IBM InfoSphere Guardium

Version 8.2

Server IP Mapping for IBM Licensing Metering Tool (ILMT)

This document describes how to get the Server IP list for each Guardium chargeable component.

PID 5725-A85 - IBM InfoSphere Guardium

CCs – IBM InfoSphere Guardium Database Activity Monitor group

The following chargeable components can be classified as belonging to an activity monitoring group that possesses the same criteria for mapping server IPs.

- IBM InfoSphere Guardium Database Activity Monitor with Privileged User Auditing
- IBM InfoSphere Guardium Database Activity Monitor with Sensitive Objects Auditing
- IBM InfoSphere Guardium Database Activity Monitor with Comprehensive Auditing
- IBM InfoSphere Guardium Database Activity Monitor for Standby Systems with Privileged User Auditing
- IBM InfoSphere Guardium Database Activity Monitor for Standby Systems with Sensitive Objects Auditing
- IBM InfoSphere Guardium Database Activity Monitor for Standby Systems with Comprehensive Auditing
- IBM InfoSphere Guardium Database Activity Monitor for Data Warehouses with Privileged User Auditing
- IBM InfoSphere Guardium Database Activity Monitor for Data Warehouses with Sensitive Objects Auditing
- IBM InfoSphere Guardium Database Activity Monitor for Data Warehouses with Comprehensive Auditing
- IBM InfoSphere Guardium Database Activity Monitor for Load Balancing with Privileged User Auditing
- IBM InfoSphere Guardium Database Activity Monitor for Load Balancing with Sensitive Objects Auditing
- IBM InfoSphere Guardium Database Activity Monitor for Load Balancing with Comprehensive Auditing

How to map

All of the above IBM InfoSphere Guardium Database Activity Monitor auditing activity can be mapped to:

1. Normally the IBM InfoSphere Guardium Database Activity Monitor monitors activity using S-TAP. The S-TAP Status report, accessed through **Tap Monitor -> S-TAP -> S-TAP Status**, shows the S-TAP Host (server IP) that the IBM InfoSphere Guardium Database Activity Monitor is monitoring.

