IBM® Information Management Software

Getting Started with IBM InfoSphere Optim Workload Replay for DB2

- Describes planning, installation, configuration, and usage details
- Covers UNIX, Linux, Windows, and z/OS platforms
- Introduces tools integration

Whei-Jen Chen
Nisanti Mohanraj
Hassi Norlen
Leif Pedersen
Patrick Titzler
Tom Toomire
John Vonau

Redbooks

ibm.com/redbooks

International Technical Support Organization

Getting Started with IBM InfoSphere Optim Workload Replay for DB2

January 2015

SG24-8221-00

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

First Edition (January 2015)

This edition applies to IBM InfoSphere Optim Workload Replay for DB2 for z/OS Version 2.1 and IBM InfoSphere Optim Workload Replay for DB2 for UNIX, Linux, and Windows Version 2.1.0.1.

Contents

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.

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.

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.

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.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX®	IBM®	pureScale®
DB2®	Informix®	RACF®
developerWorks®	InfoSphere®	Redbooks®
DRDA®	Insight™	Redbooks (logo) ®
FlashCopy®	MVS™	S-TAP®
Global Business Services®	Optim™	z/OS®
Guardium®	Passport Advantage®	

The following terms are trademarks of other companies:

Netezza, and N logo are trademarks or registered trademarks of IBM International Group B.V., an IBM Company.

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

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

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

THIS PAGE INTENTIONALLY LEFT BLANK

Preface

This IBM® Redbooks® publication will help you install, configure, and use IBM InfoSphere® Optim™ Workload Replay (InfoSphere Workload Replay), a web-based tool that lets you capture real production SQL workload data and then replay the workload data in a pre-production environment. With InfoSphere Workload Replay, you can set up and run realistic tests for enterprise database changes without the need to create a complex client and application infrastructure to mimic your production environment.

The publication goes through the steps to install and configure the InfoSphere Workload Replay appliance and related database components for IBM DB2® for Linux, UNIX, and Windows and for IBM DB2 for z/OS®. The capture, replay, and reporting process, including user ID and roles management, is described in detail to quickly get you up and running.

Ongoing operations, such as appliance health monitoring, starting and stopping the product, and backup and restore in your day-to-day management of the product, extensive troubleshooting information, and information about how to integrate InfoSphere Workload Replay with other InfoSphere products are covered in separate chapters.

Authors

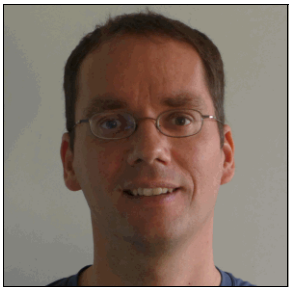
This book was produced by a team of specialists from around the world working at the International Technical Support Organization, San Jose Center.

Whei-Jen Chen is a Project Leader at the International Technical Support Organization, San Jose Center. She has extensive experience in application development, database design and modeling, and IBM DB2 system administration. Whei-Jen is an IBM Certified Solutions Expert in database administration and application development, and an IBM Certified IT Specialist.

Nisanti Mohanraj is an Advisory Software Engineer based at the IBM Silicon Valley Lab in San Jose, California. She has been a member of the InfoSphere Workload Replay development team since 2011. Before that, she was part of DB2 for z/OS Development. Nisanti holds a Master degree in Computer Science from the University of Virginia. She also co-authored the IBM Redbooks publication, *DB2 9 for z/OS: Distributed Functions,* SG24-6952-01.

Hassi Norlen is an Advisory Engineer in Information Development. He started his career at IBM a dozen years ago in the Enterprise Content Manager (ECM) field. Then, he moved to database management and monitoring software solutions. His areas of expertise are up and running documentation and user interface development with the progressive disclosure methodology. Hassi holds degrees in physics and science journalism and works out of the IBM Washington, DC, office.

Leif Pedersen is a Solution Architect working for the Optim Enablement Team at the Silicon Valley Laboratory in San Jose, California. Leif worked with database technology for more than 25 years. One of his main areas of expertise is DB2 for z/OS performance and Query optimization. Leif also worked with distributed database landscape. Today, Leif helps clients and local IBM employees with Optim products, such as Query Workload Tuner, pure Query, Optim Performance Manager, Optim Configuration Manager, and Optim Query Capture Replay. Leif co-authored many IBM Redbooks publications and articles.



Patrick Titzler is a Solution Architect in the Information Management organization, currently supporting customers in their InfoSphere Optim Workload Replay evaluation and deployment efforts. He is a frequent contributor to articles and tutorials. He developed videos, e-Learning, and other training material for several products throughout his technical career at IBM.

Patrick holds a Master degree in Computer Science from the University of Rostock, Germany.

Tom Toomire is a Senior Software Engineer, who works at the Silicon Valley Laboratory in San Jose, California. Tom has over 25 years of experience at IBM, working in DB2 database technology. Tom has extensive experience in various areas within the DB2 for z/OS product, including DB2 stored procedures, Open Database Connectivity (ODBC)/command-line interface (CLI) driver, DB2 local attach facilities, group attach facility, subsystem services, storage manager, and all of the different implementations of the IBM DB2 Java Database Connectivity (JDBC) drivers for z/OS. Tom is a co-inventor on two patents. Tom is the architect for the InfoSphere Optim Workload Replay for z/OS product.

John Vonau is a Senior Software Engineer at IBM with over 17 years of software development experience. He is the architect for InfoSphere Optim Workload Replay for Linux, UNIX, and Windows. Before this role, John worked on the design and development of various other IBM products, including OPM Extended Insight™, DB2 CLI, and the IBM DB2 JDBC Universal Driver.

Acknowledgment

Thanks to the following people for their contributions to this project:

Sherry Guo
Carlene Nakagawa

Shu Wang
IBM Software Group

Richard M Conway
Robert (Bob) Haimowitz
IBM Global Business Services®

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks

- Send your comments in an email to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:

  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

1

Overview

In this chapter, we introduce IBM InfoSphere Optim Workload Replay (InfoSphere Workload Replay), a powerful analysis tool for IT departments in today's fast changing enterprise data environment.

We describe the workload capture and replay process and lay out the use cases for how this web-based product allows Database Administrators (DBAs), quality assurance, and performance teams test and validate changes to the database production environments with realistic, even actual, captured workload data before they roll out the changes in production. We also present the product architecture and deployment options.

Finally, we outline the user roles and accompanying responsibilities that can be used within your organization to successfully roll out InfoSphere Workload Replay in your production and test environments.

1.1 Introduction

Production data server environments are a critical component in most enterprises. The production data server environment must meet the availability and performance goals set by the business to avoid any significant impact to internal and external customers. Any change to the data server environment, irrespective of whether it is minor or major and occurs infrequently or frequently, can affect the behavior of critical applications (or to be more specific, SQL workloads), as shown in Figure 1-1.

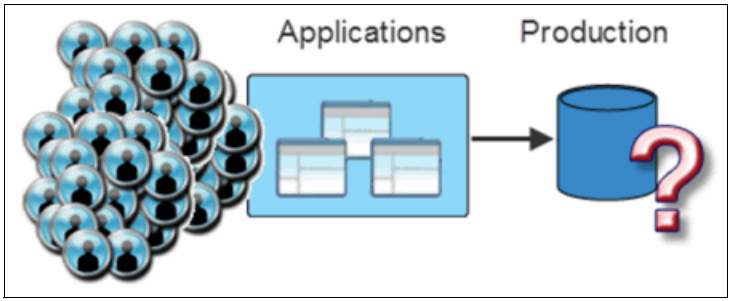


Figure 1-1 Changes can affect application behavior

Traditional testing approaches require the setup of the data server environment, application infrastructure, and test processes that can mimic realistic production workload characteristics to analyze the impact of changes in a pre-production environment before the change is implemented in production as shown in Figure 1-2.

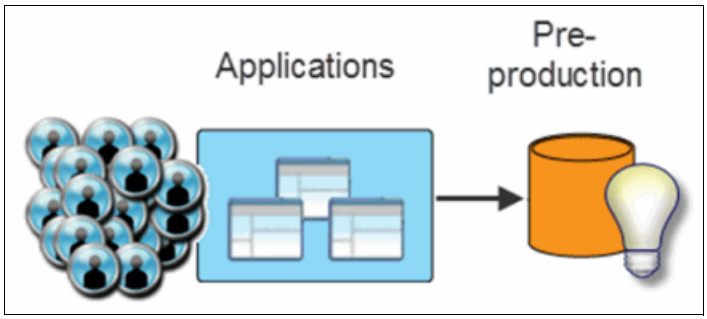


Figure 1-2 Change impact is analyzed before change is implemented

There are two potential challenges to these approaches when it comes to full-scale data layer testing:

- Test environments that closely approximate the production application infrastructure are a prized resource that is typically heavily used. This approach reduces their availability for certain types of projects and requires coordination and prioritization. Subjectively, lower priority data layer test efforts might therefore not be able to take full advantage of the infrastructure to perform the thorough analysis needed.
- Having access to an application infrastructure is not sufficient to analyze the potential impact of changes. Actual workloads that drive the infrastructure are the key to successful testing if they can sufficiently approximate production conditions. While it is relatively easy to create certain types of workloads, such as workloads that drive batch applications, other types of workloads are difficult and time-consuming to build using synthetic tests.

InfoSphere Workload Replay addresses those challenges by providing the means to capture SQL activity in production environments and to replay the captured activity in pre-production environments, without the need for the original application infrastructure, as shown in Figure 1-3.

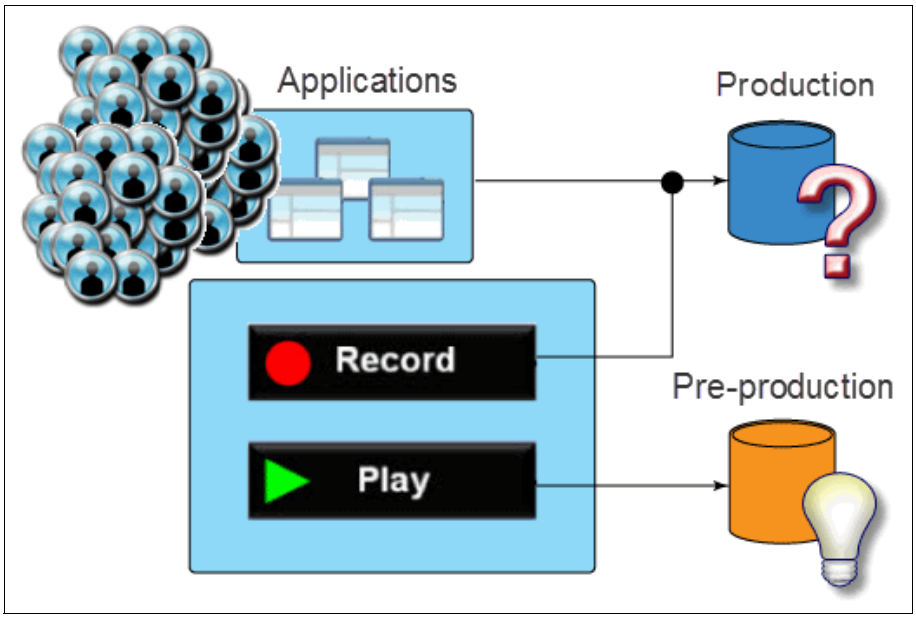


Figure 1-3 Capture and replay in pre-production

Typical use case scenarios, in which InfoSphere Workload Replay can be used, are listed:

- Database testing

  Any type of change on the database server side, whether it is hardware, software, configuration, or data related is ideally evaluated using existing SQL workloads that match production behavior. InfoSphere Workload Replay drives these kinds of tests:

  - Workload tuning
  - Database tuning
  - Database configuration changes
  - Database migration or upgrades
  - Software maintenance

- Performance testing and stress testing

  Database performance tests are typically part of capacity planning and quality of service (QoS) validation. To support these tests, InfoSphere Workload Replay provides the capability to replay SQL as is or vary the replay speed, so that you can increase (or reduce, as needed) the originally observed SQL throughput, for example:

  - Verify that an existing environment can handle workloads with higher throughputs.
  - Analyze whether a new environment can handle existing workloads under new concurrent peak conditions.
  - Verify that existing standby database server environments can handle the most recent workload characteristics.
  - Investigate how additional hardware resources (for example, in a DB2 for z/OS sysplex environment) improve workload performance.

- New database feature adoption

  Over time, IBM and other database vendors release new features that strive to improve the performance of your workloads. InfoSphere Workload Replay is well suited to evaluate the impact of these features as long as they do not require any changes on the application side, such as SQL changes:

  - DB2 with BLU Acceleration (for Linux, UNIX, and Windows)
  - DB2 Analytics Accelerator for z/OS
  - Improved access plan due to database engine improvements

- New application testing

  By its nature, this testing is performed for applications that are not yet running in production. Therefore, no workload comparison can be performed. InfoSphere Workload Replay provides value in this scenario though because it can be used to analyze the impact that a new application might have on the behavior of existing applications that are currently running in production, for example, the performance and availability impact due to a potential SQL execution contingency on the database server.

There are other test scenarios, such as application layer testing, that will not benefit from InfoSphere Workload Replay. Code changes that might be introduced in an application to deliver new functionality, optimize code, or resolve product deficiencies must be validated by using different means that are not within the scope of the product.

1.2 Solution and architecture

The solution is also referred to as the *capture and replay workflow*.

1.2.1 Solution overview

The solution, which is not use case specific, consists of two stages:

- Stage 1: Establish a baseline workload
- Stage 2: Analyze how changes affect workload execution behavior

In stage one, which is depicted in Figure 1-4, you capture a representative workload in the production environment, prepare it for replay, and replay it on a cloned copy of the database production environment.

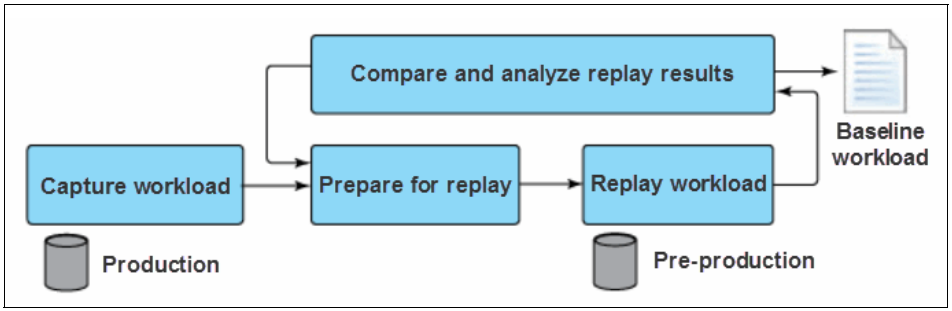


Figure 1-4 Establish a workload baseline in the pre-production environment

You use accuracy and performance reports to compare and analyze the captured workload's execution behavior with the replayed workload's execution behavior.

Accuracy reports, as shown in Figure 1-5, identify SQL statements that yielded different results during the two workload executions that you are comparing.

SQL Replay Comparison Metric	Unique	Executions	Percentage
Baseline SQL	56	8,277,947	
Matched SQL replays	50	8,270,435	99.91%
Unmatched SQL replays	6	1,520	0.02%
Different return code	5	922	0.01%
Different number of rows returned	1	598	0.01%
Different number of rows updated	3	900	0.01%

Figure 1-5 Not all SQL statements replayed with the same results in this DB2 example

Performance reports, as depicted in Figure 1-6, highlight SQL performance differences between the two workload executions, so that you can quickly identify relevant regressions or improvements. Drill-through reports provide details needed to identify SQL of interest.

Metric	Value	Percentage
Response time difference	-01:47:40.718775	37.14%
Total improvement	01:58:34.374881	40.90%
Total regression	00:10:53.656106	-3.76%
SQL statements >= 5% improvement	25 / 50	50.00%
SQL statements >= 5% regression	22 / 50	44.00%
Transactions >= 5% improvement	49 / 208	23.56%
Transactions >= 5% regression	120 / 208	57.69%

Figure 1-6 Significant differences detected between two workload executions

If the reports identify anomalies, you change the replay environment to address any relevant differences and repeat the iterative process until the replay behavior of the workload sufficiently approximates the production environment behavior.

The result of stage 1 is a workload baseline that you can use to analyze how changes in the replay database environment affect the workload's execution behavior.

In stage 2, shown in Figure 1-7, you implement the planned production change in your test environment, replay the workload, and compare and analyze if and how the workload execution behavior changed.

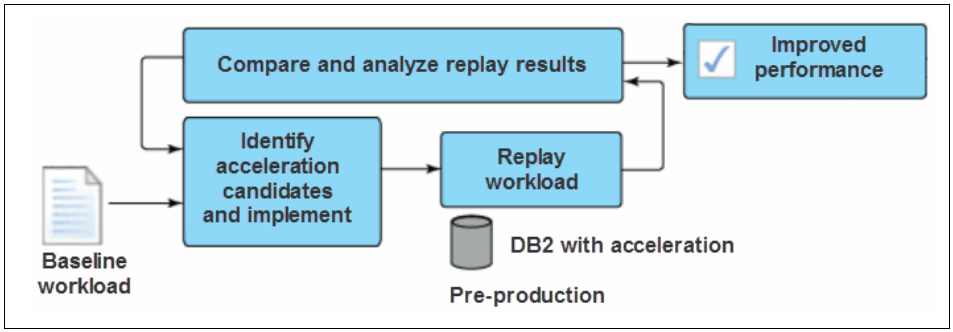


Figure 1-7 Analyze how workload execution behavior is affected by a change

Let us review the solution in the context of an adoption scenario for the DB2 Analytics Accelerator for z/OS or DB2 with BLU Acceleration. In both scenarios, your goal is to evaluate how much performance of an analytical application (for DB2 for z/OS or DB2 for Linux, UNIX, and Windows) will improve. Figure 1-8 and Figure 1-9 on page 8 illustrate stage 1 and stage 2 of the workflow.

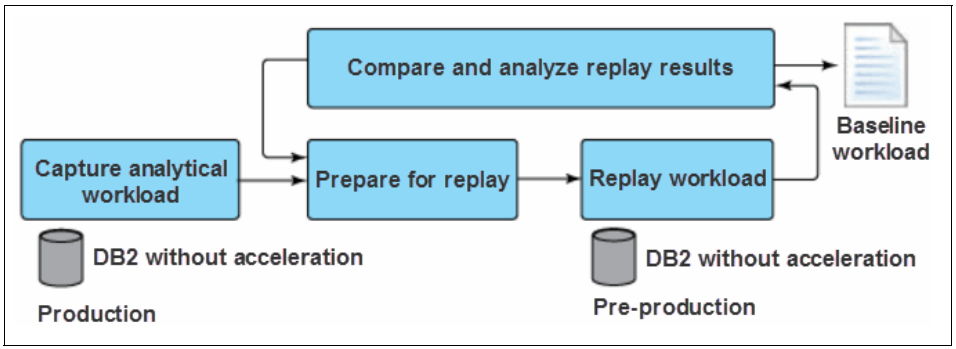


Figure 1-8 Establish a baseline workload in pre-production environment

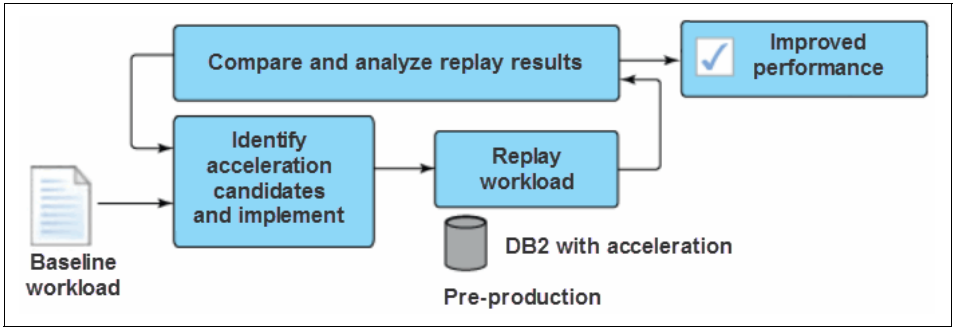


Figure 1-9 Implement acceleration and measure the performance impact

The scenario is described in more detail in the following IBM developerWorks® article:

https://www.ibm.com/developerworks/data/library/techarticle/dm-1405-db2blureplay/

1.2.2 Product architecture

InfoSphere Workload Replay is built on IBM InfoSphere Guardium®, a security solution for heterogeneous databases, such as DB2, IBM Informix®, Oracle, and Microsoft SQL Server. Both solutions have in common that they monitor, analyze, and optionally log information about incoming database traffic.

In this book, we focus on the InfoSphere Workload Replay solution for DB2 for Linux, UNIX, and Windows and DB2 for z/OS. Some of the concepts described in the following chapters do not apply to the heterogeneous solution, which supports capturing, processing, and replaying workloads on IBM Informix, Microsoft SQL Server, MySQL, Netezza® Data Warehouse, Oracle, PostgreSQL, Sybase Adaptive Server, and Teradata.

Conceptual architecture overview

Figure 1-10 on page 9 depicts the conceptual InfoSphere Workload Replay architecture, which consists of three components: multiple S-TAPs, a Workload Replay server, and remote user and administration interfaces.

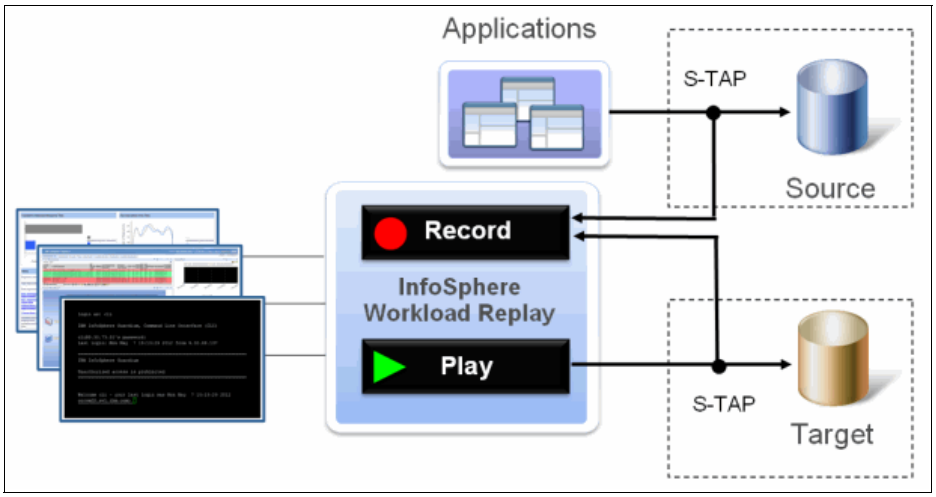


Figure 1-10 Conceptual InfoSphere Workload Replay architecture

IBM S-TAP® is a lightweight software component that is installed on each database server machine on which SQL is captured or replayed. On DB2 for Linux, UNIX, and Windows, it continuously monitors traffic and streams the traffic to its assigned Workload Replay server for processing.

Note: In z/OS environments, an additional controller component automatically starts and stops S-TAP as needed, restricting when monitored traffic is streamed to the associated Workload Replay server.

A Workload Replay server is a hardened physical or virtual appliance, running InfoSphere Guardium and InfoSphere Workload Replay software. The Workload Replay server receives traffic that is streamed by its associated S-TAPs and stores (“captures”) and processes the relevant information as needed.

Workload Replay servers are accessed using three secured interfaces, as shown in Figure 1-11 on page 10:

- The *Workload Replay web console* is used to manage workloads.
- The *Guardium web console* and the *Guardium command-line interface (CLI) interface* are Workload Replay server administration interfaces.

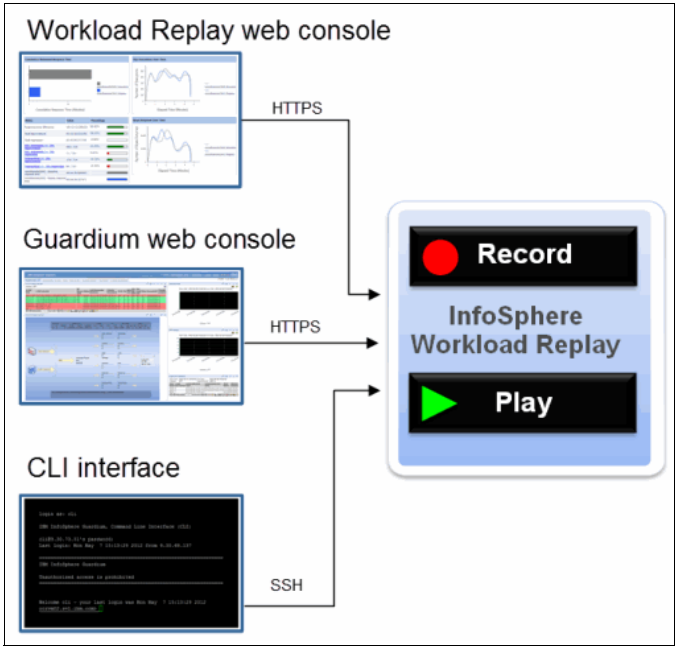


Figure 1-11 Secured remote interfaces provide access to a Workload Replay server

Access to the interfaces is restricted to certain Workload Replay roles, which we describe in 1.2.3, “Roles and responsibilities” on page 13.

