IBM Systems

Dynamic System Analysis Installation and User's Guide

Version 9.41

IBM Systems

Dynamic System Analysis Installation and User's Guide

Version 9.41

Note

Before using this information and the product it supports, read the information in "Notices" on page 85.

This edition applies to version 9.41 of Dynamic System Analysis and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this publication

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

Conventions and terminology

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

These notices are designed 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.

Publications and related information

You can view the same content in the Dynamic System Analysis topic collection in the IBM® ToolsCenter for System x® and BladeCenter® information center as a PDF document. To view a PDF file, you need Adobe Acrobat Reader, which can be downloaded for free from the Adobe website at www.adobe.com/products/acrobat/readstep.html.

Information centers and topic collections

- **IBM ToolsCenter for System x and BladeCenter information center**

  http://publib.boulder.ibm.com/infocenter/toolsctr/v1r0/index.jsp

  IBM ToolsCenter for System x and BladeCenter information center provides integrated information for multiple IBM Systems x and BladeCenter tools, including Dynamic System Analysis.

- **Dynamic System Analysis**

  publib.boulder.ibm.com/infocenter/toolsctr/v1r0/topic/dsa/dsa_main.html

  The Dynamic System Analysis topic collection provides information about how to download and use Dynamic System Analysis to collect, analyze, and diagnose system health, inventory and other information. This information is updated periodically and contains the most up-to-date documentation available for Dynamic System Analysis.

Publications

- ***http://download.boulder.ibm.com/ibmdl/pub/systems/support/system_x_pdf/ibm_dsa_installation_and_users_guide_9.40.pdf***

  This publication provides information about how to download and use Dynamic System Analysis to collect, analyze, and diagnose system health, inventory and other information.

Web resources

Listed here are the websites and information center topics that relate to Dynamic System Analysis.

Websites

- **IBM ToolsCenter for System x and BladeCenter**

  http://www-947.ibm.com/support/entry/portal/docdisplay?lndocid=tool-center

  View this website to download tools that support IBM System x and IBM BladeCenter products.
- **Dynamic System Analysis**

  http://www-947.ibm.com/support/entry/portal/docdisplay?lndocid=SERV-DSA

  View this website to download the Dynamic System Analysis tool and documentation.
- **Support for IBM BladeCenter**

  http://www-03.ibm.com/systems/bladecenter/support/

  View this website to find information about online technical support, downloads and drivers, and RETAIN tips, and to provide feedback about IBM BladeCenter products.
- **Support for IBM System x**

  http://www-03.ibm.com/systems/x/support/

  View this website to find information about online technical support, downloads and drivers, and RETAIN tips, and to provide feedback about IBM System x products.
- **IBM ServerProven®**

  www.ibm.com/servers/eserver/serverproven/compat/us/

  View this website to learn about hardware compatibility of IBM System x and IBM BladeCenter systems with IBM applications and middleware.

Forums

- **IBM System x Forum**

  https://www.ibm.com/developerworks/community/forums/html/forum?id=11111111-0000-0000-0000-000000002691#topicsPg=0

  View this website on ibm.com to learn about various forums that are available to discuss technology-related and product-related issues pertaining to IBM Systems hardware and software products. This website includes a link for accessing the forum using a Rich Site Summary (RSS) feed.

How to send your comments

Your feedback is important in helping to provide the most accurate and highest quality information.

If you have any comments about this publication or any other IBM ToolsCenter for System x and BladeCenter publication:

- Go to the IBM ToolsCenter for System x and BladeCenter information center information center website at http://publib.boulder.ibm.com/infocenter/toolsctr/v1r0/index.jsp. There you will find the feedback page where you can enter and submit comments.

- Complete one of the forms at the back of any IBM ToolsCenter for System x and BladeCenter publication and return it by mail, by fax, or by giving it to an IBM representative.

What's new

Dynamic System Analysis 9.41 provides additional systems support.

New hardware support

Dynamic System Analysis supports new systems, LSI RAID controllers, Fibre Channel adapters, and Ethernet adapters. In this release, Dynamic System Analysis now supports the following new options.

- IBM Flex System x222 Compute Node, machine type 7916
- IBM System x 3650 M4 HD, machine type 5460
- Intel Xeon Phi 7120P Adapter
- LSI N2215 SAS/SATA HBA Adapter
- LSI ServeRAID M5210 SAS/SATA Controller for IBM System x
- Nvidia Quadro K600, K2000, K4000, K5000 GPU

For a complete list of supported hardware, see “Supported hardware” on page 4.

New operating system support

Dynamic System Analysis now supports these operating systems.

- vSphere Hypervisor 5.1U1

For a complete list of supported operating systems, see “Supported operating systems” on page 9.

Chapter 1. Technical overview

Dynamic System Analysis (DSA) is a system information collection and analysis tool that is used by IBM 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

You can either create a bootable media such as CD, DVD, ISO, USB or PXE using IBM 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 the *Installation and User's Guide*.

Portable Edition

You can downloaded the Portable Edition from the IBM website and install it on removable media, such as CD, DVD, or USB flash drive, instead of the local system.

This edition of Dynamic System Analysis runs from a command line interface as a self-extracting executable file. It creates a temporary directory called `/tmp on Linux or %TEMP%` on Windows, and extracts all of the Dynamic System Analysis files to that directory. It then runs the command. When the command completes, the temporary directory and all of the Dynamic System Analysis files are deleted from the local system.

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

- System configuration
- Installed packages
- Kernel Modules
- Network interfaces and settings
- Performance data and details for running processes
- Hardware inventory, including PCI and USB information
- IBM LightPath status
- Service Processor status and configuration
- Vital product data, firmware, and basic input/output system (BIOS) information
- Drive Health Information
- ServeRAID configuration
- LSI RAID and controller configuration
- Event logs for the operating system, ServeRAID controllers, and service processors

The system information is collected into a compressed XML file that can be sent to IBM Service and Support. You can view the system information using 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, you must 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 Dynamic System Analysis

This section provides information about hardware and software requirements, downloading instructions, and updating procedures.

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 30-MB of disk space.

Memory requirements

To run Dynamic System Analysis, the system must have 256-MB or more physical memory for systems running Window and 512-MB or more physical memory systems running Linux. The amount of memory required for this process depends on the size of the logs being collected from the system. It is recommended that DSA Preboot Edition run on a system with more than 1-GB physical memory.

To display the DSA data, systems must have 30-MB to 100-MB of available memory. The amount of memory required depends on the size of the logs being viewed.

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 IBM 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 IBM systems

Server	Machine type
BladeCenter HS22	7870, 1936, 7809, 1911
BladeCenter HS22V	7871, 1949
BladeCenter HS23	7875, 1929
BladeCenter HS23E	8038, 8039
BladeCenter HX5	1909, 1910, 7872, 7873
Flex System x220 Compute Node	7906, 2585
Flex System x222 Compute Node	7916
Flex System x240 Compute Node	8737, 8738, 7863
Flex System x440 Compute Node	7917, 2584
iDataPlex® dx360 M2	7321, 7323
iDataPlex dx360 M3	6391
iDataPlex dx360 M4	7912, 7913, 7918, 7919
Smart Analytics System	7949
System x 3100 M4	2582
System x 3200 M2	4367, 4368
System x 3200 M3	7327, 7328
System x 3250 M2	7657, 4190, 4191, 4194
System x 3250 M3	4251, 4252, 4261
System x 3250 M4	2583
System x 3300 M4	7382
System x 3400 M2	7836, 7837
System x 3400 M3	7378, 7379
System x 3500 M2	7839
System x 3500 M3	7380
System x 3500 M4	7383
System x 3530 M4	7160
System x 3550 M2	7946, 4198
System x 3550 M3	7944, 4254
System x 3550 M4	7914, 7383
System x 3620 M3	7376
System x 3630 M3	7377
System x 3630 M4	7518, 7519
System x 3650 M2	7947, 4199

Table 1. Supported IBM systems (continued)

Server	Machine type
System x 3650 M3	7945, 4255, 5454
System x 3650 M4	7915
System x 3650 M4 HD	5460
System x 3690 X5	7147, 7148, 7149, 7192
System x 3750 M4	8722, 8733
System x 3755 M3	7164
System x 3850 X5	7143, 7145, 7146, 7191
System x 3950 X5	7143, 7145, 7146, 7191

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 Storage® DS4000® family
- IBM System Storage DS8000® family

