

IBM® Guardium®

Essentials-2025



Disclaimer:

- This session provides an introductory overview of product features and is intended solely as a supplementary learning resource. It is not suitable for implementation purposes. Accurate deployment requires a thorough understanding of the product, its intended use, and environment—none of which are covered in this session.
- Content is subject to change as the product evolves. We do not accept responsibility for decisions made based on this material, and any actions taken are at your own risk. We disclaim liability for any resulting damages.
- For the most current and accurate IBM documentation, please refer to: <https://www.ibm.com/docs/en/gdp>
- By continuing to participate, you acknowledge and accept these terms. If you do not agree, please disconnect from the session.

Speaker for today:



Sachin Marawar

Technical Support Professional, IBM Software Support (Data Security)



IBM Guardium Essentials-2025

8-Session Kickstart Series

Master the Foundations of Data Security Monitoring & Compliance

Session	Date	Topic	Registration Link
Session 1	Aug 26 (Tue)	What is IBM Guardium & How It Works	https://ibm.biz/IBMGE-S1
Session 2	Aug 28 (Thu)	Installing & Configuring Guardium Appliances	https://ibm.biz/IBMGE-S2
Session 3	Sep 02 (Tue)	GIM & WINSTAP Deployment	https://ibm.biz/IBMGE-S3
Session 4	Sep 04 (Thu)	Introduction to Guardium Policies	https://ibm.biz/IBMGE-S4
Session 5	Sep 09 (Tue)	GIM & S-TAP for UNIX/Linux	https://ibm.biz/IBMGE-S5
Session 6	Sep 11 (Thu)	Guardium Reports, Entities & Attributes	https://ibm.biz/IBMGE-S6
Session 7	Sep 16 (Tue)	Guardium Alerts & Audit Process	https://ibm.biz/IBMGE-S7
Session 8	Sep 18 (Thu)	Aggregation, Backup & Restore in Guardium	https://ibm.biz/IBMGE-S8

Today

Use above links to Register for each session!

Session 3:

IBM® Data Security

GIM & WINSTAP Deployment

-Sachin Marawar

Technical Support Professional, IBM Software Support (Data Security)



Agenda

- What is GIM?



- GIM Communication



- What is S-TAP?



- Installation Pre-requisites



- Demo (with and without GIM)



- Q&A



Feedback & Suggestions are welcome at:
datasec_ap_support@wwpdl.vnet.ibm.com

GIM Terminology

- GIM Agent – Collection of perl scripts run on each managed server allowing for centralized management
- GIM Server – Guardium appliance (deploy, modify, update, uninstall)
- GIM Bundle – A package of software that can be deployed with GIM. File extension .gim
Example: [guard-GIM-12.0_r120001295_1-x86_x64.gim](#)
- Module – Components of a bundle. A.gim file containing one or more modules or sub-modules. Examples: CAS, S-TAP, FAM, KTAP, ATAP, SUPERVISOR and more.
- Listener Mode – GIM Agent not yet associated with a GIM Server
- Standard Mode – GIM Agent associated with a GIM server



What is GIM?

```
ibm.com> grdapi commands gim
ID=0
Matching API Function list :
gim_assign_bundle_or_module_to_client_by_version
gim_assign_latest_bundle_or_module_to_client
gim_cancel_install
gim_cancel_uninstall
gim_get_available_modules
gim_get_client_last_event
gim_get_global_param
gim_get_modules_running_status
gim_list_bundles
gim_list_client_modules
gim_list_client_params
gim_list_mandatory_params
gim_list_registered_clients
gim_list_unused_bundles
gim_load_package
gim_remote_activation
gim_remove_bundle
gim_reset_client
gim_schedule_install
gim_schedule_uninstall
gim_set_diagnostics
gim_set_global_param
gim_unassign_client_module
gim_uninstall_module
gim_update_client_params
ok
ibm.com>
```