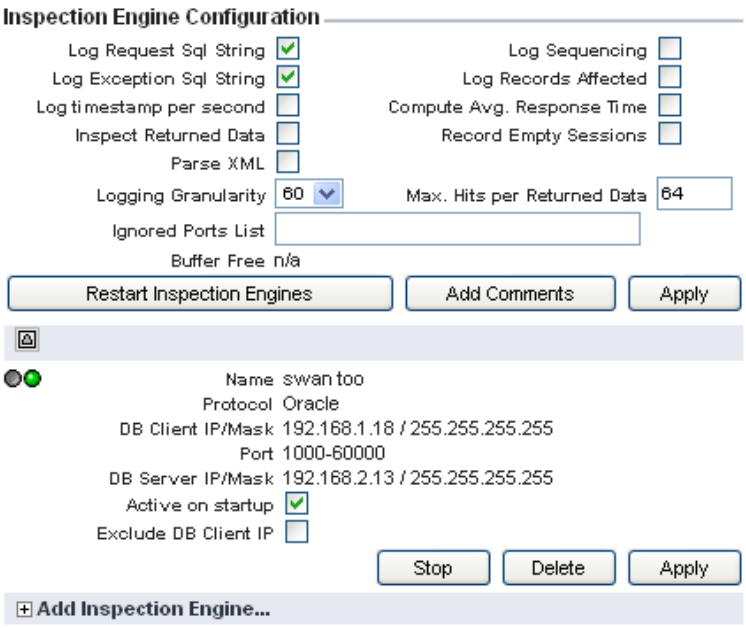
S-TAP Status

Aliases: **OFF**

S-TAP Host	S-TAP Version	DB Server Type	Status	Last Response	Primary Host Name	KTAP Installed	TEE Installed
192.168.2.20	8.21066	DB2	Active	2010-08-24 11:28:42.0	192.168.3.104	No	No
192.168.2.20	8.21066	INFORMIX	Active	2010-08-24 11:28:42.0	192.168.3.104	No	No
192.168.2.20	8.21066	MSSQL	Active	2010-08-24 11:28:42.0	192.168.3.104	No	No
192.168.2.20	8.21066	MSSQL_NP	Active	2010-08-24 11:28:42.0	192.168.3.104	No	No
192.168.2.20	8.21066	ORACLE	Active	2010-08-24 11:28:42.0	192.168.3.104	No	No
192.168.2.20	8.21066	SYBASE	Active	2010-08-24 11:28:42.0	192.168.3.104	No	No
192.168.2.21	8.21066	MSSQL	Active	2010-08-24 11:28:42.0	192.168.7.214	No	No
192.168.2.232	8.21066	MSSQL	Active	2010-08-24 11:28:42.0	192.168.7.214	No	No
192.168.2.232	8.21066	MSSQL	Active	2010-08-24 11:28:42.0	192.168.7.214	No	No
192.168.7.107	8.21066	DB2	Active	2010-08-24 11:28:42.0	192.168.7.214	No	No
192.168.7.107	8.21066	INFORMIX	Active	2010-08-24 11:28:42.0	192.168.7.214	No	No
192.168.7.107	8.21066	MSSQL	Active	2010-08-24 11:28:42.0	192.168.7.214	No	No
192.168.7.107	8.21066	MSSQL_NP	Active	2010-08-24 11:28:42.0	192.168.7.214	No	No
192.168.7.107	8.21066	ORACLE	Active	2010-08-24 11:28:42.0	192.168.7.214	No	No

Records 1 to 20 of 25

2. If not using S-TAP, but instead using network inspection you can go to the console inspection engines and see the Server IPs being monitored. Access by going to **Administration Console -> Configuration -> Inspection Engines.**



Note: Access reports, such as the **DB Server List,** accessed by going to **View -> Access Map -> DB Server List,** can be used to show a listing of the server IPs for the database servers seen during a reporting period.

