IBM Systems

Dynamic System Analysis Installation and User's Guide

Version 9.20

IBM Systems

Dynamic System Analysis Installation and User's Guide

Version 9.20

Note

Before using this information and the product it supports, read the information in "Notices" on page 87.

This edition applies to version 9.20 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**

  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

- ***Installation and User's Guide***

  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**

  www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=TOOL-CENTER&brandind=5000016

  View this website to download tools that support IBM System x and IBM BladeCenter products.

- **Dynamic System Analysis**

  www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=SERV-DSA&brandind=5000016

  View this website to download the Dynamic System Analysis tool and documentation.

- **Support for IBM BladeCenter**

  www-304.ibm.com/systems/support/supportsite.wss/brandmain?brandind=5000020

  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-947.ibm.com/support/entry/portal/Overview?brandind=Hardware~Systems~System_x

  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**

  www.ibm.com/developerworks/forums/forum.jspa?forumID=740

  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 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 9.20 provides additional systems support.

New hardware support

Dynamic System Analysis supports several new systems, LSI RAID controllers, Fibre Channel adapters, Ethernet adapters, and tape drives. For a complete list of supported hardware, see “Supported hardware” on page 4

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:

- IBM System x3200 M2, machine type 4367,4368
- IBM System x3200 M3, machine type 7327, 7328
- IBM System x3250 M2, machine type 7657, 4190, 4191, 4194
- IBM System x3250 M3, machine type 4251, 4252, 4261
- IBM System x3250 M4, machine type 2583
- IBM System x3400, machine type 7973, 7974, 7975, 7976
- IBM System x3400 M2, machine type 7836, 7837
- IBM System x3400 M3, machine type 7378, 7379
- IBM System x3500, machine type 7977
- IBM System x3500 M2 machine type 7839
- IBM System x3500 M3, machine type 7380
- IBM System x3500 M4, machine type 7383
- IBM System x3530 M4, machine type 7160
- IBM System x3550, machine type 1013, 1913, 7978
- IBM System x3550 M2, machine type 4198, 7946
- IBM System x3550 M3, machine type 4254, 7944
- IBM System x3550 M4, machine type 7914
- IBM System x3620 M3, machine type 7376
- IBM System x3630 M3, machine type 7377
- IBM System x3630 M4, machine type 7158
- IBM System x3650, machine type 1914, 7979
- IBM System x3650 M2, machine type 4199, 7947
- IBM System x3650 M3, machine type 4255, 5454, 7945
- IBM System x3650 M4, machine type 7915
- IBM System x3690 X5, machine type 7147, 7148, 7149, 7192
- IBM System x3750 M4, machine type 8722,8733
- IBM System x3755 M3, machine type 7164
- IBM System x3850 M2/System x 3950 M2, machine type 7141, 7144, 7233, 7234
- IBM System x3850 X5, machine type 7143, 7145, 7146, 7191
- IBM System x3950 M2 2-4 node, machine type 7141, 7233, 7234
- IBM System x3950 X5, machine type 7143, 7145, 7146, 7191
- BladeCenter HS12, machine type 8014, 8028, 1916
- BladeCenter HS21, machine type 1885, 8853
- BladeCenter HS21 XM, machine type 1915, 7995
- BladeCenter HS22, machine type 7870, 1936, 7809, 1911
- BladeCenter HS22V, machine type 1949, 7871
- BladeCenter HS23, machine type 7875
- BladeCenter HS23E, machine type 8038, 8039
- BladeCenter HX5, machine type 1909, 1910, 7872, 7873
- BladeCenter LS21, machine type 7971
- BladeCenter LS22, machine type 7901
- BladeCenter LS41, machine type 7972
- BladeCenter LS42, machine type 7902
- iDataplex dx320, machine type 6388
- iDataplex dx360 M2, machine type 6380, 7321,7323
- iDataplex dx360 M3, machine type 6391
- iDataplex ds360 M4, machine type 7912, 7913

- iDataPlex® Direct Water Cooled dx360 M4, machine type 7918, 7919
- IBM Flex System x220 Compute Node, machine type 7906, 2585
- IBM Flex System x240 Compute Node, machine type 8737, 8738, 7863
- IBM Flex System Manager Node (machine types 7955, 8731, 8734
- IBM Smart Analytics System, machine type 7949

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 Ethernet CFFh Expansion Card
  - Broadcom 1 Gb 4 port Mezz Card Tier 1
  - Broadcom 10 Gb Ethernet CFFh Expansion Card for IBM BladeCenter
  - Broadcom Dualrunner/Quadrunner NetXtreme I
  - Broadcom Netextreme II
  - Emulex 10 GbE vNIC w/ BE3 Chipset
  - 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 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
  - Mellanox 2x 10 GbE SFP+ ConnextX-2LowLatency, RDMA
  - Mellanox 2xFDR10 ConnectX3 Adapter
  - 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 ConnectX-2 Dual Port 10 GbE Adapter
  - Mellanox ConnectX-2 Dual Port 10 GbE Adapter for IBM System x
  - Mellanox ConnectX-3 Dual Port PCI-E 2.0 Mezzanine
  - Mellanox ConnectX-3 Dual Port QDR/FDR10 Mezzanine Card
  - Mellanox ConnectX-3 FDR14 Mezzanine Card
  - Mellanox QDR/FDR Mezzanine Card (x-only) Tier 2 (Malaya-x)
  - Mellanox 10 GB Ethernet Mezzanine Card (x-only) Tier 2 (Malaya-xnet)

  Note: Mellanox options are only supported by portable DSA, not by preboot Dynamic System Analysis in 9.00.
- **Graphics Processing units**
  - Nvidia Quadro 2000, 4000, 5000, 6000, 600, 5000update
  - Nvidia Tesla M2090, M2090update, X2090, X2090update
- **Fibre Channel adapters**
  - Emulex 4G FC exp. card
  - Emulex 4G SFF FC exp
  - Emulex 4 Gb/s FC PCI Express HBA (lpe11000/lpe11002)
  - Emulex 4 Gb/s FC PCI-X 2.0 HBA (lp11000/lp11002)
  - Emulex 8 Gb FC Single-port HBA for IBM System x
  - Emulex 8 Gb FC Dual-port HBA for IBM System x

  - Emulex 8 Gb FC Mezz card
  - Emulex x ITE-Blacktip onboard NIC for Flex
  - 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 Dual Port 10 GbE SFP+ Embedded Adapter for IBM System x
  - Emulex PCI-e Gen 2.0 Dual Port 10 Gb NIC
  - Emulex 2-Port 10 Gb Multi-function IO Adapter
  - Emulex 16 Gb Fibre Channel Single/Dual-port HBA
  - Endeavor III/Endeavor III Lite (vNIC2) using IBM FoD for FCoE Upgrade
  - QLogic 4G/8G FC CFF exp. card
  - QLogic 4G/8G SFF FC exp. card
  - QLogic 2-Gbps Fibre Channel HBA
  - QLogic 4G and 8G FC single port HBA
  - QLogic 4G and 8G FC dual port HBA
  - Qlogic 8 Gb FC 2 port mezz card Tier 1 for Flex
  - QLogic Dual Port 10 GbE SFP+ Embedded Adapter for IBM System x
  - QLogic iSCSI PCIe HBA
  - QLogic iSCSI PCIe dual port HBA
  - Brocade 4 Gb FC Single-port HBA
  - Brocade 4 Gb FC Dual-port HBA
  - Brocade 8 Gb FC Single-port HBA
  - Brocade 8 Gb FC Dual-port HBA
  - Brocade 10 Gb CNA
  - Brocade 16 Gb FC Dual-port Mezz
  - Brocade 16 Gb FC Single/Dual-port HBA
  - IBM SAS HBA controller
  - LSI 1068 SAS 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 ServeRAID C105
  - LSI MR 10is
  - LSI IR 1078, 1064, 1064e and 1068e
  - LSI x ITE-Blacktip onboard RAID (LSI 2004) for Flex
  - LSI MegaRAID 8480
  - LSI ServeRAID MR 10i, 10ie, 10is, 10k and 10m
  - LSI ServeRAID M1015, M5014, M5015 and M5025
  - LSI Feature-on-Demand M1100 Upgrade
  - LSI ServeRAID M1110
  - LSI ServeRaid H1135 Controller
  - LSI ServeRAID M1115 RAID SAS-2 6 Gb PCIe
  - LSI ServeRAID B5015
  - LSI M5016
  - LSI ServeRAID M5100 Upgrade