- A centralized tool for installing, updating, uninstalling and monitoring Guardium agents
- Consists of:
 - GIM Server (on Guardium appliance)
 - GIM Client (on monitored servers)
- Interaction through Guardium UI and command-line.
- Support of ~4000 GIM clients from single Guardium system
- GIM Bundle example: [guard-GIM-12.0_r120001295_1-x86_x64.gim](#)
- GIM agent installation requires disk space ~ 1 Gb on the Windows OS
- Once fully functional, you don't need to directly access the DB server



== For Installation ==

“Administrator”

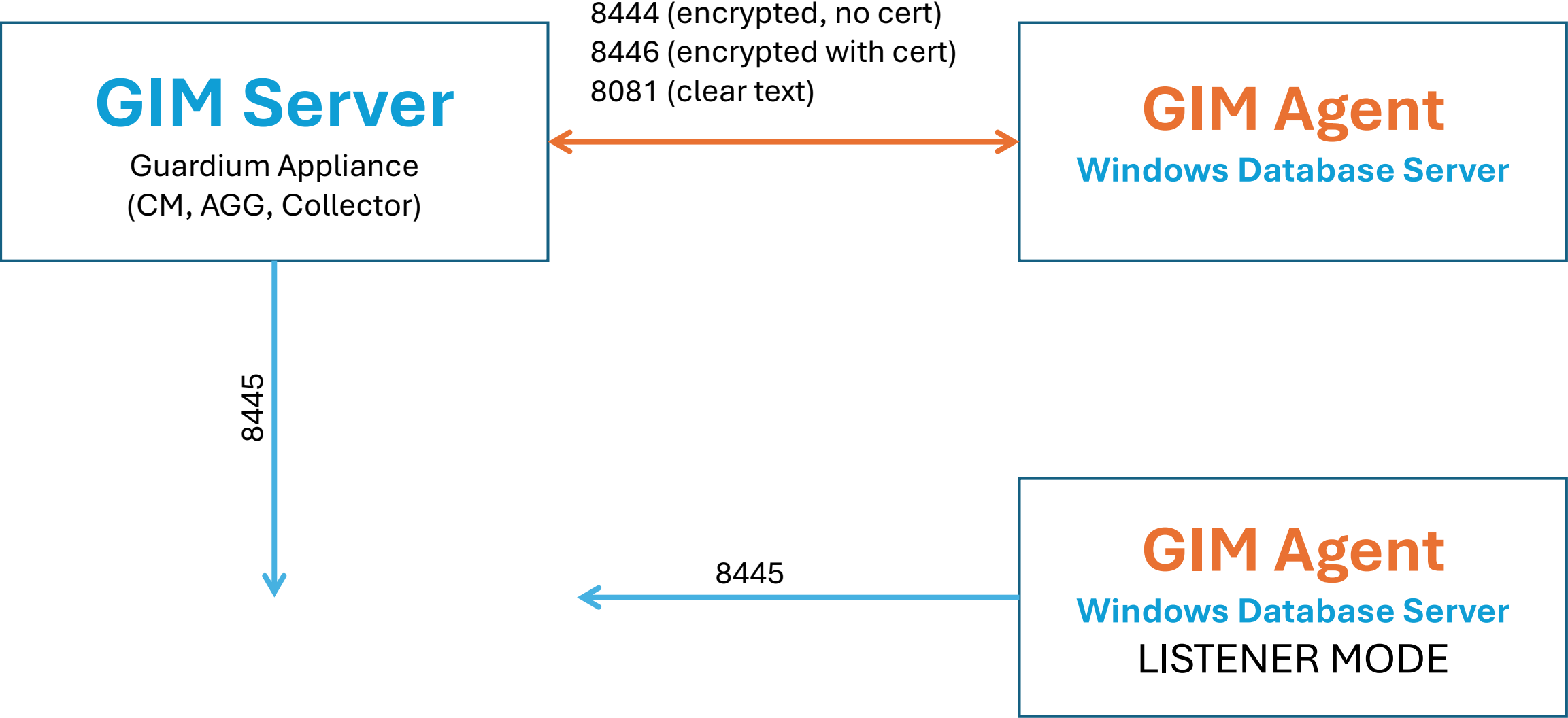
OR

User with
“Administrator” privileges
needed



Set up by Client				
✓ Choose clients Select the clients to install or update				
Select a client group to show only clients from the group				
Select client group				
Reset connection Run diagnostics View Installed Modules Filter				
☐	Client name	Client IP	Client OS	Client OS version
☐	msd-esp-0001	msd-esp-0001	Linux	rhel 8 (4.18.0-553.70.1.el8_10.x86_64)
☒	msd-esp-0002	msd-esp-0002	Windows	Microsoft Windows Server 2022 (20348)