Supported Server Options

- **Ethernet adapters**
  - Broadcom 1 Gb 4 port Mezz Card Tier 1
  - Broadcom 1 Gb Ethernet CFFh Expansion Card
  - Broadcom 10 Gb Ethernet CFFh Expansion Card for IBM BladeCenter
  - Broadcom Dualrunner/Quadrunner NetXtreme I
  - Broadcom Netextreme II
  - 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 x ITE-Blacktip onboard NIC for Flex
  - IBM NetXtreme II 1000 Express® Ethernet Adapter
  - Intel 10 GB SFP+ NIC
  - Intel X540 Dual Port 10GBaseT Embedded Adapter
  - Intel Xeon Phi 5110P
  - Intel Xeon Phi 7120P
  - Intel x520 Dual Port 10GbE SFP+ Embedded Adapter
  - Mellanox 2x 10 GbE SFP+ ConnextX-2LowLatency, RDMA
  - Mellanox 2xFDR10 ConnectX3 Adapter
  - Mellanox 2-port 40Gb Ethernet Adapter for IBM Flex System™ EN6132
  - Mellanox 2-port FRD Infiniband Adapter for IBM Flex System IB6132 (Malaya-x)
  - Mellanox 10 Gb 2-port Ethernet Adapter for IBM 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 40GbE 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 FDR FDR IB Dual Port
- Mellanox QDR/FDR Mezzanine Card (x-only) Tier 2 (Malaya-x)
- QLogic 16Gb 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 Quadro K600, K2000, K4000, K5000
  - Nvidia Tesla K20, K20X
  - Nvidia Tesla M2090, M2090 update, X2090, X2090 update
  - 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 16Gb FC Quad Port
  - Brocade 16 Gb FC Single/Dual-port HBA
  - Emulex 2-Port 10 Gb Multi-function IO Adapter
  - Emulex 2-port 16Gb FC Adapter for IBM Flex System FC5052
  - Emulex 4-port 16Gb FC Adapter for IBM 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 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 PCI-e Gen 2.0 Dual Port 10 Gb NIC
  - Endeavor III/Endeavor III Lite (vNIC2) using IBM FoD for FCoE Upgrade
  - IBM SAS HBA controller
  - 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 IBM 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 mezz card Tier 1 for Flex
  - QLogic 10Gb ASIC Update
  - 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 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 H1135 Controller
  - LSI ServeRAID M1015, M5014, M5015 and M5025
  - LSI ServeRAID M1110
  - LSI ServeRAID M1115 RAID SAS-2 6 Gb PCIe
  - 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 M5210 SAS/SATA Controller for IBM System x
  - LSI ServeRAID MR 10i, 10ie, 10is, 10k and 10m
  - LSI Shikra NGP Storage Mezzanine Expansion for IBM Flex System
  - LSI x ITE-Blacktip onboard RAID (LSI 2004) for Flex
- **Storage adapters**
  - Fusion IO 1.2TB High IOPS MLC Duo
  - Fusion IO 2.4TB High IOPS MLC Duo
  - Fusion IO 640GB High IOPS MLC Duo
  - LSI 300GB MLC Option Bulk

  - LSI 300GB SLC Option Bulk
  - LSI 600GB MLC Option Bulk
  - LSI 800GB 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
  - LSI BR10i, BR10ie, BR10il

Software requirements

Use this information to understand 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 Support for IBM System x page on the web at http://www-03.ibm.com/systems/x/support/.

The following list provides information for collecting device driver, firmware level, and log data.

- To collect SCSI & USB device information (including diagnostics), the sg driver must be loaded. Run **lsmod** and verify that 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 IBM Support website at www.ibm.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 IBM Support website at www.ibm.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 IBM Support site using 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 these 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

Use this information to identify operating systems that are supported by Dynamic System Analysis.

The following operating systems are supported by Dynamic System Analysis.

- **Windows Server 2012 Edition**
  - Microsoft Windows Server 2012
- **Windows Server 2011 Editions**
  - Microsoft Windows Small Business Server 2011
  - Microsoft Windows Small Business Server 2011 Essential
- **Windows Server 2008 Editions**
  - Microsoft Windows Server 2008, Datacenter Edition (x86, x64)
  - Microsoft Windows Server 2008, Enterprise Edition (x86, x64)
  - Microsoft Windows Server 2008 Foundation
  - Microsoft Windows Server 2008 HPC Edition

  - Microsoft Windows Server 2008 R2
  - Microsoft Windows Server 2008 R2 HPC Edition (x64, ROK)
  - Microsoft Windows Server 2008 R2 SP1
  - Microsoft Windows Server 2008, Standard Edition (x86, x64)
  - Microsoft Windows Server 2008, Web Edition (x86, x64)
  - Windows Essential Business Server 2008 Premium Edition
  - Windows Essential Business Server 2008 Standard Edition
- **Windows Server 2003 Editions**
  - Microsoft Windows Server 2003/2003 R2, Datacenter Edition (x86, x64)
  - Microsoft Windows Server 2003/2003 R2, Enterprise Edition (x86, x64)
  - Microsoft Windows Server 2003/2003 R2, Enterprise Edition with Microsoft Cluster Service (MSCS) (x86, x64)
  - Microsoft Windows Server 2003/2003 R2, Standard Edition (x86, x64)
  - Microsoft Windows Server 2003/2003 R2, Web Edition
- **Windows Preinstallation Environment**
  - Microsoft Windows Preinstallation Environment 3.0
  - Microsoft Windows Preinstallation Environment 2.1
- **SUSE Linux**
  - SUSE Linux Enterprise Server 11 (Up to SP3) (x86/x64)
  - SUSE Linux Enterprise Server 11 with Xen (Up to SP3) (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)
- **Red Hat**
  - Red Hat Enterprise Linux 6 (Up to U4) (x86, x64)
  - Red Hat Enterprise Linux 5 (Up to U9) (x86, x64)
  - Red Hat Enterprise Linux 5 (Up to U9) with Xen (x86, x64)
  - Red Hat Enterprise Linux 4 (Up to U9) (x86, x64)
- **VMware:**
  - VMware vSphere Hypervisor 5.1 (ESX5) (Up to U1) is supported only through use of the `--vmware-esxi` option
  - VMware vSphere Hypervisor 5.0 (ESX5) (Up to U2) is supported only through use of the `--vmware-esxi` option
  - VMware ESX Server, 4.1 (Up to U3)
  - VMware ESXi 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)
  - VMware ESXi 4.0 (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 USB flash drive.

About this task

Important: Ensure that the removable media has enough free space to contain the Dynamic System Analysis.

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

Procedure

1. Download the appropriate portable-edition package for the local operating system from the Dynamic System Analysis website at http://www-947.ibm.com/support/entry/portal/docdisplay?lndocid=SERV-DSA:
   - ibm_utl_dsa_*v.r.m*_portable_*plaform*.exe for Windows systems
   - ibm_utl_dsa_*v.r.m*_portable_*plaform*.bin for Linux systems

   where *installation_directory* is the path to the extracted installation files, *v.r.m* is the version of Dynamic System Analysis, and *platform* is the supported operating system.
2. Insert or mount the removable medium.
3. Copy the portable-edition package to the removable media.

Updating system support

You can update Online Dynamic System Analysis to add support for new systems by downloading System Enablement Packs (SEPs) from IBM. System Enablement Packs are collections of the files and drivers needed to allow ToolsCenter tools to support new systems. This section describes how to check for and download System Enablement Packs using Online Dynamic System Analysis.

About this task

When using Online Dynamic System Analysis with a system that was released after the release of the tool, you will receive the following message:

```
You might need to download an update for DSA to support this system.
Use the -? or -h parameter for more information about downloading updates.
Do you want to proceed anyway (function may be limited)? (Y/N)
```

You can choose to continue with limited function, or you can check for and download updates that will allow Online Dynamic System Analysis to support the new system.

Procedure

1. Optional: Check for new updates. You can check for new updates without downloading them using the **chkupd** parameter with the **collectall** command. For Windows:

   ```
   ibm_utl_dsa_v.r.m_portable_plaform --chkupd
   ```

   or for Linux:

   ```
   ./ibm_utl_dsa_v.r.m_portable_plaform --chkupd
   ```

   If new updates are available, you will be prompted to update the support list.
2. Update the support list. The **update** parameter of the **collectall** command checks for updates, and if any are found, downloads them automatically. For Windows:

   ```
   ibm_utl_dsa_v.r.m_portable_plaform --update --update-update_type
   ```

   For Linux:

   ```
   ./ibm_utl_dsa_v.r.m_portable_plaform --update --update-update_type
   ```

   Where *update_type* is used to filter the types of update to acquire:

   –update_arch 32|64
   Specifies the operating system architecture for which to acquire updates.

–update_m*machine_type*
Specifies the 4-digit machine type for which to acquire updates.

–update_os *windows* | *rhel4* | *rhel5* | *rhel6* | *sles10* | *sles11* | *vmware4.0*
Specifies the operating system

When the update has been downloaded, it is automatically added to the directory of portable DSA in a new subdirectory named `update`. The next time portable DSA is run, it will detect the update, apply it, and continue, using the latest level of support.

Chapter 3. Running diagnostic tests on the local system

About this task

Perform one of the following steps to run diagnostics on the local system.