Single-server architecture

In a single-server architecture, one Workload Replay server is used to capture and replay workloads. This architecture, as depicted in Figure 1-12 on page 11, is suitable for environments in which source and target data servers reside in the same local network. This deployment can handle small to medium-sized workloads.

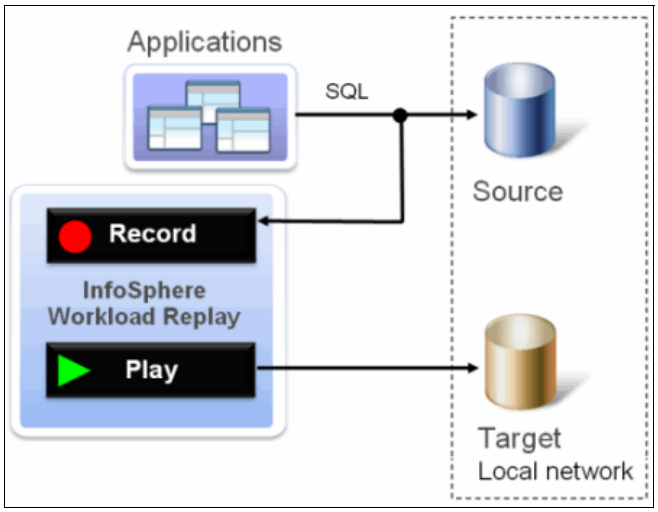


Figure 1-12 A single server captures and replays workloads on multiple database servers

We suggest co-locating the Workload Replay server on the database server's network to reduce network latency and minimize impact on other networks.

Multi-server architecture

Multiple Workload Replay servers can be configured to share capture and replay responsibility. This architecture, as shown in Figure 1-13, can handle large workloads.

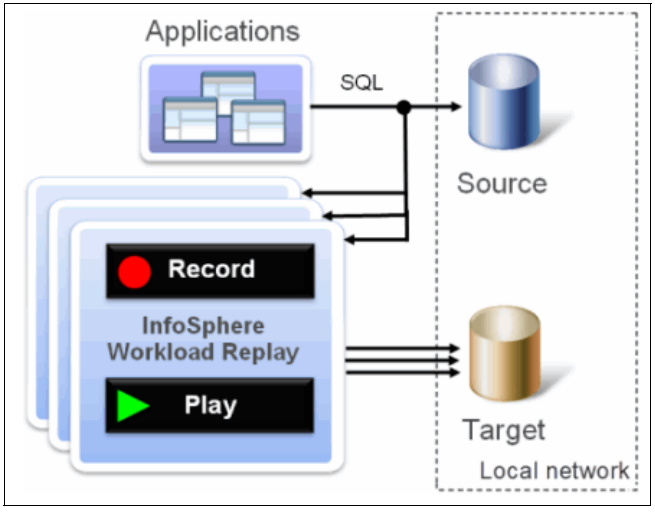


Figure 1-13 Multiple servers capture and replay workloads together

We suggest co-locating all Workload Replay servers in the database server's local network to reduce network latency and minimize impact on other networks.

Decentralized deployments

In a decentralized deployment, as shown in Figure 1-14, a single-server or multi-server installation is dedicated to capturing workloads in the source environment, and one single-server or multi-server installation is dedicated to replaying workloads in the target environment.

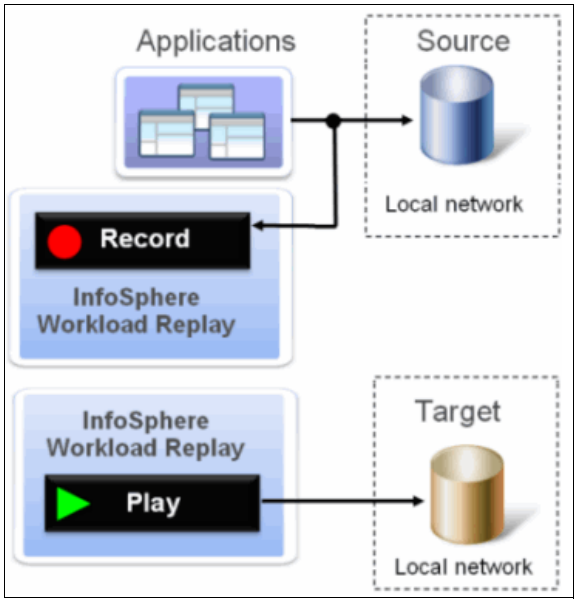


Figure 1-14 Decentralized deployments are used in isolated environments

This deployment architecture must be used if the source environment is network-isolated from the target environment or if the environments are only connected by a wide area network (WAN), which might be the case if the database servers are in different data centers.

Note: You can mix or match single-server and multi-server configurations in decentralized installations.

1.2.3 Roles and responsibilities

Three types of user groups participate in a Workload Replay deployment:

- Administrative users install, configure, and maintain the Workload Replay infrastructure.
- Workload Replay users manage the Workload Replay workflow.
- Application owners and database administrators support Workload Replay users in their efforts to capture, process, and replay workloads in the source and target database environments.

A person can have one or more of the Workload Replay roles, as governed by business restrictions.

Administrator

An administrator installs, configures, and manages Workload Replay appliances and collaborates with database server administrators during S-TAP installation, configuration, and maintenance.

Administrative activities, such as patch installation and S-TAP configuration, are performed using the CLI and the Guardium web console. An administrator cannot capture, process, or replay workloads.

The administrator collaborates closely with network, IT infrastructure, and database server administrators during product deployment.

Security administrator

The security administrator manages user access to the Workload Replay appliances, enforcing separation of duties as needed.

Access control is managed by using the Guardium web console. A security administrator cannot capture, process, or replay workloads.

Privileged users

A privileged user manages workloads and workload access by using the Workload Replay web console. Maintenance activities are performed using the Guardium web interface and CLI. A privileged user typically also performs the tasks of a regular user.

Users

A non-privileged user can capture, process, and replay workloads by using the Workload Replay web console, as governed by the privileges that were granted by a privileged user. Users collaborate closely with application owners and database owners throughout the workload replay lifecycle.

In Chapter 2, “Deployment planning” on page 17, we describe in more detail how these roles utilize the user interfaces.

1.3 About this book

The first chapters in this book guide you through a first-time deployment of InfoSphere Workload Replay for DB2 for z/OS and DB2 for Linux, UNIX, and Windows environments:

- Chapter 2, “Deployment planning” on page 17 introduces the deployment process, covers planning, and outlines the deployment activities.
- Chapter 3, “Installing and configuring IBM InfoSphere Optim Workload Replay appliances” on page 41 describes how to install and configure Workload Replay appliances. This chapter is of interest to administrators who deploy and maintain InfoSphere Workload Replay for DB2 for z/OS or InfoSphere Workload Replay for DB2 for Linux, UNIX, and Windows.
- Chapter 4, “IBM InfoSphere Optim Workload Replay for DB2 for z/OS installation and configuration” on page 77 describes how to install and configure the InfoSphere Workload Replay database server components in your DB2 for z/OS environment. This chapter is of primary interest to administrators who install and maintain InfoSphere Workload Replay for DB2 for z/OS.
- Chapter 5, “DB2 for Linux, UNIX, and Windows S-TAP installation and configuration” on page 111 details the installation and configuration of the InfoSphere Workload Replay database server components in your DB2 for Linux, UNIX, and Windows environment. This chapter is of primary interest to administrators who install and maintain InfoSphere Workload Replay for DB2 for Linux, UNIX, and Windows.

The remaining chapters cover typical activities that administrators, privileged users, or users complete after InfoSphere Workload Replay is deployed:

- Chapter 6, “Capturing and replaying workloads” on page 153 guides you through the Workload Replay workflow using step-by-step instructions. This chapter was written for users who use the product to analyze how changes affect workload execution behavior.

- Chapter 7, “Ongoing operations” on page 213 describes how to maintain an InfoSphere Workload Replay deployment. This chapter is for administrators and privileged users.
- Chapter 8, “Integration with other tools” on page 269 illustrates how other IBM products can be used to support the Workload Replay workflow.
- Chapter 9, “Troubleshooting” on page 281 provides hints and tips for common troubleshooting scenarios. This chapter is of primary interest to administrators and privileged users.

1.3.1 Recommended reading

The following IBM Redbooks publications describe three common InfoSphere Workload Replay use case scenarios in detail:

- *Architecting and Deploying DB2 with BLU Acceleration, SG24-8212*

  http://www.redbooks.ibm.com/abstracts/sg248212.html
- *Optimizing DB2 Queries with IBM DB2 Analytics Accelerator for z/OS*, SG24-8005

  http://www.redbooks.ibm.com/abstracts/sg248005.html?Open
- *Performance Management: Using IBM InfoSphere Optim Performance Manager and Query Workload Tuner*, SG24-8111

  http://www.redbooks.ibm.com/abstracts/sg248111.html?Open

We also recommend the following Redbooks publication for more information about InfoSphere Guardium deployments:

- *Deployment Guide for InfoSphere Guardium, SG24-8129*

  http://www.redbooks.ibm.com/abstracts/sg248129.html

2

Deployment planning

Deployment of IBM InfoSphere Optim Workload Replay (InfoSphere Workload Replay) consists of four major stages. During the first stage, the deployment is planned. During the second stage, the Workload Replay appliances are installed and configured. In the third stage, the database server components are installed and configured in the source and target DB2 for z/OS or DB2 for Linux, UNIX, and Windows environments. The final deployment stages focus on product verification and product adoption.

InfoSphere Workload Replay deployment planning includes the following activities:

- Analyze deployment requirements and identify a suitable deployment topology.
- Plan appliance deployments.
- Plan data server components deployments.
- Plan product validation.
- Plan product adoption.

This chapter describes the deployment planning activities for a first-time product installation.

2.1 Deployment overview

A deployment plan defines the activities that must be completed to implement a Workload Replay topology that meets the business needs of the stakeholders.

After a deployment plan is defined, the deployment is performed:

- Verify that the deployment environment meets the stated prerequisites.
- Download the installation media.
- Install and configure the Workload Replay appliances.
- Install and configure the database server components.
- Validate the deployment.

Chapter 3, “Installing and configuring IBM InfoSphere Optim Workload Replay appliances” on page 41, Chapter 4, “IBM InfoSphere Optim Workload Replay for DB2 for z/OS installation and configuration” on page 77, and Chapter 5, “DB2 for Linux, UNIX, and Windows S-TAP installation and configuration” on page 111 guide you through the installation and configuration of the Workload Replay appliance and database server components.

To install InfoSphere Workload Replay, you must have access to the media packs for DB2 for z/OS or Linux, UNIX, and Windows that are available for download in electronic form. The order fulfillment process varies by platform.

Obtaining the Workload Replay for DB2 for z/OS installation media

For details about how to access the base installation media and product maintenance, see A.1.1, “Downloading InfoSphere Workload Replay for DB2 for z/OS installation media” on page 302.

Obtaining the Workload Replay for DB2 for Linux, UNIX, and Windows installation media

For details about how to access the base installation media and product maintenance, see A.1.2, “Downloading InfoSphere Workload Replay for DB2 for Linux, UNIX, and Windows installation media” on page 309.

2.2 Analyzing deployment requirements

A Workload Replay deployment provides the infrastructure needed to capture, process, replay, and analyze workloads. The deployment requirements define how the product is implemented in production and pre-production environments.

2.2.1 Analyzing S-TAP deployment requirements

As part of the requirements analysis activities, you identify on which data servers workloads of interest are run in your source environment and in which environment those workloads will be replayed. The result of this analysis is an inventory list that defines where InfoSphere Workload Replay has to monitor database traffic.

Analyzing DB2 for z/OS deployment requirements

The inventory list for the book lab environment for DB2 for z/OS is shown in Figure 2-1:

- Workloads will be captured on a DB2 for z/OS V11.1 two member (D1J1 and D1J2) data sharing group on logical partitions (LPARs) `wtsc61.itso.ibm.com` and `wtsc62.itso.ibm.com`. The location alias for the data sharing group is `DB1J`.
- Workloads will be replayed on a DB2 for z/OS V11.1 two member (D1K1 and D1K2) data sharing group on LPARs `wtsc61.itso.ibm.com` and `wtsc62.itso.ibm.com`. The location alias for the data sharing group is `DB1K`.
- Both z/OS LPARS are on the same local network.

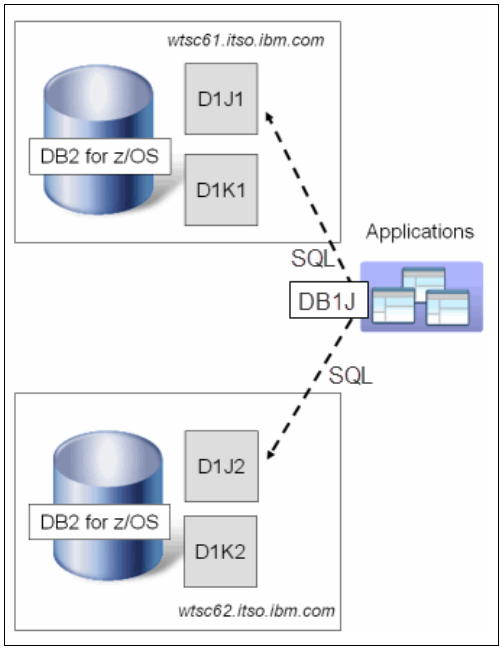


Figure 2-1 DB2 for z/OS book environment layout

Table 2-1 lists the relevant deployment requirements that are used as input to create a data server components deployment plan in 2.4.1, “Planning DB2 for z/OS deployments” on page 28.

Table 2-1 Example: Collecting data server components deployment information for z/OS

Environment	LPARs on which data server components must be installed	DB2 subsystems for which S-TAP must be configured	Location aliases in sysplex environments (members)
Capture environment 1	wtsc61.itso.ibm.com wtsc62.itso.ibm.com	D1J1 D1J2	DB1J (D1J1 and D1J2)
Replay environment 1	wtsc61.itso.ibm.com wtsc62.itso.ibm.com	D1K1 D1K2	DB1K (D1K1 and D1K2)

Analyzing DB2 for Linux, UNIX, and Windows deployment requirements

The following inventory lists are for the book lab environment for DB2 for Linux, UNIX, and Windows, which is depicted in Figure 2-2 on page 21:

- Workloads of interest will be captured on database PRODDB (DB2 10.1 on production instance `pinst1`) on `eagle.itso.ibm.com`, which runs an IBM AIX® V7.1 operating system.
- We replay those workloads on databases TESTDB and TESTDB2 (both on a DB2 10.5 test instance `tinst1`) on `hawk.itso.ibm.com`, which also runs an AIX V7.1 operating system.
- Both database servers are on the same local network.

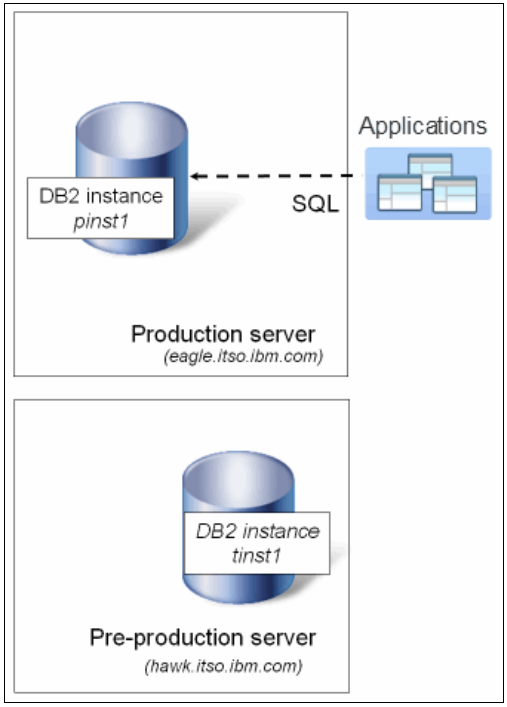


Figure 2-2 DB2 for Linux, UNIX, and Windows book environment layout

Table 2-2 summarizes the relevant information that is used to build the S-TAP deployment plan.

Table 2-2 Example: Collecting S-TAP deployment information for DB2 LUW

Environment	Host on which S-TAP must be installed	Instances that must be configured for monitoring	Databases on which SQL will be captured or replayed
Capture environment 1 (DB2 10.1 production, AIX V7.1)	eagle.itso.ibm.com	pinst1	PRODDB
Replay environment 1 (DB2 10.5 test, AIX V7.1)	hawk.itso.ibm.com	tinst1	TESTDB TESTDB2

2.2.2 Analyzing Workload Replay server requirements

The InfoSphere Workload Replay system requirements[1] provide general hardware and software guidance for initial appliance deployments.

Appliance types

Workload Replay servers can be deployed as physical appliances or virtual appliances. Physical appliances run either on IBM provided System x hardware or your own compatible hardware. You can deploy virtual appliances on supported virtualization software, such as VMware or Red Hat KVM.

Both physical appliances and virtual appliances run a hardened 64-bit Linux Red Hat operating system, which is automatically installed as part of the InfoSphere Workload Replay installation.

Space requirements

A Workload Replay appliance acts as a data sink, storing permanently large amounts of raw information that is collected by S-TAP. This information is used to perform a logical replay of the captured SQL activity and to compare workload execution results to identify similarities and differences.

Note: After a Workload Replay appliance is installed, its maximum disk size cannot be increased, whether it was configured to use local disks or a storage area network (SAN) as the storage provider[a]. If additional storage is required beyond what was initially allocated, the appliance must be rebuilt.

a. Network attached storage (NAS) is not supported.

Appliance location and network requirements

Base the decision where to place Workload Replay appliances within your existing IT infrastructure on the location of the database servers (or subsystems) on which SQL is captured or replayed.

A Workload Replay appliance receives a continuous data stream from its associated S-TAPs while a workload capture or a workload replay is in progress. Large amounts of data might be transferred between the database server and the Workload Replay appliance, depending on database activity. Workload Replay appliances must therefore reside close to the databases (or subsystems) on which SQL is captured or replayed to avoid excessive network impact.

If network bandwidth is insufficient or the network is not performing well, Workload Replay's ability to capture or replay SQL traffic can be adversely

[1] http://www.ibm.com/support/docview.wss?uid=swg27039781

affected. Deploy a decentralized topology if source and target database server environments are not in the same data center or are network isolated.

Growth considerations

The processing capacity of a Workload Replay appliance is primarily limited by the resources that are available to the appliance. You can increase processing capacity by adding additional Workload Replay appliances to your deployment topology. In a multi-server deployment, the main Workload Replay appliance acts as the coordinator and additional servers act as auxiliaries that capture or replay workloads when instructed.

For example, you can start out with a centralized, single-server deployment, consisting of a single Workload Replay appliance that captures and replays SQL workloads. You can expand the deployment to a centralized, multi-server topology, a decentralized, single-server topology, or a decentralized, multi-server topology, as shown in Figure 2-3.

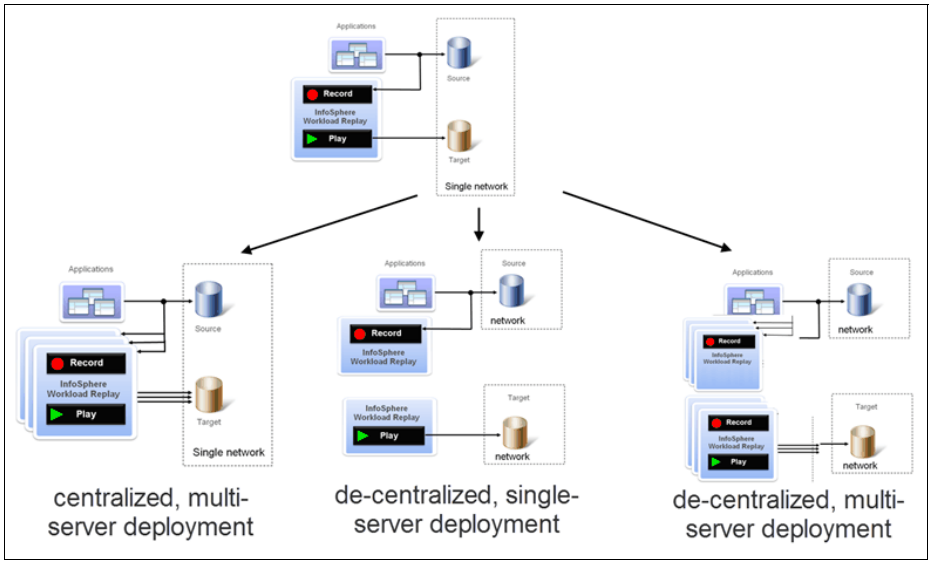


Figure 2-3 Single-server growth options

Concurrency

A Workload Replay appliance can only perform one workload capture or one workload replay at a time. This restriction also applies to multi-server deployments, where multiple Workload Replay appliances share capture or replay responsibility. If you need to perform multiple captures or replays at the same time, you must use multiple single-server or multiple multi-server installations.

The book environment is suited for two centralized deployments (one for LUW and one for z/OS) because the source and target databases (and data sharing groups, respectively) are in the same local network. For illustration, we deploy the Workload Replay appliances in a multi-server configuration, as shown in Figure 2-4.

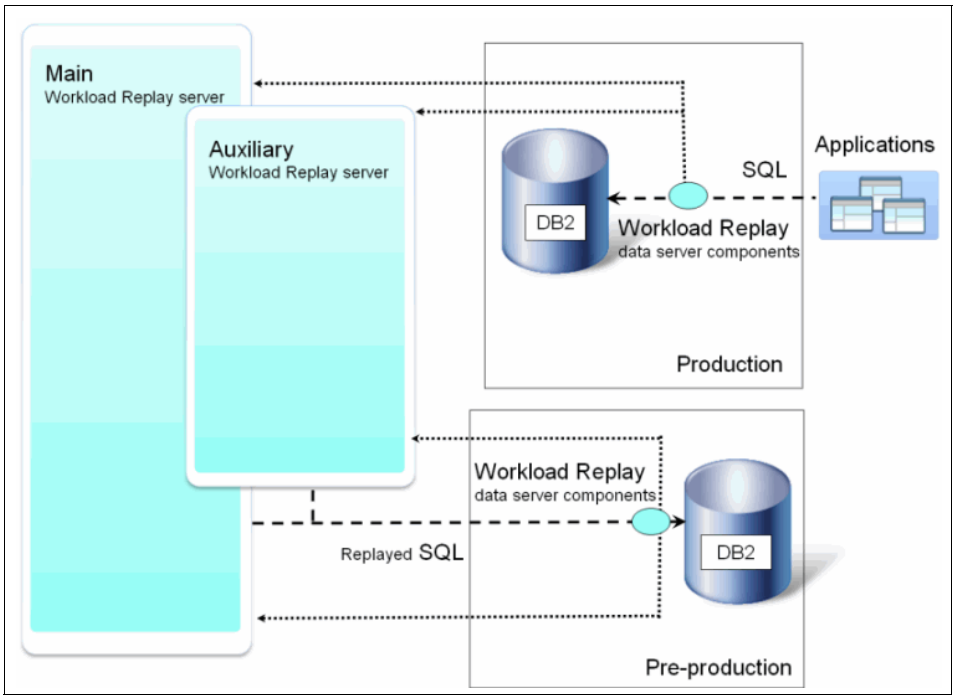


Figure 2-4 Example centralized, multi-server topology used in this book

Note: An appliance can be used to capture and replay workloads on the same DB2 platform only. It is therefore not possible to capture workloads on DB2 for Linux, UNIX, and Windows and replay workloads on DB2 for z/OS.

2.3 Planning appliance deployments

A Workload Replay appliance deployment plan is the output of the requirements analysis described in 2.2.2, “Analyzing Workload Replay server requirements” on page 22.

A Workload Replay appliance deployment consists of the following steps:

1. Rack the physical appliances or build virtual appliances and connect them to the network.
2. Install InfoSphere Guardium and complete the basic appliance configuration.
3. Install and configure the InfoSphere Workload Replay software in Guardium.

Note: No operating system needs to be installed when you rack or build the appliances. The InfoSphere Guardium installation automatically installs a hardened Red Hat Linux operating system.

We suggest installing, configuring, and validating the Workload Replay appliances that are earmarked to operate in the pre-production environment before installing appliances for the production environments.

In multi-server deployments, the main Workload Replay appliances are always installed and configured before the Workload Replay auxiliary appliances. The auxiliary appliances cannot operate independently and therefore require an operational main Workload Replay appliance before they can be validated.

Within a single environment, all appliances are deployed before the data server components are installed and configured on the associated DB2 servers.

Figure 2-5 on page 26 illustrates the example deployment sequence for the book environment, which is identical for both platforms.