  - LSI M5100 Feature-on-Demand RAID 5 cacheless, RAID 6
  - LSI ServeRAID M5100 Upgrade - 512MB Flash (P/N 81Y4484/81Y4484)
  - LSI ServeRAID M5100 Upgrade - 512MB Flash (P/N 81Y4484/81Y4487)
  - LSI ServeRAID M5100 Performance Accelerator for IBM System x
  - 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 RAID 0//10 FDE SAS-2 6 GB
  - M5100 Upgrades - 1 GB Flash
  - M5100 Upgrades - Battery
  - M5100 Upgrades - RAID 5 cacheless
- **Tape drives**
  - IBM DDS5 36/72 SCSI
  - IBM DDS5 36/72 USB
  - IBM DDS5 36/72 SATA
  - IBM DDS6 80/160 USB
  - IBM LTO2 HH 200/400 SCSI
  - IBM LTO2 FH 200/400 SCSI
  - IBM LTO3 HH 400/800 SAS
  - IBM LTO3 FH 400/800 SCSI
  - IBM LTO4 HH 400/800 SAS
  - IBM LTO5 HH 400/800 SAS
  - IBM VS160 tape drive
  - IBM GoVault tape drive
  - Pompano: RDX USB 3.0 Docks
- **Daughter cards**
  - cKVM Daughter Card for IBM BladeCenter
  - LSI BR10i, BR10ie, BR10il
  - BPE-4

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 that the appropriate service processor device drivers are 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 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-947.ibm.com/support/entry/portal/Overview?brandind=Hardware~Systems~System_x

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 provided by default in current Linux distributions does not export this information. These drivers are available for download from 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 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 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 RedHat 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 versions 2.4.1, 2.6.0, & 2.6.1

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 2011 Editions**
  - Microsoft Windows Small Business Server 2011
  - Microsoft Windows Small Business Server 2011 Essential
- **Windows Server 2008 Editions**
  - Microsoft Windows Server 2008 R2

  - Microsoft Windows Server 2008 R2 SP1
  - Microsoft Windows Server 2008, Datacenter Edition (x86, x64)
  - Microsoft Windows Server 2008, Web Edition (x86, x64)
  - Microsoft Windows Server 2008, Enterprise Edition (x86, x64)
  - Microsoft Windows Server 2008, Standard Edition (x86, x64)
  - Microsoft Windows Server 2008 HPC Edition
  - Microsoft Windows Server 2008 Foundation
  - Windows Essential Business Server 2008 Premium Edition
  - Windows Essential Business Server 2008 Standard Edition
- **Windows Server 2003 Editions**
  - Microsoft Windows Server 2003/2003 R2, Standard Edition (x86, x64)
  - Microsoft Windows Server 2003/2003 R2, Web Edition
  - Microsoft Windows Server 2003/2003 R2, Enterprise Edition (x86, x64)
  - Microsoft Windows Server 2003/2003 R2, Enterprise Edition with Microsoft Cluster Service (MSCS)
  - Microsoft Windows Server 2003/2003 R2, Datacenter Edition (x86, x64)
- **Windows Preinstallation Environment 2.1, 2.2, and 3.0**
- **SUSE Linux**
  - SUSE LINUX Enterprise Server 11 for x86/x64 including SP2
  - SUSE Linux Enterprise Server 11 with Xen for AMD64/EM64T
  - SUSE LINUX Enterprise Server 11 for AMD64/EM64T including SP1
  - SUSE LINUX Enterprise Server 11 for x86 including SP1
  - SUSE LINUX Enterprise Real Time 10 AMD64/EM64T
  - SUSE LINUX Enterprise Server 10 with Xen for AMD64/EM64T
  - SUSE LINUX Enterprise Server 10 for AMD64/EM64T
  - SUSE LINUX Enterprise Server 10 with Xen for x86
  - SUSE LINUX Enterprise Server 10 for x86
  - SUSE LINUX Enterprise Server 9 for AMD64/EM64T
  - SUSE LINUX Enterprise Server 9 for x86
- **Red Hat**
  - Red Hat Enterprise Linux 6.2 Server (x86 & x64)
  - Red Hat Enterprise Linux 6.1
  - Red Hat Enterprise Linux 6
  - Red Hat Enterprise Linux 5.8 Server (x86 & x64)
  - Red Had Enterprise Linux 5.7 Server x86, x64 Editions
  - Red Had Enterprise Linux 5.7 Server with Xen x86, x64 Editions
  - Red Hat Enterprise Linux 5 Server x64 Edition
  - Red Hat Enterprise Linux 5 Server with Xen x64 Edition
  - Red Hat Enterprise Linux 5 Server Edition with Xen
  - Red Hat Enterprise Linux 5 Server Edition
  - Red Hat Enterprise Linux 4 AS for AMD64/EM64T
  - Red Hat Enterprise Linux 4 AS for x86
  - Red Hat Enterprise Linux 4 ES for AMD64/EM64T
  - Red Hat Enterprise Linux 4 ES for x86
  - Red Hat Enterprise Linux 4 WS/HPC for AMD64/EM64T
  - Red Hat Enterprise Linux 4 WS/HPC for x86
  - Red Hat Enterprise Linux 3 AS for AMD64/EM64T
  - Red Hat Enterprise Linux 3 AS for x86
  - Red Hat Enterprise Linux 3 ES for AMD64/EM64T
  - Red Hat Enterprise Linux 3 ES for x86
  - Red Hat Enterprise Linux 3 WS for AMD64/EM64T
  - Red Hat Enterprise Linux 3 WS for x86
- **VMware:**
  - VMware vSphere Hypervisor 5.0 U1 with IBM Customization
  - VMware vSphere 5

  - VMware ESX Server, 4.1 SP1/SP2
  - VMware ESXi 4.1 SP1/SP2
  - VMware ESX Server, 4.0 SP1/SP2/SP3
  - VMware ESXi 4.0 SP1/SP2/SP3
  - VMware ESX Server 3.5
  - VMware ESXi 3.5

  Note: VMware ESXi versions are supported only through use of the `--vmware-esxi` option.
- **Hypervisor**
  - RHEV-H Blue 6.1

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 www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=SERV-DSA&brandind=5000016:
   - 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* | *rhel3* | *rhel4* | *rhel5* | *sles9* | *sles10* | *sles11* | *vmware2.0* | *vmware3.0* | *vmware3.5* | *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 these steps to run diagnostics on the local system.

1. If you are using the Preboot Dynamic System Analysis GUI:
   a. 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.
   b. Select **Quit to DSA** to exit the stand-alone memory diagnostic program.

      Note: After you exit the stand-alone memory diagnostic environment, you must restart the system before you can access this environment again.
   c. Enter **gui** or select **Click here to start diagnostics (GUI)** to launch the Dynamic System Analysis graphical environment.
   d. From the navigation pane on the left, select **Diagnostics** to open the Diagnostics panel.
   e. In the Diagnostics panel, click **Add Test** to open the All Tests window, which lists all available tests.
   f. Determine what tests will be run by using the **Add Sel/All** and **Rem Sel/All** buttons to add and remove tests from the **Test Items** field. Test in this field will be run.
   g. When you are finished selecting tests, click **Ok** to return to the Diagnostics panel, which is now populated with the tests you selected.
   h. Click the hyperlink in the **Loop** column to set the loop count for test execution.
   i. Click **Start Test** to run the selected tests.
   j. When the tests are complete, click the **Success** hyperlink in the **Status** column to view the results.
2. If you are using the Dynamic System Analysis Preboot Edition command-line interface:
   a. 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.
   b. Enter **cmd** or select **Click here to start diagnostics (CLI)** to launch the Dynamic System Analysis command environment.
   c. 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.
   d. When the tests are complete, enter **:x** to exit the menu.
   e. Select the completed tests to view the results.
3. If you are using Dynamic System Analysis on removable media:

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 -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 these steps to collect system information on the local system:

1. If you are using the Dynamic System Analysis Preboot Edition graphical user interface:
   a. 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.
   b. Select **Diagnostics** from the navigation pane.
   c. Select **Click here to start diagnostics (GUI)** or enter **`gui`** from the command line to start the graphical user interface.
   d. Select **System inventory** to launch the System Inventory page.
   e. Select the **Automatic** radio button to automatically collect all available data, or deselect it to control what information catalogs to use by adding them to or removing them from the **Data Set** table.
   f. Click **Begin** to collect the data associated with the selected catalogs.
2. If you are using the Dynamic System Analysis Preboot Edition command-line interface:
   a. 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.
   b. Select **Diagnostics** from the navigation pane.
   c. Click **Click here to start diagnostics (CLI)** or enter **`cmd`** from the command line to start the command-line interface.
   d. Select the **Data Collection** option to open the data collection menu.
   e. Select **Collect** to open the collection menu. You are asked whether to customize options. You can customize the following options:
      - **-v**: does not create compressed XML data as output.
      - **-x**: creates HTML output.
      - **-dumpxml**: creates a .xml.gz zipfile after each plugin. This preserves data already collected if an error occurs curing collection.
   f. When the collection is complete, select **View collection results** to display the results.
   g. 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:

1. If you are using Dynamic System Analysis on removable media:
   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 [-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 WinPE image

About this task

Perform these steps to run all available nondestructive diagnostic tests on all available devices in the local system using the **collectall** command:

1. Boot the local system with the Windows Preinstallation Environment (WinPE) CD.
2. If you are using Dynamic System Analysis on removable media:
   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 [-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.