Procedure

- If you are using the Preboot Dynamic System Analysis 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 complete, to display the Diagnostic details click the button located under Diagnostic Tests in the navigation pane on the left.
- If you are using the Dynamic System Analysis Preboot Edition command-line interface:
  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.
- If you are using 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:

     ```
     ibm_utl_dsa_v.r.m_portable_plaform -diags
     ```

where *v.r.m* is the version of Dynamic System Analysis, and platform is the supported Linux distribution.

Chapter 4. Collecting system information

You can use Dynamic System Analysis to collect system information and convert the collected data to another format.

Collecting system information on the local system using Preboot Edition

About this task

Perform the steps listed for one of the following Dynamic System Analysis options to collect system information on the local system :

- If you are using the Dynamic System Analysis Preboot Edition graphical user interface:
  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 diagnostic tests are performed. To skip the diagnostic tests, click **Collect Inventory Only** and click **OK** to begin the collection process.
  7. When the inventory is complete, to display the Inventory details click **Full inventory file** in the navigation pane on the left.
- If you are using the Dynamic System Analysis Preboot Edition command-line interface:
  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 **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 complete, select **View collection results** to display the results.
  6. When you are done, enter **:q** to exit the viewer.

Collecting system information on the local system

About this task

Perform these steps to collect system information on the local system if you are using Dynamic System Analysis on removable media.

Procedure

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:

   ibm_utl_dsa_*v.r.m*_portable_plaform [-x] [-v] [-text]

   where *v.r.m* is the version of Dynamic System Analysis, and 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 the VMware ESXi

Before you begin

Prerequisites:

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

About this task

Perform these steps to collect system information on a remote system running the VMWare embedded hypervisor:

Procedure

1. Insert the USB flash drive containing VMWare in the target system.
2. Boot the system.
3. Select DHCP or configure the IP address manually following VMWare instructions.
4. If you are using Dynamic System Analysis on removable media, 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 removable media.
   c. Enter the following command to collect system information:

      ibm_utl_dsa_*v.r.m*_portable_plaform --vmware-esxi *user_id:password@ip_address*

      where *v.r.m* is the version of Dynamic System Analysis and *user_id:password@ip_address* specifies the user ID, IP address, and port number to use for authentication with the hypervisor.

Collecting IPMI event logs from a remote system

About this task

Perform these steps to collect Intelligent Platform Management Interface (IPMI) event logs from a remote system using out-of-band mode if you are using removable media.

Procedure

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:

   ibm_utl_dsa_*v.r.m*_portable_plaform --ipmi-lan *system*

   where *v.r.m* is the version of Dynamic System Analysis, *platform* is the supported operating system, and *system* is the remote system to which you want to collect IPMI event logs. Specify the system using the following format: *user_id*:*password*@*ip_address*[:*port*].

Converting collected data to another format

About this task

Perform these steps to convert data collected on the local system to another format if you are using Dynamic System Analysis on removable media.

Procedure

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:

   ibm_utl_dsa_*v.r.m*_portable_*platform data_file* [-v | -text]

   where:
   - *v.r.m* is the version of Dynamic System Analysis
   - *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

You can use Dynamic System Analysis to compare collected system information.

Comparing installed and latest versions of firmware

Before you begin

Prerequisite: The local system must have Internet access.

About this task

Perform these steps to compare the installed versions of firmware and device drivers on the local system to the latest versions available on the web.

Procedure

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:

   `ibm_utl_dsa_`*`v.r.m`*`_portable_plaform -ux [-x] [-v] [-text]`

   where *v.r.m* is the version of Dynamic System Analysis, and platform is the supported operating system.

   When the comparison is completed, 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

About this task

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

Perform these steps to collect the system information on the local system and then compare the current system information to one or more system information files that were previously collected.

Procedure

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:

   `ibm_utl_dsa_`*`v.r.m`*`_portable_plaform -r `*`data_file`*` -v`

where *v.r.m* is the version of Dynamic System Analysis, 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

About this task

Perform these steps to compare two or more system information files that were previously collected.

Procedure

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 compare system information:

   `ibm_utl_dsa_`*`v.r.m`*`_portable_plaform -r` *`data_file`* `-v`

   where *v.r.m* is the version of Dynamic System Analysis, 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

About this task

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:\IBM_Support\ directory on Windows systems` or `/var/log/IBM_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 **ibm_utl_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 **ibm_utl_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 **ibm_utl_dsa_***v.r.m_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: **ibm_utl_dsa_*v.r.m_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

You can 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

Use this procedure to send collected data to IBM Service and Support or another remote system using File Transfer Protocol (FTP).

About this task

Perform one of the following steps to transfer data collected on the local system to a remote system using FTP.

Procedure

- If you are using the Dynamic System Analysis Preboot Edition command-line interface:
  1. Collect data using the command-line interface as described in "Collecting system information on the local system using 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 and specify the FTP address, port number, user name, and password to use with your FTP server.
- If you are using the Dynamic System Analysis Preboot Edition graphical user interface:
  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 IBM website automatically.
- If you are using 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:

   ibm_utl_dsa_*v.r.m*_portable_plaform [-v] [-t] *system*

   where *v.r.m* is the version of Dynamic System Analysis, 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 to IBM.

Transferring collected data to the IBM customer inventory repository

Before you begin

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

About this task

Perform these steps to transfer data from the local system to the IBM customer inventory repository.

Procedure

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 and transfer the system information file:

   ibm_utl_dsa_*v.r.m*_portable_*platform* -upload [-IBMid:*user_id*]

   where

   - *v.r.m* is the version of Dynamic System Analysis
   - *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

You can use Dynamic System Analysis to collect system information and copy the collected data to a USB device.

About this task

After you have collected data, use this procedure to copy it to a USB device.

Procedure

1. When collection process completes, click **Collection and Diagnosis** from the top navigation pane.
2. Click **Save to ...** to open the Save to Removable Media page.
3. Select the desire USB device and click **OK**.

Chapter 9. Supporting Dynamic System Analysis Features on Demand

This section provides information for using DSA Features on Demand.

Using Features on Demand for Portable Dynamic System Analysis

The topics in this section provide information about using Features on Demand for Portable DSA.

Downloading the FoD key and installing with the key file

Use this task to download the FoD key and install the key file.

Before you begin

The following prerequisites are necessary for this task:

- The DSA Portable Edition is available on a removable medium (for example, a CD-ROM or 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.

About this task

Perform these steps to download the FoD key and install using the key file. All of the FoD operations use the FoD application option and applicable subcommands. For more information, refer to the DSA FoD sections in *Appendix B*: "DSA FoD CLI switches" on page 73.

Procedure

1. Insert the removable medium with DSA Portable Edition into the machine.
2. Start the DSA Portable Edition executable on the removable medium.
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>
   ```

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]> |
   --commnuity <commnuity> | --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 not used, the default is "https" for this CIM connection.

User ID and Password is for the device interface connection.

For Switch, User ID and Password is auth info for SNMPv3.

Port is used for the CIM interface; the default is 598.

--tftp <ip:[port]>
The TFTP server for the Switch SNMP interface.

--commnuity <commnuity>
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 IMM on a portable target system

Before you begin

The following prerequisites are necessary for this task:

- The DSA Portable Edition is available on a removable medium (for example, a CD-ROM or 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.

About this task

Complete these steps to display the target system's FoD information, install, or uninstall the FoD license key(s) using IB/OOB mode.

Procedure

1. Insert the removable medium with the DSA Portable Edition into the machine.
2. Start the DSA Portable Edition executable on the removable medium.
3. Enter the following command and parameters for DSA to download the master XML from KMS and parse it to get all of the available FoD features for the target system (IMM repository), and display them in the console with status:

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

4. Enter the following command with no parameters, and the unique identifier for specified FoD features on the local system. The FoD features will be 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 USB key.

```
DSA fod export_imm_unique_ids
```

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.

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 IBM ID credential for the IBM website.

   --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.

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 will be applied. The default value of IMM port is 5989.

   If DSA failed 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 CMM on a portable target system

Before you begin

The following prerequisites are necessary for this task:

- The DSA Portable Edition is available on a removable medium (for example, a CD-ROM or 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.

About this task

Complete these steps to show the target system's FoD information, install, or uninstall the FoD license key(s) using OOB mode.

Procedure

1. Insert the removable medium with DSA Portable Edition into the laptop.
2. Start the DSA Portable Edition executable on the removable medium.
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.
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 IBM ID credential for the IBM website.

   --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).
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 failed to connect to CMM, the following error message is displayed: `Failed to connect CMM, Error code = **.`

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

Before you begin

The following prerequisites are necessary for this task:

- The DSA Portable Edition is available on a removable medium (for example, a CD-ROM or 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.

About this task

Complete these steps to display the target system's FoD information, install, or uninstall the FoD license key(s) using OOB mode.

Procedure

1. Insert the removable medium with DSA Portable Edition into the laptop.
2. Start the DSA Portable Edition executable on the removable medium.
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]>] | [--commnuity <commnuity>] |
    [--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.

   --commnuity <commnuity>
   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.
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]> |
 --commnuity <commnuity> | --authproto<MD5/SHA> | --privproto <DES/AES> |
 --privpasswd <password>
```

The definitions of the parameters are:

--ibmid userid:password>
The IBM ID credential for the IBM website.