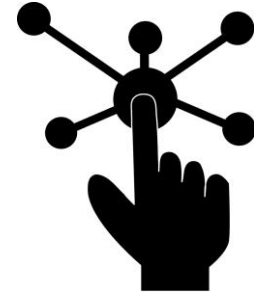
GIM Communications



GIM Installation Modes

- **Interactive Installer:** GUI-based wizard for step-by-step setup.

1. Place the installer on the database server.
2. Run setup.exe from the installer folder.



- **Silent Installation:** Command-line based, ideal for automation.

`setup.exe -UNATTENDED -INSTALLPATH "C:\Program Files (x86)\Guardium Installation Manager" -LOCALIP <GIM CLIENT IP> -APPLIANCE <Appliance IP>`

Important Parameters:

- UNATTENDED: Enables silent mode.
- LOCALIP: Required; IP of the client machine.
- APPLIANCE: Optional; if omitted, installs in Listener Mode.
- AUTO_ASSIGN_IP: Automatically assigns IP (do not use with -LOCALIP).



Post-Installation:

Logs available at: C:\IBM Windows GIM.ctl

GIM Interactive Installation:



The screenshot shows a web browser window with multiple tabs. The active tab is titled "IBM Support: Fix Centr...". The address bar shows the URL: `ibm.com/support/fixcentral/swg/downloadFixes?parent=IBM%20Security&product=ibm/Information+Management/InfoSphere+Guardium...`. The page header includes navigation links: Support, Downloads, Documentation, Forums, Cases, Monitoring, and Manage support account. The main content area is titled "IBM Security, IBM Security Guardium (12.1, All platforms)". Below this, a section titled "Download files using your web browser" provides instructions: "Right-click the download link next to each file and choose 'Save link as' or similar." A table displays the following information:

Order number:	626754541
Total size:	1.28 GB

Below the table, there are links for "Show normalized list" and "Hide normalized list". A mouse cursor is hovering over the "Hide normalized list" link. Further down, a section titled "fix pack:" lists "Guardium_12.1.0.162_GIM_Windows" with a "More Information" link. Below this, it states "The following files implement this fix." and lists a single file: "Guardium_12.1.0.162_GIM_Windows.zip (1.28 GB)". At the bottom left, there is a "Back" button. On the right side, there are two boxes: "Download options" with links for "Show terms and conditions" and "Change download options", and "Quick order" with a link for "Share this download list". A vertical "Contact and feedback" button is on the far right. A "Cookie Preferences" button is at the bottom right.

GIM Silent Installation:



IBM Guardium (ind-trg-col)

Installing the GIM client on a W

ibm.com/docs/en/gdp/12.x?topic=servers-installing-gim-client-windows-server

ind-trg-col SAMPLE_OR_A_APP DB Connection v12.1 FixCentral KTAP Compatibility 12.x Documentation

IBM Documentation Search in IBM Guardium Data Protection

IBM Guardium Data Protection

Change version

12.x

☒ Show full table of contents

Filter on titles

Installing the GIM client on a Windows server

Installing GIM and other packages on Windows servers by using the consolidated installer

Starting and stopping the GIM client on a Windows server

Managing GIM clients

Managing software with GIM

Starting and restarting GIM services and components

Installing your Guardium system

Upgrading your Guardium system

Download PDF

You can view the results of the installation in the log file at C:\IBM\Windows\GIM.ctl.

Installing the GIM client with silent installation

If you prefer, you can install the GIM client from the command prompt instead of the wizard.