Tip: You can edit the **startnet.cmd** file to run Dynamic System Analysis automatically after WinPE boots.

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:

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:
   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@ip_address
      ```

      where *v.r.m* is the version of Dynamic System Analysis and *user_id@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:

1. If you are using Dynamic System Analysis on removable media:
   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 --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:

1. If you are using Dynamic System Analysis on removable media:
   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_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:

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:

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:

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.

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 the set of HTML file 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 these steps to transfer data collected on the local system to a remote system using FTP:

1. If you are using the Dynamic System Analysis Preboot Edition command-line interface:
   a. 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**.
   b. Select **Quit to previous menu** to exit the interactive Data Collection menu.
   c. From the numerical menu, select **Send System Information to IBM Server**. You will be prompted to customize the FTP server.
   d. Enter **y** to customize the server information and specify the FTP address, port number, user name, and password to use with your FTP server.
2. If you are using the Dynamic System Analysis Preboot Edition graphical user interface:
   a. Boot to Dynamic System Analysis, either by booting to removable media or, for preinstalled Dynamic System Analysis, pressing F2 to interrupt the boot sequence.
   b. Select **Diagnostics** from the navigation.
   c. Select **Collect Logs and Transfer** to launch the Transfer page.
   d. Select **Automatic** to collect all data and automatically transfer it to IBM Service and Support, or Select **Manual** to select which logs to collect and manually send them to IBM Service and Support.
3. If you are using Dynamic System Analysis on removable media:
   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 [-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:

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. For the Preboot Edition command-line interface:
   a. Collect data as described in "Collecting system information on the local system using Preboot Edition" on page 15 and exit the viewer by entering **q**.
   b. Select **Quit to previous menu** to exit the Data Collection menu.
   c. From the numerical menu, select **Copy Collected System Information to Local Media**. You are prompted to select a device.
   d. Select the USB device to which you want to copy the data.
2. For the Preboot Edition graphical user interface:
   a. Boot to Dynamic System Analysis, either by booting to removable media or for preinstalled Dynamic System Analysis, by pressing **F2** to interrupt the boot sequence.
   b. Select **Diagnostics** from the navigation.
   c. Select **Collect Logs and Transfer** to launch the Transfer page.
   d. Select **Manual** to select which logs to collect and manually save them to the USB device.

Chapter 9. Supporting Dynamic System Analysis Features on Demand

This section provides information for using DSA Features on Demand.

Using Portable Dynamic System Analysis and Features on Demand

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

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 (CD-ROM, or USB key, for example) as a self-extracting file.
- You must be logged into system as administrator or root (or 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 sub commands. For more information, refer to the DSA FoD sections in *Appendix B*: "DSA FoD CLI switches" on page 75.

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]>`: The remote key repository. For remote key repository, default is local IMM device.http or https is for cim interface; default is https. User ID, Password is for the device

interface connection. For Switch, User ID and Password is auth info for SNMPv3. Port is for the CIM interface.The default is 5989.

- `--tftp] <ip:[port]>`: The tftp server for 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 (CD-ROM, or USB key, for example) 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.
- The commands `display_imm_available_fod` and `install_imm_fod` require Internet access.

About this task

Perform these steps to show 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 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 file from KMS and parse it to get all 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 will be exported to the `dsa_fod_ids.txt` located in the DSA output folder. You can copy this FoD Identifier file to the removable media (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 it is a 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 shown in the console.
6. Enter the following command and parameters to download specific keys for corresponding FoD features from KMS and 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 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 (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 the 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), and 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 BMC, an error message shows `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 (CD-ROM, or USB key, for example) as a self-extracting file.
- The operating system on a laptop is available for OOB mode.
- The commands `report_cmm_active_fod`, `install_cmm_fod`, and `uninstall_cmm_fod` require Internet access.

About this task

Perform 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 shown 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, an error message shows `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 (CD-ROM, or USB key, for example) as a self-extracting file.
- The operating system on a laptop is available for OOB mode.
- The commands `report_switch_active_fod`, `install_switch_fod`, and `uninstall_switch_fod` require Internet access.

About this task

Perform 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 (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 shown 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: 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: No privacy.
   - `--privpasswd <password>`: The privacy password for SNMPv3.

If DSA failed to connect to Switch, an error message shows `Failed to connect Switch, Error code = **`.

Using CD-based DSA and Features on Demand

The topics in this section provide information for using CD-based DSA and Features on Demand.

Using the Features on Demand GUI support

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 start-up device.

About this task

Perform these steps to view, download, and install the FoD License Key on a machine 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 stand-alone memory test. Otherwise, BoMC GUI will launch by default. The option to run the stand-alone 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**.

   The stand-alone memory diagnostic does not support all systems. If the machine type is not supported, 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.
4. Type `gui` to launch the graphical DSA environment.
5. Click **I accept the terms in the license agreement** to accept Preboot license.
6. From the navigation pane on the left, select the **Feature on Demand (FoD)** option.

   Use the first page of the Feature on Demand (FoD) wizard to perform FoD key activation management on three target devices (IMM, CMM, IOM/Switch).

   The **Back** button is used to navigate to the previous page of this wizard, and the **Next** button is used to navigate to the next page of this wizard. The **Reset** button is used to reset the wizard to the first page.
7. Select one of following categories:
   - **IMM**
   - **CMM**
   - **IOM/Switch**

Using the IMM option

Procedure

1. Select **IMM** and click **Next**. WAN network status will be examined first, then the available operations for IMM are displayed in next page.

   If WAN is not available, the **Install activation key** operation is not shown, and **Export FoD feature information to removable media** only exports all installed features. The **View activation key** shows only the installed features.
2. If WAN is available, the **Install activation key** is shown, and the **Export FoD feature information to removable media** exports all available features you selected. The **View activation key** shows all available features.
3. If you select the **View activation key** when WAN is not available, the next page lists all installed FoD features.
4. If you select the **View activation key** when WAN is available, the next pages require you to enter the "IBM ID". The last page will list all of the available or installed FoD features supported by the machine type.
5. Select the **Install activation key** and click **Next** to start the installation procedure when the WAN is available.
6. Enter the `IBM ID` information and click **Next**. On the next page, all of the available FoD features are displayed.
7. Click to select the items you want to install, and then click **Next**. The second page of the **Install activation key** lists all the features you have chosen to install.
8. Click **Input** at the end of each row and enter the values required for installation.
9. Click **Next**. The install starts, and a progress bar is shown. If any of the required values for features are missing, a dialog is displayed.
10. Enter the missing values and click **Continue** to continue install, or click **Skip** to skip the current feature's installation. After the install has completed, the install results of each feature are displayed.
11. Click **Finish**. The operation selection page is displayed.
12. Click **Continue** to proceed to the first page of the installation procedure. You can perform another installation from this page.
13. To uninstall any items, select **Uninstall activation key** and click **Next**. The next page lists all of the installed FoD features.
14. Click to select any features you want to uninstall and then click **Next**. The uninstall starts and the next page provides a list of the uninstall results of each feature.
15. Click **Finish** to proceed to the operation selection page, or click **Back** to return to the previous page to perform another uninstall.
16. If you select **Install activation key from removable media**, the available removable media is detected first. Click **Next** to proceed to the next page.
17. On this page you can click to select one available removable media and click **Next**. The next page provides a list of the existing files for the available removable media chosen.
18. Click to select the items you want to install and click **Next**. The install starts and a progress bar is shown. After all the key files are installed, the result page is displayed.
19. Click **Finish** to proceed to the operation selection page.

20. If you select **Export FoD feature information to removable media** when a WAN is not available, click **Next** to start the detection of available removable media. The next page provides a list of the removable media that you can export.
21. Click to select the removable media you want to export and click **Next**. The export begins. The result is displayed on the next page.
22. If you select **Export FoD feature information to removable media** when the WAN is available, click **Next** to proceed to the next page.
23. Enter the`IBM ID` values, and click **Next**. The next page shows the available removable media that was detected.
24. Click to select one removable media and click **Next**. All of the available FoD features are displayed.
25. Click to select the items you want to export and click **Next**. The export starts. The results are displayed on the next page.