--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.

--commnuity <commnuity>
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.

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]> |
 [--commnuity <commnuity>] | [--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.

--commnuity <commnuity>
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 failed to connect to Switch, the following error message is displayed:
`Failed to connect Switch, Error code = **.`

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

Before you begin

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.

About this task

Perform these steps to view, install, uninstall, and export the FoD License Key on a machine or reactivate the existing FoD activation keys on the replaced planar using the GUI.

Procedure

1. After placing the DSA Preboot Edition CD-ROM in the CD tray, start or restart the system.
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.
3. Select **Quit**.
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.
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.
6. Select **Activation Key Management** in the navigation pane or from the top menu to open the Activation Key Management page.
   - There are three categories for Activation Key Management:
     - IMM Key Management
     - CMM Key Management
     - IOM Key Management

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

Uninstall

Uninstalls selected installed activation keys.

a. Select one or more activation keys.
b. 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 IBM Website

Install activation keys from the IBM website.

a. Verify the internet connection is working.
b. Click **Install from IBM Website**. The Install Activation Key from IBM site dialog box opens for entering User Credentials and Details for each key.
c. Enter the following information.
   - IBM ID
   - User Password
   - Unique ID
   - AuthCode (optional). Authcode is required when the activation key file has not been created yet.
d. Select one or more activation keys and click **Install Now**.
e. 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 display the error message.

Install from Removable Media

Install the activation keys from local removable media.

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

Reactivate Activation Keys

Reactivates an inactive activation key.

a. Click **Reactivate Activation Keys**. The Reactivate Activation Keys dialog box is displayed. The first step is to check machine information.
b. If any of the information displayed for the machine type, machine model, or serial number needs to be updated, make the applicable changes.
c. 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.
d. Click **OK** to reboot the IMM automatically or click **Cancel** to reboot IMM manually at another time.
e. If you chose to reboot IMM immediately, click **Next** to obtain the activation keys from the removable media.

f. There are two methods for obtaining the activations keys. Select one of the following methods. The default method is **From the IBM website**.

From IBM website
Obtain activation keys from the IBM website.

Enter the following information:

- IBM ID
- User Password

From removable media
Obtain activation keys from available removable media.

g. 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 IMM key management

Procedure

1. Click **IMM** in the navigation pane.
2. Select one of the following methods of managing activations keys.
   - Manage Activation Keys for Local Machine
   - Manage Activation Keys for Remote Machine
3. If you selected **Manage Activation Keys for Remote Machine**, enter the following information:
   - IMM IP Address
   - User Name
   - Password
4. Select the protocol and enter the protocol port.
5. Click **Connect**. If the internet connection is available, all of the available activation keys will be listed, otherwise only the active activation keys are listed for that machine.
6. Select one of the activation key management operations listed in "Using Features on Demand GUI support for CD-based Preboot DSA" on page 33.
   - For the local machine, all six of the activation key management operations are supported.
   - For the remote machine, the first five activation key management operations (operation 1, 2. 3, 4, and 5) are supported.

Using CMM key management

Procedure

1. Click **CMM** in the navigation pane.
2. Enter the following information.
   - CMM IP Address
   - User Name
   - Password
3. Select the protocol and enter the protocol port for the CMM connection.

4. Click **Connect** to connect to the remote CMM. If the internet connection is available, all of the available activation keys will be listed, otherwise only the active activation keys are listed for the CMM.

   For CMM key management, the first five activation key management operations (operation 1, 2. 3, 4, and 5) are supported. For more information, see "Using Features on Demand GUI support for CD-based Preboot DSA" on page 33.

Using IOM key management

Procedure

1. Select **IOM Key Management** in the navigation pane. The connection setting is displayed in the right pane.
2. Enter the following information.
   - IP Address
   - Device Code for the IOM device
   - IP Address for the tftp server
   - Port for the tftp server setting
   - SNMP protocol setting to connect to the IOM device
3. Click **Connect** to connect to the remote IOM device. If the internet connection is available, all of the available activation keys will be listed, otherwise only the active activation keys are listed for the IOM device.

   For IOM key management, the first five activation key management operations (operation 1, 2. 3, 4, and 5) are supported. For more information, see "Using Features on Demand GUI support for CD-based Preboot DSA" on page 33.

Using Features on Demand CLI Support for CD-Based Preboot DSA

Before you begin

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.

About this task

Perform these steps to view, download, and install the FoD License Key on a machine or reinstall the existing FoD activation keys on a replaced planar using the command line interface.

Procedure

1. After placing the DSA Preboot Edition CD-ROM in the CD tray, start or restart the system.
2. Type `memtest` to launch the standalone memory test. Otherwise, the BoMC GUI launches 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.
3. Select **Quit**. This option stops the memory test and returns you to the DSA command line environment.
4. Click **Click here to start diagnostics (CLI)** to start the command line interface.

5. Select **3 - Features on Demand (FoD)**. The following options are displayed.
   - 1 - FoD Feature(s) on IMM
   - 2 - FoD Feature(s) on CMM
   - 3 - FoD Feature(s) on IOM/Switch
   - Q - Quit to Previous Menu

Using IMM key management

Procedure

1. Select **1 - FoD Feature(s) on IMM** to enter the interactive environment. A list containing four options is displayed.
2. Select **1 - Display Available FoD Feature(s)** to display the available FoD features for a specific IMM repository. If internet access is available, DSA will download the master XML from KMS and parse it to get the available FoD feature(s) for the specific system. If internet access is not available, no information is displayed.
3. Enter the following information to display the FoD features:
   - IMM authorization info: `<http(s)://userid:pwd@ip:[port]>` or press **Enter** to use the local IMM device.
   - Machine type of the system
   - IBMID Credential for the IBM website: `<userid:pwd>`
4. Select **2 - Report Active FoD key(s)** to report the active FoD key(s) on the IMM repository.
5. Enter the IMM authorization info: `<http(s)://userid:pwd@ip:[port]>` or press **Enter** to use the local IMM device.
6. Select **3 - Install FoD Key(s)** to install the FoD key(s) for specific FoD feature(s) or recover the existing FoD key(s) for a replaced planar. There are two methods for installing or recovering the FoD key(s). If internet access is available, you can install the FoD key(s) from the IBM website. If internet access is not available, you can install the FoD key(s) from removable media.
   - Install FoD Key(s) from the IBM website when internet access is available. DSA checks for internet access first.
   - Install FoD Key(s) from removable media (such as the USB key). If internet access is not available, DSA detects the removable media.
7. To report the active FoD keys, enter: IMM authorization info: `<http(s)://userid:pwd@ip:[port]>` or press **Enter** to use the local IMM device.

   The following list contains the FoD key options:

   Installing the FoDkey from the website:
   If you selected to install the FoD key from website, you will be prompted to enter the machine type. DSA downloads the master XML from KMS and parses it to get the available FoD feature(s) for that specific system.

   The available FoD feature(s) are displayed. You can select any FoD feature to install.

   An IBM authorization code and FoD UID are required to continue the installation.

   Installing the FoD key from removable media:
   If you selected to install the FoD key from removable media (such as a

USB key), a removable media with a folder named FoDKeys and all of the key files in this folder are required.

Insert the removable media to import the FoD key files. If the key file(s) is imported successfully, all of the key files are displayed in the console.

8. Select a key file to install.
9. Select **4 - Uninstall FoD Key(s)** to uninstall the FoD key(s) for specific FoD feature(s). Before the uninstallation, the active FoD key(s) are checked from the remote key repository and reported on the console.
10. To report the active FoD keys, enter: IMM authorization info: `<http(s)://userid:pwd@ip:[port]>`. After the active FoD Key(s) are displayed, you can select one or more of the FoD Keys to uninstall from the target system (IMM key repository).
11. Select **5 - Export FoD to Local Media** to export the FoD keys and FoD Unique Identifier(s). DSA collects all of the possible FoD UIDs and prompts you to insert a removable media. All of the FoD keys and the FoD UIDs are exported to the removable media.
12. Select **6 - Reactivate FoD keys**. The current Vital Product Data (VPD) information is displayed. It includes: machine type, machine model, and serial number.
13. Select **Y** to update the VPD information or **N** to skip the VPD update. When the update is complete, the new VPD will be in effect when the IMM is restarted.
14. Select **Y** to restart IMM. The restart process may take a few minutes.
15. Select one of the following methods for reactivating the keys.
    - To Reactivate from the IBM website, complete the following steps.
      a. Check the internet connection. If the internet is not available, set the proxy information.
      b. Enter the following credentials to log in to the IBM website:
         – User ID
         – Password

      As each of the FoD keys are downloaded sequentially, the keys are reactivated. A report indicating the results is displayed.
    - To Reactivate from removable media, complete the following steps.
      a. Insert the local media containing the FoD key files. DSA detects the removal media. The FoD key list is displayed.
      b. Select one of the following options:
         – Select an individual key to reactivate.
         – Enter **A** to reactivate all of the keys listed. Each of the all keys will be reactivated one by one automatically.

