file specified by the `-r` option. If you do not specify the `-i` option, this command collects the current system information on the local system before comparing it against the data file specified by the `-r` option.

Chapter 6. Viewing collected system information

When you collect system information, Dynamic System Analysis saves the collected data in the specified output directory. If you do not specify a directory, Dynamic System Analysis stores the data files in the `c:\Lenovo_Support\` directory on Windows systems or `/var/log/Lenovo_Support/` directory on Linux systems by default.

The following list provides a description of how to view system information in various formats.

To view system information in HTML format:

If you specify the `-v` format option, the `lnvgy_util_dsa_v.r.m_portable_platform` command saves the data in HTML format. By default, Dynamic System Analysis creates a set of HTML files in a subdirectory named `outputdir/mtm_serialnumber_datetime`, where *outputdir* is the default or specified output directory, *mtm* is the machine type and model of the local system, *serialnumber* is the serial number of local system, and *datetime* is the date and time when data was collected.

To view the HTML file, open the `index.html` file in a web browser. The left pane contains links for each category of system information, and the right pane displays the related information.

To view system information in ASCII text format:

If you specify the `-text` format option, the `lnvgy_util_dsa_v.r.m_portable_platform` command saves the data in TXT format. To view the text file, use any text editor.

To view system information in XML format:

If you do not specify a format option, the `lnvgy_util_dsa_dsalxxx-10.x_portable_platform` command saves the data in XML format.

To view the XML file, decompress the XML file, and then open it using any text or XML editor.

To convert an XML file to HTML format for easier viewing, run the following command: `lnvgy_util_dsa_dsalxxx-10.x_portable_platform -v -x -i path/data_file.xml.gz`

where *path* is the fully qualified path and *data_file* is the name of the compressed XML file that was previously created by Dynamic System Analysis.

Chapter 7. Transferring data and logs

The topics in this section describe how to use Dynamic System Analysis to transfer data and logs to a remote system or to the Electronic Services web portal for use in the My Systems and My Notifications functions.

Transferring collected data to a remote system

The following procedure describes how to send collected data to IBM Service and Support or another remote system using File Transfer Protocol (FTP).

Select a transfer option and complete the steps for that option.

Preboot Edition CLI

1. Collect data using the command-line interface as described in “Collecting system information on a local system using the Preboot Edition” on page 15 and exit the viewer by typing **:q**.
2. Select **Quit to previous menu** to exit the interactive Data Collection menu.
3. From the numerical menu, select **Send System Information to IBM Server**. You will be prompted to customize the FTP server.
4. Enter **y** to customize the server information.
5. To use with your FTP server, enter the following credentials:
 - FTP address
 - Port number
 - User name
 - Password

Preboot Edition GUI

1. Boot to Dynamic System Analysis, either by booting to removable media or, for preinstalled Dynamic System Analysis, pressing **F2** to interrupt the boot sequence.
2. Select **Quit to DSA** to exit the standalone memory diagnostic program.

Note: After you exit the standalone memory diagnostic environment, you must restart the system before you can access this environment again.

3. Click **I Accept** to accept the Preboot license.
4. Click **Full Inventory Collection and Diagnosis**.
5. By default diagnostic tests are performed. To skip the diagnostic tests, click **Collect Inventory Only**.
6. Select **Send to IBM Website** to save the data automatically.
7. Click **OK** to begin the collection process.
8. When the inventory is complete, the results are sent to the IBM Web site automatically.

Dynamic System Analysis on removable media:

1. Insert the media into the system, and if necessary, mount the removable media.
2. On a command line, change to the directory for the removable media.
3. Enter the following command to collect system information:
`lnvgy_utl_dsa_dsalxxx-10.x_portable_plaform [-v] [-t] system`
where the *platform* is the supported Linux distribution, and *system* is the remote system to which you want to transfer files, specified using the following format: *user_id:password@ip_address[:port]/path/*. If you do not specify a system, the data file is sent to IBM.

Note: Port 21 must be enabled for access through the firewall to transfer logs.

Transferring collected data to the customer inventory repository

The following procedure describes how to transfer data from the local system to the customer inventory repository.

The local system must have Internet access to transfer the data file, and Port 443 must be enabled for traffic through your firewall.

- Step 1. Insert the media into the system, and if necessary, mount the removable media.
- Step 2. On a command line, change to the directory for the removable media.
- Step 3. Enter the following command to collect system information and transfer the system information file:
`lnvgy_utl_dsa_dsalxxx-10.x_portable_platform -upload [-IBMid:user_id]`

where

- *platform* is the supported operating system
- *user_id* is your IBM user ID

Note: If you do not specify **-IBMid**, you will be prompted for your user ID. Dynamic System Analysis verifies the IBM ID and if it is valid, adds it to the data file. If the ID is not valid, or no ID is specified, the data file is transferred, but the ID is not included.

Chapter 8. Copying data and logs

The following procedure describes how to use Dynamic System Analysis to collect system information and copy the collected data to a USB device.

- Step 1. When collection process completes, click **Collection and Diagnosis**.
- Step 2. Click **Save to** to open the Save to Removable Media page.
- Step 3. Select the desired USB device and click **OK**.

Chapter 9. Supporting Dynamic System Analysis Features on Demand

DSA supports FoD on Portable DSA, CD-based Preboot DSA, and GUI-based Preboot DSA. The topics in this section provide detailed information about how DSA supports FoD.

Using Features on Demand for Portable Dynamic System Analysis

The topics in this section describe how to download, install and use the FoD Key for Portable Dynamic System Analysis.

Downloading the FoD key and installing with the key file

The following procedure describes how to download the FoD key and install the key file using removable media.

The following prerequisites are necessary for this task:

- The DSA Portable Edition is available on a removable medium (for example, a CD-ROM or a USB key) as a self-extracting file.
- You can be logged into the system as administrator, root, or as another user with equivalent privileges.
- DSA can connect to an external network. The command **download_fod_key** requires Internet access.

All of the FoD operations use the FoD application option and applicable subcommands. For more information, see *Appendix B: “DSA FoD CLI switches”* on page 62.

Step 1. Insert the removable medium with DSA Portable Edition into the machine.

Step 2. Start the DSA Portable Edition executable on the removable medium.

Step 3. Enter the following command and parameters to download and generate a specific FoD key file from KMS:

```
DSA fod download_fod_key --ibmid <userid:password>  
--uid <unique_id> | --authcode <code> | --mt <machinetype>
```

Step 4. Enter the following command and parameters to install the specified key file to a specific key repository:

```
DSA fod install_fod_key --keyfile <keyfile> |  
--device <device> | --host <[http(s)://[userid:password]@hostip:[port]> |  
--tftp <[userid:password]@ip:[port]> | --tftp <[userid:password]@ip:[port]> |  
--community <community> | --authproto <authproto> | --privproto <DES/AES> |  
--privpasswd <password>
```

The definitions of the parameters are:

--keyfile <keyfile>

The FoD Key(s) file name.

--device <device>

The type of key repository (IMM, CMM, or Switch).

--host <[http(s)://[userid:password]@hostip:[port]>

This option is used for the remote activation key repository.

If the **--host** parameter is not used, the default host is the local IMM.

http or *https* is used for the CIM connection, and if it is not stated, the default for this CIM connection is *https*.

User ID and Password is required for the device interface connection.
For Switch, the User ID and Password is auth info for SNMPv3.
Port is used for the CIM interface, and the default is 598.

- tftp <ip:[port]>
The TFTP server for the Switch SNMP interface.
- community <community>
The community for SNMPv1 and SNMPv2.
- authproto <authproto>
Authorization protocol for SNMPv3; default: No auth.
- privproto <DES/AES>
Privacy protocol for SNMPv3, default: No privacy.
- privpasswd <password>
The privacy password for SNMPv3.

Note: For multi-node systems, FoD support is only available for the node with the IMM IP address specified.

Using the FoD Key on an IMM for a portable target system

The following procedure describes how to view the FoD information for a target system, and how to install or uninstall the FoD license key(s) using in-band (IB) or out-of-band (OOB) mode.

The following prerequisites are necessary for this task:

- The DSA Portable Edition is available on a removable medium (for example, a CD-ROM or a USB key) as a self-extracting file.
- The operating system on the target system is available for IB mode.
- The operating system on a laptop is available for OOB mode.
- DSA has Internet access. The commands **display_imm_available_fod** and **install_imm_fod** require Internet access.

Step 1. Insert the removable medium with the DSA Portable Edition into the machine.

Step 2. Start the DSA Portable Edition executable on the removable medium.

Step 3. Enter the following command and parameters for DSA to get all of the available FoD features for the target system (IMM repository), and to display them in the console with their status:

```
DSA fod display_imm_available_fod --ibmid <userid:password>,  
--host <userid:password@hostip:[port]> |
```

Step 4. Enter the following command with no parameters and the unique identifier for specified FoD features on the local system. The FoD features are exported to the `dsa_fod_ids.txt` located in the DSA output folder. You can copy the FoD Identifier file to removable media such as a CD-ROM or a USB key.

```
DSA fod export_imm_unique_ids
```

Step 5. Enter the following command and parameters which indicate the remote key repository (IMM) and the default value for the local IMM device:

```
DSA fod report_imm_active_fod --host <[http(s)://userid:password@hostip:[port]>  
The active FoD feature(s) for the key repository are displayed in the console.
```

Step 6. Enter the following command and parameters to download specific keys for the corresponding FoD features from KMS that are installed on the target system (IMM repository).

```
DSA fod install_imm_fod --ibmid <userid:password>,  
--uid <unique_id>, --authcode <code>, --mt <machinetype>,  
--host <userid:password@hostip:[port]>
```

The definitions of these parameters are:

- ibmid <userid:password>
The KMS ID credential for the Lenovo Web site.
- uid <unique_id>
The unique identifier information of the FoD feature.
- authcode <code>
Authentication code for FoD features.
- mt <machinetype>
The machine type of target system (IMM).
- host <[http(s)://userid:password@hostip:[port]]>
The remote key repository (IMM) and the default value for it is local IMM device.

Step 7. Enter the following command and parameters to uninstall the FoD key from the target system (IMM repository).

```
DSAfod uninstall_imm_fod --keyid <keyid>  
--host <[http(s)://userid:password@hostip:[port]]>
```

The definitions of these parameters are:

- keyid<Keyid>
This is obtained from the command `DSAfod report_imm_active_fod`.
- host <[http(s)://userid:password@hostip:[port]]>
The remote key repository (IMM) and the default value for it is local IMM device.

Note: For multi-node systems, FoD support is only available for the node with the IMM IP address specified. The parameter **--host <userid:password@hostip:[port]>** is the authorization information for the remote key repository (IMM). If this parameter is not specified, the local IMM device is applied. The default value of the IMM port is 5989.

If DSA fails to connect to the Baseboard Management Controller (BMC), the following error message is displayed: Failed to connect BMC, Error code = **.

Using the FoD Key on a CMM for a portable target system

The following procedure describes how to display the FoD information of the target system, and how to install or uninstall the FoD license key(s) using out-of-band (OOB) mode.

The following prerequisites are necessary for this task:

- The DSA Portable Edition is available on a removable medium (for example, a CD-ROM or a USB key) as a self-extracting file.
- The operating system on a laptop is available for OOB mode.
- DSA has Internet access. The commands `report_cmm_active_fod`, `install_cmm_fod`, and `uninstall_cmm_fod` require Internet access.

Step 1. Insert the removable medium with DSA Portable Edition into the laptop.

Step 2. Start the DSA Portable Edition executable on the removable medium.