Using the CMM option

Procedure

1. Select **CMM** and click **Next**. The Host Auth page is displayed.
2. Enter **Host Auth** information.

   After entering this information, the LAN network status is checked. If LAN network is not available, an error page is displayed and nothing further can be done.

   If the LAN network is available, the WAN network status is checked.
3. Click **Finish** to exit the wizard if the LAN network is not available.

   Note: If the WAN is not available, the **Install activation key** operation is displayed, and the **View activation key** only shows all of the installed FoD features. Refer to the *Export FoD feature information to removable media* in the "Using the IMM option" on page 33 topic.

   If WAN is available, **Install activation key** operation is displayed, and **View activation key** shows all available features. **Export FoD feature information to removable media** is only available under IMM.
4. Click **View activation key**. If the WAN is available, the next two pages require the entry of IBM ID and Machine Type information. The last page lists all of the available FoD features supported based on the Machine Type information entered.
5. Select the **Install activation key** and click **Next** to start the installation procedure when the WAN is available. If you have not already entered information as noted in prior step, enter this information.
6. Enter **IBM ID** and **Machine Type** information and click **Next**. The next page provides a list of all of the FoD Features.
7. Click to select the FoD features you want to install and **Next**. The second page of the **Install activation key** option is displayed. All of the FoD features selected are listed.
8. Click **Input**. Enter the required information for each feature.
9. Click **Next**. The Install begins. If there is any missing information, a dialogue box opens, requesting the missing information. A progress bar is displayed during the installation.
10. Click **Continue** to continue the installation, or **Skip** to skip the current feature's installation.

11. Click **Finish** to proceed to operation selection page of the target device, or click **Continue** to perform another installation.
12. If you want to uninstall any FoD features, click **Uninstall activation key** and click **Next**. The next page provides a list of all the installed FoD features.
13. Click to select the features you want to uninstall and click **Next**. The uninstall process begins. The next page contains the uninstalled results for each feature.
14. Click **Finish** to proceed to operation selection page of the target device, or click **Back** to return to the previous page, where you can choose to perform an uninstall.
15. If you want to uninstall any FoD features, click **Uninstall activation key** and click **Next**. The next page provides a list of all the installed FoD features.
16. Click to select the features you want to uninstall, and click **Next**. The uninstall process begins. The next page contains the uninstalled results for each feature.

Using the Iom/Switch option

Procedure

1. Select **IOM/Switch** and click **Next**. The Host Auth page is displayed.
2. On the Host Auth page, enter the **Host Auth** IP address.

   After entering this information, the LAN network status is checked. If the LAN network is not available, an error page is displayed and nothing further can be done.

   If the LAN network is available, the WAN network status is checked.
3. Click **Finish** to exit the wizard if the LAN network is not available.
4. Enter the `TFTP` and `SNMP` values and click **Next**.
5. If the WAN is not available, the **Install activation key** operation is displayed, and the **View activation key** shows all of the installed FoD features. Refer to the *Export FoD feature information to removable media* in the"Using the IMM option" on page 33 topic.
6. If the WAN is available, **Install activation key** operation is displayed, and **View activation key** shows all available features. **Export FoD feature information to removable media** is only available under IMM.
7. If the WAN is available, select **View activation key**. The next two pages require the entry of IBM ID and Machine Type information. The last page lists all of the available FoD features that are supported based on the Machine Type information entered.
8. Click **Install activation key**,and click **Next** to start the install procedure when the WAN is available.
9. Enter **IBM ID** and **Machine Type** information, and click **Next**. The next page provides a list of all of the FoD Features.
10. Click to select the FoD features you want to install and **Next**. The second page of the **Install activation key** option is displayed. All of the FoD features selected are listed.
11. Click **Input**. Enter the required information for each feature.
12. Click **Next**. The Install begins. If there is any missing information, a dialogue box opens, requesting the missing information. A progress bar is displayed during the installation.
13. Click **Continue** to continue the installation, or **Skip** to skip the current feature's installation.
14. Click **Finish** to proceed to operation selection page of the target device, or click **Continue** to perform another installation.

15. If you want to uninstall any FoD features, click **Uninstall activation key**, and click **Next**. The next page provides a list of all the installed FoD features.
16. Click to select the features you want to uninstall and click **Next**. The uninstall process begins. The next page contains the uninstalled results for each feature.
17. Click **Finish** to proceed to operation selection page of the target device or click **Back** to return to the previous page, where you can choose to perform an uninstall.
18. If you want to uninstall any FoD features, click **Uninstall activation key** and click **Next**. The next page provides a list of all the installed FoD features.
19. Click to select the features you want to uninstall and click **Next**. The uninstall process begins. The next page contains the uninstalled results for each feature.

What to do next

If the collection fails and DSA crashes executing one of the collections, reboot the system.

If DSA fails to perform FoD operations or nothing is listed in the table grid, check the values in previous pages by clicking **Back**. Verify the values entered are valid and meaningful and run related action again.

Using Features on Demand GUI support for Embedded DSA Preboot

Before you begin

The following prerequisite is necessary for this task:

- 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 using the GUI.

Procedure

1. Press **F2** during the system boot to enter the diagnostic environment.
2. Enter `memtest` to launch the stand-alone memory test. Otherwise, BoMC GUI launches by default. The option to run the stand-alone 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**.

   The stand-alone memory diagnostic does not support all systems. If the machine type is not supported, **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.
4. Type `gui` to launch the graphical DSA environment.
5. Click **I accept the terms in the license agreement** to accept Preboot license.
6. From the navigation pane on the left, select the **Feature on Demand (FoD)** option.

   Using the Feature on Demand (FoD) wizard, perform FoD key activation management on three target devices (IMM, CMM, IOM/Switch).

The **Back** button is used to navigate to the previous page of this wizard, and the **Next** button is used to navigate to the next page of this wizard. The **Reset** button is used to reset the wizard to the first page.

7. Select one of following categories:
   - IMM
   - CMM
   - IOM/Switch

Using the IMM option for Embedded DSA Preboot

Procedure

1. Select **IMM** and click **Next**. WAN network status is examined first, then the available operations for IMM are displayed on the next page.

   If WAN is not available, the **Install activation key** operation is not shown, and **Export FoD feature information to removable media** only exports installed features. The **View activation key** shows only the installed features.
2. If WAN is available, the **Install activation key** is shown, and the **Export FoD feature information to removable media** exports all available features you selected. The **View activation key** shows all available features.
3. If you select the **View activation key** when WAN is not available, the next page lists all installed FoD features.
4. If you select the **View activation key** when WAN is available, the next pages require you to enter the IBM ID. The last page lists all of the available or installed FoD features supported by the machine type.
5. Select the **Install activation key**, and click **Next** to start the install procedure when the WAN is available.
6. Enter the `IBM ID` information, and click **Next**. On the next page, all of the available FoD features are displayed.
7. Click to select the items you want to install, and then click **Next**. The second page of the **Install activation key** lists all the features you have chosen to install.
8. Click **Input** at the end of each row and enter the values required for installation.
9. Click **Next**. The install starts, and a progress bar is shown. If any of the required values for features are missing, a dialog box is displayed.
10. Enter the missing values, and click **Continue** to continue install, or click **Skip** to skip the current feature's installation. After the install has completed, the install results of each feature are displayed.
11. Click **Finish**. The operation selection page is displayed.
12. Click **Continue** to proceed to the first page of the installation procedure. You are able to perform another installation from this page.
13. To uninstall any items, select **Uninstall activation key**, and click **Next**. The next page lists all of the installed FoD features.
14. Click to select any features you want to uninstall and then click **Next**. The uninstall starts and the next page provides a list of the uninstall results of each feature.
15. Click **Finish** to proceed to the operation selection page, or click **Back** to return to the previous page to perform another uninstall.
16. If you select **Install activation key from removable media**, the available removable media is detected first. Click **Next** to proceed to the next page.

17. On this page you can click to select one available removable media and click **Next**. The next page provides a list of the existing files for the available removable media chosen.
18. Click to select the items you want to install, and click **Next**. The install starts and a progress bar is shown. After all the key files are installed, the result page is displayed.
19. Click **Finish** to proceed to the operation selection page.
20. If you select **Export FoD feature information to removable media** when a WAN is not available, click **Next** to start the detection of available removable media. The next page provides a list of the removable media that you can export.
21. Click to select the removable media that you want to export, and click **Next**. The export begins. The result is displayed on the next page.
22. If you select **Export FoD feature information to removable media** when the WAN is available, click **Next** to proceed to the next page.
23. Enter the`IBM ID` values, and click **Next**. The next page shows the available removable media that was detected.
24. Click to select one removable media, and click **Next**. All of the available FoD features are displayed.
25. Click to select the items you want to export, and click **Next**. The export starts. The results are displayed on the next page.