Procedure

1. Place the GIM client installer on the database server, in any folder.
2. Open a command prompt and locate the GIM_Installer* folder under the folder where you placed the installer.
3. Enter the following command, with no line break.

```
setup.exe -UNATTENDED -LOCALIP <GIM CLIENT IP> -APPLIANCE <Appliance IP>
```

Attention:

- The **UNATTENDED** and **LOCALIP** parameters are required. **APPLIANCE** is optional and if not supplied, triggers Listener Mode.
- Do not specify both **AUTO_ASSIGN_IP** parameter and **LOCALIP**.
- Omit the **APPLIANCE** parameter to install the client in GIM listener mode. Listener mode makes the GIM client available for remote registration from a Guardium system. The following example shows how to install as listener:

```
setup.exe -UNATTENDED -INSTALLPATH "C:\Program Files\IBM\Guardium Installation Manager" -LOCALIP <GIM CLIENT IP>
```


For more information, see [GIM Remote Activation](#) and [Create a GIM Auto-discovery Process](#).
- When cloning database servers and establishing large deployments, use **auto_assign_ip 1** to allocate a random IP address from one of the valid IP addresses of a database server. Do not specify

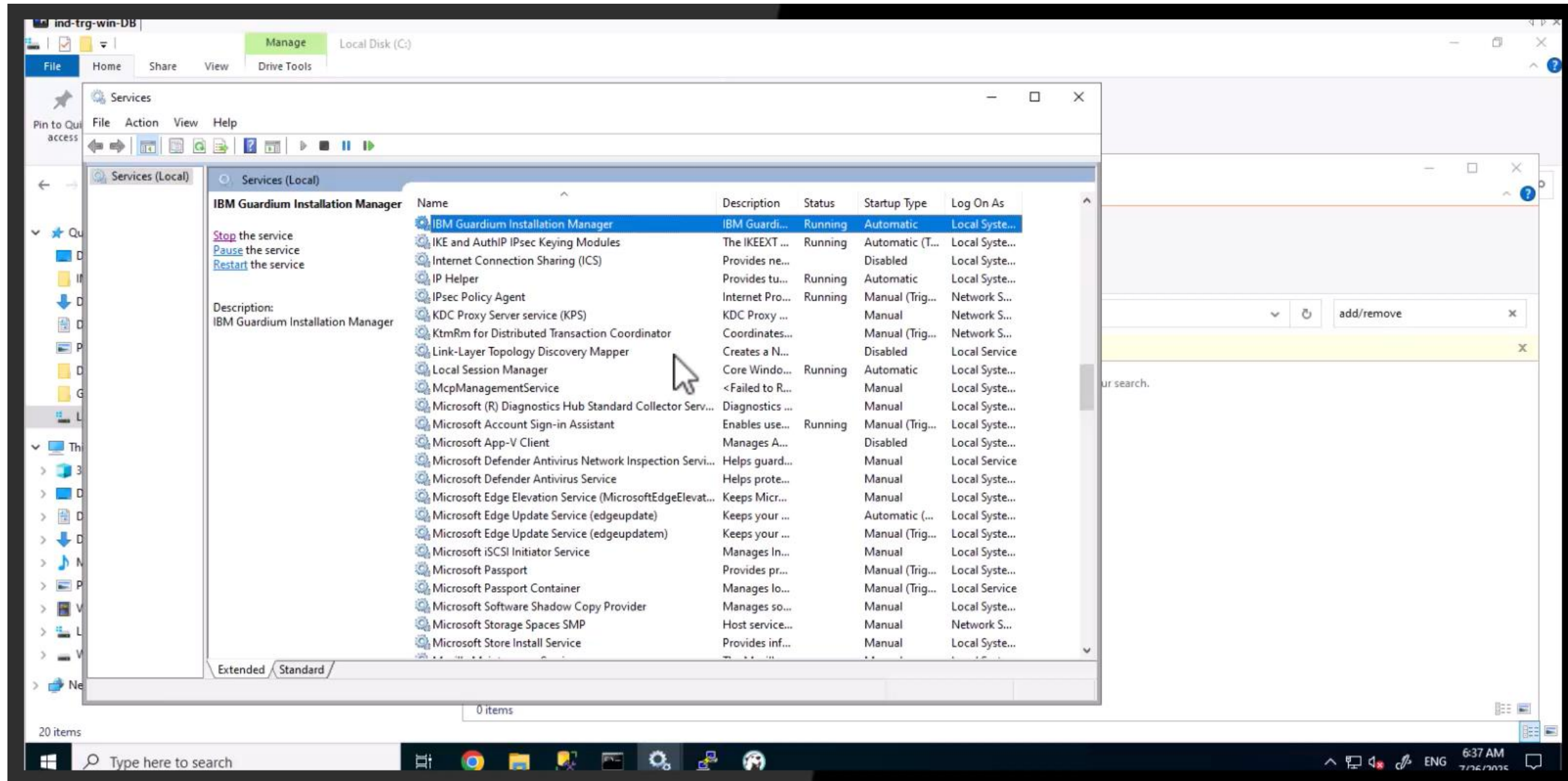
On this page

About this task

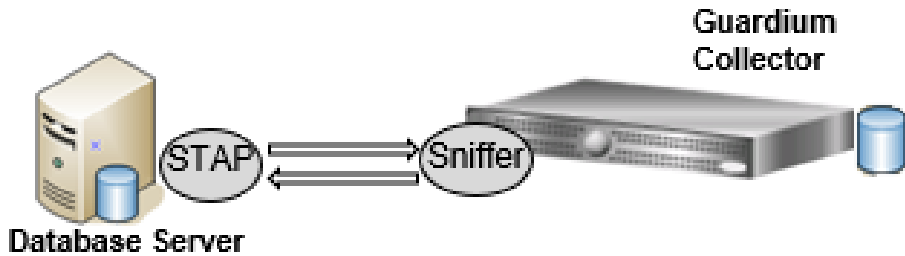
Installing the GIM client with an interactive installer

Installing the GIM client with silent installation

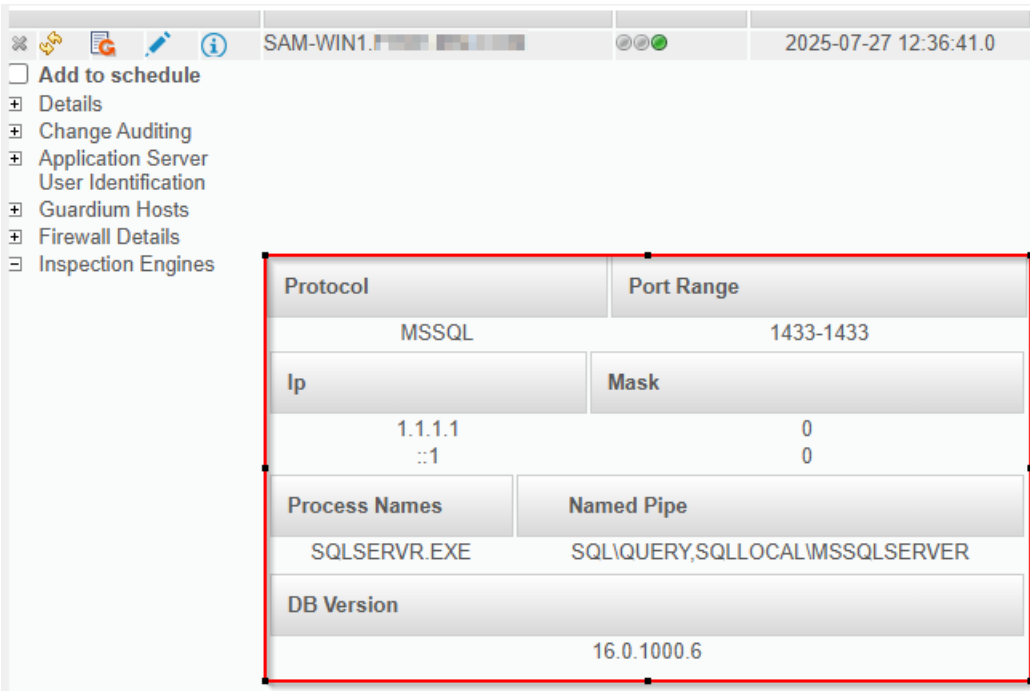
Uninstalling the GIM client



What is S-TAP?