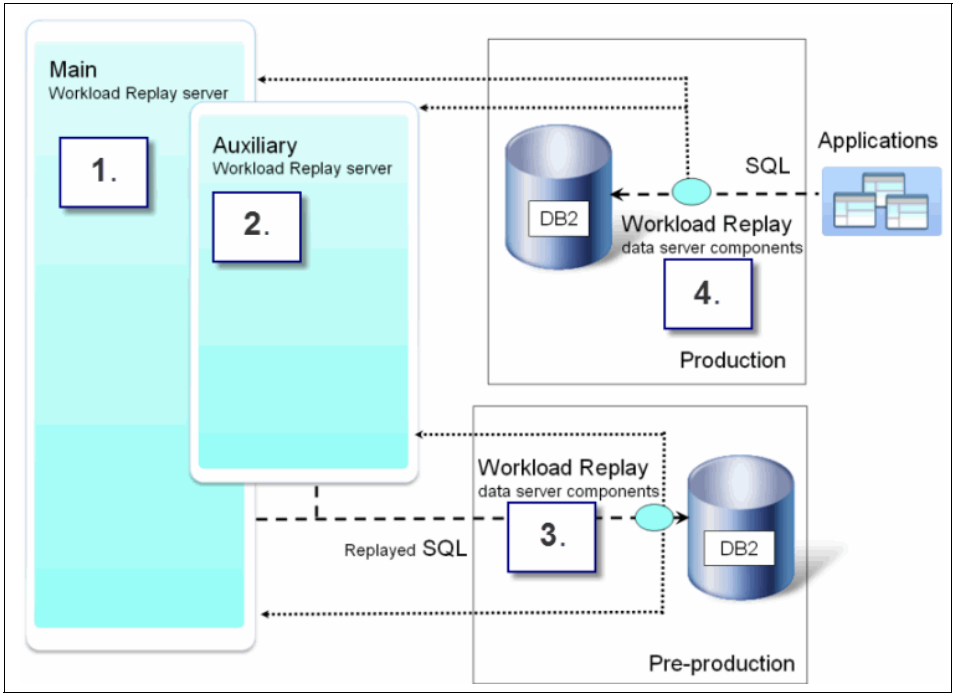


Figure 2-5 Example deployment sequence for a centralized, multi-server topology

2.3.1 Environment information to collect

During the initial configuration of a Workload Replay appliance, you must provide the following information, which you can obtain from your network and system administrator:

- Network settings:
  - IP address of the appliance
  - Host name of the appliance
  - Domain in which the host will reside
  - Subnet mask
  - Gateway or router IP address (or host name) that the appliance uses to communicate with other networks
  - Domain Name Server (DNS) IP addresses (or host names) that the appliance uses to resolve host names

- System settings:
  - Network Time Protocol (NTP) server IP addresses (or host names)
  - Time zone where the appliance is located

For more information, see A.2.1, “Appliance configuration worksheet” on page 315.

2.3.2 Considerations

When you create an appliance for the first time, consider the following information.

Access to the Guardium installation media

Before you start the installation process, ensure that the Guardium installation DVD is inserted (on physical appliances) or the Guardium installation ISO image is mapped (on virtual appliances), and the BIOS is configured to start from external media.

Note: If you downloaded the installation media, you must burn the Guardium installation image on a DVD for physical deployments.

During installation, the appliance is automatically restarted one time. To avoid accidentally restarting the installation process, remove the installation media before the appliance starts again after the operating system installation completes.

Access to the appliance’s console

You must have access to the appliance console during the initial installation and configuration to complete the network setup and allow for remote access by using the secure interfaces.

Open ports

InfoSphere Workload Replay appliances communicate with each other with their associated database server components and are accessed by using remote user interfaces. Review the open port requirements in A.3, “Open port requirements” on page 318 with your network administrator.

Default users

During product installation, a set of default administration users is created on the appliance. These users can then be used to customize the security setup after the appliance is fully configured.

Failover support

InfoSphere Workload Replay appliances do not provide automatic failover support.

2.4 Planning S-TAP deployments

An S-TAP deployment plan is created based on the information that you collected during the deployment requirements analysis. The platform-specific deployment plans are outlined in the DB2 for z/OS and DB2 for Linux, UNIX, and Windows subsections.

Irrespective of the deployment platform, data server components must be always installed, configured, and validated first in pre-production environments and only subsequently installed, configured, and validated in production environments.

2.4.1 Planning DB2 for z/OS deployments

During the requirements analysis, which we performed in “Analyzing DB2 for z/OS deployment requirements” on page 19, we collected the basic information needed to create a deployment plan. Using the following set of rules, we can create a deployment plan for the z/OS data server components:

- A Workload Replay Controller for z/OS must be installed and configured on each LPAR on which SQL traffic is monitored.
- A Workload Replay S-TAP for DB2 for z/OS must be installed and configured for each DB2 subsystem or data sharing group member in sysplex environments on which SQL is captured or replayed.
- Workload capture or replay must be enabled for each subsystem or data sharing group in sysplex environments.

Figure 2-6 on page 29 illustrates the first two rules by using a two LPAR environment.

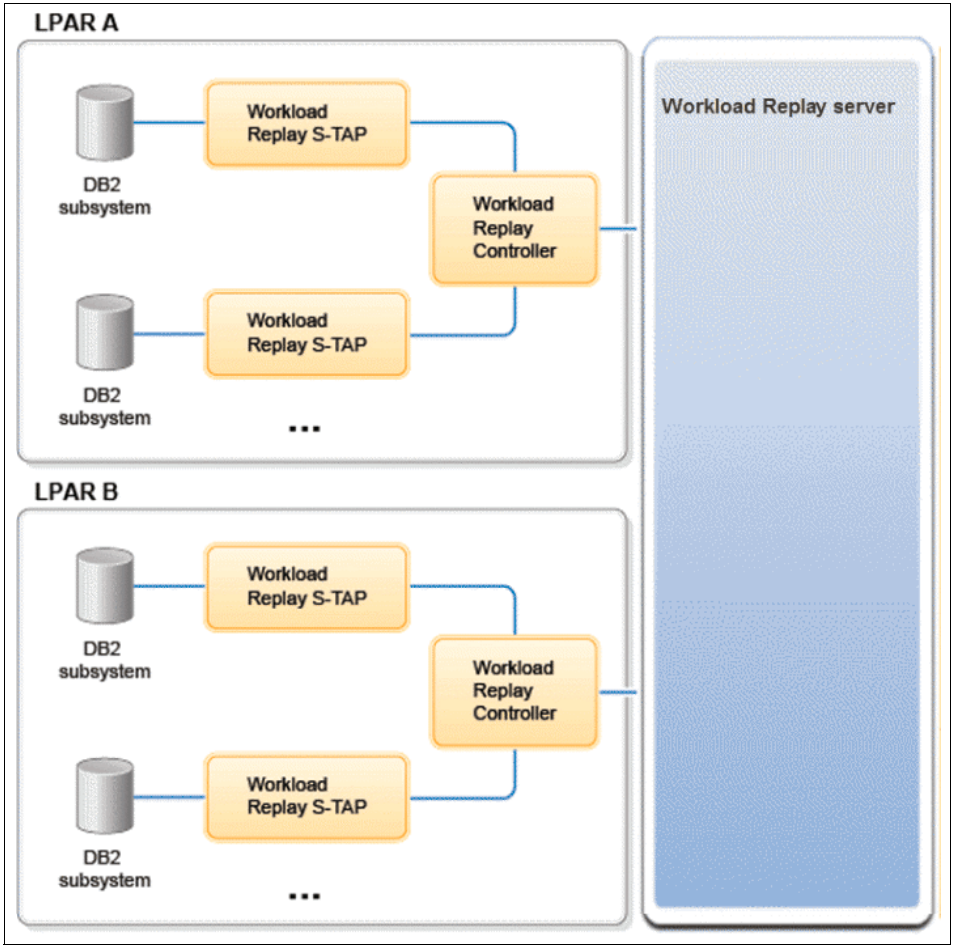


Figure 2-6 One controller per LPAR and one S-TAP per subsystem or data sharing group member

By applying these rules to the DB2 for z/OS deployment requirements of this book, you can use the following data server components deployment plan:

1. Install and configure pre-production data server components:
   a. Use SMP/E for z/OS to install the data server components on LPAR `wtsc61.itso.ibm.com`.
   b. Use SMP/E to install the data server components on LPAR `wtsc62.itso.ibm.com`.
   c. Customize S-TAP to monitor subsystem D1J2.
   d. Configure Workload Replay Controller for z/OS on `wtsc61.itso.ibm.com`.

e. Configure Workload Replay Controller for z/OS on `wtsc62.itso.ibm.com`.

f. Validate the S-TAP and Workload Replay Controller operation.

g. Enable workload capture or replay for the DB1J location alias.

2. Install and configure production data server components:

a. Configure S-TAP to monitor subsystem D1K1.

b. Configure S-TAP to monitor subsystem D1K2.

c. Validate the S-TAP and Workflow Replay Controller operation.

d. Enable workload capture or replay for the DB1K location alias.

> **Note:** In our book environment, the production and pre-production subsystems are hosted on the same LPARs. Therefore, no additional SMP/E installation step is required in the production environment.

In Chapter 4, “IBM InfoSphere Optim Workload Replay for DB2 for z/OS installation and configuration” on page 77, we describe how to implement the deployment plan on z/OS.

Coexistence

If InfoSphere Workload Replay for DB2 for z/OS is operating on the same DB2 subsystem as IBM DB2 Query Monitor for z/OS, or IBM InfoSphere Guardium for DB2 for z/OS, the products must be maintained at compatible maintenance levels. For details, see the following web address:

http://www.ibm.com/support/docview.wss?uid=swg27036808

2.4.2 Planning DB2 for Linux, UNIX, and Windows deployments

During the requirements analysis, which we performed in “Analyzing DB2 for Linux, UNIX, and Windows deployment requirements” on page 20, we collected the basic information needed to create a deployment plan. Using the following set of rules, we can create a deployment plan:

- S-TAP must be installed one time on each physical (or virtual) database server machine on which database traffic is monitored.
- S-TAP must be configured for each DB2 instance on which SQL is captured *or* replayed.
- Workload capture or replay must be enabled for the designated databases.

By applying these rules to the DB2 for Linux, UNIX, and Windows deployment requirements of this book, you use the following S-TAP deployment plan:

1. Install and configure pre-production S-TAPs:
   a. Install S-TAP on `hawk.itso.ibm.com` by using the AIX installation media.
   b. Configure S-TAP to monitor the DB2 instance tinst1.
   c. Validate the S-TAP operation.
   d. Enable workload capture or replay for databases TESTDB and TESTDB2.
2. Install and configure production S-TAPs:
   a. Install S-TAP on `eagle.itso.ibm.com` using the AIX installation media.
   b. Configure S-TAP to monitor the DB2 instance pinst1.
   c. Validate the S-TAP operation.
   d. Enable workload capture or replay for database PRODDB.

If we wanted to capture or replay SQL on two different DB2 instances on the same database server machine, we must repeat steps b and c for each instance and step d for each designated database in those instances.

In Chapter 5, “DB2 for Linux, UNIX, and Windows S-TAP installation and configuration” on page 111, we describe how to implement a deployment plan.

AIX considerations

On AIX operating systems, the database manager must be restarted after S-TAP is installed.

Collecting additional information

For each monitored DB2 instance, you must collect additional information that is required to configure S-TAP. For the details about the information that database administrators must collect, see A.2.2, “S-TAP for Linux, UNIX, and Windows configuration worksheet” on page 316.

Working with workloads in DB2 high availability environments

If DB2 is configured for high availability (HA), S-TAP must be installed and configured on each primary and standby node.

Working with workloads in DB2 DPF environments

InfoSphere Workload Replay can capture and replay SQL in database partitioning feature (DPF) environments if only a single coordinator node is used. Install S-TAP only on the coordinator node.

Working with workloads in DB2 pureScale environments

InfoSphere Workload Replay Version 2.1.0.1 does not support IBM DB2 pureScale®.

Coexistence with Guardium Database Activity Monitoring

InfoSphere Guardium and InfoSphere Workload Replay use the same S-TAP technology to monitor database traffic. You can configure S-TAP to forward traffic to a Guardium Database Activity Monitor (DAM) appliance and a single Workload Replay appliance by enabling full redundancy mode.

> **Note:** In redundancy mode, each appliance monitors the same traffic. Therefore, this configuration mode is not suitable for multi-server deployments that take advantage of the load-balancing mode, which distributes monitored traffic across multiple appliances.

2.5 Planning product validation

During product validation, you verify that the product is operational. Product validation is typically performed in two steps:

1. Functional testing: Verify that all product components are up and running and communicate with each other as expected. This testing is typically performed by using small workloads that drive different product components.
2. System testing: Verify that representative workloads can be captured, processed, and replayed, and monitor resource utilization on the DB2 data servers.

Product validation is complete after a deployment passes each of the tests outlined in this section.

Functional testing: Validating connectivity

During the initial functional validation, you verify that all components are operational and communicate with each other as expected. Functional testing is typically performed by an administrator or a privileged user.

1. Verify for each main Workload Replay appliance:
   a. You can connect to the Guardium web console as an administrator, as described in “Accessing the Guardium web console” on page 215.
   b. You can connect to the command-line interface (CLI) as an administrator, as described in “Accessing the CLI” on page 215.

c. You can connect to the Workload Replay web console as a privileged user, as described in “Accessing the Workload Replay web console” on page 215.

d. The required services are running on the appliance, as described in 7.2.2, “Monitoring the connection status of Workload Replay services” on page 236.

e. DB2 for Linux, UNIX, and Windows only: The assigned S-TAPs are communicating with this appliance, as described in 7.3.1, “Monitoring connection status on DB2 for Linux, UNIX, and Windows database servers” on page 242.

f. DB2 for z/OS only: The assigned controllers are communicating with this appliance, as described in 7.2.2, “Monitoring the connection status of Workload Replay services” on page 236.

2. In multi-server deployments, verify the following information for each auxiliary Workload Replay appliance:

a. You can connect to the Guardium web console as an administrator, as described in “Accessing the Guardium web console” on page 215.

b. You can connect to the CLI as an administrator, as described in “Accessing the CLI” on page 215.

c. You can connect to the Workload Replay web console as a privileged user, as described in “Accessing the Workload Replay web console” on page 215.

d. The required services are running on the appliance, as described in 7.2.2, “Monitoring the connection status of Workload Replay services” on page 236.

e. The auxiliary server is connected as expected to the main Workload Replay server, as described in 7.2.2, “Monitoring the connection status of Workload Replay services” on page 236.

f. DB2 for Linux, UNIX, and Windows only: The assigned S-TAPs are communicating with this appliance, as described in 7.3.1, “Monitoring connection status on DB2 for Linux, UNIX, and Windows database servers” on page 242.

g. DB2 for z/OS only: The assigned controllers are communicating with this appliance, as described in 7.2.2, “Monitoring the connection status of Workload Replay services” on page 236.

Address any identified issues before validating workload replay operations.

Functional testing: Validating workload replay operations

After connectivity is validated, you complete the capture replay workflow to verify that all components are functioning normally. Some of the stated tests are optional, depending on your deployment topology and the types of workloads (local or remote) that you will capture and replay.

> **Note:** A local workload is running on the database server itself. A remote workload is running on a machine other than the database server. Because InfoSphere Workload Replay's local and remote workload processing has some unique characteristics, we suggest running a separate test for each workload type that applies to your environment.

If you are validating a centralized deployment, run the following tests on each main appliance:

1. Capture, process, and replay a small *remote workload* by using the Workload Replay web console. Verify that the expected SQL is captured and that workload comparison reports can be created, as described in Chapter 6, "Capturing and replaying workloads" on page 153.
2. Capture, process, and replay a small *local workload* by using the Workload Replay web console. Verify that the expected SQL is captured and that workload comparison reports can be created, as described in Chapter 6, "Capturing and replaying workloads" on page 153.

If you are validating a decentralized deployment, run the following tests on each main appliance:

1. Capture a small *remote workload* on the source appliance by using the Workload Replay web console and export it to intermediary storage. Verify that the expected SQL is captured by using the single workload report, as described in Chapter 6, "Capturing and replaying workloads" on page 153.
2. Import the *remote workload* on the target appliance by using the Workload Replay web console, process it, and replay it. Verify that the workload comparison reports can be created, as described in Chapter 6, "Capturing and replaying workloads" on page 153.
3. Capture a small *local workload* on the source appliance by using the Workload Replay web console and export it to intermediary storage. Verify that the expected SQL is captured by using the single workload report, as described in Chapter 6, "Capturing and replaying workloads" on page 153.
4. Import the *local workload* on the target appliance by using the Workload Replay web console, process it, and replay it. Verify that the workload comparison reports can be created, as described in Chapter 6, "Capturing and replaying workloads" on page 153.

Functional testing: Validating backup and restore procedures

Workloads are permanently stored on the main Workload Replay appliances. If an appliance stops working and normal operation cannot be restored, all workloads are lost unless you have access to an appliance backup or a workload backup.

Practice the backup and restore procedure one time in a pre-production environment.

Complete the appliance backup and restore steps:

1. Capture, process, and replay any type of workload, as described in Chapter 6, “Capturing and replaying workloads” on page 153.
2. Create an appliance backup, delete the workload, and restore the appliance, as described in 7.5, “Backup and recovery” on page 249.

InfoSphere Workload Replay also provides backup and restore capabilities for captured workloads.

Complete the workload backup and restore steps:

1. Capture, process, and replay any type of workload, as described in Chapter 6, “Capturing and replaying workloads” on page 153.
2. Create a backup of the captured workload, delete the workload, and restore the workload, as described in 7.5.2, “Workload backup and restore” on page 253.

System testing

System testing is performed by using larger workloads that are similar in nature to the workloads you will work with after the solution is operating in production mode. We suggest performing these tests by using dedicated Workload Replay accounts that you plan to use when InfoSphere Workload Replay is released to production. As part of system testing, you typically monitor resource utilization on the data servers.

2.6 Planning product adoption

As part of deployment planning, you must define who is authorized to access the Workload Replay appliances and who can capture, process, or replay workloads after the solution is deployed.

Access to the Workload Replay appliance and user interfaces (Guardium web console, Workload Replay web console, and CLI) is always secured, due to the sensitive nature of production data. Workload Replay implements security in the following manner:

- To prevent tampering with sensitive data that is collected and stored on the appliance during workload capture or replay, no direct operating system access is provided to the appliance. However, by your request, IBM support personal can gain root access to the appliance, for example, for troubleshooting.
- All remote user interfaces use secure protocols (HTTPS and Secure Shell (SSH)) and require a login and password to prevent unauthorized access.
- A set of default administrative user IDs is created during product installation. The credentials for these default users are always stored in encrypted form on the appliance. You can create additional users as needed and configure whether their credentials are maintained on the appliance or by an external security provider, such as Lightweight Directory Access Protocol (LDAP).

Access to databases (or subsystems) for capture and replay is also protected. For a description of how you can control who can capture, process, or replay workloads on a particular database (or DB2 for z/OS subsystem), see 2.6.2, “Restricting access to workloads” on page 37.

2.6.1 Assigning Workload Replay server roles

In 1.2.3, “Roles and responsibilities” on page 13, we define four user roles in a Workload Replay deployment: administrator, security administrator, privileged user, and user. As part of deployment planning, you must identify which person has each role. A person can have one or more roles, if needed.

Each Workload Replay role requires access to one or more main Workload Replay appliance interfaces, as shown in Table 2-3.

Table 2-3 Roles requiring access to main Workload Replay appliance interfaces

Workload Replay role	Guardium web console	Workload Replay web console	CLI
Administrator	Yes	Yes	Yes
Security administrator	Yes	No	No
Privileged user	Yes	Yes	Yes
User	No	Yes	No

In multi-server deployments, only administrators, security administrators, and privileged users require access to auxiliary appliances, as listed in Table 2-4.

Table 2-4 Roles requiring access to auxiliary Workload Replay appliance interfaces

Workload Replay role	Guardium web console	CLI
Administrator	Yes	Yes
Security administrator	Yes	No
Privileged user	Yes	Yes

Note: We suggest that you assign the same roles to a person on the main and auxiliary appliances.

Table 2-5 maps Workload Replay roles to privileges, which govern which tasks can be performed in the Guardium web console, Workload Replay web console, or CLI.

Table 2-5 Mapping roles to interface privileges

Workload Replay role	Required privileges
Administrator	admin and cli
Security administrator	accessmgr
Privileged user	admin, cli, and workload-replay-admin
User	user and workload-replay-user

The security administrator implements the required security policy by creating user IDs and granting them necessary privileges as part of the product configuration. Use A.2.3, “Workload Replay appliance user mapping worksheet” on page 318 to create a suitable layout. For details about how to implement security roles, see 7.1, “Access management” on page 214.

2.6.2 Restricting access to workloads

Non-privileged and privileged users have access to the Workload Replay web console, which is used to perform capture and replay actions. Table 2-6 on page 38 lists these actions with a brief description of their purpose.

Table 2-6 Actions that are performed using the Workload Replay web console

Action	Purpose
Capture workload	Record SQL activity on a specific database, subsystem, or data sharing group for a predefined amount of time. *The privilege to perform this action does not include the privilege to review the captured workload.*
Transform workload	Prepare a workload for replay on a database, subsystem, or data sharing group.
Replay workload	Replay a previously prepared workload on a database, subsystem, or data sharing group.
Review a single workload report	Review workload information, such as SQL in workload and the execution count.
Compare two workloads	Analyze differences between a captured workload and a replayed workload or two replayed workloads.
Delete workloads	Remove workloads that are no longer needed.
Delete reports	Remove reports that are no longer needed.
Export workload	Create a password-protected encrypted archive of a captured workload that can be transferred by a privileged user to an FTP or Secure Copy Protocol (SCP) server for backup or archive.
Import workload	Import a previously exported password-protected encrypted archive on a Workload Replay server.

You can restrict per database (or subsystem on DB2 for z/OS) the action that a user (or group) can perform by creating a workload action security policy.

Note: A policy applies to all workloads that are associated with a database (or subsystem) for which the policy is defined.

To identify a security policy that is appropriate for your database (or subsystem), consider the following questions:

- Which Workload Replay actions must be completed on this database (or subsystem)?
- Who will be authorized to perform these actions on a database (or subsystem)?
- What type of potentially sensitive information can be exposed to a user?

Limiting access to Workload Replay actions

Consider the following scenario: In a critical database or subsystem, you are only planning to capture workloads. Your security policy for this database (or subsystem) might include these tasks:

- Can capture workload
- Can export workload
- Can delete workloads
- Can review a single workload report
- Can compare two workloads
- Can delete reports

We suggest using this kind of restrictive policy in production environments in which you will never replay workloads.

Limiting access to sensitive workload data

Certain actions expose workload information in the Workload Replay web console that you might consider sensitive in nature, such as SQL literal values or host variables that were captured in the source environment.

Note: Data masking is not yet supported in InfoSphere Workload Replay Version 2.1.0.1.

Table 2-7 outlines the potentially sensitive application data that might be displayed to a user performing a specific action.

Table 2-7 Captured application data can be exposed in Workload Replay web console

Action	Potentially sensitive information that might be displayed
Review single workload report	SQL statement text, including several hard-coded literal values
Replay workload	SQL statement text, including several hard-coded literal values and host variables
Compare two workloads	SQL statement text, including hard-coded literal values and host variable values, except XML or line-of-business (LOB) data

To lock down this security policy further in your production environment, you can exclude the report-specific privileges and only grant these privileges:

- Can capture a workload
- Can export a workload
- Can delete a workload

A user with only these privileges does not have access to sensitive production data that might be exposed in reports.

For information about how to define a security policy for a database or subsystem in the Workload Replay web console, see 4.5, “Enablement of workload capture and replay in the Workload Replay web console” on page 98 (for DB2 for z/OS) and 5.4, “Enablement of workload capture and replay in the Workload Replay web console” on page 140 (for DB2 for Linux, UNIX, and Windows).

3

Installing and configuring IBM InfoSphere Optim Workload Replay appliances

IBM InfoSphere Optim Workload Replay (InfoSphere Workload Replay) is installed and configured on an InfoSphere Guardium appliance. This chapter includes detailed instructions about how to install and configure the InfoSphere Guardium Appliance and subsequently install and configure InfoSphere Workload Replay.

This chapter covers the following steps:

- Installing InfoSphere Guardium V9.0
- Activating the InfoSphere Workload Replay license
- Installing the required InfoSphere Guardium patches and InfoSphere Workload Replay patches
- Activating the DB2-to-DB2 Capture Replay policy on the Guardium Appliance
- Verifying that the installation completed successfully

3.1 Overview

An InfoSphere Workload Replay appliance deployment consists of the following steps:

1. Rack the physical appliances or build virtual appliances and connect them to the network.
2. Install InfoSphere Guardium and complete the basic appliance configuration.
3. Install and configure the InfoSphere Workload Replay software in Guardium.

In this chapter, we assume that you completed the first step, set up the virtual or physical appliances, and connected them to the network.