Using the CMM option for Embedded DSA Preboot

Procedure

1. Select **CMM**, and click **Next**. The Host Auth page is displayed.
2. Enter **Host Auth** information.

   After entering this information, the LAN network status is checked. If LAN network is not available, an error page is displayed and nothing further can be done.

   If the LAN network is available, the WAN network status is checked.
3. Click **Finish** to exit the wizard if the LAN network is not available.

   Note: If the WAN is not available, the **Install activation key** operation is displayed, and the **View activation key** only shows all of the installed FoD features. Refer to the *Export FoD feature information to removable media* in the“Using the IMM option” on page 33 topic.

   If WAN is available, **Install activation key** operation is displayed, and **View activation key** shows all available features. **Export FoD feature information to removable media** is only available under IMM.
4. Click **View activation key**. If the WAN is available, the next two pages require IBM ID and Machine Type information. The last page lists all of the available FoD features supported based on the Machine Type information entered.
5. Click **Install activation key**, and click **Next** to start the install procedure when the WAN is available. If you have not already entered information as noted in prior step, enter this information.
6. Enter **IBM ID** and **Machine Type** information, and click **Next**. The next page lists of all of the FoD Features.
7. Click to select the FoD features that you want to install, and **Next**. The second page of the **Install activation key** option is displayed. All of the FoD features selected are listed.

8. Click **Input** to enter the required information for each feature.
9. Click **Next**. The Install begins. If there is any missing information, a dialogue box opens, requesting the missing information. A progress bar is displayed during the installation.
10. Click **Continue** to continue the installation, or **Skip** to skip the current feature's installation.
11. Click **Finish** to proceed to operation selection page of the target device, or click **Continue** to perform an installation.
12. If you want to uninstall any FoD features, click **Uninstall activation key** and click **Next**. The next page provides a list of all the installed FoD features.
13. Click to select the features that you want to uninstall, and click **Next**. The uninstall process begins. The next page contains the uninstalled results for each feature.
14. Click **Finish** to proceed to operation selection page of the target device, or click **Back** to return to the previous page, where you can choose to perform an uninstall.
15. If you want to uninstall any FoD features, click **Uninstall activation key**, and click **Next**. The next page provides a list of all the installed FoD features.
16. Click to select the features you want to uninstall, and click **Next**. The uninstall process begins. The next page contains the uninstalled results for each feature.

Using the IOM/Switch option for Embedded DSA Preboot

Procedure

1. Select **IOM/Switch** and click **Next**. The Host Auth page is displayed.
2. On the Host Auth page, enter the **Host Auth** IP address.

   After entering this information, the LAN network status is checked. If the LAN network is not available, an error page is displayed and nothing further can be done.

   If the LAN network is available, the WAN network status is checked.
3. Click **Finish** to exit the wizard if the LAN network is not available.
4. Enter the `TFTP` and `SNMP` values, and click **Next**.
5. If the WAN is not available, the **Install activation key** operation is displayed, and the **View activation key** only shows all of the installed FoD features. Refer to the *Export FoD feature information to removable media* in the "Using the IMM option" on page 33 topic.
6. If WAN is available, **Install activation key** operation is displayed, and **View activation key** shows all of the available features. **Export FoD feature information to removable media** is only available under IMM.
7. If WAN is available, select **View activation key**. The next two pages require IBM ID and Machine Type information. The last page lists all of the available FoD features supported based on the Machine Type information entered.
8. Click **Install activation key**, and click **Next** to start the install procedure when the WAN is available.
9. Enter **IBM ID** and **Machine Type** information, and click **Next**. The next page provides a list of all of the FoD Features.
10. Click to select the FoD features that you want to install and **Next**. The second page of the **Install activation key** option is displayed. All of the FoD features selected are listed.
11. Click **Input** to enter the required information for each feature.

12. Click **Next**. The Install begins. If there is any missing information, a dialogue box opens, requesting the missing information. A progress bar is displayed during the installation.
13. Click **Continue** to continue the installation, or **Skip** to skip the current feature's installation.
14. Click **Finish** to proceed to operation selection page of the target device, or click **Continue** to perform another installation.
15. If you want to uninstall any FoD features, click **Uninstall activation key**, and click **Next**. The next page provides a list of all the installed FoD features.
16. Click to select the features that you want to uninstall and click **Next**. The uninstall process begins. The next page contains the uninstalled results for each feature.
17. Click **Finish** to proceed to operation selection page of the target device, or click **Back** to return to the previous page, where you can choose to perform an uninstall.
18. If you want to uninstall any FoD features, click **Uninstall activation key** and click **Next**. The next page provides a list of all the installed FoD features.
19. Click to select the features you want to uninstall, and click **Next**. The uninstall process begins. The next page contains the uninstalled results for each feature.

What to do next

If the collection fails and DSA crashes executing one of the collections, reboot the system.

If DSA fails to perform FoD operations or nothing is listed in the table grid, check the values in previous pages by clicking **Back**. Verify the values entered are valid and meaningful and run related action again.

Using the command line Interface with FoD on an embedded DSA Preboot

Before you begin

The following prerequisite is necessary for this task:

- 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 using the command line interface.

Procedure

1. Press **F2** during the system boot to enter the diagnostic environment.
2. Enter `memtest` to launch the stand-alone memory test. The option to run the stand-alone 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**.

   The stand-alone memory diagnostic does not support all systems. If the machine type is not supported, **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.

4. Type `cmd` to launch the command line DSA environment.
5. Click **I accept the terms in the license agreement** to accept Preboot license.
6. From the navigation pane on the left, select the **Feature on Demand (FoD)** option.

   Using the Feature on Demand (FoD) wizard, perform FoD key activation management on three target devices (IMM, CMM, IOM/Switch).

   The **Back** button is used to navigate to the previous page of this wizard, and the **Next** button is used to navigate to the next page of this wizard. The **Reset** button is used to reset the wizard to the first page.
7. Select one of following options:
   - **1 - FoD Feature(s) on IMM**
   - **2 - FoD Feature(s) on CMM**
   - **3 - FoD Feature(s) on IOM/Switch**
   - **Q - Return to Previous Menu**

   Possible error conditions:
   - The flash procedure failed. Flash the device again.
   - The collection fails and DSA crashes executing one of the collections. Reboot the system in this event.
   - DSA fails to install the FoD License Key. Check the failure log in lower table and run related action again.

Using the CLI with FoD on IMM

Before you begin

The following prerequisite is necessary for this task:

- 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. Otherwise, DSA downloads the master xml from KMS and parses it to get the available FoD feature(s) for the specific system.
3. Enter the following information to display the FoD features:
   a. IMM authorization info: `<userid:pwd@ip:[port]>` Note: Press 'Enter' to use the local IMM device.
   b. Machine type of the system: `<userid:pwd>`
   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]>` Note: Press 'Enter' to use the local IMM device.
5. Select **3 - Install FoD Key(s)** to install the FoD key(s) for specific FoD feature(s). There are two ways to install the FoD key(s):
   - Install FoD Key(s) from IBM website when internet access is available.

- Install FoD Key(s) from removable media (such as USB key). DSA checks for the internet access first. If internet is available, you can install the FoD key(s) from IBM website. Otherwise, you can install the FoD key(s) from removable media (such as USB key).

6. Enter the following information to report the active FoD keys:
   a. IMM authorization info: `<userid:pwd@ip:[port]>` Note: Press 'Enter' to use the 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 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 needed 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 USB key), a removable media (such as USB key) with a folder named FoDKeys and all the key files in this folder are required.

      If the key file(s) is imported successfully, all the key files are shown 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]>`

   After the active FoD Key(s) are displayed, you can select any one of them to uninstall from the target system (IMM key repository).
8. Select **5 - Export FoD Ids** to export the FoD feature Identifier(s). Currently only the FoD Identifier(s) on the local system can be exported. DSA collects all the possible FoD Ids first. It prompts you to insert a removable media (such as USB key), and then the FoD Ids are exported to the removable media (such as USB key) as a file named `dsa_fod_ids.txt`.
9. Select **Q - Return to Previous Menu** to return to the previous menu.

Using the CLI with FoD on CMM

Before you begin

The following prerequisite is necessary for this task:

- 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 ways to install the FoD key(s):
   - Install FoD Key(s) from IBM website when internet access is available.