- S-TAP = Software TAP = Lightweight software agent installed on DB server
- Monitors database activities
- Can handle encrypted traffic
(**Limitation:** Windows S-TAP does not support MySQL encrypted)
- Minimal overhead to the DB env
- One installation on one OS node
- Filters to reduce network overhead
- Expected <5% performance impact on server
- No Inspection Engine = No traffic
- Auto discovery list so far includes-
oracle:db2:informix:mysql:postgres:sybase:teradata:netezza:memsql:mariadb:verticadb



Inspection Engine

Pre-requisites for WINSTAP Installation:

This PC > Downloads > WINSTAP_DOWNLOAD > Windows-STAP-V12.1.0.112 >

Name	Date modified	Type	Size
Files	7/4/2025 5:03 AM	File folder	
Google.Protobuf.dll	7/30/2024 2:32 PM	Application exten...	473 KB
IBM.Guardium.BaseForms.dll	9/5/2024 10:46 AM	Application exten...	50 KB
IBM.Guardium.Diagnostics.dll	9/5/2024 10:46 AM	Application exten...	27 KB
IBM.Guardium.Installer.dll	9/5/2024 10:47 AM	Application exten...	910 KB
IBM.Guardium.Interop.dll	9/5/2024 10:46 AM	Application exten...	129 KB
IBM.Guardium.IO.dll	9/5/2024 10:46 AM	Application exten...	23 KB
Setup.exe	9/5/2024 10:48 AM	Application	246 KB
SetupSupport.dll	9/5/2024 10:47 AM	Application exten...	1,129 KB
StapInstaller.exe	9/5/2024 10:48 AM	Application	225 KB
StapInstaller.exe.config	5/6/2024 1:40 PM	CONFIG File	1 KB



The new S-TAP protocol 8 reduces CPU usage and memory usage.

The two S-TAP protocols co-exist and use the same guard_tap.ini configuration file.

You choose which protocol you want to use for each S-TAP.



- S-TAPs require .NET Framework 4.5 or higher version.
- S-TAP installs .NET 4.5.2 if there is none.
- Guardium Services group created with first WINSTAP installation.
- Setup.exe calls StapInstaller.exe.
- Microsoft .NET framework: ~5 Gb space
- WINSTAP by GIM installation: ~300 Mb
- WINSTAP without GIM installation: ~180 Mb
- 9500/9501 TCP Alive messages Protocol 7
- 9800/9801 TCP Alive messages Protocol 8
- 9500 TCP Clear S-TAP
- 9501 TLS Encrypted S-TAP
- BFE service must be running.

Interactive WINSTAP Installation:



The screenshot shows a web browser window displaying the IBM documentation page for installing the S-TAP agent on Windows. The browser has several tabs open, including 'DB Connection', 'IBM Support: Fix Central', 'IBM Guardium (ind-trg-col)', and 'Windows: Installing S-TAP agent'. The address bar shows the URL: ibm.com/docs/en/gdp/12.x?topic=wuiwiuust-windows-installing-s-tap-agent-by-using-interactive-installer. The page header includes the IBM logo, 'Documentation', and a search bar. The left sidebar shows the 'IBM Guardium Data Protection' navigation menu with a 'Change version' dropdown set to '12.x'. The main content area features the title 'Windows: Installing S-TAP agent by using the interactive installer' and a sub-header 'Before you begin'. The page also includes a 'Download PDF' link and a 'Was this topic helpful?' feedback section.

IBM Guardium Data Protection

Change version

12.x

☒ Show full table of contents

Filter on titles

Windows: Installing S-TAP agent by using the interactive installer

Windows: Upgrading the S-TAP agent using the interactive installer

Windows: Use CLI to install, upgrade, uninstall the S-TAP

Download PDF

All products / IBM Guardium Data Protection / 12.x /

Was this topic helpful?

Windows: Installing S-TAP agent by using the interactive installer

Last Updated: 2025-01-03

The interactive installer is useful for smaller deployments or whenever a guided, step-by-step installation experience is required.