Step 3. Enter the following command and parameters that indicate the remote key repository (CMM) and the default value for its local CMM device:

```
DSA fod report_cmm_active_fod --host <userid:password@hostip:[port]  
The active FoD feature(s) for the key repository are displayed in the console.
```

- Step 4. Enter the following command and parameters to download specific keys for corresponding FoD features from KMS and installed on the target system (CMM repository):

```
DSA fod install_cmm_fod --ibmid <userid:password> |  
--uid <unique_id> | --authcode <code> | --mt <machinetype> |  
--host <[http(s)://userid:password@hostip:[port]]>
```

The definitions of the parameters are:

```
--ibmid <userid:password>  
    The KMS ID credential for the Lenovo Web site.  
--uid <unique_id>  
    The unique identifier information of the FoD feature.  
--authcode <code>  
    Authentication code for FoD features.  
--mt <machinetype>  
    The machine type of target device (CMM).  
--host <[http(s)://userid:password@hostip:[port]]>  
    The remote key repository (CMM).
```

- Step 5. Enter the following command and parameters to uninstall the FoD key from the target system (CMM repository):

```
DSA fod uninstall_cmm_fod --keyid <keyid> |  
--host <[http(s)://userid:password@hostip:[port]]>
```

The definitions of the parameters are:

```
--keyid<Keyid>  
    This is obtained from the command DSAfod_report_cmm_active_fod.  
--host <[http(s)://userid:password@hostip:[port]]>  
    The remote key repository (CMM) and the default value for its local CMM device.
```

Note: The parameter `--host <[http(s)://userid:password@hostip:[port]]>` is the authorization information for the remote key repository (CMM). http or https is the cim interface; the default is https. User ID, Password is for the device interface connection. The default value of CMM port is 5989.

If DSA fails to connect to CMM, the following error message is displayed: Failed to connect CMM, Error code = **.

Using the FoD Key on an IOM/Switch for a portable target system

The following procedure describes how to display the FoD information of the target system, and how to install or uninstall the FoD license key(s) using in-band (IB) or out-of-band (OOB) mode.

The following prerequisites are necessary for this task:

- The DSA Portable Edition is available on a removable medium (for example, a CD-ROM or a USB key) as a self-extracting file.
- The operating system on a laptop is available for OOB mode.
- DSA has internet access. The commands **report_switch_active_fod**, **install_switch_fod**, and **uninstall_switch_fod** require Internet access.

Step 1. Insert the removable medium with DSA Portable Edition into the laptop.

Step 2. Start the DSA Portable Edition executable on the removable medium.

Step 3. Enter the following command and parameters that indicate the remote key repository (Switch) and the default value for its local Switch device.

```
DSA fod report_switch_active_fod --host <userid:password@hostip:[port]> |  
--tftp <userid:password@ip:[port]> | [--community <community>] |  
[--authproto<MD5/SHA>] | [--privpasswd <password>]
```

The definitions of the parameters are:

```
--host <userid:password@hostip:[port]>  
    The remote key repository (Switch).  
  
--tftp <ip:[port]>  
    The TFTP server for Switch SNMP interface.  
  
--community <community>  
    The community for SNMPv1 and SNMPv2.  
  
--authproto<MD5/SHA>  
    Authorization protocol for SNMPv3.  
  
--privpasswd <password>  
    The privacy password for SNMPv3.
```

The active FoD feature(s) for the key repository are displayed in the console.

Step 4. Enter the following command and parameters to download specific keys for corresponding FoD features from KMS and installed on the target system (Switch repository):

```
DSA fod install_switch_fod --ibmid <userid:password> |  
--uid <unique_id> | --authcode <code> | --mt <machinetype> |  
--host <userid:password@hostip:[port]> | --tftp <ip:[port]> |  
--community <community> | --authproto<MD5/SHA> | --privproto <DES/AES> |  
--privpasswd <password>
```

The definitions of the parameters are:

```
--ibmid <userid:password>  
    The KMS ID credential for the Lenovo Web site.  
  
--uid <unique_id>  
    The unique identifier information of the FoD feature.  
  
--authcode <code>  
    Authentication code for FoD features.
```

- mt <machinetype>
The machine type of target system (Switch).
- host <userid:password@hostip:[port]>
The remote key repository (Switch).
- tftp <ip:[port]>
The TFTP server for Switch SNMP interface.
- community <community>
The community for SNMPv1 and SNMPv2.
- authproto<MD5/SHA>
Authorization protocol for SNMPv3.
- privproto <DES/AES>
The privacy protocol for SNMPv3; default is: No privacy.
- privpasswd <password>
The privacy password for SNMPv3.

Step 5. Enter the following command and parameters to uninstall the FoD key from the target system (Switch repository):

```
DSA fod uninstall_switch_fod --keyid <keyid> |
--host <userid:password@hostip:[port]> | --tftp <ip:[port]> |
[--community <community>] | [--authproto<MD5/SHA>] |
--privproto <DES/AES> | [--privpasswd <password>]
```

The definitions of the parameters are:

- keyid<Keyid>
This is obtained from the command *DSAfod_report_switch_active_fod*.
- host <userid:password@hostip:[port]>
The remote key repository.
- tftp] <ip:[port]>
The TFTP server for Switch SNMP interface.
- community <community>
The community for SNMPv1 and SNMPv2.
- authproto<MD5/SHA>
Authorization protocol for SNMPv3.
- privproto <DES/AES>
The privacy protocol for SNMPv3; default is: No privacy.
- privpasswd <password>
The privacy password for SNMPv3.

If DSA fails to connect to Switch, the following error message is displayed: Failed to connect Switch, Error code = **.

Using the Features on Demand GUI support for CD-based Preboot DSA

The following procedure describes how to view, install, uninstall, and export the FoD License Key on a machine or reactivate the existing FoD activation keys on a replaced planar using the GUI.

The following prerequisites are necessary for this task:

- The DSA Preboot Edition is available on CD-ROM.

- The BIOS settings have been modified to enable the CD-ROM as a startup device.

Step 1. After placing the DSA Preboot Edition CD-ROM in the CD tray, start or restart the system.

Step 2. Enter `memtest` to launch the standalone memory test. Otherwise, the BoMC GUI will launch by default.

The option to run the standalone memory diagnostic is displayed. If no selections are made, the quick memory test is executed and execution continues to the DSA command line environment.

Step 3. Select **Quit**.

Step 4. Select **Diagnostic** on the left and click **Click here to start diagnostics (GUI)** to start the diagnostics (GUI) for launching the graphical DSA environment.

Step 5. Select one of the following options.

Click **I Accept** to accept the license. The Welcome page is displayed.

Click **I don't Accept** to exit the preboot GUI.

Step 6. Select **Activation Key Management** in the navigation pane or from the top menu to open the Activation Key Management page.

There are six operations for Activation Key Management:

Refresh

Refreshes the activation key list.

Click **Refresh** to refresh the activation key list.

Export

Exports activation key information and installed activation keys to removable media.

1. Select one or more activation keys.
2. Click **Export**. The Export Activation Key List to Removable Media dialog box is displayed.
3. Select the removable media from the list and click **OK** to export the activation key information and installed activation keys to removable media.

Uninstall

Uninstalls selected, installed activation keys.

1. Select one or more activation keys.
2. Click **Uninstall**. The confirm dialog box is displayed. Select one of the following options:
 - Click **OK** to remove the selected keys.
 - Click **Cancel** to not remove the selected keys.

Install from Lenovo Web site

Install activation keys from the Lenovo Web site.

1. Verify the Internet connection is working.
2. Click **Install from Lenovo Website**. The Install Activation Key from Lenovo Web site dialog box opens for entering the User Credentials and Details for each key.
3. Enter the following information.
 - KMS ID
 - User Password
 - Unique ID
 - AuthCode (optional). Authcode is required when the activation key file has not been created yet.

4. Select one or more activation keys and click **Install Now**.
5. Installation of the activation keys is completed sequentially. If an install fails, an error icon is displayed. Hover the mouse over the error icon to view the error message.

Install from Removable Media

Install the activation keys from local removable media.

1. Click **Install from Removable Media**. The Install Activation Key from Removable Media dialog box is displayed.
2. Select one of the removable media. The activation key files on the removable media are displayed.
3. Select one or more of the activation key files and click the **OK**.
4. Install the selected activation key files one by one. If an install fails, an error icon is displayed. Hover the mouse over the error icon to view the error message.

Reactivate Activation Keys

Reactivates inactive activation keys.

1. Click **Reactivate Activation Keys**. The Reactivate Activation Keys dialog box is displayed. The first step is to check machine information.
2. If any of the information displayed for the machine type, machine model, or serial number needs to be updated, make the applicable changes.
3. Click **Update Machine Info** to update the modified Vital Product Information (VPD). After the VPD has updated successfully, a dialog box is displayed confirming the VPD has been updated.
4. Click **OK** to reboot the IMM automatically or click **Cancel** to reboot IMM manually at another time.
5. If you chose to reboot IMM immediately, click **Next** to obtain the activation keys from the removable media.
6. There are two methods for obtaining the activations keys. Select one of the following methods. The default method is **From the Lenovo website**.

From Lenovo website

Obtain activation keys from the Lenovo Web site.

Enter the following information:

- KMS ID
- User Password

From removable media

Obtain activation keys from available removable media.

7. Click **Next** to obtain the activation keys from the removable media. After all of the selected activation keys are activated using one of the above methods, the reactivation results are displayed. If the reactivation fails, an error message is displayed in the status field.

Using Features on Demand GUI support for Embedded Preboot DSA

The following procedure describes how to view, install, and uninstall the FoD License Key on a machine or reactivate the existing FoD activation keys on a replaced planar using the GUI.

Ensure that the DSA Preboot Edition is available on an embedded USB key.

Step 1. Press **F2** during the system boot to enter the diagnostic environment. The option to run the standalone memory diagnostic is displayed. If no selections are made, the quick memory test is executed and execution continues to the DSA command line environment.

Step 2. Select **Quit**.

The standalone memory diagnostic does not support all systems. If the machine type is not supported, the **F2** boot skips the standalone memory test. No error message is displayed.

This option stops the memory test and returns you to the DSA command-line environment.

Step 3. Type `gui` to launch the graphical DSA environment.

Step 4. Select one of the following options.

Click **I Accept** to accept the license. The Welcome page is displayed.

If you do not want to accept the license, click **I don't Accept** to exit the preboot GUI.

- Step 5. Select **Activation Key Management** in the navigation pane or from the top menu to open the Activation Key Management page.

There are six operations for Activation Key Management:

Refresh

Refreshes the activation key list.

Click **Refresh** to refresh the activation key list.

Export

Exports activation key information and installed activation keys to removable media.

Complete the following steps.

1. Select one or more activation keys.
2. Click **Export**. The Export Activation Key List to Removable Media dialog box is displayed.
3. From the drop down menu, select the removable media and click **OK** to export the activation key information and installed activation keys to the removable media.

Uninstall

Uninstall the selected installed activation keys.

Complete the following steps.

1. Select one or more activation keys.
2. Click **Uninstall**. The confirm dialog box is displayed. Select one of the following options:
 - Click **OK** to uninstall the selected keys.
 - Click **Cancel** to cancel this operation.

Install from Lenovo Website

Install an activation key from the Lenovo Web site.

Complete the following steps.

1. Verify the internet connection is working.
2. Select one or more activation keys.
3. Click **Install from Lenovo Website**. The Install Activation Key from Lenovo website dialog box is displayed for entering the User credentials and Details for each key.
4. Enter the following information.
 - KMS ID
 - User Password
 - Unique ID
 - AuthCode (optional). AuthCode is required when the activation key file was not created yet.
5. Select one or more activation keys and click **Install Now**.
6. The installation of the activation keys is sequential. If an install fails, an error icon is displayed after the status information. If you hover the mouse over the error icon, the error message is displayed.