- Install FoD Key(s) from removable media (such as USB key). DSA checkd for internet access first. If internet is available, you can install the FoD key(s) from the IBM website. Otherwise, you can install the FoD key(s) from removable media (such as USB key).

4. Enter the following information to report the active FoD keys:
   a. CMM authorization info: `<userid:pwd@ip:[port]>` Note: Press 'Enter' to use the local IMM device.
   b. 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.. You can select any FoD feature to install. An IBM authorization code and FoD UID are needed 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 USB key), a removable media (such as USB key) with a folder named FoDKeys and all the key files in this folder are required.

      If the key file(s) is imported successfully, all the key files is shown in the console.
   d. 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 needed to report the active FoD keys:
   - CMM authorization info: `<userid:pwd@ip:[port]>`

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

Using the CLI with FoD on IOM/Switch

Before you begin

The following prerequisite is necessary for this task:

- 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). Switch authorization info:
   a. Switch authorization info: `<userid:pwd@ip:[port]>`
   b. TFTP|SFTP server for SNMP interface: `<<sftp|tftp>://user:pwd@ip:[port}>`
   c. Community for SNMPv1v2: `<public|private>`
   d. Authorization protocol for SNMPv3: `<MD5|SHA>`
   e. Privacy protocol for SNMPv3 : `<DES|AES>`
   f. Privacy password for SNMPv3

4. Select **Install FoD Key(s)** to install the FoD key There are two ways to install the FoD key(s):
   - Install FoD Key(s) from the IBM website when internet access is available.
   - Install FoD Key(s) from removable media (such as USB key). DSA checks for internet access first. If internet is available, you can install the FoD key(s) from the IBM website. Otherwise, you can install the FoD key(s) from removable media (such as USB key).
5. Enter the following information to report the active FoD keys:
   a. Switch authorization info: `<userid:pwd@ip:[port]>`
   b. TFTP|SFTP server for SNMP interface: `<<sftp|tftp>://user:pwd@ip:[port}>`
   c. Community for SNMPv1v2: `<public|private>`
   d. Authorization protocol for SNMPv3: `<MD5|SHA>`
   e. Privacy protocol for SNMPv3 : `<DES|AES>`
   f. Privacy password for SNMPv3
   g. 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 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 needed to continue the installation.
   h. Insert the removable media to import the FoD key files.

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

      If the key file(s) is imported successfully, all the key files will be shown in the console
   i. Select a key file to install.
6. 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 needed to report the active FoD keys:
   a. Switch authorization info: `<userid:pwd@ip:[port]>`
   b. TFTP|SFTP server for SNMP interface: `<<sftp|tftp>://user:pwd@ip:[port}>`
   c. Community for SNMPv1v2: `<public|private>`
   d. Authorization protocol for SNMPv3: `<MD5|SHA>`
   e. Privacy protocol for SNMPv3 : `<DES|AES>`
   f. Privacy password for SNMPv3

   After the active FoD Key(s) are displayed, you can select any one of them to uninstall from the target system (Switch key repository).
7. Select **Q - Return to Previous Menu** to return to the previous menu.
8. Select **quit** to exit the DSA interactive menu.

Using command line interface to install the Features on Demand License Key

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 start-up device.

About this task

Perform these steps to view, download, and install the FoD License Key on a machine 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 stand-alone memory test. Otherwise, the BoMC GUI launches by default. The option to run the stand-alone 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**.

   The stand-alone memory diagnostic does not support all systems. If the machine type is not supported, 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.
4. Type `cmd` to launch the command line DSA environment.
5. From the numerical menu, select one of the following options to enter the interactive environment:
   - **1 - FoD Feature(s) on IMM**
   - **2 - FoD Feature(s) on CMM**
   - **3 - FoD Feature(s) on IOM/Switch**
   - **Q - Return to Previous Menu**

   Possible error conditions:
   - The collection fails and DSA crashes executing one of the collections. Rreboot the system in this event.
   - DSA fails to install the FoD License Key. Check the failure log in lower table and run related action again.

Using the FoD Feature on IMM

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 the internet access is not available, no information is displayed. Otherwise, DSA will download the master xml from KMS and parse it to get the available FoD feature(s) for the specific system.
3. Enter the following information to display the FoD features:

a. IMM authorization info: `<http(s)://userid:pwd@ip:[port]>[Local IMM Device]:`
b. Machine type of the system.
c. IBMID Credential for IBM website: `<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: `<http(s)://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). There are two ways to install the FoD key(s):
   - Install FoD Key(s) from the IBM website when internet access is available.
   - Install FoD Key(s) from removable media (such as USB key). DSA checks for internet access first. If internet is available, you can install the FoD key(s) from the IBM website. Otherwise, you can install the FoD key(s) from removable media (such as USB key).
6. Enter the following information to report the active FoD keys:
   a. IMM authorization info: `<http(s)://userid:pwd@ip:[port]>[Local IMM Device]:`

      If you selected to install the FoD key from website, you will be 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. You can select any FoD feature to install. An IBM authorization code and FoD UID are needed to continue the installation.

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

      If the key file(s) is imported successfully, all the key files are shown in the console.
   c. 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: `<http(s)://userid:pwd@ip:[port]>[Local IMM Device]:`

   After the active FoD Key(s) are displayed, you can select any one of them to uninstall from the target system (IMM key repository).
8. Select **5 - Export FoD Ids** to export the FoD feature Identifier(s). Currently only the FoD Identifier(s) on the local system can be exported. DSA collects all the possible FoD IDs first. It prompts you to insert a removable media (such as USB key), and then the FoD IDs are exported to the removable media (such as USB key) as a file named `dsa_fod_ids.txt`.
9. Select **Q - Return to Previous Menu** to return to the previous menu.

Using the FoD Feature on CMM

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 ways to install the FoD key(s):
   - Install FoD Key(s) from the IBM website when internet access is available.
   - Install FoD Key(s) from removable media (such as USB key). DSA checks for internet access first. If internet is available, you can install the FoD key(s) from the IBM website. Otherwise, you can install the FoD key(s) from removable media (such as USB key).
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 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), and then the available FoD feature(s) are displayed. You can select any FoD feature to install. An IBM authorization code and FoD UID are needed to continue the installation.

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

      If the key file(s) is imported successfully, all the key files are shown 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 needed to report the active FoD keys:
   - CMM authorization info: `<http(s)://userid:pwd@ip:[port]>`

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

Using the FoD Feature on IOM/Switch

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 the SNMP version you want to use:
      - SNMPv1 or SNMPv2
      - SNMPv3
   d. If you selected SNMPv1 or SNMPv2, **`Community`** for SNMPv1v2 is needed.
   e. If you selected SNMPv3 , the following information is needed:
      - User name for SNMPv3

- Authorization password for SNMPv3
- Authorization protocol for SNMPv3
- Privacy protocol for SNMPv3
- Privacy password for SNMPv3

4. Select **Install FoD Key(s)** to install the FoD key There are two ways to install the FoD key(s):
   - Install FoD Key(s) from the IBM website when internet access is available.
   - Install FoD Key(s) from removable media (such as USB key). DSA checks for internet access first. If internet is available, you can install the FoD key(s) from the IBM website. Otherwise, you can install the FoD key(s) from removable media (such as USB key).
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 the SNMP version you want to use:
      - SNMPv1 or SNMPv2
      - SNMPv3
   d. If you selected SNMPv1 or SNMPv2, **`Community`** for SNMPv1v2 is needed.
   e. If you selected SNMPv3 , the following information is needed:
      - User name for SNMPv3
      - Authorization password for SNMPv3
      - Authorization protocol for SNMPv3
      - Privacy protocol for SNMPv3
      - Privacy password for SNMPv3

      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 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 needed to continue the installation.

      If you selected to install the FoD key from removable media (such as USB key), a removable media (such as USB key) with a folder named FoDKeys and all the key files in this folder are required.
   a. Insert the removable media to import the FoD key files.
   b. Select a key file to install.
6. 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 needed to report the active FoD keys:
   a. `Switch host IP:`
   b. `TFTP server for SNMP interface<[user:pwd@ip]:[port]>:`
   c. Select the SNMP version you want to use:
      - SNMPv1 or SNMPv2
      - SNMPv3
   d. If you selected SNMPv1 or SNMPv2, **`Community`** for SNMPv1v2 is needed.
   e. If you selected SNMPv3 , the following information is needed:
      - User name for SNMPv3
      - Authorization password for SNMPv3

- Authorization protocol for SNMPv3
- Privacy protocol for SNMPv3
- Privacy password for SNMPv3

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 the available FoD feature. The available FoD feature are displayed. You can select any FoD feature to install. An IBM authorization code and FoD UID are needed to continue the installation.