We describe the installation and configuration process for a main and auxiliary Workload Replay appliance by using the steps that we completed to build two virtual appliances. Figure 3-1 shows the two-server topology to support workload capture, process, and replay on DB2 for z/OS in the book environment.

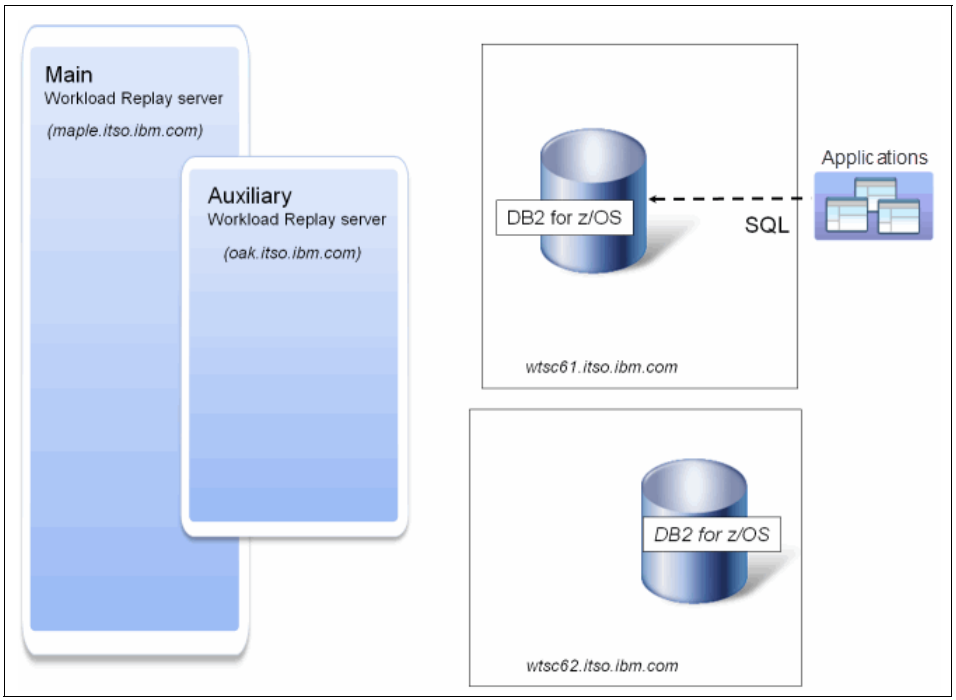


Figure 3-1 Book z/OS lab environment

We use the Guardium web console, the Workload Replay web console, and the CLI throughout the installation and configuration process. On completion of the installation and configuration steps, the software stack of a main (or auxiliary) appliance looks like Figure 3-2.

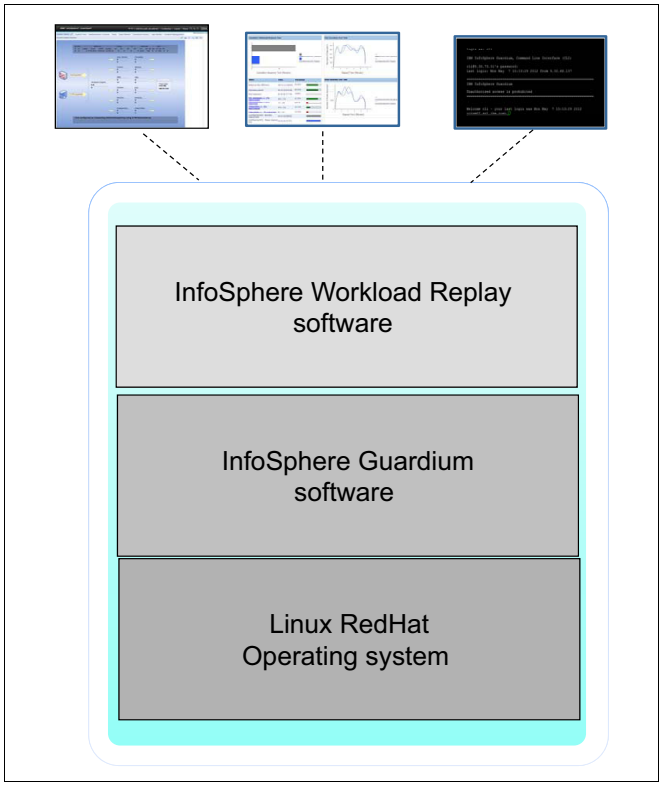


Figure 3-2 InfoSphere Workload Replay appliance software stack

3.2 Accessing the appliance installation media

The Workload Replay appliance installation media consists of the following items:

- The InfoSphere Guardium installation media that includes a hardened Linux Red Hat operating system
- InfoSphere Workload Replay prerequisite patches
- InfoSphere Workload Replay patches

- The InfoSphere Workload Replay license key
- Product documentation

The media is available for download for the z/OS and Linux, UNIX, and Windows platforms.

The appliance installation and configuration instructions are identical for both database server platforms.

3.2.1 Accessing the appliance installation media for InfoSphere Workload Replay for DB2 for z/OS

For details about how to download and prepare the installation media for a first-time appliance deployment, see A.1.1, “Downloading InfoSphere Workload Replay for DB2 for z/OS installation media” on page 302.

3.2.2 Accessing the appliance installation media for InfoSphere Workload Replay for Linux, UNIX, and Windows

For details about how to download and prepare the installation media for a first-time appliance deployment, see A.1.2, “Downloading InfoSphere Workload Replay for DB2 for Linux, UNIX, and Windows installation media” on page 309.

Note: Use the `InfoSphere_Guardium_Image_V90-64_DVD.iso` file, as advised in “Downloading the base installation media from ShopZ” on page 302.

3.3 Installing and configuring the InfoSphere Guardium software

InfoSphere Guardium provides the base infrastructure that is needed for capturing and replaying workloads.

Before you begin, complete the appliance configuration worksheet in A.2.1, “Appliance configuration worksheet” on page 315 for each appliance that you plan to deploy.

Note: If you are planning to use storage area network (SAN) storage, prepare the device by following the instructions in Appendix E of the *IBM InfoSphere Guardium Software Appliance Installation Guide*:

http://ibm.co/1sJFNdT

3.3.1 Installing InfoSphere Guardium

Ensure that the InfoSphere Guardium appliance installation image is mounted in the server and that the server is configured to start from this installation media.

Note: If you are installing InfoSphere Guardium on a physical appliance, insert the installation DVD. If you are installing InfoSphere Guardium on a virtual appliance, mount the ISO 9660 image file that you downloaded.

When you power on the server, the installation process starts. Figure 3-3 shows the installation options. Select **Standard Installation** for the book environment. For more information about the different types of installers, see the InfoSphere Guardium Knowledge Center at the following web address:

http://ibm.co/16CV5gc

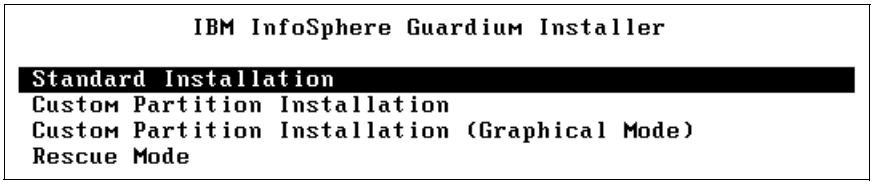


Figure 3-3 IBM InfoSphere Guardium installation options

The installer starts to partition and format the file system. When the file system is ready, the installer continues to install a hardened Red Hat V5.8 Linux operating system.

After the Red Hat Linux operating system is installed, the installation program copies the InfoSphere Guardium installation media to disk, restarts the appliance, and starts the InfoSphere Guardium installation process.

Note: To avoid accidentally restarting the installation process, remove the installation media after the operating system installation completes and before the appliance starts again.

Initializing InfoSphere Guardium default users

During product installation, several default user accounts are created that are used by the administrator and security administrator to manage the appliance. For detailed information about these accounts and how to create additional accounts, see 7.1, “Access management” on page 214.

cli account

The `cli` account is used to administer the appliance by using the command-line interface (CLI) interface. You can provide a temporary password during installation:

1. In the Command line interface password window, select **Yes** to change the default password or **No** to continue (Figure 3-4). If you choose not to change the default or if you do not make a decision within 10 seconds, the default password `guardium` is used.

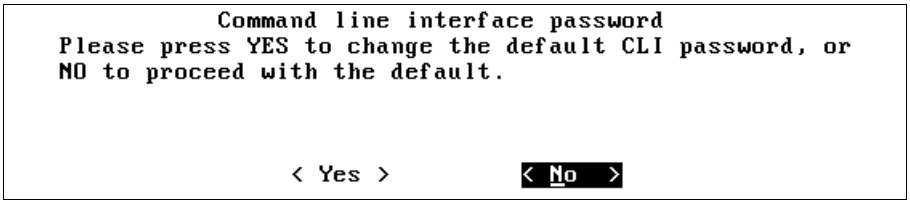


Figure 3-4 Change the default password for the cli account

> **Note:** The password must be changed the first time that someone logs on to the CLI by using this account.

2. If you select **Yes**, enter and confirm the new temporary password for the `cli` account, as shown in Figure 3-5 on page 46 and Figure 3-6 on page 47.

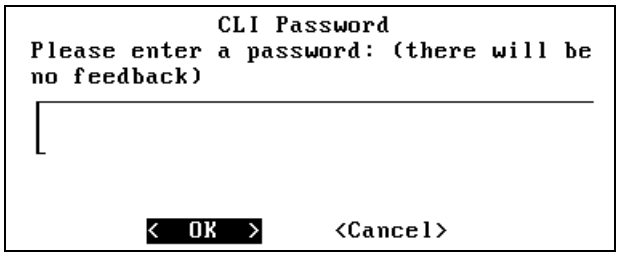


Figure 3-5 Set a temporary password for the cli user

```
        CLI Password
 Please confirm the
 password:

   < OK >   <Cancel>
```

Figure 3-6 Confirm the new password for the cli user

Additional administrative CLI accounts (`guardcli1`, `guardcli2`, `guardcli3`, `guardcli4`, and `guardcli5`) are created. Their initial passwords are set to the password of the `cli` account.

Administrator account

An administrator account, which is named `admin`, for the InfoSphere Guardium web console is created after the CLI accounts. You can change the default password. If you do not make a decision within 10 seconds, the default password `guardium` is used.

> **Note:** The password must be changed the first time that someone logs on to the Guardium web console by using this account.

If applicable, enter and confirm the new temporary password for the `admin` account, as shown in Figure 3-7 on page 47 and Figure 3-8 on page 47.

```
                    GUI ADMIN password
Please enter a password: (there will be no feedback)

                 < OK >          <Cancel>
```

Figure 3-7 Set a temporary password for the admin user

```
                    GUI ADMIN password
Please confirm the password:

                 < OK >          <Cancel>
```

Figure 3-8 Confirm the temporary password for the admin user

Security administrator account

Finally, a default account for the security administrator, which is named `accessmgr`, is created. You can change the default password. If you do not make a decision within 10 seconds, the default password `guardium` is used.

> **Note:** The password must be changed the first time that the security administrator logs on to the Guardium web console by using this account.

If applicable, enter and confirm the new temporary password for the `accessmgr` account, as shown in Figure 3-9 and Figure 3-10 on page 48.

```
                    ACCESS MANAGER password
Please enter a password: (there will be no feedback)
[
                    <  OK  >          <Cancel>
```

Figure 3-9 Set a temporary password for the accessmgr account

```
                    ACCESS MANAGER password
 Please confirm the password:
 [
                    <  OK  >          <Cancel>
```

Figure 3-10 Confirm the temporary password for the accessmgr account

Selecting the installation type

When prompted for selecting the installation type, choose **Collector** (Figure 3-11).

```
                    Install Type
Configure as a Collector or an Aggregator

            <Collector >        <Aggregator>
```

Figure 3-11 Select Install Type Collector

Accepting the license agreement

Review the license agreement (Figure 3-12).

```
International Program License Agreement

Part 1 - General Terms

BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON AN "ACCEPT" BUTTON,
OR OTHERWISE USING THE PROGRAM, LICENSEE AGREES TO THE TERMS OF THIS AGREEMENT.
IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF LICENSEE, YOU REPRESENT AND WARRAN
T THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE TO THESE TERMS. IF YOU DO NOT AG
REE TO THESE TERMS,

- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN "ACCEPT" BUTTON, OR USE TH
E PROGRAM; AND

- PROMPTLY RETURN THE UNUSED MEDIA, DOCUMENTATION, AND PROOF OF ENTITLEMENT TO T
HE PARTY FROM WHOM IT WAS OBTAINED FOR A REFUND OF THE AMOUNT PAID. IF THE PROGR
AM WAS DOWNLOADED, DESTROY ALL COPIES OF THE PROGRAM.

1. Definitions

"Authorized Use" - the specified level at which Licensee is authorized to execut
e or run the Program. That level may be measured by number of users, millions of
 service units ("MSUs"), Processor Value Units ("PVUs"), or other level of use s
pecified by IBM.

Guardium License (Use arrow keys or PgUp/PgDown to Scroll) _
```

Figure 3-12 Review the license agreement

> **Note:** Use the arrow keys or Page Up (PgUp) and Page Down (PgDown) keys to scroll through the license agreement.

Press the Q key after you review the license agreement.

Accept the license agreement by typing **yes** at the prompt (Figure 3-13).

```
ts to reflect at a minimum (i) the number of Installs of the Program that Licens
ee deploys in accordance with the definition of "Install" in this LI document; a
nd (ii) the number of applicable PVUs or RVUs in accordance with the definition
of PVU or RVU in this LI document.

The number of Resource Value Units (RVUs) Licensee requires for this Program is
based on Million Service Units (MSUs) capacity of a machine.

The required number of RVUs is determined according to the following table:

For MSU based RVUs:

For 1-3 MSUs, 1 RVU per MSU is required
For 4-45 MSUs, 0.45 RVUs per MSU is required
For 46-175 MSUs, 0.36 RVUs per MSU is required.
For 176-315 MSUs, 0.27 RVUs per MSU is required.
For 316+ MSUs, 0.2 RVUs per MSU is required.


D/N:  L-DTIS-8AUMJU
P/N:  CT5Y1ML



Do you agree to the above license? [yes/no]: yes_
```

Figure 3-13 Accept license agreement

After the installation is complete, a login prompt is displayed in the Guardium console, as shown in Figure 3-14.

```
================================================================
IBM InfoSphere Guardium

Unauthorized access is prohibited
================================================================
guard login: cli
Password: _
```

Figure 3-14 System is ready for logon

Note: You cannot yet connect to the Guardium appliance remotely because network connectivity still needs to be configured.

Log in to the system by using the `cli` account credentials.

Note: If you did not assign a custom password, the default password is `guardium`.

After you log in as `cli` for the first time, change the password by following the prompts, as shown in Figure 3-15.

```
Welcome cli - this is your first login in this system.
Your password has expired.
Changing password for 'cli'.
Enter current password:
Enter new password:
Re-enter new password: _
```

Figure 3-15 Change the password for the cli account during first logon

You can now configure InfoSphere Guardium.

3.3.2 Configuring InfoSphere Guardium

To finalize the basic InfoSphere Guardium setup, configure the network connectivity and configure the date and time settings. Use the information that you collect in the appliance configuration worksheet as described in A.2.1, “Appliance configuration worksheet” on page 315.

Configuring network connectivity

Each setup instruction is illustrated by using an example configuration of one of our book appliances.

> **Note:** In the following instructions, replace *<setting>* with the correct value from your configuration worksheet.

Complete these steps to configure network connectivity:

1. Access the appliance’s console and log in by using the `cli` account if you are not already connected.
2. Set the IP address by issuing the following CLI command (Figure 3-16):

   `store network interface ip <guardium_server_ip>`

```
guard.domain.com> store network interface ip 9.12.5.27
This change will take effect after the next network restart.
ok
guard.domain.com> _
```

Figure 3-16 Configure the appliance’s IP address

> **Note:** You can always display the current configuration setting by entering the equivalent **`show`** command. For example, to display the current IP address, enter the CLI command **`show network interface ip`**.

3. Set the network mask by using the following CLI command (Figure 3-17):

   store network interface mask <*subnet_mask*>

```
guard.domain.com> store network interface mask 255.255.240.0
This change will take effect after the next network restart.
ok
guard.domain.com> _
```

Figure 3-17 Configure the subnet mask

4. Set the network mask by using the following CLI command (Figure 3-18):

   store network routes def <*gateway_ip*>

```
guard.domain.com> store network routes def 9.12.4.1
This change will take effect after the next network restart.
ok
guard.domain.com> _
```

Figure 3-18 Configure the default gateway

5. Set the Domain Name Servers (DNS) by using the following CLI command (Figure 3-19):

   store network resolver 1 <*dns_server_ip_address*>

```
guard.domain.com> store network resolver 1 9.12.6.6
This change will take effect after restart network.
ok
guard.domain.com> store network resolver 2 9.12.6.7
This change will take effect after restart network.
ok
guard.domain.com> _
```

Figure 3-19 Configure domain name servers

Note: You can configure up to three DNS:

- store network resolver 1 *<dns_server1_ip_address>*
- store network resolver 2 *<dns_server2_ip_address>*
- store network resolver 3 *<dns_server3_ip_address>*

6. Set the host name and domain by using the following CLI commands (Figure 3-20):

   store system hostname <*guardium_host_name*>
   store system domain <*guardium_domain_name*>

```
guard.domain.com> store system hostname maple
ok
guard.domain.com> store system domain itso.ibm.com
ok
guard.domain.com> _
```

Figure 3-20 Configure host name and domain name

7. Restart the appliance by using the following CLI command (Figure 3-21):

   `restart system`

```
guard.domain.com> restart system
Restarting system
INIT: Sending processes the TERM signal
```

Figure 3-21 Restart the Guardium appliance after network configuration is complete

After the appliance restarts, you can access the remote Guardium CLI and Guardium web console by using the `cli`, `admin`, `accessmgr`, and `guardcli` default accounts.

To access the appliance's CLI, connect a Secure Shell (SSH) client to *`guardium_hostname_or_ip`* port 22.

To access the appliance's Guardium web console, direct your web browser to `https://`*`guardium_hostname_or_ip`*`:8443/sqlguard`.

Note: For additional information, see "Accessing the CLI" on page 215 and "Accessing the Guardium web console" on page 215. The Workload Replay web console is not yet installed.

Configuring date and time

Complete the following steps to set the date and time:

1. Log in to the CLI by using the `cli` account (Figure 3-22).

```
login as: cli

IBM InfoSphere Guardium, Command Line Interface (CLI)

cli@maple.itso.ibm.com's password:
Last login: Mon Sep 15 13:45:28 2014

================================================================
IBM InfoSphere Guardium

Unauthorized access is prohibited
================================================================


Welcome cli - your last login was Mon Sep 15 13:45:30 2014
maple.itso.ibm.com>
```

Figure 3-22 Log in to the appliance remotely by using the CLI

2. Configure up to three Network Time Protocol (NTP) servers by using the following CLI command (Figure 3-23):

   `store system ntp server`

```
maple.itso.ibm.com> store system ntp server
USAGE: store system ntp server
       For each server enter either ip or hostname
       Enter up to 3 NTP servers to store:
Enter ntp server: sczhmc7.itso.ibm.com
Enter ntp server: sczhmc8.itso.ibm.com
Enter ntp server:
Make sure to use "store system ntp state on" to turn ON the NTP
service.
All inspection engines refreshed.
ok
```

Figure 3-23 Configure up to three NTP servers

3. Enable the NTP servers by using the following CLI command (Figure 3-24):

   `store system ntp state on`

```
maple.itso.ibm.com> store system ntp state on
ok
```

Figure 3-24 Enable NTP servers

> **Note:** If you must reconfigure NTP settings, issue the CLI command **`store system ntp state off`** followed by the CLI command **`store system ntp state on`**.

4. Look up the correct time zone setting for this appliance by using the following CLI command (Figure 3-25):

   `store system clock timezone list`

```
maple.itso.ibm.com> store system clock timezone list
Timezone:                 Description:
---------                 -----------
Africa/Abidjan:
Africa/Accra:
Africa/Addis_Ababa:
Africa/Algiers:
Africa/Asmara:
```

Figure 3-25 Review available time zone settings

> **Note:** To scroll through the list, hold the Shift key and press the Page Up or Page Down key.

5. Configure the time zone setting that you want by using the following CLI command (Figure 3-26):

   `store system clock timezone <selected_timezone>`

```
maple.itso.ibm.com> store system clock timezone America/New_York
Current timezone America/New_York
No change for the timezone
ok
```

Figure 3-26 Configuring the appliance's time zone

The configuration of the InfoSphere Guardium appliance is now complete.

3.4 Preparing for the InfoSphere Workload Replay software installation

InfoSphere Guardium provides the infrastructure that InfoSphere Workload Replay requires to capture, process, and replay workloads. Before you install the InfoSphere Workload Replay software, activate the product license and install the prerequisite patches.

3.4.1 Installing the InfoSphere Workload Replay license

You can install a license by using the Guardium web console or the CLI.

Note: The license key file is included in the installation media. For the correct part numbers, see A.1, “Electronic installation media access” on page 302.

Installing a license by using the Guardium web console

To install the license key, complete the following steps:

1. Open the Guardium web console on the correct InfoSphere Guardium appliance:

   `https://guardium_hostname_or_ip:8443/sqlguard`

   Note: If you cannot open or connect to the web console, see 9.2.2, “Resolving Guardium web console connectivity issues” on page 287.

2. Log on by using the `admin` account, as shown in Figure 3-27.

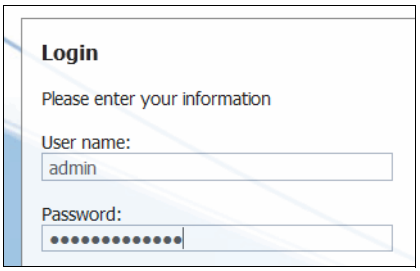


Figure 3-27 Log in to the Guardium web console

3. Because it is the first time that you log in by using the `admin` account, you must change the password. Enter the old password and the new password, confirm the new password, and click **Change Password**.

In the upper-left corner of the window, “NO LICENSE” is displayed, which indicates that this appliance cannot yet be used to capture, process, or replay workloads.

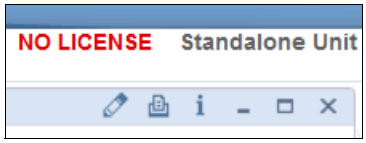


Figure 3-28 No license is installed on this appliance

4. To install a license, navigate to **Administration Console** → **Configuration** → **System**, as shown in Figure 3-29.

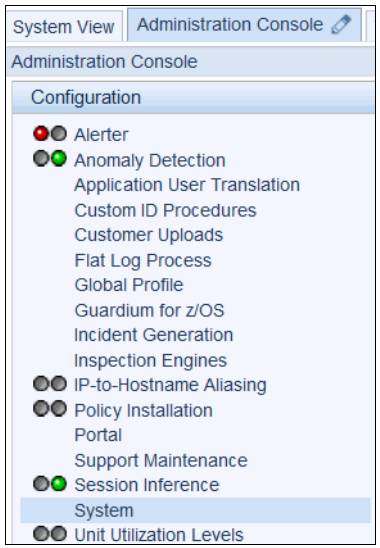


Figure 3-29 Navigate to the system configuration to enter the license key information

5. Locate the License Key field on the System Configuration panel (Figure 3-30).

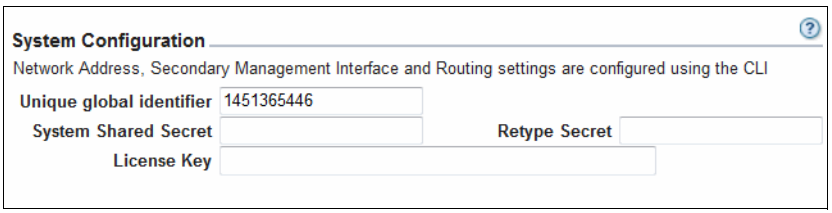


Figure 3-30 A license must be installed

6. Open your license key file and copy and paste the entire string into the License Key field (Figure 3-31), including any trailing equal signs (=).

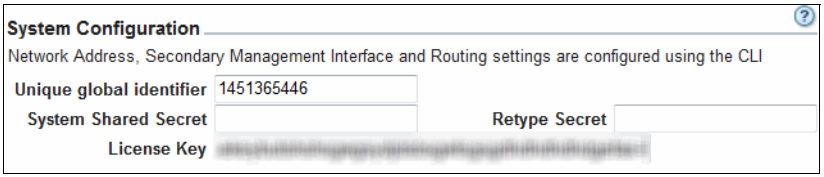


Figure 3-31 Copy and paste the license key

7. Click **Apply** to save the system configuration.
8. Verify that the license key was applied by looking at the "# of Licenses" value, as shown in Figure 3-32.