CC - IBM InfoSphere Guardium - Enterprise Integrator

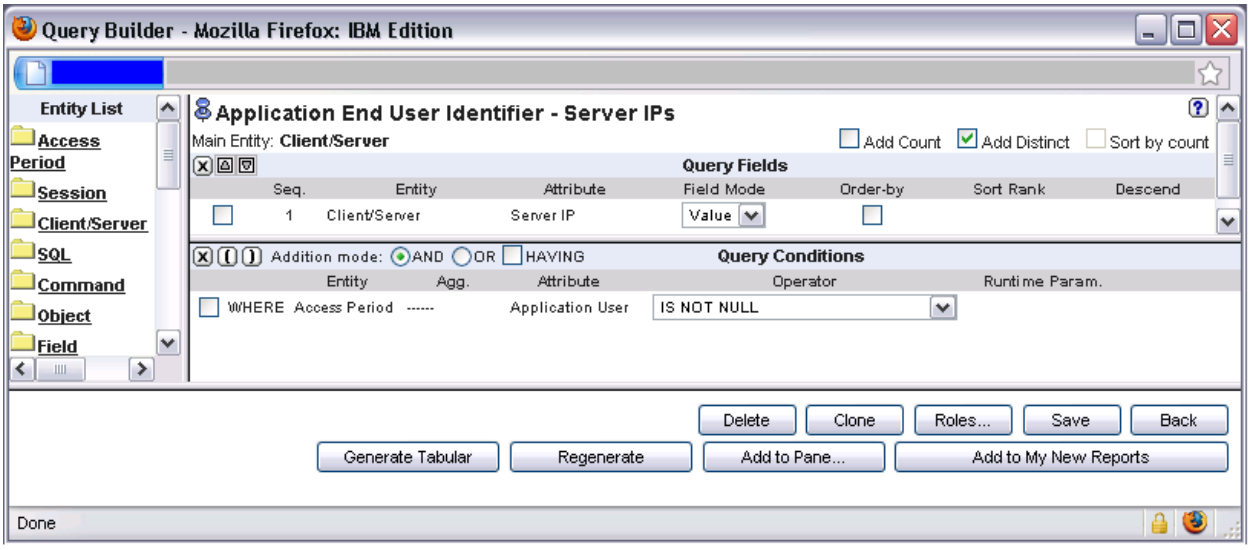
How to map

IBM InfoSphere Guardium provides the ability, through **Custom Domains**, to define any tables of data uploaded to the appliance from the customer's environment. Thus, this is the same as defined for the IBM InfoSphere Guardium Database Activity Monitor group, see above.

CC - IBM InfoSphere Guardium - Application End User Identifier

How to map

The application end user can be seen through the **Access Tracking** domain and using the **Access Period** Entity to query **Application User**. The **Access Period** entity can be joined to other entities such as **Client/Server** to find the **Server** IP. Query Builder can be used to produce a report for server IPs such as the following:



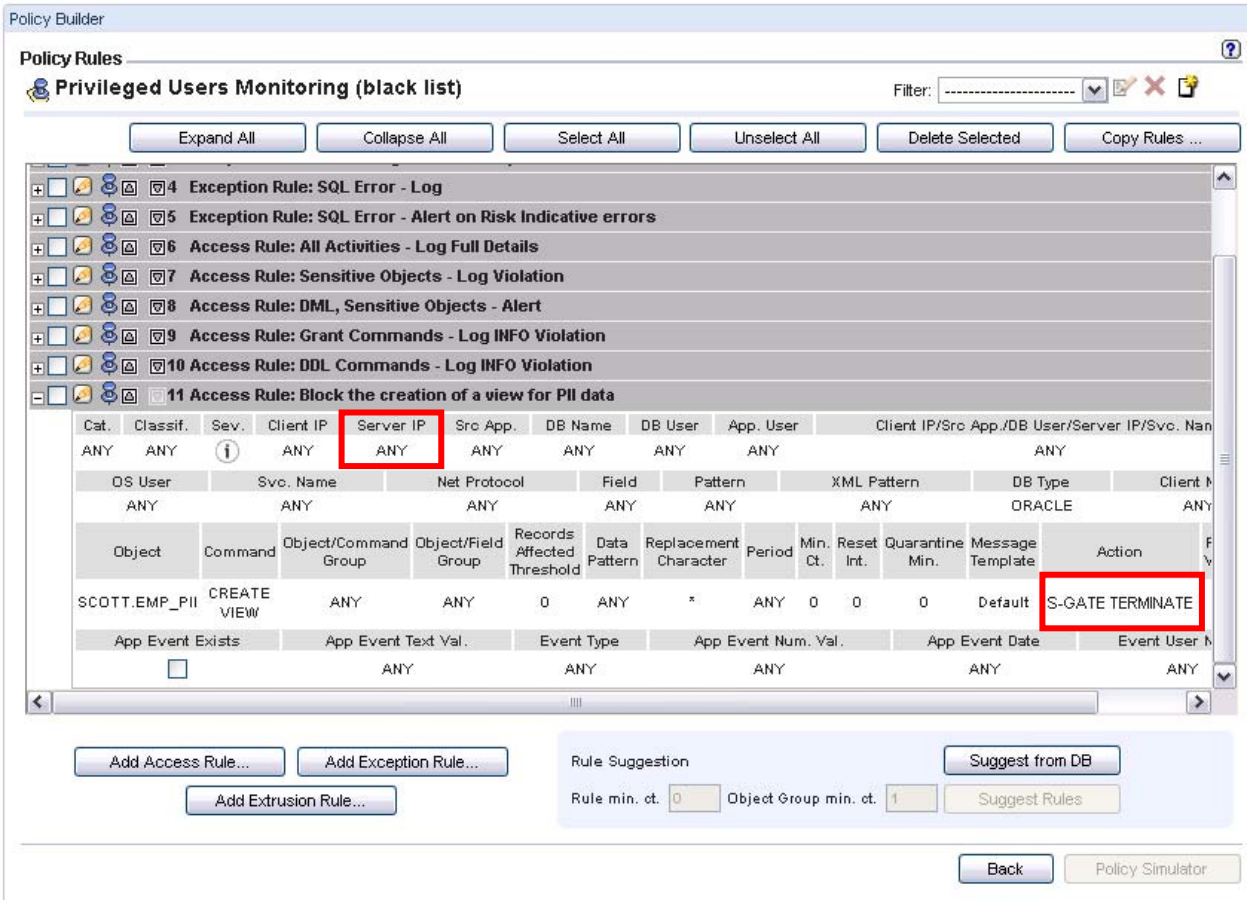
Alternatively, use the same as defined for the IBM InfoSphere Guardium Database Activity Monitor group (see above), the list of servers in scope are the relevant for this application as well.