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

After the active FoD Key(s) are displayed, you can select any one of them to uninstall from the target system (Switch key repository).

7. Select **Q - Return to Previous Menu** to return to the previous menu.
8. 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 www.ibm.com/developerworks/forums/forum.jspa?forumID=740.

Known limitations, problems, and workarounds

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

Known limitations for the 9.20 release

The following list contains the known limitations for the current release.

- 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 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 (multitool 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 LSI megacli utility issue, for a System x3650 M4 with a connected ServeRAID card, the LSI firmware log may be missing in the raw data section of LSI Controller information on the Hardware Inventory page.
- Due to an 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.

- 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 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.
- With Mellanox options installed on Windows 2008, a popup window appears when running DSA. Close the window, and DSA will continue processing without any functional lost.

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.
- For the x3550 system, the system fans are physically attached together as pairs, and each pair has a single LightPath LED attached. The DSA LightPath report displays each pair of fans as a single Fan LED.
- If you are running DSA on a multi-node IBM eServer like the xSeries 460 system, DSA cannot specify to which node certain hardware belongs. This is due to limitations of either Windows APIs or SMBIOS. The x460 appears to Windows and SMBIOS as a single, complete system and not as split up into nodes. Also, since LightPath and IPMI logs are only populated by the primary node, specific details regarding non-primary nodes are not collected.
- DSA collects CPLD firmware levels (Super I/O card firmware, PCI-X card firmware, CPU card firmware) on systems where there is CPLD inside. 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 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.
- When you execute DSA with -ux on Windows XP or Windows Vista, the results in the UpdateXpress section might be unavailable or inaccurate.
- When you execute DSA with -ux on HS12 (8014/8028/1916), the result in UpdateXpress for LSI 1064e SAS controller may be inaccurate. It shows the latest level is 1.26.80 but actually it should be 1.26.84.
- Memory Manufacturer information is missing on HS21 (8853/1885) and HS12 (8014, 8028,1916).
- Current State in LED Settings cannot report some failures of DIMM in LS21/LS41). It is recommended that you check the IPMI event and get the failure DIMM event.
- 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.
- The Config LED is missing from Lightpath Information in x3650 (7979/1914) and x3550 (7978/1913).
- QLogic iSCSI Controller info cannot be collected in Sles10 Realtime and Red Hat5 Realtime.
- For HS22(7870/1936), iDataplex(7321/7322), X3650 M2(7947), 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 FW 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 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 X3400/x3500(7973/7974/7975/7976/7977), X3200M2(4367/4368), X3250 M2(4190/4191/4194), X3350(4192/4193), X3550M2(7946/4198) on Windows2008.
- LSI raid configured as level "1E" will be recognized as level "1" in 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.

- UpdateXpress function by specifying -ux when executing DSA is not supported on the following systems:
  - x336
  - x260
  - Intellistation Z40
  - iDataplex dx320, dx360
- Using windows HPC server edition all RSA nodes are not available on x3950, x3850 M2 and x3950 M2.
- Using Microsoft Windows2003/Windows2008 Enterprise edition all RSA nodes are not available on x3950, x3850 M2 and x3950 M2. Please refer to Server Proven for specific OS support per system.
- The raw data of MegaRaid Information only can be reviewed in HTML/XML output.
- 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.
- On 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.
- LS21/LS41 Lightpath information might only show the first 8 DIMMs and first 2 CPUs LED 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).
- On LS22/LS42, some IPMI events show:

  ```
  Severity: Transition to Critical from less severe.
  ```
- If IMM information is not collected, please check the RNDIS device network configuration. The IP address & 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 disk is configured as RAID, DSA does not report disk error upon spin speed reduction.
- On iDataplex dx320, DSA has limited support.
- 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 using --update or --chkupd, sometimes it is due to the remote server down and may not be an internet connection problem.
  - Sometimes the NIC device eth0 is missing in the report generated for Brocade CNA.
  - Sometime description of port 1 of Brocade FC HBA is missing.
  - When Brocade CNA is present, sometimes the firmware 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 x3850 X5 dual node configuration, DSA shows incorrect core numbers (always show one core) for processors on 2nd node (CPU5-8).
- On X3850 X5 Standard (7145, 7146) and 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:
  - x3655 (7985, 7943)
  - x3850 M2 (7141, 7144, 7233, 7234)
  - x3850 X5 (7145, 7146)
  - x3950 M2 (7141, 7233)
  - x3950 X5 (7145, 7146)
  - x3650 (7979, 1914)
  - HS12(8014, 8028, 1916)
  - HS21 (8853, 1885)
  - HS22V (7871)
  - LS21/LS41 (7971, 7972)
  - LS22/LS42 (7901, 7902)
  - 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 Windows2008 R2 SP1, you might receive a dialog box indicating that `IBMSPREM.EXE has stopped working`.
- On Windows 2008, if the adapter event logs of a MegaRAID controller are full, a dialog box appears and displays the message `Megacli.exe has stopped`. You can avoid this by clearing the adapter event logs using the following command:

  ```
  MegaCli -AdpEventLog -Clear -aALL
  ```
- 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 Windows 2008 SP2 64bit, when the device driver of a Broadcom HT1000 SATA controller is updated to the latest version (1.1.8049.1) on 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, this will be left blank. This is most often encountered in common tables containing instances from multiple data sources.

- On Windows, you might need to turn off **check for server certificate revocation (requires restart)** from the **Tools** > **Internet Options** > **Advanced** > **Security** menu when trying to run DSA with the option **-upload** through a proxy environment.
- 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 HX5(7872,1909) multiple node, only Diagnostic 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.
- When you execute DSA with **-ux**, the ATI video driver comparison result in the UpdateXpress might be downlevel. For example, driver ATI2MTAG.SYS, shows 6.14.10.6744 for the latest version. This should be 8.24.50. Please see www.ibm.com for the latest firmware and driver updates.
- When you execute DSA with -ux on Windows XP or Windows Vista, the result in the UpdateXpress section might not be available or it might be inaccurate.
- When you execute DSA with -ux on the LS20 (8850), the BIOS comparison result in the UpdateXpress section might be downlevel. For example, it shows the latest version is 1.28, but it should be 1.29. Also, the ServeRaid driver comparison might be downlevel. For example, it shows the latest version of NFRD960.SYS as 7.10.0.0, but it should be 7.12.11. Refer to www.ibm.com for the latest firmware and driver updates.
- When you execute DSA with **-ux** on x346 (8840), the result in UpdateXpress for device driver file NFRD960.SYS is 7.10.0.0, when it should be 7.12.11.
- When you execute DSA with **-ux** on HS12 (8014/8028/1916), the result in UpdateXpress for LSI 1064e SAS controller might be inaccurate. It shows the latest level is 1.26.80 but actually it should be 1.26.84.
- Window Components cannot be collected in Windows 2008.
- Broadcom Firmware information cannot be collected in X3200M2 (4367/4368) on Windows 2008.
- For HS22 (7870/1936), iDataplex (7321/7322), X3650 M2 (7947), 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, but if you update iMM FW using the iMM website, the RNDIS driver is not installed on the OS. In this case, you must install RNDIS manually to collect the SP configuration, Chassis event log, and environment data.
- Slot of PCI-E/PCI adapters is blank in PCI information Section in X3400/x3500 (7973/7974/7975/7976/7977), X3200M2 (4367/4368), X3250 M2 (4190/4191/4194), X3350 (4192/4193), X3550M2 (7946/4198) on Windows 2008.
- On HS12, the PCI slot information might not reflect the real status. It might show On Board when there is a PCI device plugged in.
- Using windows HPC server edition, all RSA nodes are not available on x3950, x3850 M2, and x3950 M2.