Install from Removable Media

Install the activation keys from the local removable media.

Complete the following steps.

1. Click **Install from Removable Media**. The Install Activation Key from Removable Media dialog box is displayed.
2. Select one of the removable media. The activation key files in the removable media are displayed.

3. Select one or more of the activation key files and click the **OK**.
4. The installation of the activation keys is sequential. If an install fails, an error icon is displayed after the status information. If you hover the mouse over the error icon, the error message is displayed.

Reactivate Activation Keys

Reactivates inactive activation keys.

Complete the following steps.

1. Click **Reactivate Activation Keys**. The Reactivate Activation Keys dialog box is displayed. The first step is to check machine information.
2. If any of the information displayed for machine type, machine model, or serial number needs to be updated, make the applicable changes.
3. Click **Update Machine Info** to update the modified Vital Product Information (VPD). After the VPD has updated successfully, a dialog box is displayed confirming the VPD has been updated.
4. Click **OK** to reboot the IMM automatically or click **Cancel** to reboot IMM manually at another time.
5. If you chose to reboot IMM immediately, click **Next** to obtain the activation keys from the removable media.
6. On the Obtain Keys page, there are two methods for obtaining the activations keys. Select one of the following methods. The default method is **From the Lenovo website**.

From Lenovo website

To obtain activation keys from the Lenovo Web site, perform the following steps.

- Enter the following information:
 - KMS ID
 - User Password
- Click **Next** to obtain the activation keys from the Lenovo Web site.

From removable media

All available removable media is detected.

7. Click **Next** to obtain the activation keys from the removable media.

After all of the selected activation keys are activated, the reactivation results are displayed. If a reactivation fails, an error message is displayed in the status field.

Chapter 10. Troubleshooting and support

Use this section to troubleshoot and resolve problems with LenovoDynamic System Analysis.

For solutions to problems that other customers have encountered, see the [System x Forum website](#) customer forum at [developerWorks Forums](#).

Known limitations, problems, and workarounds

Use this section to troubleshoot and resolve problems with Dynamic System Analysis.

Known limitations for the 10.4 release

The following list contains new limitations for the current release.

- Broadcom NX1 card cannot be updated with UpdateXpress System Pack Installer 9.X when both Broadcom NX1 card adapters and Broadcom NX2 card adapters are installed on your system.
- When the Intel Network Adapter is installed on your system, in the html report of the Preboot DSA, the firmware information of the Intel Adapter is not shown in the Firmware/VPD section.
- According to the design of Preboot DSA, in the html report of the Preboot DSA, the firmware information of the Intel Adapter is not shown in the Firmware/VPD section. For the new version of the Intel Adapters (for example, X710 family adapters), the VPD information might be shown in Other VPD table.
- When running the portable DSA on Red Hat Enterprise Linux 7, IMM related information will not be captured if the system has a bridge virtual network or if the USB LAN device name is not usb0.

User can remove the bridge virtual network, and modify the USB LAN device name to usb0. For example, if the USB LAN device is named as enpsxxxxx on Red Hat Enterprise Linux 7, users can modify the name property of `/etc/sysconfig/network-scripts/ifcfg-enpsxxxxx` to usb0. Then, rename the file name to `ifcfg-usb0` and add a new file `70-persistent-net.rules` to `/etc/udev/rules.d` with the content: `SUBSYSTEM=="net", ACTION=="add", DRIVERS=="*", ATTR{address}=="MAC address", ATTR { type } == "1", KERNEL=="eth*", NAME="usb0"`. Restart the system.

- The Preboot DSA diagnostic test does not include LAN card test item for Broadcom NX2 card. Use Preboot DSA 10.2 A8I to do the diagnostic test for the Broadcom NX2 card.
- For Preboot DSA, if Intel I340-T2 card and X540-T2 card are installed at the same time, "FIFO" item for Intel I340-T2 will be shown on the diagnostic test list. Ignore the "FIFO" item result.
- Most PCI device IRQs are 0 on the DSA inventory html page after running the DSA inventory command. In the Windows operating systems, use the Windows system tool named `msinfo32` to show the IRQs. In the Linux operating systems, use system command `lspci -b -vv` to show the IRQs.
- If a customer has an application using the "169.254.95.xx" network, the customer should use the `--no-imm-lan`.parameter to avoid changes to the network configuration (such as, to the routing table). Running portable DSA without this option will cause cluster applications, such as Oracle RAC, to crash unexpectedly.
- If you select nVidia diagnostic items and another diagnostic item with loop times greater than 1 in CMD mode, there is only one loop diagnostic log in DSA log.
- In the DSA report on the LSI Controller page, only the basic RAID level is shown. For example, RAID 00 is a subclass of RAID0, while RAID R1-EC is subclass of RAID 1, DSA only shows them as RAID 0 and RAID 1. This is because the LSI CIM provider cannot detect the exact configuration of the RAID class level of the subclass RAID level.
- DSA v10.1 has limited support for SLES12. The DSA report, lists only some of the links on the software panel, such as: system overview, network settings, resource utilization, processes, and os configuration.

The following information is missing: installed package, kernel modules, operating systems, timezone, linux config file, and current user.

- The DSA provider **networkinfo** does not implement the standard simple **get_instance** function, but instead implements the **enum_instance** function. Therefore, when you use the client with **gi**, the **get_instance** operation to get **IBMSG_BcmDeviceFirmwareElement**, it returns the **CIM_ERR_NOT_FOUND** error.
- The CD-based preboot DSA no longer supports the nVidia GPU diagnostic, because the new nVidia driver does not support the diagnostic any longer. If you want to run a diagnostic on nVidia Tesla series GPU, refer to the following link for a detailed user guide and diags tools that can be downloaded from: <https://www-947.ibm.com/support/entry/portal/docdisplay?Indocid=MIGR-5096046&brandind=5431802&myms=purflex&mync=R>
- In Preboot DSA GUI, after you select the **diags** item, you can input the loop count with 1-25, after you finish running all of the diagnostics in 25 loop with Emulex 10G options included, DSA only records the Diagnostics log once in the DSA Diagnostics Completion Log. The earlier diagnostics record will be erased.
- When using the GUI, if there are two ports of a machine trying to connect to the Extranet at the same time, the machine cannot send the DSA log to the IBM server. Click **Test Internet Connection** to resolve this problem.
- The Red Hat Enterprise Linux operating system does not support the "Merged Device" page inventory because there is no system command for querying this.
- The CPU and Memory stress test only supports 1 loop.
- Diablo Flash DIMM does not support win32, sles10, and sles10_64 because the vendor does not support these operating systems.
- In standalone mode, if a Single Bit Error (SBE) occurs, the system does not show an event log item in the chassis event log and ipmi event log page.
- On a multi-node server, if you customized the USB LAN ip settings, you need to ensure that the USB LAN IMM (was configured with the ASU tool or on the IMM remote page) and the Host ip (configured by the OS) has been configured properly. This allows the USB LAN host to ping to the IMM side ip successfully. If not, some IMM information (IMM Configuration, Enviromentals, Chassis Event Log) might be missed if it failed to configure the USB LAN.

The following list contains limitations that existed prior to the 10.4 release.

•

OpenSSL limitation on ESXi

OpenSSL on ESXi4.1, ESXi5.0, and ESXi5.1 supports only Transport Layer Security (TLS) level 1.0. If you set IMM TLS to a minimum level of 1.1 or 1.2, DSA fails to get the following information through the ESXi system:

- IMM Configuration
 - Environmentals
 - Chassis Event Log
 - Light Path
 - IMM, uEFI, and DSA firmware version
- Immv1 embedded Preboot DSA does not support any new drivers due to the limited image size.
 - The DSA TXT report has some format issues for the long text description. There may be some instances of ... in the TXT report. For more information refer to the HTML report.
 - The System Card Information table on the hardware inventory page for ESXi OS is missing the **Name** information due to an ESXi limitation.

- DSA version 3.4 does not support the VMware ESXi page report for the ESXi 5.x key due to a *vmvisor-offline-query* limitation.
- Due to a Brocade device driver limitation, SLES 11.2 and RHEL 5.8 do not support all of the Brocade functions.
- After running the LSI HDD diagnostic test when the Software RAID is configured, DSA displays No result or Aborted. DSA does not currently support this configuration.
- Due to a Mellanox provider limitation, Mellanox functions on a 32-bit operating system are not supported.
- On VMware ESXi, the following issue may be found: The memory type would be reported as Unknown in the Memory section of the Hardware Information report.
- Due to a Nvidia utility support limitation on a Windows 32-bit operating system in IBM Service, the Nvidia GPU Info link is not available (multi-tool only).
- Due to a QLogic device driver limitation for QLogic 10 Gb CNA, Option 42C1800, the QLogic information on the Hardware Inventory page is not collected on Windows 2008 Enterprise 64-bit operating system.
- Due to a QLogic utility limitation for QLogic 8 Gb FC Dual-port HBA, Option 42D0510, the QLogic information on the Hardware Inventory page is not collected on Red Hat Enterprise Linux 6 Update 2 (RHEL 6.2).
- Due to an LSI CIM provider issue, running DSA for data collection in a 2-node System x3850 takes many hours to complete on Microsoft Windows Small Business Server 2011.
- Due to an Emulex issue for a BladeCenter HS23, on the DSA data collection result page for PCI Information on the Hardware Inventory page, the Emulex 1 GB port is shown as a 10 GB port.
- Due to Windows API limitation, when configuring SATA HDDs without a RAID controller to a system with Windows 2008 R2, Web Edition 64-bit operating system, information for the Drive Health on the Hardware Inventory page is missing.
- Due to Windows API limitation, when configuring tape (with a USB connector) to a system with Windows 2008 R2, 64-bit operating system, information for the Drive Health on the Hardware Inventory page is missing.

Pre-existing limitations

- To ensure quality and stability of the DSA code, some display functionality of RAID information has been reverted to what was used in previous versions of DSA. This affects RAID display on the following adapters:
 - Megaraid 8480
 - Serveraid MR10i
 - Serveraid MR10is
 - Serveraid MR10m
 - Serveraid MR10k
 - Serveraid M1015
 - Serveraid M5014
 - Serveraid M5015

On these adapters, the RAID information is generated from the output of separate command-line tools and the format might not match other output in DSA.
- When an adapter is removed from the system that was previously configured in a network virtual team using the Intel PROSet software package, DSA may report that the adapter is still present with a corrupt MAC address. You can safely disregard the information returned for this adapter.
- On systems where the service processor clock does not have the same timezone settings as the local system, the merged log may appear to be out of order. The entries are sorted correctly but look incorrect because the timezone setting is not displayed.
- When DSA collects dates and times that are before January 1, 1970, 00:00:00, or after January 19, 2038, 03:14:07, DSA reports these dates and times as January 1, 1970, 00:00:00. These dates fall outside the valid range for a date in DSA.