      The reactivation results are displayed.
16. Select **Q - Quit to Previous Menu** to return to the previous menu.

Using CMM key management

Procedure

1. Select **2 - FoD Feature(s) on CMM** to enter the interactive environment. A list containing four options is displayed.
2. Select **1 - Report Active FoD key(s) to report the active FoD key(s)** to report the active FoD key(s) on the CMM repository.

a. Enter CMM authorization info: `<userid:pwd@ip:[port]>`

3. Select **Install FoD Key(s)** to install the FoD key. There are two methods for installing the FoD key(s). If internet access is available, you can install the FoD key(s) from the IBM website. If internet access is not available, you can install the FoD key(s) from removable media.
   - Install FoD Key(s) from the IBM website when internet access is available. DSA checks for internet access first.
   - Install FoD Key(s) from removable media (such as a USB key). If internet access is not available, DSA detects the removable media.
4. Enter the following information to report the active FoD keys:
   a. CMM authorization info: `<http(s)://userid:pwd@ip:[port]>`
      - If you selected to install the FoD key from the website, you are prompted to enter the machine type. DSA downloads the master XML from KMS and parses it to get the available FoD feature(s) for the specific system. All of the available FoD feature(s) are displayed. You can select any FoD feature to install. An IBM authorization code and FoD UID are required to continue the installation.
      - If you selected to install the FoD key from removable media (such as a USB key), removable media with a folder named FoDKeys and all of the key files in this folder are required.

   b. Insert the removable media to import the FoD key files.

      If the key file(s) imported successfully, all of the key files are displayed in the console.

   c. Select a key file to install.
5. Select **4 - Uninstall FoD Key(s)** to uninstall the FoD key(s). Before the uninstallation, the active FoD key(s) are checked from the remote key repository and reported on the console. The following information is required for reporting the active FoD keys:
   - CMM authorization info: `<http(s)://userid:pwd@ip:[port]>`

   After the active FoD Key(s) are displayed, select the FoD keys you want to uninstall from the target system (CMM key repository).
6. Select **Q - Return to Previous Menu** to return to the previous menu.

Using IOM key management

Procedure

1. Select **3 - FoD Feature(s) on IOM/Switch** to enter the interactive environment. A list containing four options is displayed.
2. Select **1 - Report Active FoD key(s)** to report the active FoD key(s) on the Switch repository.
3. Enter the following information to report the active FoD key(s):
   a. `Switch host IP`
   b. `TFTP server for SNMP interface<[user:pwd@ip]:[port]>`
   c. Select one of the following SNMP versions:
      - SNMPv1 or SNMPv2
      - SNMPv3
   d. If you selected SNMPv1 or SNMPv2, the **`Community`** parameter is required.
   e. If you selected SNMPv3 , enter the following information.
      - User name
      - Authorization password

- Authorization protocol
- Privacy protocol
- Privacy password

4. Select **Install FoD Key(s)** to install the FoD key. There are two methods for installing the FoD key(s):
   - Install FoD Key(s) from the IBM website when internet access is available. DSA checks for internet access first.
   - Install FoD Key(s) from removable media (such as a USB key). If internet access is not available, DSA detects the removable media.
5. Enter the following information to report the active FoD keys:
   a. `Switch host IP`
   b. `TFTP server for SNMP interface<[user:pwd@ip]:[port]>`
   c. Select one of the following SNMP versions:
      - SNMPv1 or SNMPv2
      - SNMPv3
   d. If you selected SNMPv1 or SNMPv2, the **`Community`** parameter is required.
   e. If you selected SNMPv3 , enter the following information.
      - User name
      - Authorization password
      - Authorization protocol
      - Privacy protocol
      - Privacy password
      - If you selected to install the FoD key from the website, you are prompted to enter the machine type for downloading the master XML from KMS and parse it to get all of the available FoD feature(s). The available FoD feature(s) are displayed. You can select any FoD feature to install. An IBM authorization code and FoD UID are required to continue the installation.
      - If you selected to install the FoD key from removable media, removable media with a folder named `FoDKeys` and all of the key files in this folder are required.
6. Complete the following steps.
   a. Insert the removable media to import the FoD key files.
   b. Select a key file to install.
7. Select **3 - Uninstall FoD Key(s)** to uninstall the FoD key(s). Before the uninstallation, the active FoD key(s) are checked from the remote key repository (Switch) and reported on the console. The following information is required to report the active FoD keys:
   a. `Switch host IP`
   b. `TFTP server for SNMP interface<[user:pwd@ip]:[port]>`
   c. Select one of the following SNMP versions:
      - SNMPv1 or SNMPv2
      - SNMPv3
   d. If you selected SNMPv1 or SNMPv2, the **`Community`** parameter is required.
   e. If you selected SNMPv3 , enter the following information.
      - User name
      - Authorization password
      - Authorization protocol

- Privacy protocol
- Privacy password

If you selected to install the FoD key from removable media, removable media with a folder named FoDKeys and all of the key files in this folder are required.

f. If you selected to install the FoD key from website, you are prompted to enter the machine type. DSA downloads the master XML from KMS and parses it to get the available FoD feature(s) for the specific system. The available FoD features are displayed. You can select any FoD feature to uninstall. An IBM authorization code and FoD UID are required to continue.

After the active FoD Key(s) are displayed, select the FoD keys you want to uninstall from the target system (Switch key repository).

8. Select **Q - Return to Previous Menu** to return to the previous menu.
9. Select **Quit** to exit the DSA interactive menu.

Using Features on Demand GUI support for Embedded Preboot DSA

Before you begin

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

About this task

Perform these steps to view, install, or uninstall the FoD License Key on a machine or reactivate the existing FoD activation keys on a replaced planar using the GUI.

Procedure

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.
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.
3. Type `gui` to launch the graphical DSA environment.
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.
5. Select **Activation Key Management** in the navigation pane or from the top menu to open the Activation Key Management page.
   - There are three categories for Activation Key Management:
     - IMM Key Management
     - CMM Key Management
     - IOM Key Management

   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.

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

Uninstall

Uninstall the selected installed activation keys.

Complete the following steps.

a. Select one or more activation keys.
b. 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 IBM Website

Install an activation key from the IBM website.

Complete the following steps.

a. Verify the internet connection is working.
b. Select one or more activation keys.
c. Click **Install from IBM Website**. The Install Activation Key from IBM site dialog box is displayed for entering user credentials and details for each key.
d. Enter the following information.
   - IBM ID
   - User Password
   - Unique ID
   - AuthCode (optional). AuthCode is required when the activation key file was not created yet.
e. Select one or more activation keys and click **Install Now**.
f. 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.

a. Click **Install from Removable Media**. The Install Activation Key from Removable Media dialog box is displayed.
b. Select one of the removable media. The activation key files in the removable media are displayed.
c. Select one or more of the activation key files and click the **OK**.
d. 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

Install the activation keys from local removable media.

Complete the following steps.

a. Click **Reactivate Activation Keys**. The Reactivate Activation Keys dialog box is displayed. The first step is to check machine information.

b. If any of the information displayed for machine type, machine model, or serial number needs to be updated, make the applicable changes.

c. 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.

d. Click **OK** to reboot the IMM automatically or click **Cancel** to reboot IMM manually at another time.

e. If you chose to reboot IMM immediately, click **Next** to obtain the activation keys from the removable media.

f. 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 IBM website**.

From IBM website

To obtain activation keys from the IBM website, perform the following steps.

- Enter the following information:
  - IBM ID
  - User Password
- Click **Next** to obtain the activation keys from the IBM website.

From removable media

All available removable media is detected.

g. 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.

Using IMM Key Management

Procedure

1. Click **IMM** in the navigation pane.
2. Select one of the following methods of managing activations keys.
   - Manage Activation Keys for Local Machine
   - Manage Activation Keys for Remote Machine
3. If you select Manage Activation Keys for Remote Machine, enter the following information:
   - IMM IP Address
   - User Name
   - Password
4. Select the protocol and enter the protocol port.

5. Click **Connect**. If the internet connection is available, all of the available activation keys are listed, otherwise only the active activation keys are listed for the machine.
6. Select one of the activation key management operations listed in "Using Features on Demand GUI support for Embedded Preboot DSA" on page 41.
   - For the local machine, all six of the activation key management operations are supported.
   - For the remote machine, the first five activation key management operations (operation 1, 2. 3, 4, and 5) are supported.