- Using Microsoft Windows2003/Windows2008 Enterprise edition, all RSA nodes are not available on x3950, x3850 M2, and x3950 M2. Refer to Server Proven for specific OS support per system.
- Using Microsoft WindowsPE, all RSA nodes and BMC nodes are not available on x3950, x3850 M2, and x3950 M2. Refer to Server Proven for specific OS support per system.
- 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 x3250 M2 no Broadcom NIC firmware information is collected.
- For x3550 or x3550 M2 when a dual port PCI NIC is plugged, DSA shows one port as in use 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 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 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 X3850 X5 Standard (7145, 7146) and HS22V (7871) with Windows 2008, IMM Configuration, the 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`.
- On 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 -aALL
  ```

- Broadcom Network cards firmware information cannot be determined in a WinPE environment.
- In Windows, you might need to turn off **check for server certificate revocation (require restart)** from > **Tools** > **Internet Options** > **Advanced** > **Security** when trying to run DSA with the **`-upload`** option through a proxy environment.
- If you uninstall the USB Over LAN driver manually, it will cause the Preboot firmware update to fail.
- If you are running DSA on a multi-node system such as e the xSeries 460, DSA cannot specify to which node certain hardware belongs. This is due to limitations of either Windows APIs or SMBIOS. The x460 appears to Windows and SMBIOS as a single, complete system and not as multiple nodes. Also, since LightPath and IPMI logs are only populated by the primary node, specific details regarding non-primary nodes are not be collected.

- If the USB Memory Key you are using does not appear in the list of media available to copy to, you can upload the DSA output directly if the machine is connected to a network or copy it to a floppy for upload later.
- While flashing Wflash on a new installed Windows 2003 R2, a Windows pop-up asking `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 dx360 M2, no ethernet NIC test is available in the diagnostics list in Preboot DSA.
- On HS12, Preboot DSA cannot be updated by UXSPI 3.0.
- Remote Supervisor Adapter (RSA) II remote control session is sometimes lost when accessing F2 Diagnostics, resulting in a black screen and then an error message saying that the connection is lost. When you close the remote control window and start a new one, you will see that the diagnostics memory test is already taking place, but have no control of the remote session.
- When booting from the image created by BoMC, you can select **Diagnostics** and click **Gui option** to enter GUI mode. Select **Diagnostic test**and add NIC items to test. When the NIC is triggered with an error (such as removing the NIC), `TestLoopBackMAC` to test status keeps `Running`. The diagnostics only apply to a NIC with a stable state (either normal or defective during test).
- When an error occurs to the hard disk during the HDD test, the test might complete with `No Result`. The diagnostics only apply to a HDD with 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 minimum 29B. After you upgrade the IMM firmware to 29B or higher, DSA Preboot will continue to flash without error.
- 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 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 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 x3200 M3 and x3250 M3
  - uEFI Y4E145B or greater for x3400 M2, x3400 M3, x3500 M2, and x3500 M3

  - uEFI D6E145C or greater for x3550 M2, x3550 M3, x3650 M2, and x3650 M3
- On x3250 M3 (4251, 4252, 4261), the firmware and BIOS version of the Emulex 10 GbE Virtual Fabric Adapter is missing in the Firmware/VPD page.
- On 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 user clicks 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 x3850 X5 dual node.
- On the System x3550, the information about `ErrorCorrectionType` is not displayed correctly on the Hardware Inventory page.
- 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.
- 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 System x3100 M4 and x3250 M4 systems, you might encounter these issues:
  - The IMM configuration, environmental, 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.
- Due to lack of SFTP support in RHEL3 and SLES9, FFDC data cannot be acquired from the CMM when running DSA with the `--remote-ffdc` option.
- Due to the limitations of QLogic driver on SUSE Linux Enterprise Linux (SLES) 11 32bit/64bit, the data collection on QLogic adapter is not supported on SLES11 OS.
- The FIFO test of NIC diagnostics is not supported on the Intel I350 Quad Port GbE. Powerville has shared FIFO and shared FIFO registers, making a test impossible if four ports are running at once.
- Online DSA shows `Unknown NIC` in the item `NIC Type` for the Intel NIC on the page "Network Settings" collected on Windows. Retain Tip: H203676.
- The description about Intel ethernet controller is shown 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 x3100 M4, x3250 M4, and x3755 M3, you might encounter the following issues due to limitations of the IMM:
  - The IMM configuration and Environmentals information, such as "IMM configuration", "Environmentals", and "Chassis Event Log", are reported as "SP Configurations", "BIST Results", and "SP Logs".
  - The IMM configuration and Environmentals 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 shows "Unknown" in the item "PartitionSubType" in the table "Disk Information" in the page "Hardware Inventory" when HDD is in the GUID Partition Table (GPT) format on uEFI systems.
- For Emulex Options, the Emulex Bios Version information in **Firmware"/VPD-** > **BIOS/uEFI** page and **Emulex** > **EMXCNA BIOS** page is not collected and shown due to the limitation of Emulex Utility.
- For reliable detection of IBM 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 doesn't support the data collection on QLogic adapter since the QLogic driver 1.01.02.d4 packaged in MCP 5.2 can't 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 onoboard card and the Robalo option card are not supported by VMware ESXi 5.0: The Name is be 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 first 32-port to second 32-port, and inverse sequence for the downgrade (Key uninstallation), or the error message `Firmware Version/Update Issue` may be prompted.
- 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 the you run DSA with the option **-upload** 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 USB key) for further usage.
- On 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 (like 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 following command of iflash to flash Preboot DSA levels between the Preboot DSA levels with the different naming conventions successfully: **`iflash64 --package [upd file name] --openoptions 16 --force`**
- Retain Tip H197177 - DSA PREBOOT INCORRECTLY DISPLAYS CHINESE LICENSE AGREEMENT
- Retain Tip H197142 - DSA "VOLUMES/MOUNT POINTS" TABLE "LABEL"...COLUMNS ARE EMPTY
- Retain tip H202792 - On x3100 M4 and x3250 M4, DSA will show "No result" or "Aborted" after running the LSI HDD diagnostic test when Software RAID is configured. DSA does not currently support this configuration.
- Retain tip H203200 - NVIDIA 2075/2090 GPU FAILS IN DSA PREBOOT DIAGS
- Retain tip H202676 - 2582: NVIDIA QUADRO 600 IS NOT RECOGNIZED BY DSA PREBOOT
- Retain tip H202743 - BROCADE 10 GIGABIT DUAL-PORT CNA LOOPBACK TEST FAILED The following two (2) loop back tests fail diagnostics:
  - ExternalEthLoopbacktest
  - ExternalLoopbackTest
- Retain tip H204309- THE SLOT INFO OF PCI DEVICES WILL SHOW BLANK OR ONBOARD
- RHEL6 and RHEL6.1 Support limitations:
  - The LSI CIM provider does not support RHEL6.x. The reported LSI Configuration in 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 user to install 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 will show **Onboard** if the corresponding PCI device is option card.
- When transferring files via FTP in an IPv6 network, you must add the port number to successfully upload. 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 environmentals information, such as 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 outputs collected by Preboot DSA on the following systems with VMware ESXi key, no page is displayed for VMware ESXi due to the limitation of MCP6.1:
  – x3755 M3
  – x3100 M4
  – x3250 M4
- Preboot DSA embedded cannot be flashed on VMWare ESX 4.1 on System x3755 M3.
- 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, 1909 multiple node configurations, on the **Software** > **System Overview** > **Report Highlights** page, some event logs are duplicated on node 1 and node 2. Only one node has these events, but DSA cannot determine which one.
- On x3200 M3 and x3250 M3, when the AC power cord is pulled out and plugged in, preboot DSA embedded might show an error message and fail to boot up. Cycling AC power without unplugging the cord might correct the problem.
- On x3850/3950 X5 multiple node, Portable DSA might throw out an exception when running with the option **-ipmilan -v** in Windows 2008 R2. In this case, the DSA log is created without any lost function.
- On RHEL3 and SLES 9, portable DSA does not work with the option **-t** due to the limitation of the library libcurl.

Dynamic System Analysis event log

All diagnostic test status and error information are 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 **ibm_utl_dsa_*v.r.m_portable_platform*.exe** to run this 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*.

-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.

--extract *directory*
Extracts the DSA executable files into the specified directory.

-f Collects the full ISMP service processor log.

--ffdc
This option is used to collect IMM FFDC log via In-Band mode.

-? | -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 3.5.

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***

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:\Program Files\IBM\DSA\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:\Program Files\IBM\DSA\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 subcommand and option switches for key management

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

Syntax

```
DSA fod<subcommand> [options]
```

Table 1. 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 1. 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 usage 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.
	--sftp or *--tftp*	userid:password @ip:[port]	This option is used to specify the sftp/tftp server for snmp interface.

Table 1. 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.

Subcommand 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 2. 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 2. 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 2. 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.

Subcommand and option switches for key management on CMM

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

Syntax

Table 3. 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 3. 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.

Subcommand and option switches for key management on IOM

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

Syntax

Table 4. 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.
	--sftp or *--tftp*	userid:password @ip:[port]	This option is used to specify the sftp/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 4. 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.
	--sftp or *--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 4. 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.
	--sftp or *--tftp*	userid:password @ip:[port]	This option is used to specify the sftp/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 semi-colon. 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 semi-colon. 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_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 9.20

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.

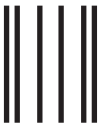
If you would like a response from IBM, please fill in the following information:

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 D06A
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