- DSA may report the memory speed as **Unknown** in the Memory section of the Hardware Information report. This is due to issues with SMBIOS support on some systems.
- DSA collects Complex Programmable Logic Device (CPLD) firmware levels (Super I/O card firmware, PCI-X card firmware, CPU card firmware) on systems that have CPLD. The information about the individual CPLD firmware levels versus the CPLD package version on the web (for example, version 1.06) can be obtained in `ver_chk.txt`, which is located on each CPLD disk. The first column in this file is the SIO card CPLD version, the second column is the PCI-X card CPLD version, the third column is the CPU card CPLD version and the last column is the overall disk version number.
- The Intelligent Platform Management Interface (IPMI) device driver must be installed to collect IPMI BIST information.
- GoVault (part number 25R0006) is not recognized as a tape drive in DSA Diagnostics (version 2.02 and prior) and does not appear in the tape drive section of the HTML viewer. GoVault appears as a hard disk due to the hardware implementation and device driver. DSA can still recognize the device, but it is listed in the disk drive section.
- When you execute DSA with `-ux`, the ATI video driver comparison result in UpdateXpress may be downlevel. For example, Driver `ATI2MTAG.SYS` shows 6.14.10.6744 for the latest version. It should be 8.24.50. Refer to www.ibm.com for latest firmware and driver updates.
- Windows components cannot be collected in Windows 2008.
- Broadcom firmware information cannot be collected on System x3200M2 (4367/4368) on Windows 2008.
- Some SMART Attributes in Drive Health may be missing in iDataplex (7321/7322).
- DSA is unable to retrieve QLogic FC Controller from the HS22 blade. The QLogic `scli` utility cannot detect the card on HS22.
- QLogic iSCSI Controller info cannot be collected in Sles10 Realtime and Red Hat5 Realtime.
- For BladeCenter HS22 (7870/1936), iDataplex (7321/7322), System x3650 M2 (7947), and System x3550 M2 (7946), if the RNDIS driver is not installed in your system, environmental data and chassis event logs will not be collected. The RNDIS driver can be installed automatically when IMM firmware is updated in the OS. If you update IMM firmware from the IMM Web site, the RNDIS driver will not be installed on the OS. In this case, you must install the RNDIS driver manually, or the SP Configuration Chassis event log and environment data cannot be collected.
- The slot information for PCI-E/PCI adapters is blank in PCI information Section for Systems x3400/x3500 (7973/7974/7975/7976/7977), x3200M2 (4367/4368), x3250 M2 (4190/4191/4194), x3350 (4192/4193), and x3550M2 (7946/4198) on Windows 2008.
- LSI RAID configured as level "1E" will be recognized as level "1" in the DSA data collection.
- Due to Emulex issue for Blade System HS23, on the DSA data collection result page for PCI Information on the Hardware Inventory page, the Emulex 1 GB port is shown as a 10 GB port.
- The raw data of MegaRaid information can only be reviewed in HTML/XML output.
- In Windows, when a Broadcom Ethernet device is disabled in **Network Connections**, no relevant information regarding this device is collected.
- In Windows, ServeRaid 8e card information cannot be collected.
- On Systems x3550 or x3550 M2 when a dual port PCI NIC is plugged in, DSA shows one port as in use and the other port as on board in PCI device information. DSA sometimes does not show the IPv4 address & duplex status.
- When you use DSA Portable Edition (Windows) on Windows PreInstallation Environment (WinPE), the following information might be inaccurate, invalid or blank:
 - Current User
 - Installed Date (for application)
 - USB Hub Description
 - Onboard RAID controller

- Information related to Lan Over USB, such as IMM configuration, chassis events, and environmental information.
- On BladeCenter server, please ignore any information shown by DSA regarding Remote Supervisor Adapter (RSA).
- If IMM information is not collected, please check the RNDIS device network configuration. The IP address and subnet mask should be compliant with the IMM user guide description. Otherwise, no IMM configuration or environmental information is viewable and might be displayed as **SP Configuration**.
- When a server is configured with multiple RAID controllers (both IR & MR), the physical drive information associated with the IR might be invisible in **LSI Information**. This problem does not impact the functionality of the RAID or disk.
- This version of DSA does not support the ServeRAID B5015 SSD controller.
- When LSI IR ServeRAID is configured to RAID 1E, DSA might show the configuration as "10".
- When a disk is configured as RAID, DSA does not report a disk error upon spin speed reduction.
- When **--chkupd** or **--update** is used to acquire update packs for Dynamic System Analysis (DSA) and DSA is executed with the update pack, pay attention to the following usage:
 - When the message Unable to connect to internet is shown **--chkupd** or **--update**, sometimes it is due to the remote server being down and may not be an Internet connection problem.
 - Sometimes the NIC eth0 device is missing in the report generated for Brocade CNA.
 - Sometimes the description of port 1 of a Brocade FC HBA is missing.
 - When Brocade CNA is present, sometimes the firmware vital product data (VPD) and device ID information is not correctly shown.
 - DSA runs slowly when Brocade FC HBA or CNA is present on SLES10 or under Preboot DSA.
- On System x3850 X5 dual node configuration, DSA shows incorrect core numbers (always show one core) for processors on the 2nd node (CPU5-8).
- On System x3850 X5 Standard (7145, 7146) and BladeCenter HS22V (7871) with Windows 2008, the IMM Configuration, Environmentals, and Chassis Event Logs are missing in some cases. This information would be ready if the customer runs DSA again.
- The association between PCI Slot and Device might be inaccurate on the following systems:
 - System x3655 (7985, 7943)
 - System x3850 M2 (7141, 7144, 7233, 7234)
 - System x3850 X5 (7145, 7146)
 - System x3950 M2 (7141, 7233)
 - System x3950 X5 (7145, 7146)
 - System x3650 (7979, 1914)
 - BladeCenter HS12 (8014, 8028, 1916)
 - BladeCenter HS21 (8853, 1885)
 - BladeCenter HS22V (7871)
 - BladeCenter LS21/LS41 (7971, 7972)
 - BladeCenter LS22/LS42 (7901, 7902)
 - BladeCenter HX5 (7872, 1909)
- DSA can only detect the duplex speed information of one network adapter on RHEL5 U3 with Xen if multiple network adapters exist.
- After installing the chipset driver on Windows 2008 R2 SP1, you might receive a dialog box indicating IBMSPREM.EXE has stopped working.
- Broadcom Network cards firmware information cannot be determined in the WinPE environment.
- Some error logs intended for use by Support might display in DSA Error Log. These can be safely ignored.
- On the Windows 2008 SP2 64-bit operating system, when the device driver of a Broadcom HT1000 SATA controller is updated to the latest version (1.1.8049.1) on System x3455, it might cause unrecoverable

errors during a DSA run. You must exclude DSA providers (smart, tapehdd) with the command **set DSA_EXCLUDE=smart,tapehdd** before running DSA.

- When LSI RAID controller connects with SATA hard disk, DSA displays the manufacturer of hard disk as ATA in the Physical Drive Information table.
- The information about Level 1, 2, 3 Cache Enable might be inaccurate.
- If there is no data for a particular field, the field is blank. This is most often encountered in common tables containing instances from multiple data sources.
- On a Windows operating system when trying to run DSA with the option -upload through a proxy environment, you might need to turn off check for server certificate revocation (requires restart) from the **Tools → Internet Options → Advanced → Security** menu .
- When using DSA to collect the Brocade inventory, you might receive a warning message that the BCU and driver versions do not match and no Brocade information is collected. You can avoid this by updating the driver version 2.2.0.
- On a BladeCenter HX5 (7872,1909) multiple node system, only Diagnostic vital product data (VPD) for the primary node is shown in Diagnostic VPD table.
- The User Name is not available in the Current User table when running DSA with the parameter **--ipmi-lan**.
- Limited inventory is collected by DSA on the standard VMware ESXi image and the basic IBM customized VMware ESXi image.
- When an adapter is removed from the system that was previously configured in a network virtual team using the Intel PROSet software package, DSA might report that the adapter is still present with a corrupt MAC address. Disregard the information returned for this adapter.
- Window Components cannot be collected in Windows 2008.
- Broadcom Firmware information cannot be collected on a System x3200 M2 (4367/4368) running Windows 2008.
- For BladeCenter HS22 (7870/1936), iDataplex (7321/7322), System x3650 M2 (7947), and System x3550 M2 (7946), if the RNDIS driver is not installed in your system, environmental data and chassis event logs are not collected. The RNDIS driver can be installed automatically when IMM firmware is updated in the OS. However, if you update the IMM firmware using the IMM Web site, the RNDIS driver is not installed on the OS. In this case, you must install RNDIS manually to collect the System Package (SP) configuration, Chassis Event log, and Environment data.
- On a Windows 2008 operating system, the slot for PCI-E/PCI adapters is blank in the PCI information Section for the following System x machines: x3400/x3500 (7973/7974/7975/7976/7977), x3200 M2 (4367/4368), x3250 M2 (4190/4191/4194), x3350 (4192/4193), and x3550 M2 (7946/4198).
- In Windows, when Broadcom Ethernet Device is disabled in Network Connections, no relevant information regarding this device is collected.
- In Windows, ServeRaid 8e card information cannot be collected.
- For System x3250 M2, no Broadcom NIC firmware information is collected.
- For System x3550 or x3550 M2, when a dual port PCI NIC is plugged in, DSA shows one port is in use by another port, as on board in PCI device information. DSA sometimes does not show the IPv4 address & duplex.
- When you use DSA Portable Edition (Windows) on Windows Pre-Installation Environment (WinPE), the following information might be inaccurate, invalid or blank:
 - Current User
 - Installed Date (for application)
 - USB Hub Description
 - Onboard RAID controller
 - Information related to the IMM LAN Over USB, such as IMM configuration
 - Chassis events

– Environmentals

- If IMM information is not collected, check the RNDIS device network configuration. The IP address & subnet mask should be compliant with the IMM user guide description. Otherwise, no IMM configuration and environmental information is viewable and might be displayed as SP Configuration.
- When disk is configured as RAID, DSA does not report disk error upon spin speed reduction.
- On System x3850 X5 Standard (7145, 7146) and BladeCenter HS22V (7871) with Windows 2008, the IMM Configuration, Environmentals, and Chassis Event Log might be missing in some cases. You might be able to gather this information by running DSA again.
- After installing the chipset driver on Windows 2008 R2 SP1, a dialog box is opened to indicate IBMSPREM.EXE has stopped working.
- In Windows 2008, if the adapter event log of a MegaRAID controller is full, a dialog box appears and displays the message Megacli.exe has stopped. This error can be avoided by clearing the adapter event logs using the following command:
`MegaCli -AdpEventLog -Clear -ALL`
- Broadcom Network cards firmware information cannot be determined in a WinPE environment.
- In Windows, when trying to run DSA with the **-upload** option through a proxy environment. you might need to turn off **check for server certificate revocation (require restart)** from **Tools → Internet Options → Advanced → Security**.
- If you uninstall the USB Over LAN driver manually, it will cause the Preboot firmware update to fail.
- If the USB Memory Key you are using does not appear in the list of media available for copying to, you can upload the DSA output directly if the machine is connected to a network, or you can copy it to a floppy for upload later.
- While flashing Wflash on a newly installed Windows 2003 R2 system, a Windows dialog box stating: Do you want to restart your computer now? is displayed for each node being flashed. This occurs only for new installations.
- When DSA boots from a USB key, the disk partition size might be incorrect.
- The UpdateXpress section is not available with DSA Preboot.
- On iDataPlex dx360 M2, there is no ethernet NIC test available in the diagnostics list in Preboot DSA.
- When booting from the image created by BoMC, you can select **Diagnostics** and click **Gui option** to enter GUI mode. Select **Diagnostic test** to add NIC items to test. When the NIC is triggered with an error (such as removing the NIC), the TestLoopBackMAC test keeps checking status and displays Running. The diagnostics only applies to a NIC with a stable state (either normal or defective during test).
- When an error occurs to the hard disk drive during the HDD test, the test might complete and indicate: No Result. Diagnostics only apply to an HDD with a stable state (either normal or defective during test).
- When flashing DSA Preboot using Wflash or Lflash, if you notice a build mismatch error, make sure the IMM firmware level is a minimum of 29B. After you upgrade the IMM firmware to 29B or higher, DSA Preboot will continue to flash without error.
- DSA implemented signature in product build. This requires you to update IMM to 1A0034V or later before updating Preboot DSA, or a flash failure will occur.
- Under **Hardware Inventory → Video Controller information** there is no video controller information collected by the Preboot Edition.
- If you update Preboot DSA to DSA Preboot 3.0 with the file starting with oem_fw_dsynt, there is no way to roll back to the version of Preboot DSA before the update.
- When running DSA preboot, network interfaces load in the order they are detected by the operating system device driver. This can result in physical port 1 being labeled *eth0* in some cases, but it could also be labeled *eth1* or *eth2*, depending on the number of network adapters in the system. This is valid for onboard network controllers and network controllers.