CC- IBM InfoSphere Guardium - Data-Level Access Control

How to map

To find if a policy has been configured to use S-GATE, you can look at the policy rules and their actions by going to **Tools -> Policy Builder -> Selecting the Policy -> Edit Rules** and then expanding the individual rules to see if **S-GATE** is part of the **Actions** defined. If S-GATE rules are in use then the list of server IPs would then be one of the following:

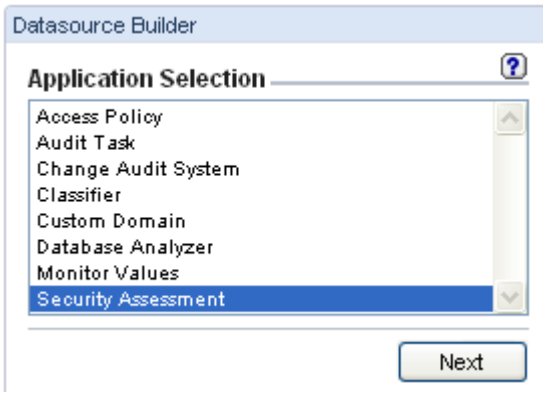
- If the S-GATE Policy Rules include specific Server IPs (or a group of IPs) – then these IPs are in scope
- If the S-GATE Policy Rules have 'ANY' for Server IPs – use the Server IPs are defined for the IBM InfoSphere Guardium Database Activity Monitor group (see above).

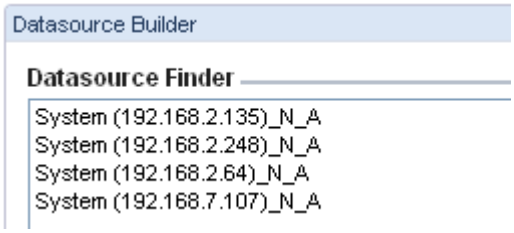


CC - IBM InfoSphere Guardium - Database Vulnerability Assessment

How to map

The list of datasources defined under **Tools -> Datasource Definitions -> Security Assessment (Application Selection)** will provide the database server IPs being used.
(Note: when datasource presents just the hostname, you'd need to click the 'Modify' button to see its IP address for)





CC- IBM InfoSphere Guardium - Database Protection Knowledgebase

How to map

This is the same as IBM InfoSphere Guardium – Database Vulnerability Assessment, see above.

CC- IBM InfoSphere Guardium - Configuration Audit System for Database Servers

How to map

The configuration, as seen through **Assess/Harden -> Change Reports -> Configuration** for CAS Instances and CAS Instance Config will display the list of server IPs.