Using CMM key management

Procedure

1. Click **CMM** in the navigation pane.
2. Enter the following information.
   - CMM IP Address
   - User Name
   - Password
3. Select the protocol and enter the protocol port for the CMM connection.
4. Click **Connect** to connect to the remote CMM. If the internet connection is available, all of the available activation keys are listed, otherwise only the active activation keys are listed for the CMM.

   For CMM key management, the first five activation keys management operations (Operation 1, 2, 3, 4, and 5) are supported. For more information, see "Using Features on Demand GUI support for CD-based Preboot DSA" on page 33.

Using IOM key management

Procedure

1. Select **IOM Key Management** in the navigation pane. The connection setting is displayed in the right pane.
2. Enter the following information.
   - IP Address of the IOM device
   - Device Code for the IOM device
   - IP Address for tftp server
   - Port for the tftp server
   - SNMP protocol setting to connect to the IOM device
3. Click **Connect** to connect to the remote IOM device. If the internet connection is available, all of the available activation keys are listed, otherwise only the active activation keys are listed for the IOM device.

   For IOM key management, the first five activation keys management operations (Operation 1, 2, 3, 4, and 5) are supported. For more information, see "Using Features on Demand GUI support for CD-based Preboot DSA" on page 33.

Using Features on Demand CLI Support for Embedded Preboot DSA

Before you begin

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

About this task

Perform these steps to view, download, and install the FoD License Key on a machine or reinstall the existing FoD activation keys on a replaced planar using the command line interface.

Procedure

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.
2. Select **Quit**.

   The standalone memory diagnostic does not support all systems. If the machine type is not supported, the **F2** boot will skip the standalone memory test. No error message is displayed. This option stops the memory test and returns you to the DSA command-line environment.
3. Type `cmd` to launch the command line DSA environment.
4. Select **3 - Feature on Demand (FoD)**. The following FoD Feature options are displayed.
   - 1 - FoD Feature(s) on IMM
   - 2 - FoD Feature(s) on CMM
   - 3 - FoD Feature(s) on IOM/Switch
   - Q - Quit to Previous Menu

Using IMM key management

Before you begin

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

Procedure

1. Select **1 - FoD Feature(s) on IMM** to enter the interactive environment. A list containing four options is displayed.
2. Select **1 - Display Available FoD Feature(s)** to display the available FoD features for a specific IMM repository. If internet access is not available, no information is displayed.
3. Enter the following information to display the FoD features:
   a. IMM authorization info: `<userid:pwd@ip:[port]>[Local IMM Device]:`
   b. Machine type of the system.
   c. IBMID Credential for IBM website to continue:**<userid:pwd>**
4. Select **2 - Report Active FoD key(s)** to report the active FoD key(s) on the IMM repository:
   a. IMM authorization info: `<userid:pwd@ip:[port]>[Local IMM Device]:`
5. Select **3 - Install FoD Key(s)** to install the FoD key(s) for specific FoD feature(s) or recover the existing FoD key(s) for a replaced planar. There are two methods for installing or recovering the FoD key(s). If internet access is available, you can install the FoD key(s) from the IBM website. If internet access is not available, you can install the FoD key(s) from removable media.
   - Install FoD Key(s) from IBM website when internet access is available. DSA checks for internet access first.

- Install FoD Key(s) from removable media (such as a USB key). If internet access is not available, DSA detects the removable media.

6. Enter the following information to report the active FoD keys:
   a. IMM authorization info: `<userid:pwd@ip:[port]>[Local IMM Device]:`
   b. Machine type of the system. If you selected to install the FoD key from website, you are prompted to enter the machine type to download the master XML from KMS and parse it to get all of the available FoD feature(s). The available FoD feature(s) are displayed. You can select any FoD feature to install. An IBM authorization code and FoD UID are required to continue the installation.
   c. Insert the removable media to import the FoD key files.

      If you selected to install the FoD key from removable media (such as a USB key), removable media with a folder named FoDKeys and all of the key files in this folder are required.

      If the key file(s) is imported successfully, all of the key files are displayed in the console.
   d. Select a key file to install.
7. Select **4 - Uninstall FoD Key(s)** to uninstall the FoD key(s) for specific FoD feature(s). Before the uninstallation, the active FoD key(s) are checked from the remote key repository and reported on the console. The following information is needed to report the active FoD keys:

   IMM authorization info: `<userid:pwd@ip:[port]>[Local IMM Device]:` After the active FoD Key(s) are displayed, select the key(s) you want to uninstall from the target system (IMM key repository).
8. Select **5 - Export FoD to Local Media** to export the FoD keys and FoD Unique Identifier(s). DSA collects all of the possible FoD UIDs and then prompts you to insert removable media. All of the FoD keys and the FoD UIDs are exported to the removable media.
9. Select **6 - Reactivate FoD Keys**. The current Vital Product Data (VPD) information is displayed and includes: machine type, machine model, and serial number.
10. Select **Y** to update the VPD information or **N** to skip the VPD update. When the update is complete, the new VPD will take effect when the IMM is restarted.
11. Select **Y** to restart the IMM. The restart process may take a few minutes.
12. Select one of the following methods for reactivating the keys.
    - To Reactivate from the IBM website, complete the following steps.
      a. Check the internet connection. If the internet is not available, set the proxy information.
      b. Enter the following credentials to log into the IBM website:
         – User ID
         – Password

      The FoD keys are downloaded sequentially, and the keys are reactivated. A report providing the results is displayed.
    - To Reactivate from removable media, complete the following steps.
      a. Insert the local media containing the FoD key files. DSA detects the removal media. The FoD key list is displayed.
      b. Select a key or enter **A** to reactivate this key. A report indicating the results is displayed.

Each of the selected FoD keys will be reactivated. A report providing the results is displayed.

13. Select **Q - Quit to Previous Menu** to return to the previous menu.

Using CMM key management

Before you begin

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

Procedure

1. Select **2 - FoD Feature(s) on CMM** to enter the interactive environment. A list containing four options is displayed.
2. Select **1 - Report Active FoD key(s) to report the active FoD key(s)** to report the active FoD key(s) on the CMM repository.
   a. Enter CMM authorization info: `<userid:pwd@ip:[port]>`
3. Select **Install FoD Key(s)** to install the FoD key. There are two methods for installing the FoD key(s). If internet access is available, you can install the FoD key(s) from the IBM website. If internet access is not available, you can install the FoD key(s) from removable media.
   - Install FoD Key(s) from IBM website when internet access is available. DSA checks for internet access first.
   - Install FoD Key(s) from removable media (such as a USB key). If internet access is not available, DSA detects the removable media.
4. Complete the following steps to report active FoD keys:
   a. Enter the following information to report the active FoD keys:
      - CMM authorization info:`<userid:pwd@ip:[port]>` or press**Enter** to use the local IMM device.
      - Machine type of the system.

        If you selected to install the FoD key from the website, you are prompted to enter the machine type. DSA downloads the master XML from KMS and parses it to get the available FoD feature(s) for the specific system. The available FoD feature(s) are displayed. You can select any of the FoD features to install. An IBM authorization code and FoD UID are needed to continue the installation.

   b. Insert the removable media to import the FoD key files.

      If you selected to install the FoD key from removable media (such as a USB key), removable media with a folder named FoDKeys and all of the key files in this folder are required.

      If the key file(s) is imported successfully, all of the key files are displayed in the console.

   c. Select a key file to install.
5. Select **4 - Uninstall FoD Key(s)** to uninstall the FoD key(s). Before the uninstallation, the active FoD key(s) are checked from the remote key repository and reported on the console. The following information is required to report the active FoD keys:
   - CMM authorization info: `<userid:pwd@ip:[port]>`

   The active FoD Key(s) are displayed.
6. Select one of the following options to uninstall a key(s) from the target system (CMM key repository):

- Select an individual key to uninstall.
- Enter **A** to uninstall all of the keys listed. Each of the all keys will be uninstalled one by one automatically.