Before you begin

Verify the following before you begin:

- Review the Windows S-TAP installation requirements at [Windows: Prerequisites: Installing S-TAP](#).
- Verify that your database server and operating system are supported. For more information, see [System requirements](#) and the [Windows: S-TAP monitoring mechanisms support matrix](#).
- Identify the IP address of the database server where you are installing the S-TAP, including any virtual IP addresses.

On this page

- Before you begin
- About this task
- Procedure
- What to do next

Service Control & Driver Query:

C:\Users\Administrator>**sc query | findstr -i guard**
SERVICE_NAME: GUARDIUM_STAP
DISPLAY_NAME: IBM Security Guardium S-TAP
DISPLAY_NAME: IBM Security Guardium Database Monitor Service x64
DISPLAY_NAME: IBM Security Guardium Database Monitor Service x86

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.4052]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>sc query | findstr -i guard
DISPLAY_NAME: IBM Security Guardium Database Monitor Service x64
DISPLAY_NAME: IBM Security Guardium Database Monitor Service x86
DISPLAY_NAME: IBM Guardium Installation Manager
SERVICE_NAME: GUARDIUM_STAP
DISPLAY_NAME: IBM Security Guardium S-TAP
```

```
C:\Users\Administrator>driverquery -v | findstr -i guard
Correlator  IBM Security Guardium  IBM Security Guardium  Kernel  Auto  Running  OK  TRUE  FA
LSE 0 32,768 0 8/16/2024 9:04:10 AM \??\C:\Program Files\IBM\Windows S-TAP\Bin\Co
rre 4,096
NmpMonitor  IBM Security Guardium  IBM Security Guardium  Kernel  Auto  Running  OK  TRUE  FA
LSE 0 122,880 0 8/16/2024 9:04:16 AM \??\C:\Program Files\IBM\Windows S-TAP\Bin\Nm
pMo 4,096
NmpProxy  IBM Security Guardium  IBM Security Guardium  Kernel  Auto  Running  OK  TRUE  FA
LSE 0 49,152 0 8/16/2024 9:04:10 AM \??\C:\Program Files\IBM\Windows S-TAP\Bin\Nm
pPr 4,096
PrcMonitor  IBM Security Guardium  IBM Security Guardium  Kernel  Auto  Running  OK  TRUE  FA
LSE 0 20,480 0 8/16/2024 9:04:09 AM \??\C:\Program Files\IBM\Windows S-TAP\Bin\Pr
cMo 4,096
WfpMonitor  IBM Security Guardium  IBM Security Guardium  Kernel  Auto  Running  OK  TRUE  FA
LSE 0 200,704 0 8/16/2024 9:04:14 AM \??\C:\Program Files\IBM\Windows S-TAP\Bin\Wf
pMo 4,096
```

```
C:\Users\Administrator>driverquery -v | findstr WfpMonitor
WfpMonitor  IBM Security Guardium  IBM Security Guardium  Kernel  Auto  Running  OK
TRUE  FALSE  0 200,704 0
8/16/2024 9:04:14 AM
\??\C:\Program Files\IBM\Windows S-TAP\Bin\WfpMo 4,096
```



WINSTAP Installation with GIM:

A screenshot of a web browser window displaying the IBM Guardium login interface. The browser's address bar shows the URL 'ind-trg-col' and a 'Not secure' warning. The page has a dark blue background with the 'IBM Guardium' logo centered. A white login box is centered on the page, containing two input fields: 'User name' and 'Password'. A mouse cursor is hovering over the 'Password' field. Below the input fields is a blue 'Login' button. At the bottom of the login box, there is a block of small text providing copyright and trademark information for IBM.

IBM Guardium®

User name

Password

Login

Licensed Materials - Property of IBM
5725-I11, 5725-I12, 5725-V56, 5737-D57, 5737-M13
Licensed Materials
5737-H30, 5737-H31
© Copyright IBM Corp. 2002, 2024 All Rights Reserved.
*Trademark of International Business Machines

Querying modules state:

```
grdapi gim_list_client_modules clientIP="client ip"
```

State	Description
INSTALLED	Module is installed.
PENDING-INSTALL	Module is pending to be scheduled for installation.
PENDING-UNINSTALL	Module is pending to be scheduled for uninstallation.
PENDING-UPDATE	Module is pending to be scheduled for update.
IP	Module installation is in progress.
FAILED	Module's last operation failed.
IP-PR	Module requires client reboot to complete the installation process.



WINSTAP Uninstall:



Settings

Home

Find a setting

Apps

Apps & features

Default apps

Apps for websites

Startup

Apps & features

Choose where to get apps

Installing apps only from Microsoft Store helps protect your device.

Anywhere

Apps & features

Optional features

App execution aliases

Archive apps

Search, sort, and filter by drive. If you would like to uninstall or move an app, select it from the list.

S-TAP

Sort by: Name Filter by: All drives

1 app found

IBM® Security Guardium® S-TAP

IBM

45.0 MB

7/4/2025

Some parameters in guard_tap.ini:

PARAMETER NAME	DESCRIPTION
ALL_CAN_CONTROL	Any collector that can see the S-TAP in S-TAP Control can change the config
BUFFER_FILE_SIZE	Applicable for PROTOCOL=7 only. Default value 50 Mb. Can go to 1000 Mb.
DB_IGNORE_RESPONSE	Use this function for an easier configuration for ignoring responses from the database, without loading the network. DB_IGNORE_RESPONSE=ALL or DB_IGNORE_RESPONSE=MSSQL,DB2. Supported DB types: ALL, MSSQL_NP, MSSQL, MYSQL, TRD, PGRS, MSSYB, ORACLE, DB2, DB2_EXIT, INFORMIX, KERBEROS, FTP, CIFS.
PARTICIPATE_IN_LOAD_BALANCING	0, 1, 2 and 3 are the possible values. 0 = no load balancing 1 = Load balancing 2 = mirror / redundancy 3 = hardware load balancing
SOFTWARE_TAP_HOST	The database server host where S-TAP is installed. Can be IP or hostname.
SQLGUARD_IP	IP address or hostname of the Guardium system

Some parameters in guard_tap.ini (conted..):

PARAMETER NAME	DESCRIPTION
AUTO_DISCOVERY	Enables auto discovery of database instances, populates inspection engines, and updates guard_tap.ini Note: Auto discovery does not ensure detection of all listening ports for all supported databases. For example, when using Microsoft SQL Server Always On, auto discovery cannot discover the listening ports. You can manually add inspection engines for the listening ports that were not automatically discovered.
UPLOAD_FEATURE	Collects all of the information (dump file, log files, etc.) from Program Files\IBM\Windows S-TAP\Logs. Compresses the files. Uploads the .zip file to the collector and/or central manager, to the folder /var/IBM/Guardium/log/stap_diagnostic. 0: No automatic upload. 1: Upload files to the collector and the central manager. 2: Upload files only to the collector, even if there is a central manager.

References:

<https://www.ibm.com/docs/en/gdp/12.x?topic=guardium-installation-manager>

<https://www.ibm.com/docs/en/gdp/12.x?topic=tools-guardium-installation-manager>

<https://www.ibm.com/docs/en/gdp/12.x?topic=system-guardium-port-requirements>

<https://www.ibm.com/docs/en/gdp/12.x?topic=servers-installing-gim-client-windows-server>

<https://www.ibm.com/docs/en/gdp/12.x?topic=manager-install-upgrade-uninstall-gim-clients-windows-servers>

<https://www.ibm.com/docs/en/gdp/12.x?topic=agent-windows-prerequisites-installing-s-tap>

<https://www.ibm.com/docs/en/gdp/12.x?topic=gim-cli-commands>

<https://www.ibm.com/docs/en/gdp/12.x?topic=guide-windows-s-tap-protocol-8>

Q&A

Any
Questions?



Thank you for your attention!



- Register for-
04-Sep-2025
Thursday

Session 4: ibm.biz/IBMGE-S4

Policy
&
Policy
&
Policy

Feedback & Suggestions are welcome at:
datasec_ap_support@wwpdl.vnet.ibm.com