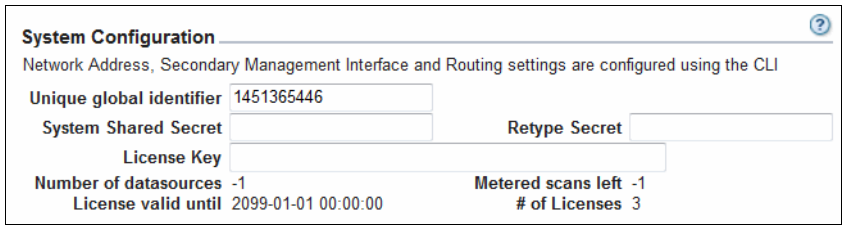


Figure 3-32 Verify that the license key was applied

Installing a license by using the CLI

To install the license, complete the following steps:

1. Log in to the CLI by using the `cli` account (Figure 3-33).

```
login as: cli

IBM InfoSphere Guardium, Command Line Interface (CLI)

cli@maple.itso.ibm.com's password:
Last login: Mon Sep 15 13:45:28 2014

=================================================================
IBM InfoSphere Guardium

Unauthorized access is prohibited
=================================================================


Welcome cli - your last login was Mon Sep 15 13:45:30 2014
maple.itso.ibm.com>
```

Figure 3-33 Log in to the appliance by using the CLI

Note: For information about how to log in, see “Accessing the CLI” on page 215.

2. Determine whether a license is already applied by using the following command (Figure 3-34):

   `show license`

```
maple.itso.ibm.com> show license
License key is NULL
ok
```

Figure 3-34 Apply a license to use this appliance for InfoSphere Workload Replay

3. Install a license by using the following command (Figure 3-35):

   `store license console`

```
maple.itso.ibm.com> store license console
Please paste the string received from customer services.
Then press <ENTER> to continue.


Store license successfully.
The web interface will be restarted.
Restarting gui
Changing to port 8443
Stopping.......
Safekeeping xregs
ok
```

Figure 3-35 Install an InfoSphere Workload Replay license by using the CLI

4. Verify that the license was successfully applied by using the following command (Figure 3-36):

   `show license`

```
maple.itso.ibm.com> show license
License:


Number of License: 3
Metering: -1
Number of Datasources: -1
Host MAC: 00:50:56:82:14:46
Valid Until: 2099-01-01 00:00:00

Licensed Applications:


        Replay
```

Figure 3-36 Verify that the license was applied

Note: Verify that Replay is listed under Licensed Application.

This appliance is now licensed for InfoSphere Workload Replay.

3.4.2 Installing the DB2-to-DB2 policy

1. Open the Guardium web console on the InfoSphere Guardium appliance:

   `https://`*`guardium_hostname_or_ip`*`:8443/sqlguard`

Note: If you DB2 for Linux, UNIX, and Windows it, see 9.2.2, “Resolving Guardium web console connectivity issues” on page 287.

2. Log on by using the `admin` account (Figure 3-37).

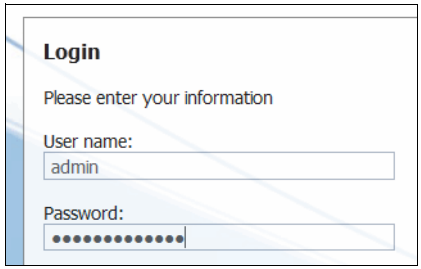


Figure 3-37 Log in to the Guardium web console to install a policy

3. Navigate to **Administration Console** → **Configuration** → **Policy Installation** (Figure 3-38).

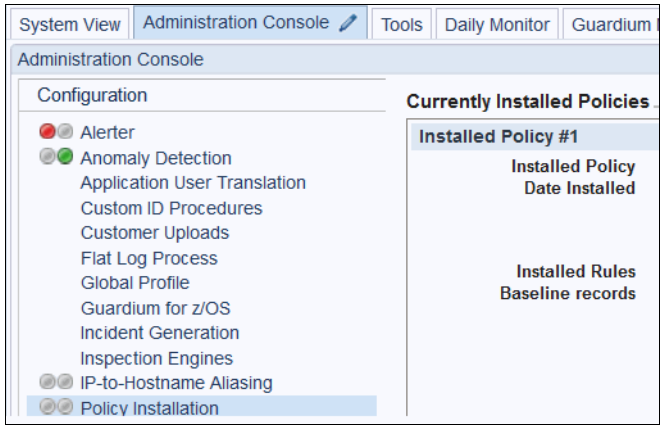


Figure 3-38 Navigate to the Guardium policy installer

4. Under Policy Installer, select **Capture and Replay - DB2-to-DB2** and **Install & Override** as the installation action (Figure 3-39).

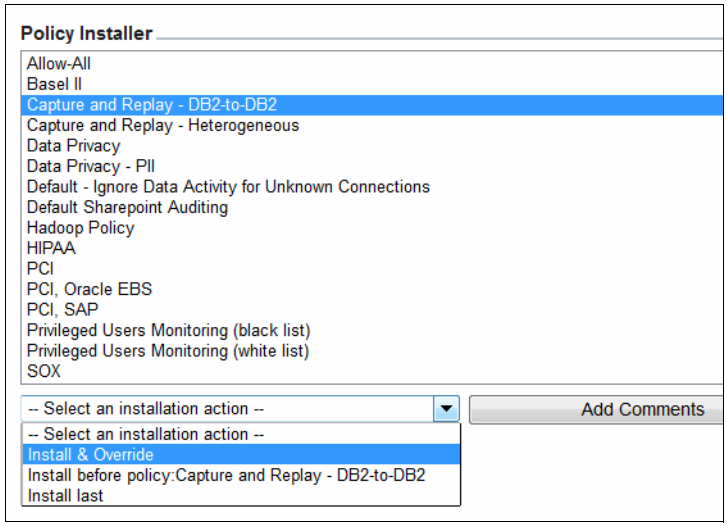


Figure 3-39 Install the Capture and Replay - DB2-to-DB2 policy

5. Confirm the policy installation.
6. Verify that the “Capture and Replay - DB2-to-DB2” policy is listed as the currently installed policy in Guardium (Figure 3-40).

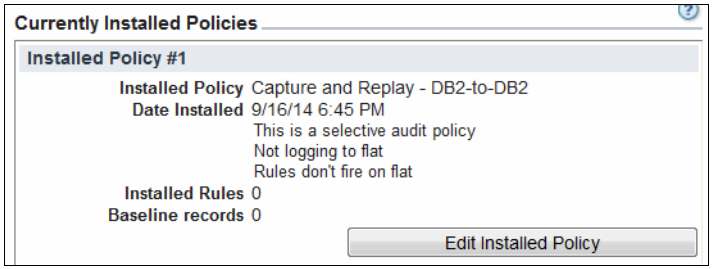


Figure 3-40 Verify Capture and Replay - DB2-to-DB2 policy is installed in Guardium

Next, install the prerequisite patches.

3.4.3 Installing the prerequisite patches

Before you can install the InfoSphere Workload Replay software on the appliance, you must install the prerequisite patches that upgrade the base version of InfoSphere Guardium, which you installed in 3.3.1, “Installing InfoSphere Guardium” on page 45.

Identifying the prerequisite patches

For information about how to identify and download prerequisite patches for the version of InfoSphere Workload Replay that you are installing, see the “Identifying prerequisite patches” topic in A.1.1, “Downloading InfoSphere Workload Replay for DB2 for z/OS installation media” on page 302, and in A.1.2, “Downloading InfoSphere Workload Replay for DB2 for Linux, UNIX, and Windows installation media” on page 309.

For InfoSphere Workload Replay Version 2.1.0.1, the following patches are required and must be installed in this order:

1. `SqlGuard-9.0p9997.tgz.enc`
2. `SqlGuard-9.0p200_GPU_March_2014_64-bit.tgz.enc`
3. `SqlGuard-9.0p1033.tgz.enc`
4. `SqlGuard-9.0p3990_WorkloadReplay_Prereq.tgz.enc`

Note: A Guardium Patch Update (GPU) is a collection of enhancements and fixes.

You can install patches on an appliance from two different locations within your environment:

- Y*our local file system*: If patches must be installed on a single appliance, you can upload them directly from your desktop or notebook.
- *FTP or Secure Copy Protocol (SCP) servers*: If you have access to FTP or SCP servers that are colocated in the same network as the appliances on which you want to apply the patches, use this approach.

In this chapter, we describe how to install patches that are in the local file system. For instructions about how to install patches from an FTP or SCP server, see 7.6.3, “Installing maintenance on an appliance” on page 262.

To install one or more patches that are on your local machine, upload the patches to the appliance, invoke the patch installation, and monitor the installation progress:

1. Log in to the CLI of the appliance as an administrator by using the `cli` account.
2. Review the patches that are already installed by using the following command (Figure 3-41):

   `show system patch installed`

```
maple.itso.ibm.com> show system patch installed
P#      Who       Description                     Request Time
Status
50      CLI       Guardium Patch Update (GPU) for 2014-09-02
04:38:00  DONE: Patch installation Succeeded.
ok
```

Figure 3-41 List installed patches

3. Use the appliance's file server to upload and download files. Issue the **`fileserver`** command and specify the IP address of your local machine (Figure 3-42) to launch the file server:

   `fileserver <`*`client_ip_address`*`>`

```
maple.itso.ibm.com> fileserver 9.55.156.227
Creating the index file.

Starting the file server. You can find it at
http://pine.itso.ibm.com
The timeout has been set to 3600 seconds and it may timeout
during the uploading.

The upload will only be accessible from the IP you are logged in
from: 9.55.156.227

Press ENTER to stop the file server.
```

Figure 3-42 Start the file server on the appliance to upload patch files

Note: If you are connecting to the appliance by using a proxy, specify the proxy server's IP address instead of your local IP address.

Note: The file server automatically terminates all connections after a customizable amount of time passes since the server started, irrespective of whether a file upload or download is in progress. The default timeout is 600 seconds.

To display the current timeout value, issue the following CLI command:

```
show timeout fileserver_session
```

To increase the timeout, run the following CLI command:

```
store timeout fileserver_session <timeout_in_seconds>
```

The maximum timeout value is 3600 seconds if GPU 200 is installed on the appliance. The maximum timeout value is lower in older GPU levels.

4. Open a web browser to the URL that is returned by the **`fileserver`** command and click **Upload a patch** (Figure 3-43).

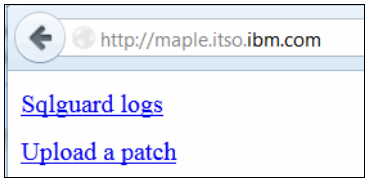


Figure 3-43 Open the patch upload page

5. On the upload page, click **Browse** to open the File Upload dialog and select the patch file to upload, as shown in Figure 3-44.

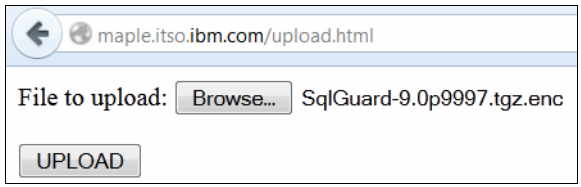


Figure 3-44 Open the file upload dialog

6. Click **UPLOAD** and wait for the patch upload to complete.

Note: You can only upload one patch at a time.

Repeat the steps if you want to upload more than one patch.

7. Close the browser window.
8. Stop the file server in the CLI by pressing Enter, as shown in Figure 3-45.

```
Press ENTER to stop the file server.

Stopping process

Register patch files in the directory:
SqlGuard-9.0p9997.tgz.enc
Register succeeded
ok
maple.itso.ibm.com>
```

Figure 3-45 Patch upload is completed

9. Review the list of available patches by running the following command (Figure 3-46):

   `show system patch available`

```
maple.itso.ibm.com> show system patch available

Attempting to retrieve the patch information. It may take time.
Please wait.

P#      Description                                    Version
Md5sum                                Dependencies
9997    Health Check for GPU and Upgrade installation 9.0
d44e31151bd670e527 0c7703004d25e1
ok
```

Figure 3-46 List patches that were uploaded to the appliance

10. Install uploaded patches by using the following command and follow the prompts (Figure 3-47 on page 67):

    `store system patch install sys`

```
maple.itso.ibm.com> store system patch install sys

The backup profile is not set for saving the backup file if patch
installation fails.
If you want to save the backup file, please answer "NO" to the
question and run CLI command "store backup profile" to set up the
parameters.
Do you want to continue (yes or no)? yes

List the files in the patches directory:

1. SqlGuard-9.0p9997.tgz.enc

Please choose patches to install (1-1, or multiple numbers
separated by ",", or q to quit): 1
Install item 1

Patch has been submitted, and will be installed according to the
request time, please check installed patches report or CLI (show
system patch installed).

Please don't forget to remove your media if necessary.
ok
```

Figure 3-47 Install a manually uploaded patch

Note: You can schedule the installation of several patches by entering multiple patch numbers, such as 1, 2, 3. The patches will be installed in the specified order.

11. Monitor the patch installation progress by running the following command (Figure 3-48):

show system patch installed

```
maple.itso.ibm.com> show system patch installed
P#      Who       Description                     Request Time
Status
50      CLI       Guardium Patch Update (GPU) for 2014-09-02 04:38:00
DONE: Patch installation Succeeded.
9997    CLI       Health Check for GPU and Upgrad 2014-09-02 06:45:54
DONE: Patch installation Succeeded.
ok
```

Figure 3-48 Patch installation is completed

Note: The patch installation of Guardium Patch Updates (GPU) might take time.

12. Repeat the steps until all prerequisite patches are installed, as shown in Figure 3-49.

```
maple.itso.ibm.com> show system patch installed
P#      Who       Description                     Request Time
Status
50      CLI       Guardium Patch Update (GPU) for 2014-09-02 04:38:00
DONE: Patch installation Succeeded.
9997    CLI       Health Check for GPU and Upgrad 2014-09-02 06:45:54
DONE: Patch installation Succeeded.
200     CLI       Guardium Patch Update (GPU) for 2014-09-02 06:51:18
DONE: Patch installation Succeeded.
1033    CLI       Patch 1 for Optim Capture and R 2014-09-02 07:26:05
DONE: Patch installation Succeeded.
3990    CLI       Pre-req to setup Aux server     2014-09-02 07:35:57
DONE: Patch installation Succeeded.
ok
```

Figure 3-49 All prerequisite patches are installed

Note: During the installation of GPU 200, the appliance is automatically restarted.

You can now designate the appliance as a main Workload Replay appliance or an auxiliary Workload Replay appliance. For details, see 3.5, “Installing a main Workload Replay appliance” on page 68 and 3.6, “Installing an auxiliary Workload Replay appliance” on page 71.

3.5 Installing a main Workload Replay appliance

In our example deployment plan, we designated `maple.itso.ibm.com` as the main Workload Replay appliance that handles DB2 for z/OS workloads.

The installation process for a main Workload Replay appliance consists of a single step that installs the InfoSphere Workload Replay software, which is delivered and installed like the prerequisites as an InfoSphere Guardium patch.

Note: Installation of the InfoSphere Workload Replay software fails if the prerequisite patches are not installed.

To install the current InfoSphere Workload Replay patch, which is at the time of writing V2.1.0.1, follow the patch installation process, described in 3.4, “Preparing for the InfoSphere Workload Replay software installation” on page 56.

Important: Unless explicitly stated otherwise, in the patch documentation, InfoSphere Workload Replay patches are cumulative. Therefore, you do not need to install Version 2.1 before you install Version 2.1.0.1 (or later versions, as they become available.)

To designate the appliance as a main Workload Replay server, install the patch `SqlGuard-9.0p3423_WorkloadReplay_Install_2014_08_06_20_49.tgz.enc` by using the instructions in 3.4, “Preparing for the InfoSphere Workload Replay software installation” on page 56 or by following the instructions in 7.6.3, “Installing maintenance on an appliance” on page 262.

On completion, the successfully installed patch list looks similar to the list in Figure 3-50.

```
maple.itso.ibm.com> show system patch installed
P#      Who       Description                     Request Time
Status
50      CLI       Guardium Patch Update (GPU) for 2014-09-02 04:38:00
DONE: Patch installation Succeeded.
9997    CLI       Health Check for GPU and Upgrad 2014-09-02 06:45:54
DONE: Patch installation Succeeded.
200     CLI       Guardium Patch Update (GPU) for 2014-09-02 06:51:18
DONE: Patch installation Succeeded.
1033    CLI       Patch 1 for Optim Capture and R 2014-09-02 07:26:05
DONE: Patch installation Succeeded.
3990    CLI       Pre-req to setup Aux server     2014-09-02 07:35:57
DONE: Patch installation Succeeded.
3423    CLI       IOWR Install 2.1.348 2014_08_06 2014-09-02 08:02:00
DONE: Patch installation Succeeded.
ok
```

Figure 3-50 InfoSphere Workload Replay server software installed on main appliance

Note: You can redesignate a main Workload Replay appliance as an auxiliary appliance by uninstalling InfoSphere Workload Replay (but not the prerequisite patches) and by following the installation instructions in 3.6, “Installing an auxiliary Workload Replay appliance” on page 71.

3.5.1 Verifying the installation

Use the following steps to verify that the software installation completed successfully:

1. Log in to the CLI of the appliance as an administrator by using the `cli` account.
2. Issue the following CLI command and verify that `Sink` is listed (Figure 3-51):

   `show unit type`

```
maple.itso.ibm.com> show unit type
Standalone Netinsp Sink stap
ok
```

Figure 3-51 Display the appliance unit type to verify a successful installation

> **Note:** InfoSphere Workload Replay cannot capture any workloads unless the unit type is configured correctly. If `Sink` is not listed, run the following commands:
>
> **`store unit type sink`**
> **`restart inspection-core`**
>
> Then, run the **`show unit type`** command to verify the change.

3. Open the InfoSphere Workload Replay web console by directing your browser to `https://guardium_hostname_or_ip:8443/dsweb/console/ocr/index.jsp`. The IBM InfoSphere Optim Workload Replay Log In panel opens, as shown in Figure 3-52.

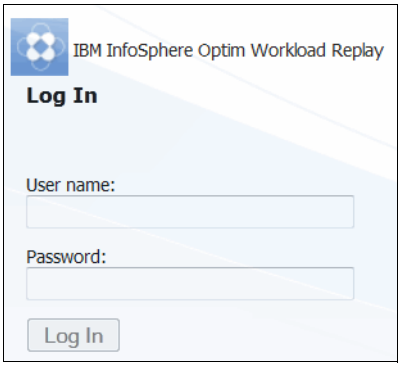


Figure 3-52 The Workload Replay web console login panel

> **Note:** You must implement a security policy first before you can log on to the Workload Replay web console. To enforce the separation of duties, the `admin` and `accessmgr` Guardium accounts cannot access this interface.

3.5.2 Implementing a main appliance security policy

A security policy governs the users that can access the three secured interfaces that provide access to this main appliance.

During the InfoSphere Guardium installation, a set of default users (`admin`, `accessmgr`, and `cli`) is created, several of which you use to install and configure the product. We suggest that you create additional accounts that are used for day-to-day operations by employees with the administrator or security administrator role.

No default Workload Replay accounts are created during the product installation.

Implement the initial security policy for the appliance. For details about how to customize account settings and create accounts for employees with the administrator, security administrator, privileged user, or user role on the appliance, see 7.1, “Access management” on page 214.

3.6 Installing an auxiliary Workload Replay appliance

In our example deployment, we designated `oak.itso.ibm.com` as an auxiliary Workload Replay appliance to `maple.itso.ibm.com`.

The installation process for an auxiliary Workload Replay appliance consists of two steps that designate this appliance as an auxiliary and install the InfoSphere Workload Replay software.

> **Note:** Installation of the InfoSphere Workload Replay software fails if the prerequisite patches are not installed.

We use the following steps to designate the appliance as an auxiliary Workload Replay appliance to `maple.itso.ibm.com`:

1. Log in to the CLI of the appliance as an administrator by using the `cli` account.
2. Run the following CLI command:

   `store ocr_aux_controller ocr_server_IP <guardium_ip>`

   Replace ***<guardium_ip>*** with the IP address of the main Workload Replay appliance to associate `oak.itso.ibm.com` with main Workload Replay server `maple.itso.ibm.com`, as shown in Figure 3-53.

```
oak.itso.ibm.com> store ocr_aux_controller ocr_server_IP 9.12.5.27
The auxiliary server configuration completed.
Software tracing has been enabled.
ok
```

Figure 3-53 Associate oak.itso.ibm.com with maple.itso.ibm.com

> **Note:** If you do not yet know the IP address of your main server, enter any valid IPv4 address. You can change the IP address after the installation by reissuing the same command. You must stop and start the controller after you change the IP address of the main server by running the CLI command **`stop ocr_aux_controller`** followed by the **`start ocr_aux_controller`** command.

3. Install the patch `SqlGuard-9.0p3423_WorkloadReplay_Install_2014_08_06_20_49.tgz.enc` by using the instructions in 3.4, “Preparing for the InfoSphere Workload Replay software installation” on page 56 or follow the instructions in 7.6.3, “Installing maintenance on an appliance” on page 262.

   On completion, the installed patch list looks similar to the list that is shown in Figure 3-54 on page 73.

```
oak.itso.ibm.com> show system patch installed
P#      Who       Description                     Request Time
Status
50      CLI       Guardium Patch Update (GPU) for 2014-08-28 09:37:31
DONE: Patch installation Succeeded.
9997    CLI       Health Check for GPU and Upgrad 2014-09-02 09:11:56
DONE: Patch installation Succeeded.
200     CLI       Guardium Patch Update (GPU) for 2014-09-02 09:14:20
DONE: Patch installation Succeeded.
1033    CLI       Patch 1 for Optim Capture and R 2014-09-02 10:01:15
DONE: Patch installation Succeeded.
3990    CLI       Pre-req to setup Aux server     2014-09-02 10:09:34
DONE: Patch installation Succeeded.
3423    CLI       IOWR Install 2.1.348 2014_08_06 2014-09-02 10:21:03
DONE: Patch installation Succeeded.
ok
```

Figure 3-54 InfoSphere Workload Replay server software installed successfully on the auxiliary appliance

Note: You can redesignate an auxiliary Workload Replay appliance as a main Workload Replay appliance by uninstalling InfoSphere Workload Replay (but not the prerequisite patches) and following the installation instructions in 3.5, “Installing a main Workload Replay appliance” on page 68.

3.6.1 Verifying the installation

Use the following steps to verify that the software installation completed successfully:

1. Log in to the CLI of the appliance as an administrator by using the `cli` account.
2. Issue the following CLI command (Figure 3-55) to verify that `Sink` is listed:

   `show unit type`

```
oak.itso.ibm.com> show unit type
Standalone Netinsp Sink stap
ok
```

Figure 3-55 Display the unit type to validate successful installation

> **Note:** InfoSphere Workload Replay cannot capture any workloads unless the unit type is configured correctly. If `Sink` is not listed, run the following commands:
>
> ```
> store unit type sink
> restart inspection-core
> ```
>
> Then, run the **`show unit type`** command to verify the change.

Unlike the main Workload Replay appliances, the Workload Replay web console does not run on the auxiliary Workload Replay appliances. Use the following steps to verify that this auxiliary Workload Replay appliance is successfully connected to its designated main Workload Replay appliance:

1. Direct your web browser to the Workload Replay web console of the designated main Workload Replay appliance:

   `https://`*`guardium_hostname_or_ip`*`:8443/dsweb/console/ocr/index.jsp`

   The login window is displayed.

   > **Note:** You must implement a security policy on the main Workload Replay appliance first before you can log on to the Workload Replay web console. To enforce the separation of duties, the `admin` and `accessmgr` Guardium accounts do not have access to this interface.

2. Log in by using the account of a privileged user or user.
3. Open the System Status page by navigating to **Open** → **Administration** → **System Status**, as shown in Figure 3-56.

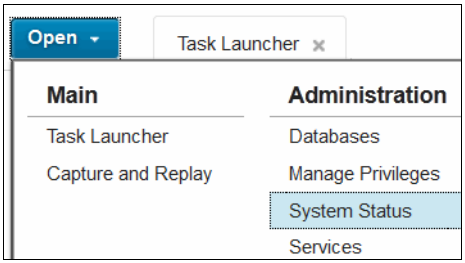


Figure 3-56 Validate the auxiliary Workload Replay appliance connected successfully

4. The System Status page displays the auxiliary Workload Replay appliances that are currently connected to the main Workload replay appliance, as shown in Figure 3-57.

Main workload replay server:

Host Name	IP Address	Version
maple.itso.ibm.com	9.12.5.27	2.1.348

Workload replay controllers:

Host Name	IP Address	Type	ID	Status
maple.itso.ibm.com	9.12.5.27	Controller for auxiliary server	1451365446	Connected
oak.itso.ibm.com	9.12.5.104	Controller for auxiliary server	1451375097	Connected

Figure 3-57 The auxiliary appliance oak.itso.ibm.com is connected

Note: A main Workload Replay appliance also acts as an auxiliary Workload Replay appliance. Therefore, an additional entry is shown for the main appliance if the required services are running.