7. Select **Q - Return to Previous Menu** to return to the previous menu.

Using IOM key management

Before you begin

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

Procedure

1. Select **3 - FoD Feature(s) on IOM/Switch** to enter the interactive environment. A list containing four options is displayed.
2. Select **1 - Report Active FoD key(s)** to report the active FoD key(s) on the Switch repository.
3. Enter the following information to report the active FoD key(s) on the Switch repository.
   - Switch authorization info: `<userid:pwd@ip:[port]>`
   - TFTP server for SNMP interface: `<<tftp>://user:pwd@ip:[port}>`
   - Community for SNMPv1 or SNMPv2: `<public|private>`
   - Authorization protocol for SNMPv3: `<MD5|SHA>`
   - Privacy protocol for SNMPv3 : `<DES|AES>`
   - Privacy password for SNMPv3
4. Select **Install FoD Key(s)** to install the FoD key. There are two methods to install the FoD key(s). If internet access is available, you can install the FoD key(s) from the IBM website. If internet access is not available, you can install the FoD key(s) from removable media.
   - Install FoD Key(s) from the IBM website when internet access is available. DSA checks for internet access first.
   - Install FoD Key(s) from removable media (such as a USB key). If internet access is not available, DSA detects the removable media.
5. Enter the following information to report the active FoD keys:
   - Switch authorization info: `<userid:pwd@ip:[port]>`
   - TFTP server for SNMP interface: `<<tftp>://user:pwd@ip:[port}>`
   - Community for SNMPv1 or SNMPv2: `<public|private>`
   - Authorization protocol for SNMPv3: `<MD5|SHA>`
   - Privacy protocol for SNMPv3 : `<DES|AES>`
   - Privacy password for SNMPv3
   - Machine type of the system.

     If you selected to install the FoD key from the website, you are prompted to enter the machine type to download the master XML from KMS and parse it to get all the available FoD feature(s). The available FoD feature(s) are displayed. Select any FoD feature to install. An IBM authorization code and FoD UID are needed to continue the installation.
6. Insert the removable media to import the FoD key files.

   If you selected to install the FoD key from removable media (such as a USB key), removable media with a folder named FoDKeys and all of the key files in this folder are required.

If the key file(s) is imported successfully, all of the key files are displayed in the console

7. Select a key file to install.
8. Select **3 - Uninstall FoD Key(s)** to uninstall the FoD key(s). Before the uninstallation, the active FoD key(s) are checked from the remote key repository (Switch) and reported on the console. The following information is required to report the active FoD keys:
9. Enter the following required information for reporting the active FoD keys:
   - Switch authorization info: `<userid:pwd@ip:[port]>`
   - TFTP server for SNMP interface: `<<tftp>://user:pwd@ip:[port}>`
   - Community for SNMPv1 or SNMPv2: `<public|private>`
   - Authorization protocol for SNMPv3: `<MD5|SHA>`
   - Privacy protocol for SNMPv3 : `<DES|AES>`
   - Privacy password for SNMPv3

   After the active FoD Key(s) are displayed, select the key(s) you want to uninstall from the target system (Switch key repository).
10. Select **Q - Return to Previous Menu** to return to the previous menu.
11. Select **Quit** to exit the DSA interactive menu.

Chapter 10. Troubleshooting and support

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

For solutions to problems that other customers have encountered, see the IBM System x Forum customer forum at https://www.ibm.com/developerworks/community/forums/html/forum?id=11111111-0000-0000-0000-000000002691#topicsPg=0.

Known limitations, problems, and workarounds

This section describes limitations, problems, and workarounds that are applicable to Dynamic System Analysis. See the Readme document for the version of Dynamic System Analysis that you are using for the most recent limitations, problems, and workarounds.

Known limitations for the 9.41 release

Note to Reviewers: In addition to adding the following new limitation for 9.41, I have edited this topic for clarity, grammar, etc. Please review. Thanks, Jeanne

The following list contains the known limitations for the current 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, DSA firmware version
- Immv1 embedded pDSA 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 website, 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, please 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 run 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 IBM 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 fatal 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 website, 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 a 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 *1AOO34V* or later before updating pDSA, 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_dsyt`, 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 the 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 IBM 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 IMMv1systems, 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 MCP 5.2 for legacy systems. Preboot DSA standalone (CD boot or USB-key boot) uses MCP 6.1 for all systems.
  - Preboot DSA (embedded or standalone) using MCP 6.1 does not support the data collection on the QLogic adapter since the QLogic driver 1.01.02.d4 packaged in MCP 5.2 cannot be used in MCP 6.1.
  - The Software License Agreement (SLA) has traditional Chinese wording issue in MCP 5.2. This issue is fixed in MCP 6.1 in Preboot DSA 4.00 in 2011. However, those systems with Preboot DSA embedded based on MCP 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 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 (e.g. DSYT89O)
  - The Preboot DSA level starting with D6YT (e.g. D6YT29A)
  - The Preboot DSA level starting with TMYT (e.g. TMYT19A)
  - The Preboot DSA level starting with yuoo (e.g. yuoo890)
  - The Preboot DSA level starting with y4yt (e.g. 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 via 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 MCP6.1 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

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 configures, 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 will be lost.

Dynamic System Analysis core dump file

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

On Windows, the core dump file, name DSA_CORE.dmp, is created in the directory where DSA was run.

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

Getting help and technical assistance

Use this information to locate technical assistance for your IBM System x and BladeCenter tools.

About this task

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This section contains information about where to go for additional information about IBM and IBM 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

Use this information before you call Service and Support and report a problem.

About this task

Before you call, make sure that you have taken these steps to try to solve 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 the IBM support website at www.ibm.com/systems/support/ to check for technical information, hints, tips, and new device drivers.
- Use an IBM discussion forum on the IBM website to ask questions.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the documentation that is provided with your IBM product. The documentation that comes with IBM systems 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

Use this information for locating detailed information on using the documentation.

About this task

Information about your IBM system and preinstalled software, if any, or optional device is available in the documentation that comes with the product. That documentation can include information centers, online documents, printed documents, readme files, and help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to the IBM support website at www.ibm.com/systems/support/ and follow the instructions. Also, some documents are available through the IBM Publications Center website at www.ibm.com/shop/publications/order/. Documentation for IBM System x and BladeCenter tools are available in the IBM ToolsCenter website at www.ibm.com/shop/publications/order/.

Getting help and information from the World Wide Web

Use this information to find the latest information about IBM systems, optional devices, services, and support.

About this task

On the World Wide Web, the IBM website has up-to-date information about IBM systems, optional devices, services, tools, and support. The address for IBM System x information is www.ibm.com/systems/x/. The address for IBM BladeCenter information is www.ibm.com/systems/bladecenter/. The address for IBM IntelliStation® information is www.ibm.com/intellistation/.

You can find service information for IBM systems and optional devices at www.ibm.com/systems/support/.

Software service and support

Use this information to contact IBM service and support with questions about your IBM System x and BladeCenter tools.

About this task

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with System x servers, BladeCenter products, IntelliStation workstations, and appliances. For information about which products are supported by Support Line in your country or region, see www.ibm.com/services/sl/products/.

For more information about Support Line and other IBM services, see www.ibm.com/services/, or see www.ibm.com/planetwide/ for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

Hardware service and support

Use this contact information to order new equipment or request IBM service support.

About this task

You can receive hardware service through IBM Services or through your IBM reseller, if your reseller is authorized by IBM to provide warranty service. See www.ibm.com/planetwide/for support telephone numbers, or in the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

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 IBM ToolsCenter for System x and BladeCenter information center, and its related publications, are accessibility-enabled.

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

IBM and accessibility

See the IBM Human Ability and Accessibility Center website for more information about the commitment that IBM has to accessibility.

Appendix B. Dynamic System Analysis commands

You can preform 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 **ibm_utl_dsa_v.r.m_portable_platform** command to collect information about the local system.