- When a system is booted to DSA Preboot Edition with ServeRaid (M1015) SAS/SATA controller loaded, there might be no ServeRaid information collected.
- When Preboot DSA is booted from a CD/DVD, sometimes the CD/DVD is not automatically ejected (as expected) after you exit the DSA main menu. If this occurs, reboot the server and manually eject the CD/DVD ROM by pressing the button on the front panel for the optical drive.
- When running the Intel NIC test, there might be some redundant messages shown that are not relevant to the test result.
- On System x3400 M2 (7836, 7837) and x3500 M2 (7839), the SMART Error Logs table might be missing from the Drive Health page.
- ServeRAID (M1015) SAS/SATA Controller, 46M0831 require one of the following:
 - uEFI GYE133A or greater for Systems x3200 M3 and x3250 M3
 - uEFI Y4E145B or greater for Systems x3400 M2, x3400 M3, x3500 M2, and x3500 M3
 - uEFI D6E145C or greater for Systems x3550 M2, x3550 M3, x3650 M2, and x3650 M3
- On System x3250 M3 (4251, 4252, 4261), the firmware and BIOS version of the Emulex 10 GbE Virtual Fabric Adapter is missing on the Firmware VPD page.
- On BladeCenter HX5 (7872,1909) multi-node, only Diagnostic VPD for the primary node is shown in Diagnostic VPD table.
- An unexpected menu may pop up if you click the right mouse button during the initialization of the GUI. Wait for the GUI startup to complete before attempting to use the tool.
- You must disable the **x2apic** parameter in the uEFI settings before launching Embedded Preboot DSA on the System x3850 X5 dual node.
- Video controller information is missing from the Hardware Inventory page under Windows when running DSA from a remote desktop. To get this information, you must run DSA locally on the target system.
- If you encounter extended collection times, it might be helpful to disconnect external devices temporarily. This can include unplugging fibre cables or additional USB devices where information on these devices is not essential to the data collection.
- Having an excessive number of HDDs creates a situation where DSA is not actually hanging but rather takes days to complete.
- The FIFO test of NIC diagnostics is not supported on the Intel I350 and I340 Quad Port GbE.
- On VMware ESX 4.0u2, DSA displays the tape **IBM DDS GEN5** as **Virtual disk** in the **Hardware Inventory → System Devices** field due to an operating system limitation.
- On VMware ESX 4.1u2, due to operating system limitations, you must perform the following steps to complete tape diagnostics:
 1. Run this command to stop the usbarbitrator service: **/etc/init.d/usbarbitrator stop.**
 2. Disconnect and reconnect the USB key or disk device media.
 3. Run DSA tool to process tape diagnostic tests.
 4. After using the device, run this command to start the usbarbitrator service: **/etc/init.d/usbarbitrator start.**
- VMware 4.0u3 standard has the following issues:
 - Memory type returned as *Unknown* in the Memory section of the Hardware Information Report.
 - Redundant cache information is displayed in the Memory section of the Hardware Information Report.
- On Systems x3100 M4 and x3250 M4, you might encounter these issues:
 - The IMM configuration, Environmentals, and Chassis Event logs are reported as SP Configurations, BIST results , and SP Logs respectively.
 - Information on the IMM LAN Over USB, such as IMM configuration, chassis events, and environmental data, is missing.

- Powerville has shared FIFO and shared FIFO registers, making a test impossible if four ports are running at once.
- Online DSA displays *Unknown NIC* for **NIC Type** for the Intel NIC on the Network Settings page collected in Windows. Refer to Retain Tip: H203676.
- The description about the Intel Ethernet controller is displayed as Not Available on the Network Settings page under RHEL6.
- On VMware ESXi 4.0u3, you might encounter the following issues:
 - The memory type is reported as Unknown in the Memory section of the Hardware Information report.
 - Duplicate cache information is displayed in the Memory section of the Hardware Information report.
- On Systems x3100 M4, x3250 M4, and x3755 M3, you might encounter the following issues due to limitations of the IMM:
 - The IMM configuration, Environmentals, and Chassis Event logs are reported as SP Configurations, BIST results, and SP Logs respectively.
 - The IMM configuration and environmental information, such as IMM configuration, Environmentals, and Chassis Event Log, are not collected and displayed.
- On legacy BIOS and uEFI IMMv1 systems, PCI devices might miss the corresponding mappings of PCI slots due to limitations in SMBIOS 2.5.
- Portable DSA is displayed as *Unknown* in the item **PartitionSubType** in the Disk Information table on the Hardware Inventory page when the HDD is in the GUID Partition Table (GPT) format on uEFI systems.
- For Emulex options, the Emulex Bios version information on the Firmware"/VPD-BIOS/uEFI page and the Emulex EMXCNA BIOS page is not collected and shown due to the limitation of Emulex Utility.
- For reliable detection of IBM Linear Tape Open (LTO) tape devices on Windows operating systems, ensure that the tape device driver is installed in non-exclusive mode. For further details on this requirement, refer to the tape device driver documentation. Additionally, it may be necessary to stop backup related services to allow DSA to query the device.
- Preboot DSA embedded uses Customized Linux Kernel 5.2 for legacy systems. Preboot DSA standalone (CD boot or USB-key boot) uses Customized Linux Kernel 6.1 for all systems.
 - Preboot DSA (embedded or standalone) uses Customized Linux Kernel 6.1 and does not support the data collection on the QLogic adapter since the QLogic driver 1.01.02.d4 packaged in Customized Linux Kernel 5.2 cannot be used in Customized Linux Kernel 6.1.
 - The Software License Agreement (SLA) has traditional Chinese wording issue in Customized Linux Kernel 5.2. This issue is fixed in Customized Linux Kernel 6.1 in Preboot DSA 4.00 in 2011. However, those systems with Preboot DSA embedded based on Customized Linux Kernel 5.2 still have this issue.
- On VMware ESXi 5.0, the following issues may be found because the Emulex BE3 onboard card and the Robalo option card are not supported by VMware ESXi 5.0: The Name is reported as blank in the ELXUCNA Product section of the Emulex report.
- When installing the FoD key file(s) on CMM, Switch, or Remote IMM, you must ensure that the network connection is not affected by the following:
 - Http service
 - Firewall
 - Authorization
- When running FoD key management on the Compass Switch, the upgrade sequence (Key installation) must start from the first 32-port to the second 32-port, and use an inverse sequence for the downgrade (Key uninstallation), or the error message Firmware Version/Update Issue may be displayed.
- On RHEL6.x, the following issue may be found because the LSI CIM provider has limited support: The reported LSI Configuration in log file is different from other Operation Systems.
- When using DSA to collect the QLogic inventory, some redundant debug information may be included in the RAW data due to the limitation of the QLogic utility.

- On WinPE, when you run DSA with the **-upload** option through the proxy environment, the DSA output log file may not be uploaded due to a security reason. You may need to copy the DSA output log file to a removable media (such as a USB key) for further usage.
- On System x3500 M4, the following issues may be found under Windows 2008 due to the problem of uEFI SMBIOS Type 9: The **Slot** information in the Devices table on the CI Information page P shows *Onboard* or blank if the corresponding PCI device is an option card and not an onboard card.
- Flashing Preboot DSA between the Preboot DSA levels such as those listed in the following examples) with the different naming conventions on windows or Linux might fail:
 - The Preboot DSA level starting with DSYT (for example, DSYT890)
 - The Preboot DSA level starting with D6YT (for example, D6YT29A)
 - The Preboot DSA level starting with TMYT (for example, TMYT19A)
 - The Preboot DSA level starting with yuoo (for example, yuoo890)
 - The Preboot DSA level starting with y4yt (for example, y4yt21a)

You can use the **iflash** command to flash Preboot DSA levels between the Preboot DSA levels with the different naming conventions successfully: **iflash64 --package [upd file name] --openoptions 16 --force**

- RHEL6 and RHEL6.1 support limitations:
 - The LSI CIM provider does not support RHEL6.x. The reported LSI Configuration in the log file on RHEL6.x is different from other operating systems.
 - The PMC CIM provider does not support RHEL6.x.
 - The QLogic scli utility needs requires installing the GLIBC library first.
- On Windows Small Business Server 2011, DSA might run slowly on systems with the LSI option. This is caused by a provider limitation.
- On System x3755 M3, the **Slot** information in the Devices table on the PCI Information page displays *Onboard* if the corresponding PCI device is an option card.
- When transferring files by FTP in an IPv6 network, you must add the port number to upload successfully. The default port number is 21. The command format is:
[Portable DSA binary] -v -t user:password@[IPv6 IP]:21
- On System x3755 M3, the iBMC configuration and environmental information, such as the SP Configurations, Environmentals, and SP Logs may not be collected and displayed.
- On System x3755 M3, for the Name item in the Processor/Core table on the Hardware Inventory page, the Node number is displayed and is the same as the CPU number. (For example, Node 1 CPU 1, Node 2 CPU 2, or Node 3 CPU 3.)
- In the HTML output collected by Preboot DSA with VMware ESXi key, no page is displayed for VMware ESXi due to the limitation of Customized Linux Kernel 6.1 on the following systems:
 - System x3755 M3
 - System x3100 M4
 - System x3250 M4
- Embedded Preboot DSA cannot be flashed on System x3755 M3 with VMware ESX 4.1.
- When performing memory tests, DSA supports up to 4 CPUs. If any CPU is not installed or has no memory installed, that CPU cannot be selected for the memory test.
- On BladeCenter HX5 (types 7872 and 1909 multiple node configurations), some event logs are duplicated on node 1 and node 2 on the **SoftwareSystem Overview** Report Highlights page. Only one node has these events, but DSA cannot determine which one.
- On Systems x3200 M3 and x3250 M3, when the AC power cord is pulled out and plugged back in, Embedded Preboot DSA might display an error message and fail to boot. Cycling the AC power without unplugging the cord might correct the problem.

- On Systems x3850 and x3950 X5 multiple node, Portable DSA might have an exception when running with the `-ipmilan -v` option in Windows 2008 R2. In this case, the DSA log is created without any lost function.

Retain Tips

29908

When you run portable Dynamic System Analysis 9.60 on System x3950 X6 to collect the Central Processing Unit (CPU) information, the core information for the second node will not be shown on the generated HTML page.

29955

When running Dynamic System Analyze with the `--vmware-esxi` command on Windows 2008 R2 to collect inventory of another server with ESXi 5.1u2 installed, the second node **SN/UUID** information is same as the first node, which is incorrect. (where ESXi = VMware vSphere, SN = serial number, UUID = Universally Unique Identifier) When you run portable Dynamic System Analysis 9.60 on System x3950 X6 to collect the Central Processing Unit (CPU) information, the core information for the second node will not be shown in the generated HTML page.

29937

Dynamic System Analysis (DSA) 9.60 might display the incorrect serial number of a System x3950 X6 machine, when it is run on SUSE Linux Enterprise Server 11.3.

30006

The Dynamic System Analysis (DSA) tool cannot see the **Flash package version** in VMware ESXi 5.5.

30024

BROCADE DIAGNOSTICS FAIL WHEN RUNNING DYNAMIC SYSTEM ANALYSIS

The ExternalLoopback Test fails when you set up a Brocade LAN card.