3.6.2 Implementing an auxiliary appliance security policy

A security policy governs who can access the three secured interfaces that provide access to this auxiliary appliance. During the InfoSphere Guardium installation, a set of default users (`admin`, `accessmgr`, and `cli`) is created, several of which are used to install and configure the product. We suggest that you create additional accounts that are used for day-to-day operations by employees with the administrator or security administrator role.

No default Workload Replay accounts are created during the product installation.

Implement the initial security policy for the appliance. For details about how to customize account settings and create accounts for employees with the administrator, security administrator, and privileged user roles on the appliance, see 7.1, “Access management” on page 214.

Note: Employees with the user role do not require access to auxiliary Workload Replay appliances because no Workload Replay web console is running on this appliance type.

4

IBM InfoSphere Optim Workload Replay for DB2 for z/OS installation and configuration

This chapter provides instructions to install and customize the IBM InfoSphere Optim Workload Replay for DB2 for z/OS (InfoSphere Workload Replay for DB2 for z/OS) components that are installed on the z/OS system. This chapter also provides instructions to enable InfoSphere Workload Replay for DB2 for z/OS in the Workload Replay web console.

4.1 Overview

InfoSphere Workload Replay for DB2 for z/OS has program number 5655-O18. To install InfoSphere Workload Replay for DB2 for z/OS, the following software must be available:

- IBM z/OS, V1.12 (5694-A01), or later; or IBM z/OS, V2.1 (5650-ZOS), or later
- IBM SMP/E for z/OS V3.5 (5655-G44), or later
- IBM InfoSphere Optim Workload Replay for DB2 for z/OS, V2.1 (5655-O18)
- IBM DB2 Data Access Common Collector for z/OS, V1.1 (5639-OLC)
- IBM Tools Base for z/OS, V1.4 (5655-V93) (optional)

If all of the required software is not installed, see A.1.1, “Downloading InfoSphere Workload Replay for DB2 for z/OS installation media” on page 302.

The first part of the installation is to run the SMP/E steps, which are described in the following program directories:

- *Program Directory for IBM InfoSphere Optim Workload Replay for DB2 for z/OS*, GI10-8980-00
- *Program Directory for IBM DB2 Data Access Common Collector for z/OS*, GI10-8973-01
- *IBM InfoSphere Guardium S-TAP for DB2 on z/OS*, GI13-2067-02

For the remainder of this chapter, we assume that the SMP/E installation steps as described in the program directories are complete, so the SMP/E installation steps are not described in this chapter.

IBM Tools Customizer for z/OS can be used to assist in the customization and deployment of InfoSphere Workload Replay for DB2 for z/OS. Because you only need to complete a few customization tasks, in our deployment example, we show how to manually customize the necessary jobs and files. For more information about the Tools Customizer, see Tools Customizer for z/OS in the IBM Knowledge Center at the following web address:

http://www.ibm.com/support/knowledgecenter/SSS8US_1.3.0/com.ibm.db2tools.ccq.doc.ug/topics/ccq_home.htm?lang=en

The instructions in this chapter assume that you successfully installed and configured at least one InfoSphere Workload Replay appliance, as described in Chapter 3, “Installing and configuring IBM InfoSphere Optim Workload Replay appliances” on page 41.

During the initial deployment planning in 2.4.1, “Planning DB2 for z/OS deployments” on page 28, we created a deployment plan for the production and test environments. After deployment is complete, workloads can be captured and replayed in those environments.

For the book environment, the production environment is a DB2 for z/OS V11.1 two member (D1J1 and D1J2) data sharing group on LPARs `wtsc61.itso.ibm.com` and `wtsc62.itso.ibm.com`. The data sharing group name and location alias for the capture data sharing group is `DB1J`. The test environment is a DB2 for z/OS V11.1 two member (D1K1 and D1K2) data sharing group on LPARs `wtsc61.itso.ibm.com` and `wtsc62.itso.ibm.com`. The data sharing group name and location alias for the replay data sharing group is `DB1K`.

Figure 4-1 depicts the book environment before the database server components are installed. Both Workload Replay appliances have no connectivity to the database servers.

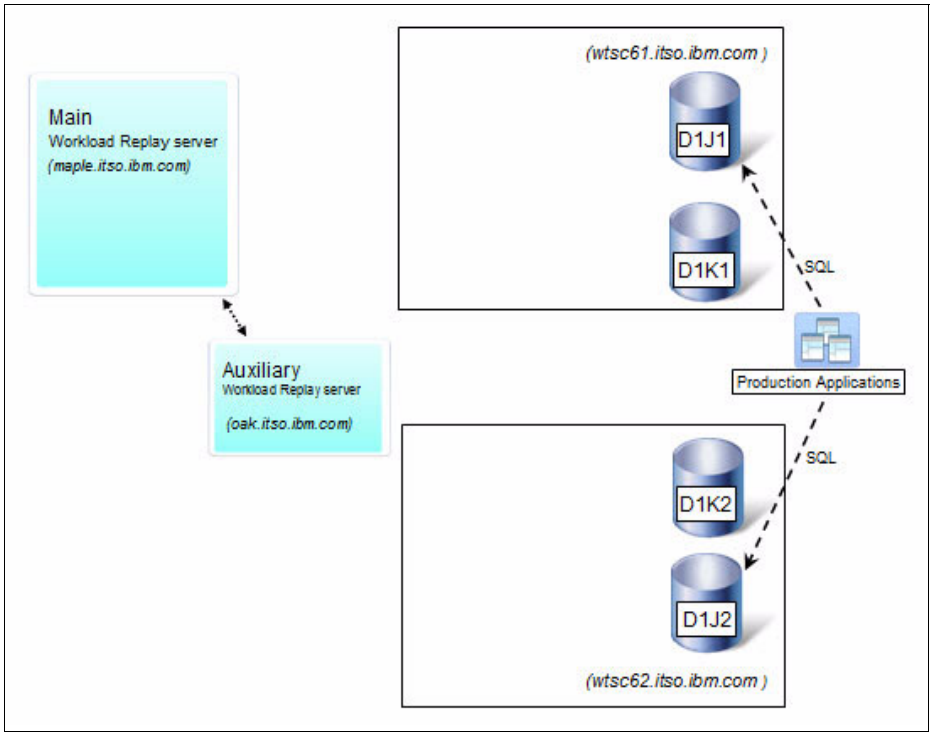


Figure 4-1 Book environment before the z/OS components are installed and configured

Figure 4-2 depicts the book environment after the installation and configuration are complete for both the InfoSphere Workload Replay S-TAP for DB2 for z/OS (S-TAP) and the IBM Workload Replay Controller for z/OS (Workload Replay Controller). Although Figure 4-2 shows the S-TAPs monitoring the DB2 members and sending traffic to the main and auxiliary Workload Replay appliances, the S-TAPs are only started when a capture or replay is actively running.

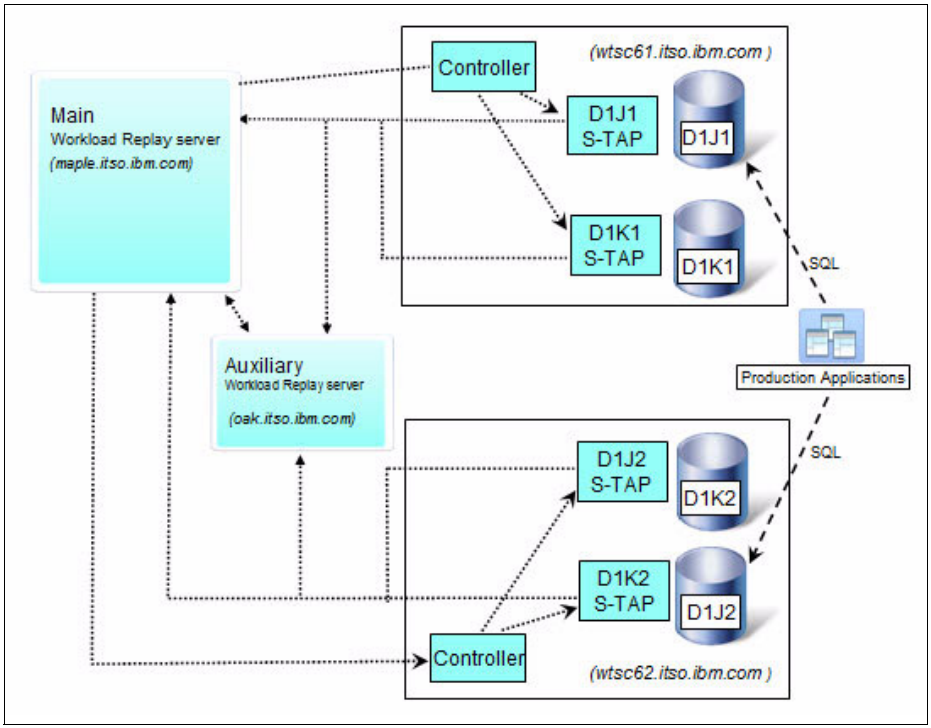


Figure 4-2 Book environment after the z/OS components are installed and configured

The InfoSphere Workload Replay for DB2 for z/OS installation and configuration tasks that are covered in this chapter are grouped into the following sections:

- General z/OS setup
- InfoSphere Workload Replay S-TAP for DB2 for z/OS
- Workload Replay Controller for DB2 for z/OS (CQZSERV)
- Enablement of workload capture and replay in the Workload Replay web console

4.2 General z/OS setup

This section covers the general z/OS setup and configuration tasks that are associated with the deployment of the components of InfoSphere Workload Replay for DB2 for z/OS. These tasks include the creation and association of user IDs to the started tasks that will run on z/OS, and the creation of the UNIX System Services directories that will be used by the z/OS components of InfoSphere Workload Replay for DB2 for z/OS.

4.2.1 Protected user for S-TAP

You must create a protected user ID that runs the started task for InfoSphere Workload Replay S-TAP for DB2 for z/OS. Although this step is not required, we suggest associating the new protected user ID with a security group ID that is created specifically for InfoSphere Workload Replay for DB2 for z/OS. By using a dedicated security group ID, the management of the UNIX System Services file permissions is easier. For the book environment, we created the `STAPUSR` user and associated the new user ID with the group ID `OWRSYS`. The user ID must have the following authorities and permissions:

- Permission to start InfoSphere Workload Replay S-TAP for DB2 for z/OS processes.
- Read access to the SFECLOAD, SCQCLOAD, and SCQRLOAD data sets.
- Read access to the DB2 SDSNEXIT and SDSNLOAD data sets.
- Permission to implicitly start the secondary address space for InfoSphere Workload Replay S-TAP for DB2 for z/OS.
- Read access to directories and files in the Workload Replay Controller for the z/OS working directory. The default directory is `/var/ioqcr`. For instructions to create the directory, see “Workload Replay Controller for z/OS working directory” on page 83.
- Read access to the directories and files on the `cr_installation_directory` file system. The default directory is `/usr/lpp/ioqcrv2r1`.
- IBM RACF® permission to connect to DB2.
- Authorization to add modules dynamically to Link Pack Area (LPA), CSVDYLPA. For details, see 4.3.2, “Running the installation jobs” on page 89.

4.2.2 Protected user ID to run the started task for Workload Replay Controller for z/OS (CQZSERV)

You must create a protected user ID to run the started task for Workload Replay Controller for z/OS. Although this step is not required, we suggest associating the new protected user ID with a security group ID that is created specifically for InfoSphere Workload Replay for DB2 for z/OS. By using a dedicated security group ID, management of the UNIX System Services file permissions is easier. For the book environment, we created the `CQZUSR` user and associated the new user ID with the group ID `OWRSYS`. The user ID must have the following authorities and permissions:

- Read access to the SFECLOAD, SCQCLOAD, and SCQRLOAD data sets.
- Read access to the DB2 SDSNEXIT, SDSNLOAD, and SDSNLOD2 data sets.
- Read access to the directories and files on the `cr_installation_directory` file system. The default directory is `/usr/lpp/ioqcrv2r1`.
- Read access to the directories and files in the Workload Replay Controller for z/OS configuration directory. The default directory is `/etc/ioqcr`. For instructions to create the directory, see “Workload Replay Controller for z/OS configuration directory” on page 82.
- Read/write access to directories and files in the Workload Replay Controller for z/OS working directory. The default directory is `/var/ioqcr`. For instructions to create the directory, see “Workload Replay Controller for z/OS working directory” on page 83.
- RACF permission to connect to DB2.

4.2.3 Creating directories in the UNIX System Services file system

The Workload Replay Controller for z/OS requires the creation of two directories in the UNIX System Services file system. The first required directory is used to store the InfoSphere Workload Replay configuration files. The second required directory is used by the Workload Replay Controller for z/OS as a working directory for temporary work files.

Workload Replay Controller for z/OS configuration directory

The Workload Replay Controller for z/OS configuration directory is used to store the files that contain the InfoSphere Workload Replay for DB2 for z/OS configuration information.

The Workload Replay Controller for z/OS configuration directory likely contains only a few small files, so you do not need to consider any special allocations or sizes. The protected user ID, which is `CQZUSR` in our case, that is created for the Workload Replay Controller for z/OS started task must have Read access to the InfoSphere Workload Replay for DB2 for z/OS configuration directory. We suggest that the owner of the directory is the user ID, which is `CQZUSR` in our case, that is created for the Workload Replay Controller for z/OS started task. The InfoSphere Workload Replay for DB2 for z/OS configuration directory will not contain any sensitive data, so the directory permissions can be set to `755`.

The InfoSphere Workload Replay for DB2 for z/OS configuration directory must be created manually. The default for the InfoSphere Workload Replay for DB2 for z/OS configuration directory is `/etc/ioqcr`. You can use a different directory. In a z/OS sysplex environment, we suggest that you create a system-specific Workload Replay Controller for z/OS configuration directory for each of the LPARs in your sysplex.

The book environment is a z/OS sysplex with two LPARs (`SC61` and `SC62`) so we created system-specific Workload Replay Controller for z/OS configuration directories as `/SC61/etc/ioqcr` and `/SC62/etc/ioqcr`.

Workload Replay Controller for z/OS working directory

The Workload Replay Controller for z/OS working directory is used for temporary work files, temporary message logs, trace files (optional), and the policy files that are used by S-TAP for filtering.

Because the Workload Replay Controller for z/OS working directory is used by the product for workload-related files that can vary in both size and content, these factors must be considered when you create the working directory. In addition, the temporary workload-related files might contain sensitive workload data; therefore, access to the working directory needs to be limited to only allow the required product user IDs.

The protected user ID, which is `CQZUSR` in our case, that is created for the Workload Replay Controller for z/OS started task must have Read/write access to the working directory. The protected user ID, which is `STAPUSR` in our case, that runs the started task for InfoSphere Workload Replay S-TAP for DB2 for z/OS must have Read access to this working directory. We suggest that the owner of the directory is the user ID, which is `CQZUSR` in our case, that is used for the Workload Replay Controller for z/OS started task.

We also suggest that the owning group for the directory is a group ID, such as OWRSYS, that only contains privileged started task user IDs (CQZUSR and STAPUSR). The Workload Replay Controller for z/OS working directory permissions need to be set to limit access to only the authorized CQZUSR and STAPUSR users. If the Workload Replay Controller for z/OS working directory is created with the owner user ID CQZUSR and the owning group ID OWRSYS, the directory permissions can be set to 750.

The Workload Replay Controller for z/OS working directory must be created manually. The default for the Workload Replay Controller for z/OS working directory is /var/ioqcr. You can use a different directory. In a z/OS sysplex environment, we suggest that you create a system-specific Workload Replay Controller for z/OS working directory for each of the LPARs in your sysplex.

The book environment is a z/OS sysplex with two LPARs (SC61 and SC62) so we created system-specific Workload Replay Controller for z/OS configuration directories as /SC61/var/ioqcr and /SC62/var/ioqcr.

To create a directory in the UNIX System Services file system, use the following command:

```
mkdir name_of_dir
```

The user ID for Workload Replay Controller for z/OS must be the owner of the directory or must be a member of the group that is assigned to the directory. If CQZUSR is not the owner but is getting access through the group, the file permissions must be 770 for CQZSERV to write to the directory.

Use the following command to change the owner and group of the directory:

```
chown user:group name_of_dir
```

To change the permission to 750, use the following command:

```
chmod 750 name_of_dir
```

Figure 4-3 shows how to issue these commands from a Secure Shell (SSH) client.

```
WJCRES5 @ SC61:/u/wjcres5> cd /SC61/var
WJCRES5 @ SC61:/SC61/var> mkdir ioqcr
WJCRES5 @ SC61:/SC61/var> chown cqzusr:owrsys ioqcr
WJCRES5 @ SC61:/SC61/var> chmod 750 ioqcr
WJCRES5 @ SC61:/SC61/var> ls -dal ioqcr
drwxr-x---   2 CQZUSR   OWRSYS       256 Oct 10 12:45 ioqcr
WJCRES5 @ SC61:/SC61/var> _
```

Figure 4-3 Sample of how to create the /var/ioqcr directory

4.2.4 Authority to dynamic LPA

The user ID for the S-TAP started task must have the authorization to add modules dynamically to the link pack area (LPA). This is controlled by the RACF general resource FACILITY profile class. To define the profile and assign the started task user ID `STAPUSR` to the profile, run the following RACF commands:

```
RDEFINE FACILITY CSVDYLPA.ADD.CQRA UACC(NONE)
SETROPTS GENERIC(FACILITY)
PERMIT CSVDYLPA.ADD.CQRA CLASS(FACILITY) ID(STAPUSR) ACCESS(UPDATE)
SETROPTS RACLIST(FACILITY) REFRESH
```

For more information about RACF, see the IBM z/OS Knowledge Center at the following web address:

http://www.ibm.com/support/knowledgecenter/SSLTBW_2.1.0/com.ibm.zos.v2r1/zos-v2r1-home.html?lang=da

4.2.5 Authorized program facility (APF) authorization of data sets

As part of the SMP/E installation, verify that the following library data sets are authorized program facility (APF)-authorized:

- SCQCLOAD
- SCQRLOAD
- SFECLOAD

> **Note:** Use the IBM MVS™ command **`D PROG, APF`** to display data sets that are currently APF-authorized.

Verify that the DB2 and the following required library data sets have APF authority:

- SDSNLOAD
- SDSNLOD2
- SCEERUN

Validate that the required executable file and library on the file system in UNIX System Services have APF authority:

- `installation_dir/bin/ocrserver`
- `installation_dir/lib/libioqcrcqzzos.so`
- `installation_dir/lib/llibdb2jcct2zos4.so`
- `installation_dir/lib/llibdb2jcct2zos4_64.so`

The `installation_dir` is the installation directory path in UNIX System Services that is created by the installation job `CQRISMKD` that is run as part of the SMP/E installation. The default installation directory path is `/usr/lpp/ioqcrv2r1`.

Log in to UNIX System Services either through OMVS or by using an SSH client, such as PuTTY. Navigate to the `bin` directory, which is a subdirectory of the installation directory. The default path to the bin directory is `/usr/lpp/ioqcrv2r1/bin`. Figure 4-4 shows the use of the **`ls -E`** command to list the extended attributes of the files. Verify that the flags **`a`** and **`s`** are set.

```
WJCRES5 @ SC61:/u/wjcres5>cd /usr/lpp/ioqcrv2r1/bin
WJCRES5 @ SC61:/pp/ioqcrv2r1/bin>ls -E
total 256
drwxr-xr-x        2 HAIMO    SYS1        8192 Aug  7 14:13 IBM
-rwxr-xr-x  a-s-  2 HAIMO    SYS1      114688 Aug  7 14:13 ocrserver
WJCRES5 @ SC61:/pp/ioqcrv2r1/bin>_
```

Figure 4-4 Verify the extended attributes of the files in bin

Navigate to the `/usr/lpp/ioqcrv2r1/lib` directory and use the **`ls -E`** command to list the extended attributes of the files. Verify that the flags **`a`** and **`s`** are set for all files. See Figure 4-5.

```
WJCRES5 @ SC61:/pp/ioqcrv2r1/bin>cd ../lib
WJCRES5 @ SC61:/pp/ioqcrv2r1/lib>ls -E
total 3264
drwxr-xr-x        2 HAIMO    SYS1        8192 Aug  7 14:13 IBM
-rwxr-xr-x  a-s-  2 HAIMO    SYS1      704512 Aug  7 14:13 libdb2jcct2zos4.so
-rwxr-xr-x  a-s-  2 HAIMO    SYS1      806912 Aug  7 14:13 libdb2jcct2zos4_64.so
-rwxr-xr-x  a-s-  2 HAIMO    SYS1      118784 Aug  7 14:13 libioqcrcqzzos.so
WJCRES5 @ SC61:/pp/ioqcrv2r1/lib>_
```

Figure 4-5 Verify the extended attributes of the files in lib

4.3 InfoSphere Workload Replay S-TAP for DB2 for z/OS

This section describes how to configure and run InfoSphere Workload Replay S-TAP for DB2 for z/OS.

4.3.1 Customize InfoSphere Workload Replay S-TAP for DB2 for z/OS

All the members in the SCQRSAMP data set are used to customize the InfoSphere Workload Replay S-TAP for DB2 for z/OS.

Table 4-1 on page 87 shows the members of SCQRSAMP.

Table 4-1 Members of SCQRSAMP

Member	Description
CQR#CTLF	Define each subsystem or data sharing member to S-TAP.
CQRBIND	Bind the S-TAP plan and packages for subsystem or data sharing group.
CQRCNTFL	Define the VSAM control file for S-TAP.
CQREMAC1	ISPF Edit Macro to customize S-TAP.
CQRMSTR	Started task procedure that can be used to stop the InfoSphere Workload Replay S-TAP for DB2 for z/OS.
CQRPARMS	S-TAP parameters for each subsystem or member of data sharing group.
CQRPROC	S-TAP started task, one per subsystem or member of data sharing group.

To make the manual customization of the InfoSphere Workload Replay S-TAP for DB2 for z/OS easier, an ISPF Edit Macro `CQREMAC1` is delivered as part of the SCQRSAMP data set.

Table 4-2 shows the CQREMAC1 customization variables with sample values that are used for the book environment DB2 data sharing member `D1J1`.

Table 4-2 CQREMAC1 customizing variables and sample values

Variable	Sample value	Description
#DB2S#	`D1J1`	The DB2 subsystem ID.
#USER#	`STAPUSR`	User ID for S-TAP.
#PORT#	`16016`	IP port number for the main Workload Replay appliance.
#MSTR#	`CQRMSTR`	Name of the S-TAP master address space.
#SRVR#	`9.12.5.27`	IP address of the main Workload Replay appliance (`maple.itso.ibm.com`).
#CQRPARMS#	`CQR.PARMLIB(D1J1OWR)`	Name of parameter member for S-TAP.
#CQRSCLS#	`SCCOMP`	DFSMS Storage class.

Variable	Sample value	Description
#CQRHILVL#	CQR	High-level qualifier (HLQ) for the CQR data sets.
#FECHILVL#	FEC	HLQ for the FEC data sets.
#CQCHILVL#	CQC	HLQ for the CQC data sets.
#SDSNLOAD#	DB1JT.SDSNLOAD	Name of the SDSNLOAD data set.
#DB2LIB1#	DB1JT.SDSNEXIT	Name of the SDSNEXIT data set.
#DB2LIB2#	DB1JT.SDSNLOAD	Name of the SDSNLOAD data set.
#DB2LIB3#	DB2LIB3	Name of other DB2 data set.
#DB2LIB4#	DB2LIB4	Name of other DB2 data set.
#DB2LIB5#	DB2LIB5	Name of other DB2 data set.
#CQRPLAN#	CQRPLAN	Name of the plan that is used by S-TAP.
#ZPARM#	D1J1PARM	Name of the DSNZPARM member for the subsystem.
#BSDS1#	DB1JD.D1J1.BSDS01	Name of BSDS01 data set.
#BSDS2#	DB1JD.D1J1.BSDS02	Name of BSDS02 data set.
#DB2PARMS#	CQR.STAP.CONTROL	Name of VSAM data set that contains subsystem definitions for S-TAP.
#CQRPLCY#	'/var/ioqcr/D1J1POLICYFILE.xml'	File name of the S-TAP filter policy file. The referenced file is created dynamically by the Workload Replay Controller for z/OS when a capture or replay is run. This file name must be set to a value of *<Workload Replay Controller for z/OS working directory>/<DB2 Subsystem ID>*POLICYFILE.xml. The path name is case sensitive.

CQREMAC1 must be customized and saved in a data set that is allocated to the SYSPROC DDNAME to be invoked.

Edit each of the members in the SCQRSAMP and run the CQREMAC1 ISPF Edit Macro to customize them.

4.3.2 Running the installation jobs

The following three members in SCQRSAMP contain jobs that must be customized and then run:

- CQRCNTFL
- CQR#CTLF
- CQRBIND

Sample member CQRCNTFL

The CQRCNTFL job defines the S-TAP VSAM control data set that contains information about each DB2 subsystem or member of a Data Sharing group. We suggest that you define one control data set for each of the levels of environments, for example, production, quality assurance, and test.