Syntax

```
ibm_utl_dsa_v.r.m_portable_platform -? | -h

ibm_utl_dsa_v.r.m_portable_platform -l

ibm_utl_dsa_v.r.m_portable_platform -b

ibm_utl_dsa_v.r.m_portable_platform -diags

ibm_utl_dsa_v.r.m_portable_platform --chkupd --proxy-address=ip_address
--proxy-port=portnum --proxy-user=userid --proxy-password=password

ibm_utl_dsa_v.r.m_portable_platform [-i data_file]
```

```
ibm_utl_dsa_v.r.m_portable_platform -r [data_file] -v [-i data_file]

ibm_utl_dsa_v.r.m_portable_platform -t [user_id:password@IP[:port]/path/]]
-i data_file

ibm_utl_dsa_v.r.m_portable_platform --update

ibm_utl_dsa_v.r.m_portable_platform -ux [-x] [-v] [-text]

ibm_utl_dsa_v.r.m_portable_platform --ipmi-lan
user_id:password@ip_address[:port]

ibm_utl_dsa_v.r.m_portable_platform --vmware-esxi
user_id:password@ip_address[:port]

ibm_utl_dsa_v.r.m_portable_platform [-x] [-text] [-v [-html]] [-i
data_file] [-d output_directory] [-dumpxml] [-f]

ibm_utl_dsa_v.r.m_portable_platform --update --proxy-address=ip_address
--proxy-port=portnum --proxy-user=userid --proxy-password=password

ibm_utl_dsa_v.r.m_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, you must 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\IBM\DSA`). Use the **ibm_utl_dsa_v.r.m_portable_platform.exe** command.

To run this command on a system running Linux, use **ibm_utl_dsa_v.r.m_portable_platform**.

If no options are specified, this command collects and saves information in a compressed XML file in the `installation_directory\IBM_Support\` on Windows systems or`/var/log/IBM_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 CIM Web-Based Enterprise Management (WBEM) website 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 IBM website 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*.

--cmm userid:password@hostip:[port]
This option is used to collect CMM data via Out-of Band mode.

-d *output_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%/IBM_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.

Tips:
- 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 via 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)

Tips:

- 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.

-i *data_file*
Reads input from the specified file instead of collecting data from the local server.

-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.

-r *data_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.

Tip:

- 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 via Out-Of-Band mode. In this mode, portable DSA collects FFDC log from CMM/IMM. Currently only FFDC from CMM is available.

-t [*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.

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.

Tip: If you specify this option with no arguments, the data file is transferred to the testcase.boulder.ibm.com/eserver/toibm/xseries/ FTP server by default.

-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 IBM 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_arch *32*|*64*
Used with --chkupd or --update options to specify the architecture.

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

--update_os
windows|*rhel4*|*rhel4*|*rhel5*|*sles9*|*sles10*|*sles11*|*vmware3.5*|*vmware4.0*
Used with --chkupd or --update options to specify the operating system.

-upload [IBMid:*id***]**
Sends inventory data to the Electronic Services web portal for use in proactive support functions such as My Systems and My Notifications. The data is sent using HTTPS.

The IBM ID is the ID that is authorized to view the inventory data sent using the Electronic Services web portal page. If you specify this option with no IBM ID, the data is sent, but you will not be able to access it using the Electronic Services web portal.

-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-esxi *user_id*:*password*@*ip_address*[:*port*]
Collect system information from the specified remote system running VMware ESXi.

Tip: 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.

Tips:

- 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*\IBM_Support\ on Windows systems or /var/log/IBM_Support on Linux systems.

   Windows **ibm_utl_dsa_*v.r.m_portable_platform*.exe**

   Linux **ibm_utl_dsa_*v.r.m_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:\IBM_Support\` and then saves the data in HTML and text format.

   Windows **ibm_utl_dsa_*v.r.m_portable_platform*.exe -i *input***

   Linux **ibm_utl_dsa_*v.r.m_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:\IBM_Support\` and then saves the data in default output directory in HTML and text format.

   Windows **ibm_utl_dsa_*v.r.m_portable_platform*.exe -v -text -i *input***

   Linux **ibm_utl_dsa_*v.r.m_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. This interface (FoD) is executed using sub commands after 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.	*--help*	None	Output subcommand **display_available_fod** usage help screen to stdout.
	--device	device	This option is used to specify the target key repository for the supported devices: IMM, CMM, and Switch.
	--ibmid	userid: password	This option is used to specify the credential IBM ID for the interactive authorization by IBM website.
	--host	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.
	--mt	machinetype	This option is used for the machine type of device (IMM, CMM, Switch).

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

Subcommand	Command-line option (case sensitive)	Argument	Description
download_fod_key: This subcommand is used to acquire and download the activation key from an IBM website (KMS).	*--help*	None	Output subcommand download_fod_key usage help screen to stdout.
	--ibmid	userid: password	This option is used to specify the IBM ID credential for the interactive authorization by IBM website.
	--uid	unique_id	This option is the unique identifier information of FoD feature.
	--authcode	[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.
	--mt	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.	*--help*	None	Output subcommand **install_fod_key** help screen to stdout.
	--keyfile	keyfile	This option is used to specify a single activation key file.
	--device	device	This option is used to specify the target key repository. The supported devices: IMM, CMM, Switch.
	--host	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.
	--tftp	userid:password @ip:[port]	This option is used to specify the TFTP server for snmp interface.

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

Subcommand	Command-line option (case sensitive)	Argument	Description
	--community	community	This option is used to specify the community for snmpv1v2, default: public.
	--authproto	[--authproto]	This option is used to specify the authorization protocol for snmpv3, default: No auth.
	--privproto	[DES/AES]	This option is used to specify the privacy protocol for snmpv3. Default: No privacy.
	--privpasswd	[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.	*--help*	None	Output subcommand export_imm_uid usage help screen to stdout.
	--export_imm_uid	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.	*--help*	None	Output subcommand report_imm_active_fod usage help screen to stdout.

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

Subcommand	Command-line option (case sensitive)	Argument	Description
	--host	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.	*--help*	None	Output subcommand install_imm_fod usage help screen to stdout.
	--ibmid	userid: password	This option is used to specify the credential IBM ID for the interactive authorization by IBM website.
	--uid	unique_id	This option is the unique identifier information of FoD feature.
	--authcode	[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.
	--mt	machinetype	This option is used to specify the machine type of target device.
	--host	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.	*--help*	None	Output subcommand uninstall_imm_fod usage help screen to stdout.
	--keyid	keyid	This option is used to specify the activation key ID returned from report command. If *keyid* is all, it will uninstall all keys.

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

Subcommand	Command-line option (case sensitive)	Argument	Description
	--host	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.	*--help*	None	Output subcommand report_cmm_active_fod usage help screen to stdout.
	--host	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.	*--help*	None	Output subcommand install_cmm_fod usage help screen to stdout.
	--ibmid	userid: password	This option is used to specify the IBM ID credential for the interactive authorization by IBM website. **Note:** Requires an internet connection.
	--uid	unique_id	This option is the unique identifier information of FoD feature.

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

Subcommand	Command-line option (case sensitive)	Argument	Description
	--authcode	[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.
	--mt	machinetype	This option is used to specify the machine type of the target device.
	--host	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.	*--help*	None	Output subcommand uninstall_cmm_fod usage help screen to stdout.
	--keyid	keyid	This option is used to specify the activation key ID returned from report command. If *keyid* is all, it will uninstall all keys.
	--host	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.	*--help*	None	Output subcommand report_switch_ active_fod usage help screen to stdout.
	--host	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.
	--host	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.
	--tftp	userid:password @ip:[port]	This option is used to specify the TFTP server for the snmp interface.
	--community	community	This option is used to specify the community for snmpv1v2; default: public.
	--authproto	report_switch_ active_fod	This option is used to specify the authorization protocol for snmpv3; default: No auth.
	--privproto	[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.	*--help*	None	Output subcommand install_switch_fod usage help screen to stdout.
	--ibmid	userid: password	This option is used to specify the credential IBM ID for the interactive authorization by the IBM website.

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

Subcommand	Command-line option (case sensitive)	Argument	Description
	--uid	unique_id	This option is the unique identifier information of FoD feature.
	--authcode	[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.
	--mt	Machinetype	This option is used to specify the machine type of target device.
	--host	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.
	--tftp	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.
	--community	community	This option is used to specify the community for snmpv1v2; default: public.
	--authproto	[--authproto]	This option is used to specify the authorization protocol for snmpv3; default: No auth.
	--privproto	[DES/AES]	This option is used to specify the privacy protocol for snmpv3; default: No privacy.
	--privpasswd	[--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.	*--help*	None	Output subcommand uninstall_switch_fod usage help screen to stdout.

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

Subcommand	Command-line option (case sensitive)	Argument	Description
	--keyid	Keyid	This option is used to specify the activation key ID returned from the report command. If *keyid* is all, it will uninstall all keys.
	--host	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.
	--tftp	userid:password @ip:[port]	This option is used to specify the TFTP server for the snmp interface.
	--community	community	This option is used to specify the community for snmpv1v2; default: public.
	--authproto	[--authproto]	This option is used to specify the authorization protocol for snmpv3; default: No auth.
	--privproto	[DES/AES]	This option is used to specify the privacy protocol for snmpv3; default: No privacy.
	--privpasswd	[--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**).

Tip:

- The plug-in names are displayed when collection occurs.
- The *DSA_INCLUDE* and *DSA_EXCLUDE* variables are mutually exclusive.
- To reset the effect of this 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 IBM 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**).

Tips:

- The plug-in names are displayed when collection occurs.
- The *DSA_INCLUDE* and *DSA_EXCLUDE* variables are mutually exclusive.
- To reset the effect of this 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 IBM 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 IBM 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.

Notices

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

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

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

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

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

IBM World Trade Asia Corporation
Licensing 2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

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

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

IBM Corporation
MW9A/050
5600 Cottle Road
San Jose, CA 95193
U.S.A.

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

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

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

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

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

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

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

Trademarks

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

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

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

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

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

Index

Readers' Comments — We'd Like to Hear from You

IBM Systems
Dynamic System Analysis
Installation and User's Guide
Version 9.41

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Send your comments to the address on the reverse side of this form.

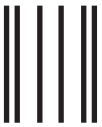
If you would like a response from IBM, please fill in the following information:

Name	Address
Company or Organization	
Phone No.	Email address

Readers' Comments — We'd Like to Hear from You

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape



NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
ATTN: Dept IPRA
PO Box 12195
Research Triangle Park, NC
USA 27709-9990

Fold and Tape **Please do not staple** Fold and Tape

Cut or Fold
Along Line

Printed in USA