30093

When you run Dynamic System Analysis (DSA) with `--vmware-esxi`, remotely parsing the information of a Flex System x880 X6 Compute Node with the VMware ESXi Operating System (OS) installed, due to the ESXi limitation that it can at most register two (2) namespaces, the DSA log will miss the third and fourth node's Integrated Management Module (IMM) related information (for example: IMM configuration, environments, chassis log, IPMI eventlog, lightpath). (where IPMI = Intelligent Platform Management Interface)

30048

Dynamic System Analysis (DSA) cannot restore configured **usb0/usb1** Internet Protocol (IP) addresses on Windows after finishing the information collection. This occurs if DSA cannot establish a connection to IMM with the **USB0/1** host IP. DSA will change the **USB0/1** host IP to the same subnet with IMM IP, to communicate with IMM to collect information. (where IPMI = Intelligent Platform Management Interface)

30091

On a system with the Windows 2008 R1 32-bit or 64-bit Operating System (OS) installed and **usb0/usb1** is down, after running Dynamic System Analysis (DSA), the network status will not remain as down.

30556

EEPROM ERROR CAN NOT BE DETECTED BY DYNAMIC SYSTEM ANALYSIS

If you cause an EEPROM error in Diagnostics, the DSA Diagnostic test cannot detect an EEPROM error.

90382

DSA IS NOT SHOWING LSI CONTROLLER ON VMWARE 5.5

You cannot see the LSI data on VMware 5.5 with Inglewood installed on System x 3850 X6/x3960 X6. What is the actual product name to use in place of Inglewood?

90383

DSA DOES NOT DISPLAY THE LSI LOGICAL AND PHYSICAL DRIVE INFORMATION

On a Flex System x240 M5 with SLES11.3, DSA does not display the LSI Logical and Physical Driver information.

90194**DSA DISPLAYS INCORRECT INFORMATION ON THE LSI CONTROLLER PAGE**

When using build RAID level 00 and R1-EC, the LSI Controller information is incorrect with the LSI vero card.

90192**HDD DIAGNOSTICS DO NOT SHOW THE EXTENDED RESULTS**

System shows abort after running the disk stress test with a specific HDD (IBM 300 GB 10K 6 Gbps SAS 2.5" G3HS HDD).

90311**DSA INTEL X710 SFP+ ADAPTER FIFO DIAGS FAIL IN X3550 M5**

If connecting 4Fort and Mayo 4 Port at the same time, the system displays 4Fort and Mayo 4 Port FIFO item --> Fail, and runs 4Fort FIFO item in diagnostics test. The system then displays 406-902-000 : A failure was detected during the FIFO test.

90073**PREBOOT DSA CANNOT GET INFO FOR THE INTEL XEON PHI 7120P ON NX360 M5**

The DSA Log does not have the Intel MIC information with Intel Xeon Phi 7120P.

H197177

DSA Preboot incorrectly displays the Chinese license agreement.

H197142

The DSA Volumes/Mount Points table **LABEL** columns are empty.

H202792

On Systems x3100 M4 and x3250 M4 when RAID software is configured, DSA displays No result or Aborted after running the LSI HDD diagnostic test. DSA does not currently support this configuration.

H203200

Nvidia 2075/2090 GPU fails in DSA Preboot diagnostics.

H202676 - 2582

Nvidia QUADRO 600 is not recognized by DSA Preboot.

H202743

The Brocade 10 GB Dual-Port CNA Loopback test failed. The following two loop back tests fail diagnostics:

- ExternalEthLoopbacktest
- ExternalLoopbackTest

H204309

The slot info of PCI devices displays as blank or onboard.

Dynamic System Analysis event log

All diagnostic test status and error information is recorded in the DSA event log.

Each log record contains:

- Time stamp
- Source
- Message type
- Message text

You can set the name and location of the log file using the *DSA_LOGFILE* environment variable. This variable takes a string that contains a valid path on the system on which DSA is running. The file does not need to exist, but the path to the file must exist. If this variable is not set, logging is lost.

Dynamic System Analysis core dump file

A core dump file is created when Dynamic System Analysis ends unexpectedly.

On a Windows system the core dump file named `DSA_CORE.dmp`, is created in the directory where DSA was run.

On Linux, the core dump is disabled by default. To enable the core dump file, run the `ulimit c` command. When enabled, the core dump file, is named using random numbers such as `dump01043`, and is created in the directory where DSA was run.

Getting help and technical assistance

Use information in this section to assist you in locating technical assistance for your System x, BladeCenter, and Flex System tools.

If you need help, service, technical assistance or would like more information about products, there is a variety of resources available to assist you. The topics in this section provide information about where to go for additional information about products, what to do if you experience a problem with your system, and whom to call for service, if it is necessary.

Before you call

Review and use this information before you call Service and Support to report a problem.

Complete these steps to try and resolve the problem yourself:

- Ensure that you have the latest version of the tool installed.
- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system.
- Go to [Lenovo Service and Support](#) to check for technical information, hints, tips, and new device drivers.
- Use a Lenovo or IBM discussion forum to ask questions.

You can solve many problems without assistance by following the troubleshooting procedures that Lenovo provides in the online help or in the documentation that is provided with your product. The documentation that comes with your system also describes the diagnostic tests that you can perform. Most systems, operating systems, and programs come with documentation that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Using the documentation

Information about your system, preinstalled software, or an optional device is available in the documentation that comes with the product. Product documentation sources include: information centers, online documents, printed documents, readme files, and help files.

The troubleshooting information in your system documentation might include instructions for using diagnostic programs. The troubleshooting information or the diagnostic programs could indicate that you need additional or updated device drivers or other software. Check these Web sites for additional information and updates:

[Lenovo Service and Support](#) and the <http://www.lenovo.com/support> have the latest technical information, device drivers, and updates.

The [Publications Center](#) has additional documentation.

Getting help from the World Wide Web

You can get the latest information about product compatibility, supported systems and devices, warranties and licenses, and service and support from this list of Web sites.

- [Lenovo ToolsCenter website](#)
<https://support.lenovo.com/us/en/documents/LNVO-CENTER>
- [Lenovo BladeCenter Product and Support site](#)
<http://shop.lenovo.com/us/en/systems/servers/blades/bladecenter/>
- [Flex System overview website](#)
<http://shop.lenovo.com/us/en/systems/servers/blades/flex-system/>
- [Lenovo ServerProven](#)
<http://www.lenovo.com/us/en/serverproven/>

Software service and support

You can get assistance for your BladeCenter, Flex System, and System x tools by contacting Service and Support.

- For a list of Lenovo support telephone numbers, see the [Lenovo Support Phone List](http://support.lenovo.com/us/en/supportphonenumberlist) Web site at <http://support.lenovo.com/us/en/supportphonenumberlist>.
- For Lenovo support services, see the [Lenovo Service and Support](http://support.lenovo.com/us/en/) Web site at <http://support.lenovo.com/us/en/>.
- For information about supported Lenovo products, see the [Lenovo Support website](http://datacentersupport.lenovo.com) at <http://datacentersupport.lenovo.com>.

Hardware service and support

You can get assistance with ordering new equipment or requesting service support. Hardware service and support are available from Service and Support or from your Lenovo reseller, if your reseller is an authorized Lenovo warranty service provider.

- U.S. and Canada, hardware service and support are available 24 hours a day, 7 days a week. For a list of Lenovo support telephone numbers, see the [Lenovo Support Phone List](http://support.lenovo.com/us/en/supportphonenumberlist) Web site at <http://support.lenovo.com/us/en/supportphonenumberlist>.

Appendix A. Accessibility features for Dynamic System Analysis

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

The following list includes the major accessibility features in Dynamic System Analysis:

- Can be operated using only the keyboard
- Communicates all information independent of color
- Supports the attachment of alternate output devices
- Provides help information in an accessible format
- (Microsoft Windows systems only) Supports interfaces commonly used by screen readers and screen magnifiers

The Dynamic System Analysis topic collection in the ToolsCenter for Lenovo x86 Servers Information Center information center, and its related publications, are accessibility-enabled.

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

Lenovo and accessibility

See the [Lenovo Accessibility](#) Web site for more information about the commitment that Lenovo has to accessibility.

Appendix B. Dynamic System Analysis commands

You can perform all Dynamic System Analysis functions from a command-line interface.

How to read syntax diagrams

Review the conventions used in syntax diagrams to understand the command descriptions.

The syntax diagram consists of options and option arguments. Options consist of a hyphen and single letter (for example, -h) or two hyphens and multiple letters (for example, --help). Options can be followed by one or more *option arguments* (for example, as illustrated in [-cd=*volume*]).

Consider these conventions when reading syntax diagrams:

- Options that are enclosed in brackets ([]) are optional. Do not include these brackets in the command.
- Options that are enclosed in braces ({ }) are required. Do not include these braces in the command.
- Options that are not enclosed in either brackets or braces are required.
- The names of options are case sensitive and must be typed exactly as shown. Options preceded by two dashes (--) must be specified in their entirety.
- The names of option arguments that require substitution by actual values are italicized.
- The pipe (|) character signifies that you choose one option or the other. For example, [a | b] indicates that you can choose either a or b, but not both. Similarly, {a | b} indicates that you must choose either a or b.
- An ellipsis (...) signifies that you can repeat the option argument on the command line.

DSA command

Use the `lnvgy_utl_dsa_dsalxxx-10.x_portable_platform` command to collect information about the local system.

Syntax

```
lnvgy_utl_dsa_dsalxxx-10.x_portable_platform -? | -h
```

```
lnvgy_utl_dsa_dsalxxx-10.x_portable_platform -l
```

```
lnvgy_utl_dsa_dsalxxx-10.x_portable_platform -b
```

```
lnvgy_utl_dsa_dsalxxx-10.x_portable_platform -diags
```

```
lnvgy_utl_dsa_dsalxxx-10.x_portable_platform --chkupd --proxy-address=ip_address --proxy-port=portnum --proxy-user=userid --proxy-password=password
```

```
lnvgy_utl_dsa_dsalxxx-10.x_portable_platform [-i data_file]
```

```
lnvgy_utl_dsa_dsalxxx-10.x_portable_platform -r [data_file] -v [-i data_file]
```

```
lnvgy_utl_dsa_dsalxxx-10.x_portable_platform -t [user_id:password@IP[:port]/path/] -i data_file
```

```
lnvgy_utl_dsa_dsalxxx-10.x_portable_platform --update
```

```
lnvgy_utl_dsa_dsalxxx-10.x_portable_platform -ux [-x] [-v] [-text]
```

```
lnvgy_utl_dsa_dsalxxx-10.x_portable_platform --ipmi-lan user_id:password@ip_address[:port]
```

```
lnvgy_utl_dsa_dsalxxx-10.x_portable_platform --vmware-esxi user_id:password@ip_address[:port]
```

```
lnvgy_utl_dsa_dsalxxx-10.x_portable_platform [-x] [-text] [-v [-html]] [-i data_file] [-d output_directory] [-dumpxml] [-f]
```

```
lnvgy_utl_dsa_dsalxxx-10.x_portable_platform --update --proxy-address=ip_address --proxy-port=portnum --proxy-user=userid --proxy-password=password
```

```
lnvgy_utl_dsa_dsalxxx-10.x_portable_platform -upload [IBMid:id]
```

Description

Important:

- To install or use Dynamic System Analysis, you must be logged in to the local system using a user ID that has administrator or root privileges. On a Linux system, you must log in using the **root** user name and privilege.
- On Linux systems, run Dynamic System Analysis from a journaling file system (such as ext3 or ReiserFS). You cannot run these commands from a virtual machine file system (VMFS).