Sample member CQR#CTLF

The CQR#CTLF job contains the control statements to update the S-TAP VSAM control data set with information of each DB2 subsystem or member of a data sharing group. CQR#CTLF also contains samples of control statements to maintain the information in the S-TAP VSAM control data set. Example 4-1 shows the CQR#CTLF JCL that is customized for the book environment `D1J1` data sharing member.

Example 4-1 CQR#CTLF JCL

```
//CQR@CTLF JOB (999,POK),'SCQR WORK',CLASS=A,MSGCLASS=T,
// REGION=0M,TIME=NOLIMIT,NOTIFY=&SYSUID TYPRUN=HOLD
/*JOBPARM L=9999,SYSAFF=SC61
//*
//*******************************************************************
//*                                                                 *
//* Licensed Materials - Property of IBM                            *
//* 5655-018                                                        *
//* © Copyright IBM Corp. 2011, 2013 All Rights Reserved.           *
//* © Copyright Rocket Software, Inc. 2011-2013 All Rights Reserved. *
//* US Government Users Restricted Rights - Use, duplication or     *
//* disclosure restricted by GSA ADP Schedule Contract with IBM Corp. *
//*                                                                 *
//* DESCRIPTION: THIS JCL IS USED TO MANAGE ENTRIES IN THE DB2PARMS *
//*              DATASET.                                           *
//*                                                                 *
//*******************************************************************
//*
//STEP1   EXEC PGM=CQR#CTLF,REGION=6M
//STEPLIB  DD DSN=CQR.SCQRLOAD,DISP=SHR
```

```
//         DD DSN=FEC.SFECLOAD,DISP=SHR
//         DD DSN=CQC.SCQCLOAD,DISP=SHR
//DB2PARMS DD DSN=CQR.STAP.CONTROL,DISP=SHR
//*
//* SAMPLE ADD OPERATION
//*
//SYSIN    DD *
    ADD(D1J1)
        BSDS_DSNAME(DB1JD.D1J1.BSDS01)
        BSDS_DSNAME(DB1JD.D1J1.BSDS02)
        ZPARMS_MEMBER(D1J1PARM)
        DB2_LOADLIB(DB1JT.SDSNEXIT)
        DB2_LOADLIB(DB1JT.SDSNLOAD)
        PLAN(CQRPLAN)
//*
//* IF UPDATING PARAMETERS FOR A DB2 SUBSYSTEM IN THE
//*    DB2PARMS CONTROL FILE, ADD THE FOLLOWING KEYWORD
//*    TO THE ADD PARAMETERS:
//*
//*     REPLACE(Y)
//*
//* TO DELETE A DB2 SUBSYSTEM ENTRY FROM THE DB2PARMS
//*    CONTROL FILE, USE THE FOLLOWING PARAMETER:
//*
//* DELETE(D1J1)
//*
```

Sample member CQRBIND

The CQRBIND job binds a package and plan that are used by the S-TAP. This package and plan must be bound for each DB2 subsystem or data sharing group.

Sample member CQRPROC

Member CQRPROC contains a JCL procedure for the S-TAP. This member must be copied to a proclib. We suggest that you copy this procedure to the same proclib where the procedures for the DB2 subsystem are stored.

CQRPROC must be renamed to *ssid*CQR where *ssid* is the DB2 subsystem ID or Data Sharing member ID (not the Data Sharing group name). This procedure is subsystem or member specific and must have CQR as a suffix. Example 4-2 on page 91 shows the customized and renamed CQRPROC JCL for the book environment D1J1 data sharing member.

Example 4-2 CQRPROC after it is renamed

```
//D1J1CQR PROC HILEVEL='CQR',FECLEVEL='FEC',
//   CQCLEVEL='CQC'
//*
//*******************************************************************
//* NAME = CQRPROC                                                  *
//*                                                                 *
//* Licensed Materials - Property of IBM                            *
//* 5655-O18                                                        *
//* © Copyright IBM Corp. 2011, 2013 All Rights Reserved.           *
//* © Copyright Rocket Software, Inc. 2011-2013 All Rights Reserved.  *
//* US Government Users Restricted Rights - Use, duplication or     *
//* disclosure restricted by GSA ADP Schedule Contract with IBM Corp. *
//*                                                                 *
//* DESCRIPTION: THIS JCL IS USED TO START                          *
//*  IBM InfoSphere Optim Workload Replay S-TAP for DB2 for z/OS V2.1 *
//*                                                                 *
//* CAUTION:     YOU WILL HAVE TO MAKE MODIFICATIONS                *
//*              TO THIS JCL PRIOR TO STARTING QUERY CAPTURE        *
//*                                                                 *
//*******************************************************************
//*
//CQRPROC  EXEC PGM=CQR#MAIN,REGION=0M,DYNAMNBR=200,TIME=1440
//STEPLIB  DD DSN=&HILEVEL..SCQRLOAD,DISP=SHR
//         DD DSN=&FECLEVEL..SFECLOAD,DISP=SHR
//         DD DSN=&CQCLEVEL..SCQCLOAD,DISP=SHR
//*
//SYSPRINT DD SYSOUT=*
//CQRLOG   DD SYSOUT=*
//CQRKAFLT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//*
//DB2PARMS DD DSN=CQR.STAP.CONTROL,DISP=SHR
//CQRPARMS DD DSN=CQR.PARMLIB(D1J1OWR),DISP=SHR
//CQRPLCY  DD PATH='/var/ioqcr/D1J1POLICYFILE.xml'
//*
```

The Workload Replay Controller for z/OS automatically starts the CQRPROC procedure when running a capture or replay. After the capture or replay is completed, the Workload Replay Controller for z/OS automatically stops this procedure.

The CQRPARMS DD card specifies the configuration parameters for the S-TAP started tasks. A customized version of the CQRPARMS must be created for each DB2 subsystem or member of a Data Sharing group that will be used for InfoSphere Workload Replay for DB2 for z/OS. We suggest that you name this member *ssid*OWR, for example, where *ssid* is the subsystem ID or member ID of a Data Sharing group. Copy this member to the parmlib that is specified in the value of `#CQRPARMS#` in CQREMAC1.

Example 4-3 shows the customized settings of CQRPARMS for the book environment D1J1 data sharing member.

Example 4-3 CQRPARMS

```
CAPTURE(D1J1)                    -
SUBSYS(D1J1)                     -
MASTER_PROCNAME(CQRMSTR)         -
AUTHID(STAPUSR)                  -
APPLIANCE_PORT(16016)            -
APPLIANCE_SERVER(9.12.5.27)      -
APPLIANCE_PING_RATE(5)           -
APPLIANCE_RETRY_INTERVAL(3)      -
APPLIANCE_CONNECT_RETRY_COUNT(0) -
SEND_FAIL_EVENT_COUNT(100)       -
STAGE1_FILTER(Y)                 -
ZIIP_FILTER(Y)
```

The UNIX System Services hierarchical file system (HFS) file that is specified by the `CQRPLCY DD` is dynamically created by the Workload Replay Controller for z/OS when a capture or replay is run. The file is created in the working directory that is specified in the Workload Replay Controller for z/OS configuration file. We created this working directory in “Workload Replay Controller for z/OS working directory” on page 83. The file name must be specified in this form: *<working directory>/<DB2 Subsystem ID>*`POLICYFILE.xml`. For example, in the book environment, the correct `CQRPLCY DD` file name for the DB2 subsystem `D1J1` is `/var/ioqcr/D1J1POLICYFILE.xml`.

Sample Member CQRMSTR

Member CQRMSTR is a procedure that can be used to stop the InfoSphere Workload Replay S-TAP for DB2 for z/OS Master address space. The name of the InfoSphere Workload Replay S-TAP for DB2 for z/OS Master address space is specified by the `MASTER_PROCNAME` setting in the `CQRPARMS` data set. This Master address space must be shared by the InfoSphere Workload Replay S-TAP for DB2 for z/OS, Query Monitor, and Query Common Collector subsystems that are monitoring the same DB2 subsystem. If the Master address space is shared, it can be stopped only if all InfoSphere Workload Replay S-TAP for DB2 for z/OS, Query Monitor, and Query Common Collector subsystems that use this shared Master address space are stopped.

4.4 Workload Replay Controller for DB2 for z/OS (CQZSERV)

CQZSERV is a started task procedure that is used to run the Workload Replay Controller for z/OS process. The Workload Replay Controller for z/OS performs several functions on the z/OS LPARs to support capturing and replaying workloads. Workload Replay Controller for z/OS starts and stops the S-TAP collectors, and creates local replay dispatchers that are used to replay local DB2 workloads.

4.4.1 Customizing the CQZSERV started task JCL

The sample CQZSERV started procedure JCL is stored in the SCQZSAMP library. This member must be customized and copied to a proclib. We suggest that you copy this procedure to the same proclib where the procedures for the DB2 subsystem are stored.

A sample of the `cqzserv.envvars` file is in the `/usr/lpp/ioqcrv2r1/samples` directory and it can be copied to the directory `/etc/ioqcr/`.

We suggest that the `cqzserv.envvars` file is owned by the user ID for the Workload Replay Controller for z/OS or that this user ID is a member of the group assigned to the file. To change the owner and group of the directory, use the following command:

```
chown user:group name_of_file
```

Figure 4-6 on page 94 shows how to copy the sample `cqzserv.envvars` file to the `/etc/ioqcr/` directory.

```
WJCRES5 @ SC61:/u/wjcres5>cd /usr/lpp/ioqcrv2r1/samples
WJCRES5 @ SC61:/pp/ioqcrv2r1/samples>ls
IBM                     IOQCRSERVER.properties  cqzserv.envvars
WJCRES5 @ SC61:/pp/ioqcrv2r1/samples>cp cqzserv.envvars /etc/ioqcr
WJCRES5 @ SC61:/pp/ioqcrv2r1/samples>cd /etc/ioqcr
WJCRES5 @ SC61:/SC61/etc/ioqcr>chown cqzusr:sys1 cqzserv.envvars
WJCRES5 @ SC61:/SC61/etc/ioqcr>ls -al | grep cqzserv
-rw-r--r--   1 CQZUSR   SYS1         690 Sep 12 09:09 cqzserv.envvars
WJCRES5 @ SC61:/SC61/etc/ioqcr>_
```

Figure 4-6 Copy the sample cqzserv.envvars file to the /etc/ioqcr/ directory

The `cqzserv.envvars` file is used to specify the environmental settings for the Workload Replay Controller for z/OS, such as the HFS installation directory for Workload Replay Controller for z/OS, the installation directory for the JDK, and the configuration directory for the Workload Replay Controller for z/OS. If a 64-bit JDK is installed on your system, we suggest that you uncomment and set the optional **JAVA64_HOME** environmental variable to specify the installation location of the 64-bit JDK. If the **JAVA64_HOME** environmental variable is set, the Workload Replay Controller for z/OS uses a Java 64-bit environment when it replays the local SQL workloads.

> **Note:** The `JAVA_HOME` setting is required. It must point to a 32-bit JDK installation even if you also set the optional **JAVA64_HOME** environmental variable.

The `cqzserv.envvars` file must be updated with installation-specific settings. Example 4-4 shows a sample of the settings in the `cqzserv.envvars` file.

Example 4-4 Sample cqzserv.envvars file

```
IOQCR_HOME=/usr/lpp/ioqcrv2r1
IOQCR_CONFIG_DIR=/etc/ioqcr
JAVA_HOME=/usr/lpp/java160/J6.0

# Optional - If set, specifies directory for Java 64-bit SDK
#JAVA64_HOME=/usr/lpp/java160/J6.0_64

# Disable UNIX System Services Address Space Sharing
_BPX_SHAREAS=NO

# JAVA_DUMP_TDUMP_PATTERN env var specifies the MVS dataset name
pattern used for
# any dynamically allocated transaction dump (TDUMP) files that are
requested.
# Example showing 'CQZSERV' used as the dataset HLQ
```

```
#JAVA_DUMP_TDUMP_PATTERN=CQZSERV.JVM.TDUMP.%job.D%y%m%d.T%H%M%S
# Default
JAVA_DUMP_TDUMP_PATTERN=%uid.JVM.TDUMP.%job.D%Y%m%d.T%H%M%S

# JAVA_DUMP_OPTS="ON<condition>(<agent>,<agent>),
ON<condition>(<agent>,...),...)"
JAVA_DUMP_OPTS="ONERROR(SYSDUMP,JAVADUMP),ONEXCEPTION(SYSDUMP,JAVADUMP)
,ONOUTOFMEMORY(HEAPDUMP,JAVADUMP,SYSDUMP)"
```

When the Workload Replay Controller for z/OS is started, it reads the *filename*.properties configuration in the configuration directory (default: /etc/ioqcr). The *filename* is the required value of the CQZPARM parameter (default: IOQCRSERVER.properties).

A sample of the IOQCRSERVER.properties file is in the /usr/lpp/ioqcrv2r1/samples directory. It can be copied to the /etc/ioqcr/ directory.

We suggest that the IOQCRSERVER.properties file is owned by the user ID for the Workload Replay Controller for z/OS or that this user ID is a member of the group that is assigned to the file.

Figure 4-7 shows how to copy the sample IOQCRSERVER.properties to the /etc/ioqcr/ directory.

```
WJCRES5 @ SC61:/u/wjcres5>cd /usr/lpp/ioqcrv2r1/samples
WJCRES5 @ SC61:/pp/ioqcrv2r1/samples>ls
IBM                     IOQCRSERVER.properties  cqzserv.envvars
WJCRES5 @ SC61:/pp/ioqcrv2r1/samples>cp IOQCRSERVER.properties /etc/ioqcr
WJCRES5 @ SC61:/pp/ioqcrv2r1/samples>cd /etc/ioqcr
WJCRES5 @ SC61:/SC61/etc/ioqcr>chown cqzusr:sys1 IOQCRSERVER.properties
WJCRES5 @ SC61:/SC61/etc/ioqcr>ls -al | grep IOQCRSERVER
-rw-r--r--   1 CQZUSR   SYS1         531 Sep 12 09:17 IOQCRSERVER.properties
WJCRES5 @ SC61:/SC61/etc/ioqcr>_
```

Figure 4-7 Copy the sample IOQCRSERVER.properties to /etc/ioqcr/

The IOQCRSERVER.properties file must be updated with installation-specific settings, such as the IP address of the Workload Replay Controller for z/OS. Example 4-5 on page 96 shows the contents of the book environment Workload Replay Controller for z/OS configuration file, IOQCRSERVER.properties, after customization.

Note: The OCRServerControllerAddress property is set to the IP address for maple.itso.ibm.com, which is the book environment main Workload Replay server appliance.

Example 4-5 Sample IOQCRSERVER.properties

```
# Replace with the Guardium Appliance IP name or address
OCRServerControllerAddress=9.12.5.27

# Server trace level - default is 0
OcrServerTraceLevel=0

# Server trace dir -
OcrServerTraceDir=/var/ioqcr/traces

# Server diag level - default is 0
OcrServerDiagLevel=0

# Server working dir -
OcrServerWorkingDir=/var/ioqcr

# Maximum JVM Heap Size, in Megabytes, for the CQZSERV
# created processes (for example, z/OS local replay dispatcher).
# The supported range is 300 to 1024.
# The default is 700.
#OcrServerMaxJvmHeapSize=700
```

The `OcrServerTraceDir` property in `IOQCRSERVER.properties` specifies the directory where trace files will be written to if tracing is enabled. The default directory is the `/var/ioqcr/traces` directory. The directory setting for `OcrServerTraceDir` can be changed. The directory that is specified for saving traces must be created manually.

The traces might contain sensitive workload data; therefore, limit access to the traces directory to only the required product user IDs and support personnel.

The protected user ID, which is `CQZUSR` in our case, that is created for the Workload Replay Controller for z/OS started task must have Read/write access to the traces directory. We suggest that the owner of the directory is the user ID for the Workload Replay Controller for z/OS started task, which is `CQZUSR` in our case. We also suggest that the owning group for the directory is a group ID that only contains privileged started task user IDs (`CQZUSR` and `STAPUSR`), such as `OWRSYS`. Set the Workload Replay Controller for z/OS working directory permissions to limit access to only the authorized `CQZUSR` user and the `OWRSYS` group. If the Workload Replay Controller for z/OS trace directory is created with the owner user ID `CQZUSR` and the owning group ID `OWRSYS`, the directory permissions can be set to `750`.

Figure 4-8 on page 97 shows samples to create the default `/var/ioqcr/traces` directory.

```
WJCRES5 @ SC61:/u/wjcres5> cd /SC61/var/ioqcr
WJCRES5 @ SC61:/SC61/var/ioqcr> mkdir traces
WJCRES5 @ SC61:/SC61/var/ioqcr> chown cqzusr:owrsys traces
WJCRES5 @ SC61:/SC61/var/ioqcr> chmod 750 traces
WJCRES5 @ SC61:/SC61/var/ioqcr> ls -dal traces
drwxr-x---   2 CQZUSR   OWRSYS       256 Oct 10 13:01 traces
WJCRES5 @ SC61:/SC61/var/ioqcr> ...
```

Figure 4-8 How to create the directory that is used for traces

4.4.2 Starting and stopping CQZSERV

Workload Replay Controller for z/OS does not need to run all the time, but it must be active when you want to use Workload Replay for z/OS to either capture a workload or to replay a workload.

To start the CQZSERV started task procedure, use the MVS start command:

```
s cqzserv
```

When CQZSERV starts, it starts the minimum of two started task procedures, CQZSERV and CQZSERV1, as shown in Figure 4-9.

```
  Display  Filter  View  Print  Options  Search
-------------------------------------------------
SDSF DA SC61      SC61      PAG  0  CPU/L/Z   2/
COMMAND INPUT ===> _
NP    JOBNAME  StepName ProcStep JobID    Owner
      CQZSERV1 STEP1             STC18631 CQZUSR
      CQZSERV  CQZSERV  CQZSERV  STC18647 CQZUSR
```

Figure 4-9 CQZSERV is running

To verify that the Workload Replay Controller for z/OS is running, browse the job log and check the messages at the end to see whether the connection to the primary server is established. Figure 4-10 on page 98 shows a job log example.

```
  Display  Filter  View  Print  Options  Search  Help
 ------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY CQZSERV  STC18647  DSID   103 LINE 1       COLS 13- 92
 COMMAND INPUT ===> _                                         SCROLL ===> CSR
 IOQCR Server Version 2.1.348
 Invocation program /usr/lpp/ioqcrv2r1/bin/ocrserver
 CVTSNAME is defined as: SC61
 IOQCR_HOME is defined as: /usr/lpp/ioqcrv2r1
 IOQCR_CONFIG_DIR is defined as: /etc/ioqcr
 JAVA_HOME is defined as: /usr/lpp/java/J6.0.1
 CPU RLIMIT is defined as: UNLIMITED/UNLIMITED (current/max).
 NOFILE RLIMIT is defined as: 65535/65535 (current/max).
 Address Space Size RLIMIT is defined as: 1530896384/UNLIMITED (current/max).
 LIBPATH=/usr/lpp/ioqcrv2r1/lib:/usr/lpp/java/J6.0.1/bin:/usr/lpp/java/J6.0.1/bi
 PATH=/usr/lpp/java/J6.0.1/bin:/usr/lpp/java/J6.0.1/bin/classic
 CLASSPATH -Djava.class.path=/usr/lpp/ioqcrv2r1/classes/iocr.jar:/usr/lpp/ioqcrv
 Creating the JVM.
 Starting the OcrServer.
CQZSERV ID IOQCRSERVER is now connected to the Primary Controller 9.12.5.27
******************************** BOTTOM OF DATA ********************************
```

Figure 4-10 CQZSERV started successfully

You can also verify that the Workload Replay Controller for z/OS successfully connected to the main Workload Replay server appliance by viewing the system status page on the main Workload Replay server. For steps to access the Workload Replay server system status page, see 7.2.2, “Monitoring the connection status of Workload Replay services” on page 236.

To stop the Workload Replay Controller for z/OS when it is no longer needed, use the MVS cancel command:

```
c cqzserv
```

This command stops both of the running started task procedures: CQZSERV and CQZSERV1.

4.5 Enablement of workload capture and replay in the Workload Replay web console

Before privileged users or users can capture, process, or replay workloads on a database, a database connection profile must be created in the Workload Replay web console of the main Workload Replay server. This profile provides the appliance with access to the database that is required to perform housekeeping and authorization checking tasks.

In this section, we describe how to create a database connection profile and how to manage authorization for the Workload Replay tasks. The steps are illustrated by using the D1K1 subsystem to set up the database connection profile for the DB1K data sharing location name. DB1K is both the location name and the data sharing group name in the book environment. The D1K1 subsystem is running on LPAR SC61, with host name `wtsc61.itso.ibm.com`.

Before you begin

Before you can create a database connection profile, verify that the following tasks are completed for the LPAR on which the subsystems reside for which you are creating the profile:

- Workload Replay Controller for z/OS is installed, configured, and running on the LPAR.
- S-TAP is customized for each subsystem that is associated with this connection profile.
- The DB2 for z/OS database that you are creating the database connection profile for is active and accessible by using TCP/IP.

Gather the following information:

- The location name or location alias (in data sharing environments)
- The host name or IP address of the LPAR
- The port number
- The user ID and password of a DB2 user with at least the following authority:
  - User-defined function creation capability on the database (See A.4, “Workload Replay artifacts that reside in capture or replay databases or subsystems” on page 320)
  - The execute privilege on the SYSPROC.ADMIN_COMMAND_DB2 stored procedure on the subsystem or data sharing group
  - The DB2 authority to issue the **`DB2 -DISPLAY GROUP`** and **`-DISPLAY DDF`** commands

Procedure

To create a database connection profile, complete the following steps:

1. Open the Workload Replay web console on the main Workload Replay server with the following web address:

   `https://`*`guardium_hostname_or_ip`*`:8443/dsweb/console/ocr/index.jsp`

Note: If you cannot open or connect to the web console, see 9.2.1, “Resolving Workload Replay web console connectivity issues” on page 286.

2. As a privileged user, log on by using the correct account, as shown in Figure 4-11.

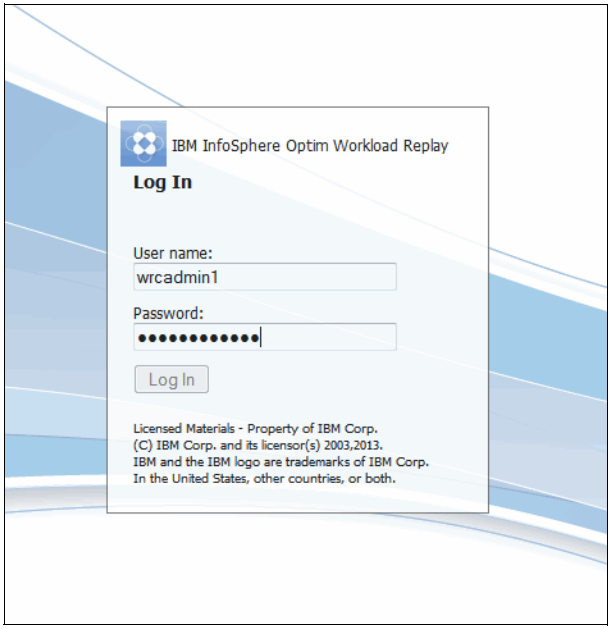


Figure 4-11 Log in to the Workload Replay web console as a privileged user account

3. Navigate to **Open** → **Administration** → **Databases**, as shown in Figure 4-12 on page 101.

   The Database Connections window, which displays currently defined database connection profiles, opens. The database connection profiles provide the Workload Replay appliance access to DB2 for z/OS subsystems.

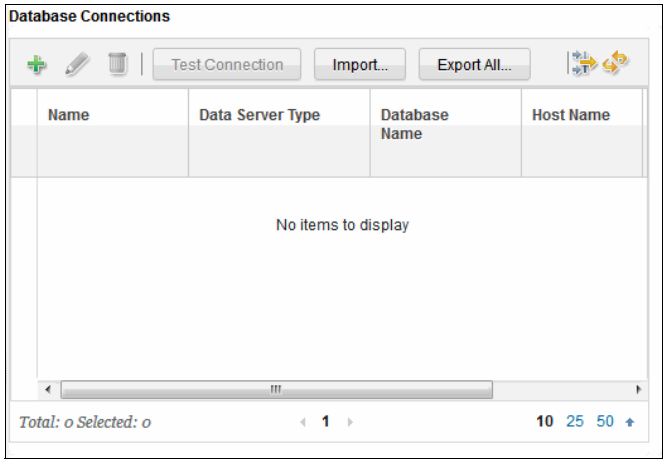


Figure 4-12 Database Connections Test Connection tab

4. Click the green plus (+) icon on the upper-left side to create a new database connection profile.

> **Note:** You can import database connection profiles that you created on other main Workload Replay servers.