CAS Instances

Aliases: **OFF** DB_Type: **LIKE %**
Host_Name: **LIKE %** INSTANCE: **LIKE %**
OS_Type: **LIKE %**

Host Name	Template Content	OS Type	DB Type	Instance Name
192.168.2.248	/dev/async	UNX	N_A	System (192.168.2.248)
192.168.2.248	/etc/passwd.*	UNX	N_A	System (192.168.2.248)
192.168.2.248	$SCRIPTS/.+	UNX	N_A	System (192.168.2.248)
192.168.2.135	/dev/async	UNX	N_A	System (192.168.2.135)
192.168.2.135	/etc/passwd.*	UNX	N_A	System (192.168.2.135)
192.168.2.135	$SCRIPTS/.+	UNX	N_A	System (192.168.2.135)
192.168.2.64	%SCRIPTS_DIR_PTN%/.+	WIN	N_A	System (192.168.2.64)
192.168.7.107	%SCRIPTS_DIR_PTN%/.+	WIN	N_A	System (192.168.7.107)

Records 1 to 8 of 8

CAS Instance Config

Aliases: **OFF** Host_Name: **LIKE %**
OS_Type: **LIKE %**

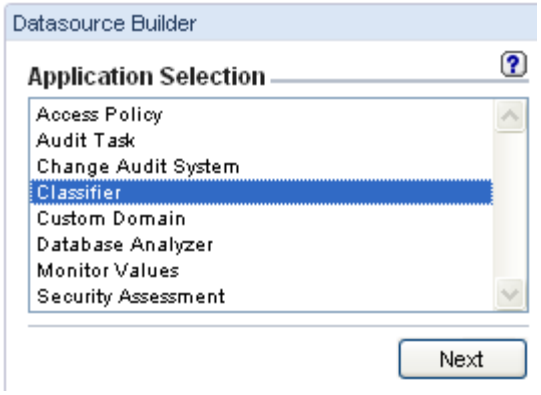
Host Name	Template Content	OS Type	DB Type	Instance	Status	Last Status Change
192.168.2.248	/dev/async	UNX	N_A	System (192.168.2.248)	Enabled	2010-08-18 11:09:29.0
192.168.2.248	/etc/passwd	UNX	N_A	System (192.168.2.248)	Enabled	2010-08-18 11:09:29.0
192.168.2.248	/var/tmp/gregcas/scripts/netezza_log_scan.sh	UNX	N_A	System (192.168.2.248)	Enabled	2010-08-18 11:09:29.0
192.168.2.248	/var/tmp/gregcas/scripts/mysql_datadir_owner.sh	UNX	N_A	System (192.168.2.248)	Enabled	2010-08-18 11:09:29.0
192.168.2.248	/var/tmp/gregcas/scripts/sybase_logfile_scan.sh	UNX	N_A	System (192.168.2.248)	Enabled	2010-08-18 11:09:29.0
192.168.2.248	/var/tmp/gregcas/scripts/oracle_logfile_scan.sh	UNX	N_A	System (192.168.2.248)	Enabled	2010-08-18 11:09:29.0
192.168.2.248	/var/tmp/gregcas/scripts/sybase_sysdevice_type_test.sh	UNX	N_A	System (192.168.2.248)	Enabled	2010-08-18 11:09:29.0
192.168.2.248	/var/tmp/gregcas/scripts/mysql_logfile_scan.sh	UNX	N_A	System (192.168.2.248)	Enabled	2010-08-18 11:09:29.0
192.168.2.248	/var/tmp/gregcas/scripts/db2_spm_log_path_group_test.sh	UNX	N_A	System (192.168.2.248)	Enabled	2010-08-18 11:09:29.0
192.168.2.248	/var/tmp/gregcas/scripts/db2_get_db_cfg.sh	UNX	N_A	System (192.168.2.248)	Enabled	2010-08-18 11:09:29.0
192.168.2.248	/var/tmp/gregcas/scripts/informix_logfile_scan.sh	UNX	N_A	System (192.168.2.248)	Enabled	2010-08-18 11:09:29.0
192.168.2.248	/var/tmp/gregcas/scripts/db2_logfile_scan.sh	UNX	N_A	System (192.168.2.248)	Enabled	2010-08-18 11:09:29.0
192.168.2.248	/var/tmp/gregcas/scripts/teradata_put_web.sh	UNX	N_A	System (192.168.2.248)	Enabled	2010-08-18 11:09:29.0
192.168.2.248	/var/tmp/gregcas/scripts/informix_onstat.sh	UNX	N_A	System (192.168.2.248)	Enabled	2010-08-18 11:09:29.0
192.168.2.248	/var/tmp/gregcas/scripts/sybase_sysdevice_owner_test.sh	UNX	N_A	System (192.168.2.248)	Enabled	2010-08-18 11:09:29.0
192.168.2.248	/var/tmp/gregcas/scripts/postgresql_conf.sh	UNX	N_A	System (192.168.2.248)	Enabled	2010-08-18 11:09:30.0
192.168.2.248	/var/tmp/gregcas/scripts/informix_rootpath_owner.sh	UNX	N_A	System (192.168.2.248)	Enabled	2010-08-18 11:09:29.0
192.168.2.248	/var/tmp/gregcas/scripts/netezza_conf.sh	UNX	N_A	System (192.168.2.248)	Enabled	2010-08-18 11:09:29.0
192.168.2.248	/var/tmp/gregcas/scripts/oracle_spoolmain_exists.sh	UNX	N_A	System (192.168.2.248)	Enabled	2010-08-18 11:09:29.0
192.168.2.248	/var/tmp/gregcas/scripts/sybase_dsync_option_test.sh	UNX	N_A	System (192.168.2.248)	Enabled	2010-08-18 11:09:29.0