To run this command on a system running Windows, change to the directory where Dynamic System Analysis was installed (for example, C:\Program Files\Lenovo\DSA). Use the **lnvgy_utl_dsa_dsalxxx-10.x_portable_platform.exe** command.

To run this command on a system running Linux, use **lnvgy_utl_dsa_dsalxxx-10.x_portable_platform.bin**.

If no options are specified, this command collects and saves information in a compressed XML file in the installation_directory\Lenovo_Support\ on Windows systems or /var/log/Lenovo_Support on Linux systems. This file contains the collected data and the consolidated property specification documents from each collector that collects data. The file is named mtm_serialnumber_datetime.xml.gz, where **mtm** is the machine type and model number of the local system, **serialnumber** is the serial number of the local system, and **datetime** is the date and time that data was collected. If Dynamic System Analysis cannot obtain a valid machine type, model number, or serial number of the system, any resultant output file and subdirectory will use the string "Unknown" in place of these values.

For more information about the standard of CIM-XML specifications, see the [Distributed Web-Based Enterprise Management \(WBEM\)](http://www.dmtf.org/standards/wbem/) Web site at www.dmtf.org/standards/wbem/.

Commands and options

-b

Runs in batch (unattended) mode. When this option is specified, user-interactive prompts are not displayed.

--chkupd--proxy-address=ip_address--proxy-port=portnum--proxy-user=userid--proxy-password=password

Checks the Web site for available System Enablement Packs (SEPs). You can add support for new devices by downloading and installing new SEPs. This function is available for Online Dynamic System Analysis only.

proxy-address=

The IP address of the proxy server used to connect to the Internet.

proxy-port=

The port number on the proxy server.

proxy-user=

The username to connect to the proxy server.

proxy-password=

The password for the *proxy-user*.

--cmmuserid:password@hostip:[port]

This option is used to collect CMM data by Out-of Band mode.

-doutput_directory

Specifies the fully-qualified or relative directory where the data files are to be placed (for example: /tmp/DSA or c:\temp\DSA for Windows). If the specified directory does not exist, it will be created. By default, files are placed in %SystemDrive%/Lenovo_Support.

-diags

Runs all nondestructive diagnostics tests for the applicable devices.

The nondestructive diagnostic tests include:

- Optical drive tests, including verify media, read error, and drive self test
- Tape drive tests, including tape presence, tape alert, tape load, and tape self-test

--disable-imm-lan

Disables the USB Over LAN interface after running DSA.

-dumpxml

Saves the compressed CIM-XML file to disk after each collector plug-in runs.

- This option significantly slows down the collection process and is intended only for debugging purposes.
- This option cannot be used with the -x and -i options.

-f

Collects the full ISMP service processor log.

--ffdc

This option is used to collect IMM FFDC log by In-Band mode for all nodes.

-? | -h

Displays information about this command, including syntax and option descriptions.

-html output_directory

Specifies the fully-qualified or relative directory where the HTML data files are to be placed (for example: /tmp/DSA or c:\temp\DSA for Windows)

- If you do not specify this option, the set of HTML data files is saved in the `outputdir\mtm_serialnumber_datetime` directory, where `outputdir` is the output directory specified by the -d option, **mtm** is the machine type and model of the local system, **serialnumber** is the serial number of local system, and **datetime** is the date and time when data was collected.
- If you do not specify the -c option, the specified output directory must exist on the local system.

-idata_file

Reads input from the specified file instead of collecting data from the local server. The command is valid only when the file is generated by running DSA, and the file is with xml extension or xml.gz extension.

-ibmid

Allows you to specify your IBM Identifier, for use with the -upload option.

--ipmi-lan user_id:password@ip_address[:port]

Collects IPMI event log on the specified remote server using out-of-band mode.

-l

Displays the license text.

--no-imm-lan

This option is used to skip DSA data collection for IMM when running DSA, USB Over LAN state is kept unchanged.

-rdata_file[data_file...]

Compares current system information against one or more specified system information files, in compressed CIM-XML format. Use fully-qualified file names (for example, /tmp/compfile.xml.gz or c:\temp\DSA\compfile.xml.gz). Separate multiple file names using a space.

- If you specify the **-r** option, you must also specify the **-v** option, which creates output in HTML format.
- If the **-i** option is also specified, this command compares the data files specified with the **-r** option to the current data file specified by the **-i** option instead of collecting the current system information.

-remote-ffdc

CMM FFDC support

--remote-ffdc [user_id:password@port]

This option is used to collect FFDC log by Out-Of-Band mode. In this mode, portable DSA collects FFDC log from CMM/IMM. Currently only FFDC from CMM is available.

-t [ftp(sftp)://user_id:password@ip_address[:port] /path/]

Transfers the inventory data file to the specified system using the specified File Transfer Protocol (FTP). Specify the system using these arguments:

user_id:password

The credentials needed to access the FTP server, but the password of the FTP server cannot contain special characters include ~!@#\$\$%^&*()_+.=.

ip_address

The IP address or host name of the FTP server.

port

The port number to use to access of the FTP server.

path

The directory on the FTP server in which you want to copy the inventory data files.

-text

Creates output in ASCII text format.

Collected data is placed in the output directory in a single text file named **mtm_serialnumber_datetime.txt**, where **mtm** is the machine type and model number of the local system, **serialnumber** is the serial number of the local system, and **datetime** is the date and time that data was collected. Data is grouped in to high-level categories (for example, system overview, network settings, and installed application). Related system information for the high-level categories is categorized further and printed into several tables that contain properties and their value.

--update--proxy-address=ip_address--proxy-port=portnum--proxy-user=userid--proxy-password=password

Checks for available System Update Packs on the Support site, and downloads them if they are available. System Update Packs allow you to add support for systems that have been released since the most recent release of Dynamic System Analysis. This function is available for Online Dynamic System Analysis only.

proxy-address=

The IP address of the proxy server used to connect to the Internet.

proxy-port=

The port number on the proxy server.

proxy-user=

The username to connect to the proxy server.

proxy-password=

The password for the *proxy-user*.

--update_arch32|64

Used with --chkupd or --update options to specify the architecture.

--update_mmachine_type

Used with --chkupd or --update options to specify the machine type to update.

--update_oswindows|rhel4|rhel4|rhel5|sles9|sles10|sles11|vmware3.5|vmware4.0

Used with --chkupd or --update options to specify the operating system.

-ux [--proxy-address=address] [--proxy-port=port] [--proxy-user=user_ID] [--proxy_password=password]

Compares the installed firmware levels with the latest version of firmware levels.

Important: The local system must have Internet access.

-v

Creates output in HTML format.

Collected data is categorized and placed in a set of HTML files (for example, *system_overview.html* for system-overview information, *net.html* for network settings information, and *installedapp.html* for installed-application information). In each HTML file, related system information is categorized further and printed into several tables that contain properties and their value.

This option also creates an *index.html* file from which you can view all system information. When you display this file in a web browser, the left pane contains links for each category of information, and the right pane displays the related information.

--vmware-esxiuser_id:password@ip_address[:port]

Collect system information from the specified remote system running VMware ESXi.

This option cannot be used with the **--ipmi-lan**, **-r**, **-diags**, and **-f** options.

-x

Does not create output in the compressed CIM-XML format.

- This command creates output in the compressed CIM-XML format by default.
- If you specify the **-x** option, you must specify either the **-v** or **-text** options.


Examples


1. **Collect data in a compressed CIM-XML output**This example illustrates how to collect data in a compressed CIM-XML file in the *installation_directory\Lenovo_Support* on Windows systems or */var/log/Lenovo_Support* on Linux systems.

 **invgy_util_dsa_Invgy_util_dsa_dsalxxx-10.x_portable_platform.exe**


 **invgy_util_dsa_Invgy_util_dsa_dsalxxx-10.x_portable_platform.bin**

2. **View previously collected data**This example illustrates how to import an existing data file named *system1.xml.gz* in the default output directory *C:\Lenovo_Support* and then saves the data in HTML and text format.

 **invgy_util_dsa_dsalxxx-10.x_portable_platform.exe -i input**

 **Invgy_util_dsa_dsalxxx-10.x_portable_platform -i system1.xml.gz**

3. **Convert collected data into HTML and text output** This example illustrates how to import an existing data file named `system1.xml.gz` in the default output directory `C:\Lenovo_Support\` and then saves the data in default output directory in HTML and text format.

 **Invgy_util_dsa_dsalxxx-10.x_portable_platform.exe -v -text -i input**

 **Invgy_util_dsa_dsalxxx-10.x_portable_platform -v -text -i system1.xml.gz**

DSA FoD CLI switches

DSA also provides a command-line interface for Feature on Demand (FoD) activation key management. The FoD interface is executed using subcommands after the DSA execution program. Execution is controlled by the subcommand and command-line switches. All command-line switches are case-insensitive.

Common subcommands and option switches for key management

Common subcommands and option switches for FoD activation key management are listed in the following table.

Syntax

DSA fod<subcommand> [options]

Table 2. Common subcommands and options for key management

Subcommand	Command-line option (case sensitive)	Argument	Description
display_available_fod: This subcommand is used to get and display the available FoD key(s) for a key repository (IMM, CMM, or IOM switch). The available FoD key(s) information can be got only if Internet is available.	<code>--help</code>	None	Output subcommand display_available_fod usage help screen to stdout.
	<code>--device</code>	device	This option is used to specify the target key repository for the supported devices: IMM, CMM, and Switch.
	<code>--ibmid</code>	userid: password	This option is used to specify the credential KMS ID for the interactive authorization by Lenovo Web site.
	<code>--host</code>	userid:password @hostip:[port]	This option is used for the device interface connection to the remote key repository. The default is the local IMM device. The default port is 5989.
	<code>--mt</code>	machinetype	This option is used for the machine type of device (IMM, CMM, Switch).
download_fod_key: This subcommand is used to acquire and download the activation key from a Lenovo Web site(KMS).	<code>--help</code>	None	Output subcommand download_fod_key usage help screen to stdout.

Table 2. Common subcommands and options for key management (continued)

Subcommand	Command-line option (case sensitive)	Argument	Description
	<i>--ibmid</i>	userid: password	This option is used to specify the KMS ID credential for the interactive authorization by Lenovo Web site.
	<i>--uid</i>	unique_id	This option is the unique identifier information of FoD feature.
	<i>--authcode</i>	[code]	This option is used to specify IBM authorization code and is optional. Once this switch is used, a key generation will be performed by KMS.
	<i>--mt</i>	machinetype	This option is used to specify the machine type of target device (IMM, CMM, Switch).
install_fod_key: This subcommand is used to install activation key(s) from user specified location (such as removable media) to the key repository.	<i>--help</i>	None	Output subcommand install_fod_key help screen to stdout.
	<i>--keyfile</i>	keyfile	This option is used to specify a single activation key file.
	<i>--device</i>	device	This option is used to specify the target key repository. The supported devices: IMM, CMM, Switch.
	<i>--host</i>	userid:password @hostip:[port]	This option is used for the device interface connection to the remote key repository. The default is the local IMM device. The default port is 5989.
	<i>--tftp</i>	userid:password @ip:[port]	This option is used to specify the TFTP server for snmp interface.
	<i>--community</i>	community	This option is used to specify the community for snmpv1v2, default: public.
	<i>--authproto</i>	[--authproto]	This option is used to specify the authorization protocol for snmpv3, default: No auth.
	<i>--privproto</i>	[DES/AES]	This option is used to specify the privacy protocol for snmpv3. Default: No privacy.
	<i>--privpasswd</i>	[privpassword]	This is optional switch to specify the privacy password for SNMPv3.

Subcommands and option switches for key management on IMM

The subcommand and option switches for FoD activation key management on IMM are listed in the following table.