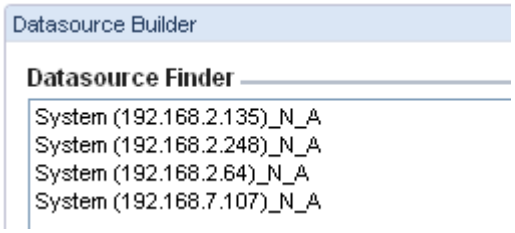
Records 1 to 20 of 73

CC - IBM InfoSphere Guardium - Database and Sensitive Data Finder

How to map

The list of datasources defined under **Tools -> Datasource Definitions -> Classifier (Application Selection)** will provide the database server IPs being used.
(Note: when datasource presents just the hostname, you'd need to click the 'Modify' button to see its IP address for)





CC - IBM InfoSphere Guardium - Advanced Compliance Workflow Automation

How to map

IBM InfoSphere Guardium provides the ability, through **Compliance Workflow Automation**, to streamline the compliance workflow process by consolidating the database activity that is uploaded to the appliance from the customer's environment. Thus, this is the same as defined for the IBM InfoSphere Guardium Database Activity Monitor group, see above.

CC - IBM InfoSphere Guardium - Entitlement Reports

How to map

The list of datasources that entitlement reviews have been run can be seen through **View -> DB Entitlements -> (Select database).**

PID 5726-A86 - IBM InfoSphere Guardium - Central Manager and Aggregator

CC- IBM InfoSphere Guardium - Central Manager and Aggregator

How to map

This is the same as defined for the IBM InfoSphere Guardium Database Activity Monitor group, see above.

PID 5725-A87 - IBM InfoSphere Guardium Database Vulnerability Assessment Solution

CC- IBM InfoSphere Guardium Database Vulnerability Assessment Solution

How to map

This is the same as IBM InfoSphere Guardium – Database Vulnerability Assessment, see above.

PID 5725-A89 - IBM InfoSphere Guardium - Software Appliance

- CC- IBM InfoSphere Guardium Database Activity Monitor with Privileged User Auditing - Virtual Machine Image
- CC- IBM InfoSphere Guardium Database Activity Monitor with Sensitive Objects Auditing - Virtual Machine Image
- CC- IBM InfoSphere Guardium Database Activity Monitor with Comprehensive Auditing - Virtual Machine Image

How to map

This is the same as defined for the IBM InfoSphere Guardium Database Activity Monitor group, see above.

PID 5725-A90 - IBM InfoSphere Guardium - Central Manager and Aggregator - Software Appliance

CC- IBM InfoSphere Guardium - Central Manager and Aggregator - Virtual Machine Image

How to map

This is the same as defined for the IBM InfoSphere Guardium Database Activity Monitor group, see above.

PID 5725-A91 - IBM InfoSphere Guardium Vulnerability Assessment Solution - Software Appliance

CC- IBM InfoSphere Guardium Vulnerability Assessment Solution - Virtual Machine Image

How to map

This is the same as IBM InfoSphere Guardium – Database Vulnerability Assessment, see above.

PID 5725-F32 - Processor InfoSphere Guardium Database Activity Value Unit Monitoring Suite Software Appliance

A Guardium Suite bundle contains functions that are identical to itemized offerings. See the individual offering above for instructions on how to determine the Server IP list.

- IBM InfoSphere Guardium Database Activity Monitor - Sensitive Objects Auditing
- IBM InfoSphere Guardium Central Manager and Aggregator
- IBM InfoSphere Guardium Application End User Identifier
- IBM InfoSphere Guardium Database and Sensitive Data Finder
- IBM InfoSphere Guardium Data Level Access Control
- IBM InfoSphere Guardium Enterprise Integrator
- IBM InfoSphere Guardium Configuration Audit System for Database Servers
- IBM InfoSphere Guardium Entitlement Reports
- IBM InfoSphere Guardium Advanced Compliance Workflow Automation
- IBM InfoSphere Guardium Database Vulnerability Assessment
- IBM InfoSphere Guardium Database Protection Knowledgebase

PID 5725-F33 - Processor InfoSphere Guardium Database Activity Value Unit Monitoring Suite Hardware Appliance

A Guardium Suite bundle contains functions that are identical to itemized offerings. See the individual offering above for instructions on how to determine the Server IP list.

- IBM InfoSphere Guardium Database Activity Monitor - Sensitive Objects Auditing
- IBM InfoSphere Guardium Central Manager and Aggregator
- IBM InfoSphere Guardium Application End User Identifier
- IBM InfoSphere Guardium Database and Sensitive Data Finder
- IBM InfoSphere Guardium Data Level Access Control
- IBM InfoSphere Guardium Enterprise Integrator
- IBM InfoSphere Guardium Configuration Audit System for Database Servers
- IBM InfoSphere Guardium Entitlement Reports
- IBM InfoSphere Guardium Advanced Compliance Workflow Automation
- IBM InfoSphere Guardium Database Vulnerability Assessment
- IBM InfoSphere Guardium Database Protection Knowledgebase

PID 5725-F34 - Application InfoSphere Guardium Database Vulnerability Instance Assessment Suite Software Appliance

A Guardium Suite bundle contains functions that are identical to itemized offerings. See the individual offering above for instructions on how to determine the Server IP list.

- IBM InfoSphere Guardium Database Activity Monitor - Sensitive Objects Auditing
- IBM InfoSphere Guardium Central Manager and Aggregator
- IBM InfoSphere Guardium Application End User Identifier
- IBM InfoSphere Guardium Data Level Access Control
- IBM InfoSphere Guardium Enterprise Integrator
- IBM InfoSphere Guardium Advanced Compliance Workflow Automation
- IBM InfoSphere Guardium Database and Sensitive Data Finder
- IBM InfoSphere Guardium Configuration Audit System for Database Servers
- IBM InfoSphere Guardium Entitlement Reports
- IBM InfoSphere Guardium Database Vulnerability Assessment
- IBM InfoSphere Guardium Database Protection Knowledgebase