Syntax

Table 3. Common subcommands and option switches for key management on IMM

Subcommand	Command-line option (case sensitive)	Argument	Description
export_imm_uid: This subcommand is used to export the unique identifier(s) of FoD feature(s) to a file saved in DSA output path, and then save to removable media.	<i>--help</i>	None	Output subcommand export_imm_uid usage help screen to stdout.
	<i>--export_imm_uid</i>	None	This subcommand is used to export the unique identifier(s) of FoD feature(s) to a file saved in DSA output path, and then save to removable media.
report_imm_active_fod: This subcommand is to report inventory information of installed activation key(s) in the IMM repository.	<i>--help</i>	None	Output subcommand report_imm_active_fod usage help screen to stdout.
	<i>--host</i>	userid:password@hostip:[port]	This option is used for the device interface connection to the remote key repository. The default is the local IMM device. The default port is 5989.
install_imm_fod: This subcommand is used to download and install activation key(s) to the IMM repository.	<i>--help</i>	None	Output subcommand install_imm_fod usage help screen to stdout.
	<i>--ibmid</i>	userid: password	This option is used to specify the credential KMS ID for the interactive authorization by Lenovo Web site.
	<i>--uid</i>	unique_id	This option is the unique identifier information of FoD feature.
	<i>--authcode</i>	[code]	This option is used to specify IBM authorization code and is optional. Once this switch is used, a key generation will be performed by KMS.
	<i>--mt</i>	machinetype	This option is used to specify the machine type of target device.

Table 3. Common subcommands and option switches for key management on IMM (continued)

Subcommand	Command-line option (case sensitive)	Argument	Description
	<i>--host</i>	userid:password @hostip:[port]	This option is used for the device interface connection to the remote key repository. The default is the local IMM device. The default port is 5989.
uninstall_imm_fod : This subcommand is used to uninstall specific activation key (s) from the IMM repository.	<i>--help</i>	None	Output subcommand uninstall_imm_fod usage help screen to stdout.
	<i>--keyid</i>	keyid	This option is used to specify the activation key ID returned from report command. If <i>keyid</i> is all, it will uninstall all keys.
	<i>--host</i>	userid:password @hostip:[port]	This option is used for the device interface connection to the remote key repository. The default is the local IMM device. The default port is 5989.

Subcommands and option switches for key management on CMM

The subcommands and option switches for FoD activation key management on CMM are listed in the following table.

Syntax

Table 4. Common subcommands and options for key management on CMM

Subcommand	Command-line option (case sensitive)	Argument	Description
report_cmm_active_fod : This subcommand is used to report inventory information of installed activation key(s) on the CMM repository.	<i>--help</i>	None	Output subcommand report_cmm_active_fod usage help screen to stdout.
	<i>--host</i>	userid:password @hostip:[port]	This option is used for the device interface connection to the remote key repository (CMM). The default port is 5989. Note: Requires a LAN connection.
install_cmm_fod : This subcommand downloads and installs activation key(s) to the CMM repository.	<i>--help</i>	None	Output subcommand install_cmm_fod usage help screen to stdout.

Table 4. Common subcommands and options for key management on CMM (continued)

Subcommand	Command-line option (case sensitive)	Argument	Description
	<i>--ibmid</i>	userid: password	This option is used to specify the KMS ID credential for the interactive authorization by Lenovo Web site. Note: Requires an Internet connection.
	<i>--uid</i>	unique_id	This option is the unique identifier information of FoD feature.
	<i>--authcode</i>	[code]	This option is used to specify the IBM authorization code and is optional. Once this switch is used, a key generation is performed by KMS.
	<i>--mt</i>	machinetype	This option is used to specify the machine type of the target device.
	<i>--host</i>	userid:password @hostip:[port]	This option is used for the device interface connection to the remote key repository (CMM). The default port is 5989.
uninstall_cmm_fod: This subcommand is to uninstall specific activation key(s) from the CMM repository.	<i>--help</i>	None	Output subcommand uninstall_cmm_fod usage help screen to stdout.
	<i>--keyid</i>	keyid	This option is used to specify the activation key ID returned from report command. If <i>keyid</i> is all, it will uninstall all keys.
	<i>--host</i>	userid:password @hostip:[port]	This option is used for the device interface connection to the remote key repository (CMM). The default port is 5989. Note: Requires a LAN connection.

Subcommands and option switches for key management on IOM

The subcommands and option switches for FoD activation key management on IOM are listed in the following table.

Syntax

Table 5. Common subcommands and options for key management on IOM

Subcommand	Command-line option (case sensitive)	Argument	Description
report_switch_active_fod: This subcommand reports inventory information of installed activation key(s) on the IOM switch repository.	<i>--help</i>	None	Output subcommand report_switch_active_fod usage help screen to stdout.
	<i>--host</i>	userid:password @hostip:[port]	This option is used for the device interface connection to the remote key repository (IOM/Switch). The default port is 5989. Note: Requires a LAN connection.
	<i>--tftp</i>	userid:password @ip:[port]	This option is used to specify the TFTP server for the snmp interface.
	<i>--community</i>	community	This option is used to specify the community for snmpv1v2; default: public.
	<i>--authproto</i>	report_switch_active_fod	This option is used to specify the authorization protocol for snmpv3; default: No auth.
	<i>--privproto</i>	[DES/AES]	This option is used to specify the privacy protocol for snmpv3; default: No privacy.
install_switch_fod: This subcommand is used to download and install activation key(s) to the CMM repository.	<i>--help</i>	None	Output subcommand install_switch_fod usage help screen to stdout.
	<i>--ibmid</i>	userid: password	This option is used to specify the credential KMS ID for the interactive authorization by the Lenovo Web site.
	<i>--uid</i>	unique_id	This option is the unique identifier information of FoD feature.
	<i>--authcode</i>	[code]	This option is used to specify the IBM authorization code and is optional. Once this switch is used, a key generation is performed by KMS.

Table 5. Common subcommands and options for key management on IOM (continued)

Subcommand	Command-line option (case sensitive)	Argument	Description
	<i>--mt</i>	Machinetype	This option is used to specify the machine type of target device.
	<i>--host</i>	userid:password @hostip:[port]	This option is used for the device interface connection to the remote key repository (IOM/Switch). The default port is 5989.
	<i>--tftp</i>	userid:password @ip:[port]	This option is used for the device interface connection to the remote key repository (IOM/Switch). The default port is 5989.
	<i>--community</i>	community	This option is used to specify the community for snmpv1v2; default: public.
	<i>--authproto</i>	[--authproto]	This option is used to specify the authorization protocol for snmpv3; default: No auth.
	<i>--privproto</i>	[DES/AES]	This option is used to specify the privacy protocol for snmpv3; default: No privacy.
	<i>--privpasswd</i>	[--privpasswd]	This option is an optional switch to specify the privacy password for SNMPv3.
uninstall_switch_fod : This subcommand is to uninstall specific activation key(s) from the IOM/Switch repository.	<i>--help</i>	None	Output subcommand uninstall_switch_fod usage help screen to stdout.
	<i>--keyid</i>	Keyid	This option is used to specify the activation key ID returned from the report command. If <i>keyid</i> is all, it will uninstall all keys.
	<i>--host</i>	userid:password @hostip:[port]	This option is used for the device interface connection to the remote key repository (IOM/Switch). The default port is 5989.
	<i>--tftp</i>	userid:password @ip:[port]	This option is used to specify the TFTP server for the snmp interface.
	<i>--community</i>	community	This option is used to specify the community for snmpv1v2; default: public.
	<i>--authproto</i>	[--authproto]	This option is used to specify the authorization protocol for snmpv3; default: No auth.

Table 5. Common subcommands and options for key management on IOM (continued)

Subcommand	Command-line option (case sensitive)	Argument	Description
	<i>--privproto</i>	[DES/AES]	This option is used to specify the privacy protocol for snmpv3; default: No privacy.
	<i>--privpasswd</i>	[--privpasswd]	This option is optional switch to specify the privacy password for SNMPv3.

Appendix C. Environment variables

These environment variables are used by Dynamic System Analysis:

DSA_INCLUDE

Specifies one or more plug-ins that are to be included when **collectall** is run. Separate the plug-ins by a space, comma, or semicolon. Use the base plug-in name (for example, **Ddinfo; installedapps**).

- The plug-in names are displayed when collection occurs.
- The *DSA_INCLUDE* and *DSA_EXCLUDE* variables are mutually exclusive.
- To reset the effect of the environmental variables, set empty values to the variables (for example, *DSA_INCLUDE=*).

Attention: Do not change this environment variable. This variable is used for debugging and is intended for use only by Lenovo technical support.

DSA_EXCLUDE

Specifies one or more plug-ins that are to be excluded when **collectall** is run. Separate the plug-ins by a space, comma, or semicolon. Use the base plug-in name (for example, **Ddinfo; installedapps**).

- The plug-in names are displayed when collection occurs.
- The *DSA_INCLUDE* and *DSA_EXCLUDE* variables are mutually exclusive.
- To reset the effect of the environmental variables, set empty values to the variables (for example, *DSA_INCLUDE=*).

Attention: Do not change this environment variable. This variable is used for debugging and is intended for use only by Lenovo technical support.

DSA_LOGLEVEL

Indicates the level of detail requested for logging. You can specify one of these values:

- **0:** Error
- **1:** Warning
- **2:** Status
- **3:** Debug
- **4:** Verbose

Attention: Do not change this environment variable. This variable is used for debugging and is intended for use only by Lenovo technical support.

DSA_LOGFILE

Specifies the path and file name for the DSA event log.

Important:

- The path must exist on the local system on which DSA is running.
- If this variable is not defined, logging may be lost.

DSA_EVENTLOG_MAX

Specifies the maximum number of entries collected from each system event log. The value must be a positive integer with six or fewer digits. The default value is 5000.

Appendix D. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

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

*Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing*

LENOVO 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 jurisdictions 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. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

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

Any references in this publication to non-Lenovo 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 Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result 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 measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

LENOVO, FLEX SYSTEM, SYSTEM X, NEXTSCALE SYSTEM, and XCLARITY are trademarks of Lenovo.

Intel and Intel Xeon are trademarks of Intel Corporation in the United States, other countries, or both.

Internet Explorer, Microsoft, and Windows are trademarks of the Microsoft group of companies.

Linux is a registered trademark of Linus Torvalds.

All other trademarks are the property of their respective owners. © 2018 Lenovo.

Important notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1 024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity can vary depending on operating environments.

Lenovo makes no representations or warranties with respect to non-Lenovo products. Support (if any) for the non-Lenovo products is provided by the third party, not Lenovo.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Index

A

accessibility
 features 55
 keyboard 55
 shortcut keys 55

C

command 71
 DSA command 57
common subcommands and option switches for CMM 65
common subcommands and option switches for IMM 64
common subcommands and option switches for IOM 67
common subcommands for key management 62
contacting support 39
conventions, syntax diagram 57
core dump file 51

D

disability 55
DSA fod <Subcommand>[options] 62
Dynamic System Analysis
 installing 3

E

event log 50

F

features, accessibility 55

G

getting help and technical assistance 51
getting help from the World Wide Web 52

H

hardware
 requirements 3
 supported 3
hardware service and support 53

I

important notices 74
installing Dynamic System Analysis 3

K

key management 62
keyboard 55

L

log
 events 50

N

notes, important 74
notices 73

O

operating systems, supported 11
option switches for key management 62

P

problem solving 39

R

requirements
 hardware 3
 software 10

S

service and support, before you call 52
shortcut keys 55
software
 requirements 10
software service and support 53
solving problems 39
support, contacting 39
supported hardware 3
supported operating systems 11
syntax diagram conventions 57

T

trademarks 74
troubleshooting 39

U

using the documentation 52

Lenovo