5. Enter the database connection information:
   - Specify a unique database connection name that users can easily associate with the database.
   - Select **DB2 for z/OS** as the data server type.
   - Enter the location name.
   - Specify the database's host name or IP address.
   - Specify the DB2 for z/OS IBM Distributed Relational Database Architecture (DRDA®) defined TCP/IP port number of the DB2 for z/OS in the port number field.
   - Select **Clear text password** for Java Database Connectivity (JDBC) security.
   - Enter the user ID that will own this database connection profile in the User ID field.
   - Specify the password for the user ID in the password field.

> **Note:** Mandatory fields are marked with an asterisk (*).

On Figure 4-13, you provide connectivity information for the database on which you want to capture or replay workloads. Figure 4-13 shows a completed example database connection profile for the book environment DB2 data sharing location DB1K. The book environment network setup does not have a data sharing group IP defined, so the host and port information is from the D1K1 data sharing member.

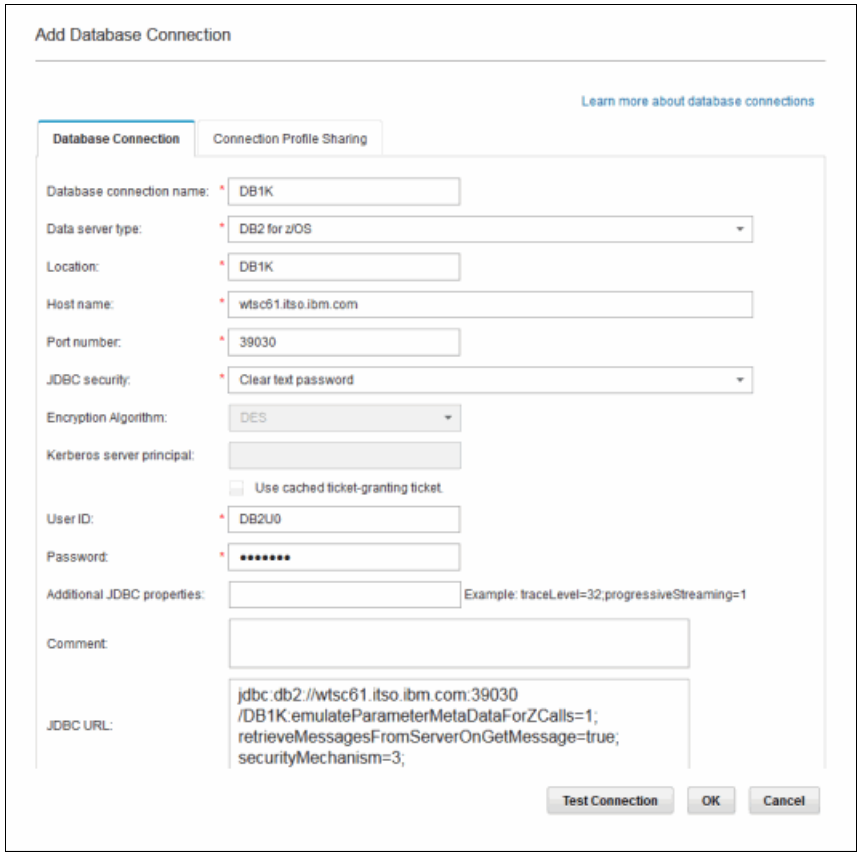


Figure 4-13 Connectivity information for the database to capture or replay workloads

6. Click **Test Connection** to verify the database connectivity.

   If the connection information is successfully verified, a message similar to Figure 4-14 on page 103 is displayed. Click **OK** to close the dialog window.

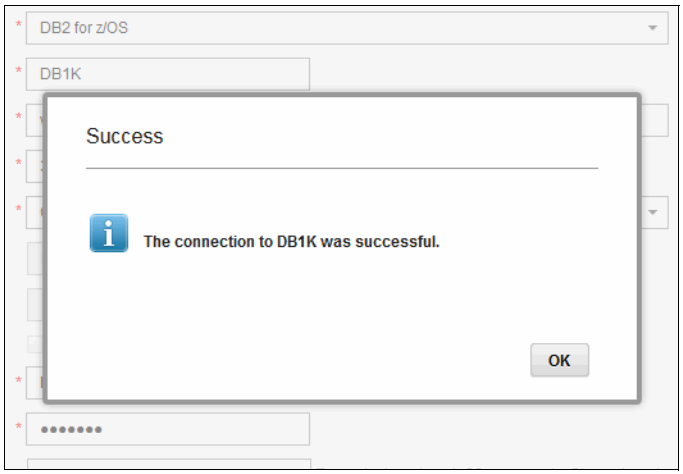
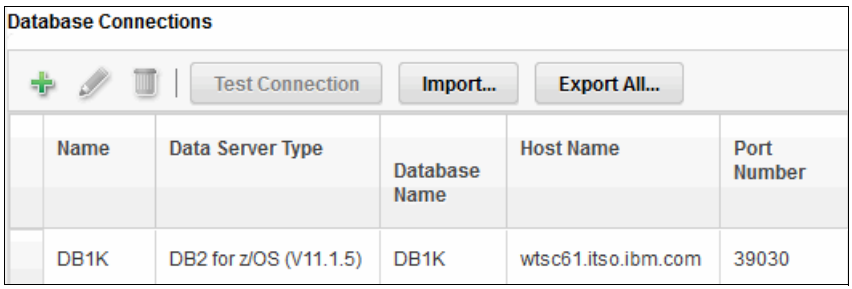


Figure 4-14 Connectivity to DB1K location is successfully verified

7. Click **OK** in the Add Database Connection dialog to save the database connection profile.

> **Note:** When a database connection is created, a set of user-defined functions (UDFs) is created in the database. The UDFs control who can capture, process, or replay workloads on this database. For more information about the UDFs, see A.4, “Workload Replay artifacts that reside in capture or replay databases or subsystems” on page 320.

The new database connection profile is displayed. Figure 4-15 depicts the profile for the DB1K data sharing location.



Name	Data Server Type	Database Name	Host Name	Port Number
DB1K	DB2 for z/OS (V11.1.5)	DB1K	wtsc61.itso.ibm.com	39030

Figure 4-15 Review the new database connection profile

8. Repeat these steps for each DB2 for z/OS location on which you want to capture or replay workloads.

Note: You must not create a database connection profile for a subsystem that is not customized for S-TAP. No workloads can be captured or replayed on that subsystem.

4.5.1 Managing access to capture and replay actions

When a privileged user creates a database connection profile, the default security policy is applied, restricting access to workload capture, processing, and replay actions. To perform an action, a privileged user or user must implicitly have the privileges that are listed in Table 4-3.

Table 4-3 Required privileges for workload capture, processing, and replay actions

Workload Replay actions	Capture subsystems	Replay subsystems
Capture workload	Can capture workload	N/A
Transform workload	Can capture workload	Can replay workload
Replay workload	N/A	Can replay workload
Review captured SQL	Can create report	N/A
Review transformed SQL	N/A	Can create report
Review replayed SQL	N/A	Can create report
Compare two workloads	Can create report	Can create report
Delete captured workload	Can delete captured workload	N/A
Delete transformed workload	Can delete captured workload	Can delete replayed workload
Delete replayed workload	N/A	Can delete replayed workload
Delete workload comparison report	Can delete report	Can delete report
Delete captured SQL report	Can delete report	N/A
Delete transformed SQL report	N/A	Can delete report
Delete replayed SQL report	N/A	Can delete report
Export workload	Can export workload	N/A
Import workload	Can import workload	N/A

The following actions are possible:

- Replay workloads
- Compare two workload executions
- Delete replayed workloads
- Delete workload comparison reports

To implement this policy, locate the actions that you want in Table 4-3 on page 104, note the required privileges, and grant them to the user (or group).

The following list is the privilege list for this example scenario:

- On the capture database:
  - Can create report
  - Can delete report
- On the replay database:
  - Can replay workload
  - Can create report
  - Can delete replayed workload
  - Can delete report

Note: A security policy is implemented by InfoSphere Workload Replay through a set of UDFs that are created in each database for which a connection profile is added in the Workload Replay web console. For detailed information, see A.4, “Workload Replay artifacts that reside in capture or replay databases or subsystems” on page 320.

You *do not* need to grant specific privileges for any user IDs that are already authorized to run the UDFs (for example, a user ID with the authorities DBADM and DATAACCESS). These users have the required privileges to capture, replay, or create reports.

Before you begin

Identify the privileges that must be granted to a user or group on a database connection profile.

Procedure

To manage the access to Workload Replay actions for a specific location, use these steps:

1. Open the Workload Replay web console on the main Workload Replay server:

   `https://guardium_hostname_or_ip:8443/dsweb/console/ocr/index.jsp`

   > **Note:** If you cannot open or connect to the web console, see 9.2.1, “Resolving Workload Replay web console connectivity issues” on page 286.

2. As a privileged user, log on by using the correct account, as shown in Figure 4-16. You use a privileged user account on the Log in window to the Workload Replay web console to manage access to workload capture, processing, and replay actions.

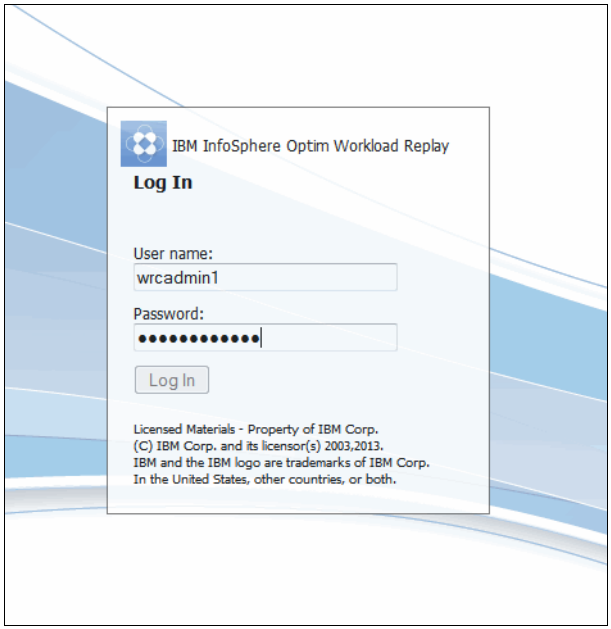


Figure 4-16 Log in to manage access to Workload Replay actions

3. Navigate to **Open** → **Administration** → **Manage Privileges**.

   The Manage Privileges tab opens, as shown in Figure 4-17 on page 107.

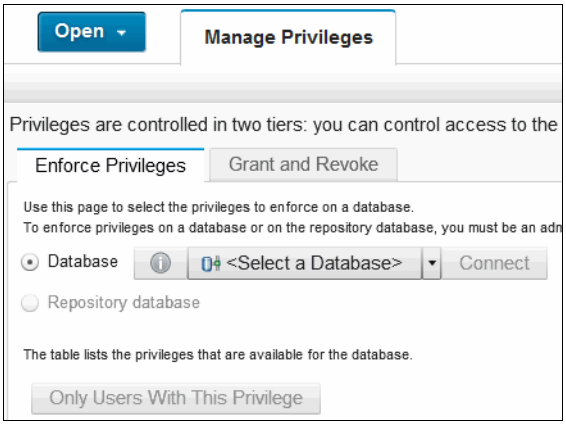


Figure 4-17 Open the security policy wizard

4. Open the **Grant and Revoke** tab (Figure 4-18).

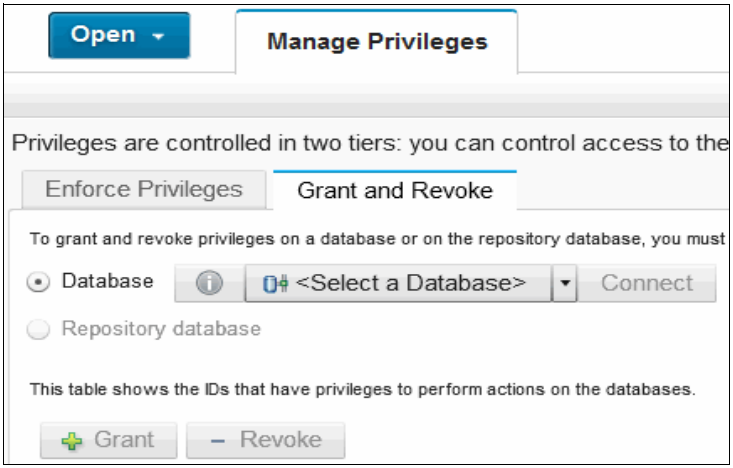


Figure 4-18 Access the policy management wizard

5. In the Database list box, click **<Select a Database>**. The dialog, as shown in Figure 4-19 on page 108, displays the currently defined database connection profiles. The pre-production DB2 in the book environment is DB1K. You use this window to select the database connection profile for which you implement the security policy.

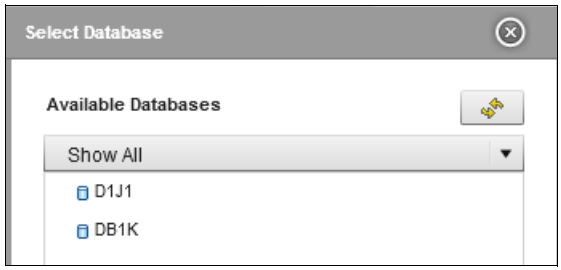


Figure 4-19 Select the database connection profile to implement the security policy

Note: Refresh the list if you cannot see the database connection profile that you want to manage.

Before you can modify the security policy, you must connect to the selected DB2 for z/OS database, as shown in Figure 4-20.

Figure 4-20 Connect to the DB1K database

6. Enter the credentials of a user that can modify the security policy and click **Log In**.

   The Workload Replay security policy for the selected database is displayed, as shown in Figure 4-21 on page 109. You can grant privileges to users or roles, or you can revoke them.

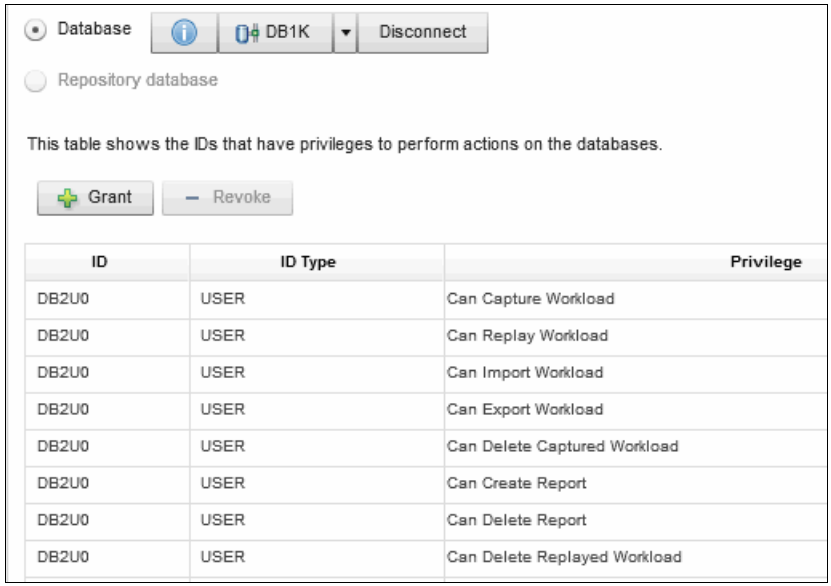


Figure 4-21 Review the current security policy for this database

Note: By default, the owner of the database connection profile has all privileges.

7. To grant a privilege, click **Grant**.
8. In the Grant Privilege window, enter an ID and select the correct ID type (USER or ROLE). Figure 4-22 depicts an example that grants user WRU1 the authority to replay workloads on this database.

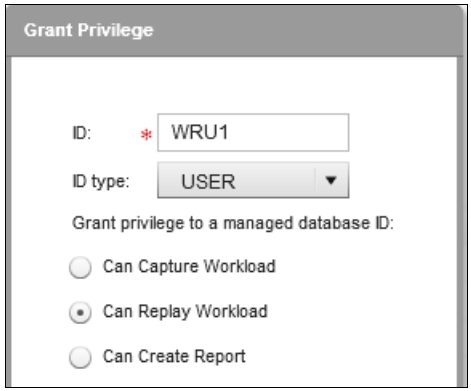
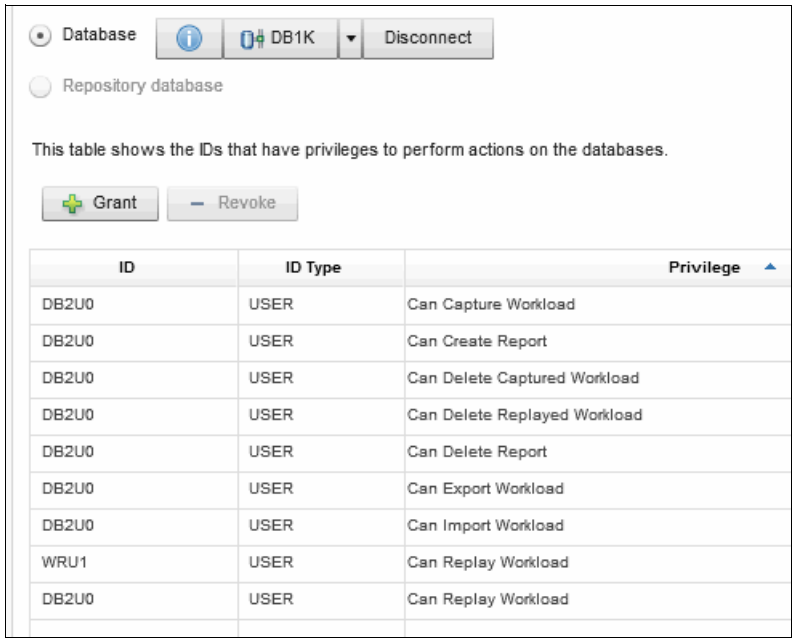


Figure 4-22 Grant a privilege to a user

9. Close any confirmation messages.

   The updated security policy after you grant user WRU1 the authority to replay a workload on DB1Ks is shown in Figure 4-23.



ID	ID Type	Privilege
DB2U0	USER	Can Capture Workload
DB2U0	USER	Can Create Report
DB2U0	USER	Can Delete Captured Workload
DB2U0	USER	Can Delete Replayed Workload
DB2U0	USER	Can Delete Report
DB2U0	USER	Can Export Workload
DB2U0	USER	Can Import Workload
WRU1	USER	Can Replay Workload
DB2U0	USER	Can Replay Workload

Figure 4-23 Updated security policy after granting authority to replay a workload

10. To revoke a privilege, select it and click **Revoke**.
11. Repeat the steps as needed to implement the security policy that you want.

5

DB2 for Linux, UNIX, and Windows S-TAP installation and configuration

This chapter provides detailed instructions about how to configure IBM InfoSphere Optim Workload Replay to monitor DB2 for Linux, UNIX, and Windows database traffic. It includes the following instructions:

- Installing S-TAP software on a database server machine
- Configuring S-TAP to monitor DB2 instance traffic
- Configuring S-TAP for Workload Replay multi-server support
- Enabling workload capture and replay on a database
- Managing access to workload capture, processing, and replay tasks for individual databases

The instructions in this chapter assume that you successfully installed and configured at least one InfoSphere Workload Replay appliance, as described in Chapter 3, “Installing and configuring IBM InfoSphere Optim Workload Replay appliances” on page 41.

5.1 Overview

During the initial deployment planning in 2.4.2, “Planning DB2 for Linux, UNIX, and Windows deployments” on page 30, we created a deployment plan for the production and test environments. After deployment is complete, workloads can be captured and replayed in those environments. Figure 5-1 depicts the book environment before the database server components are installed. Both Workload Replay appliances have no connectivity to the database servers.

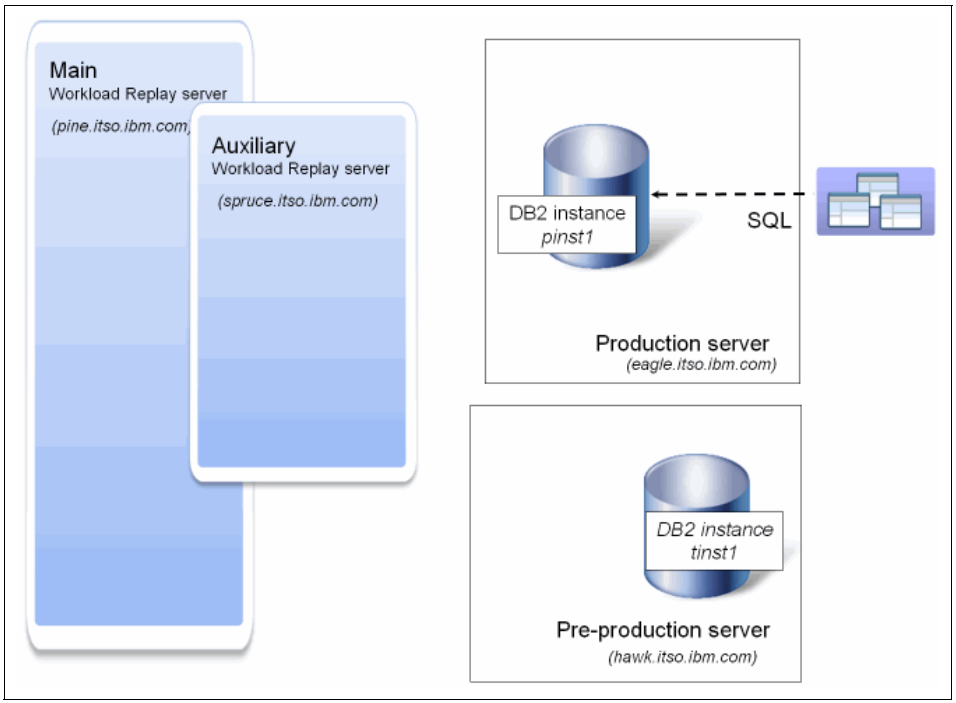


Figure 5-1 Book environment before the database server components are installed

Figure 5-2 on page 113 depicts the book environment after S-TAP installation and configuration are complete. S-TAPs are monitoring both DB2 instances and send traffic to the main and auxiliary Workload Replay appliances.

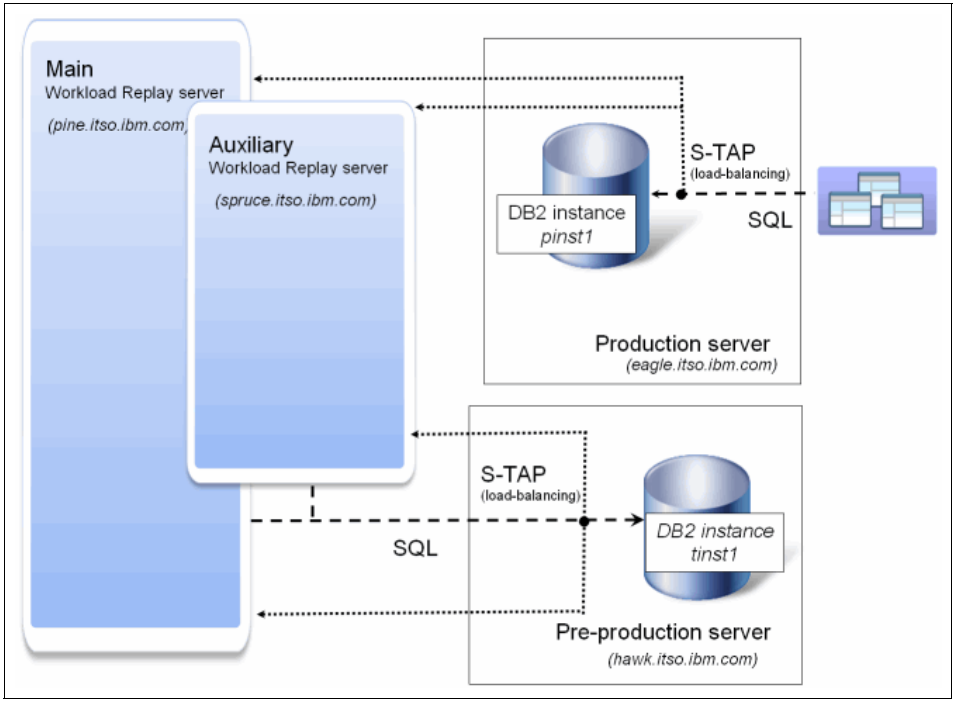


Figure 5-2 Book environment with S-TAP installation and configuration

Deployment plan recap

A generic DB2 for Linux, UNIX, and Windows S-TAP deployment plan consists of the following activities:

1. Install S-TAP software on each physical (or virtual) database server machine on which you plan to capture or replay workloads.

   Note: In database partitioning feature (DPF) environments, S-TAP is only installed on the coordinator node.

2. Configure each installed S-TAP to monitor the relevant DB2 instances.
3. Enable workload capture or replay for the instances of the designated databases.

In this chapter, we provide detailed instructions for each activity by using the book's deployment plan example:

1. In 5.2, "Installing S-TAP" on page 114, we install S-TAP in the pre-production environment on two AIX database servers: `hawk.itso.ibm.com` and `eagle.itso.ibm.com`.
2. In 5.3, "Configuring S-TAP to monitor database traffic" on page 126, we configure this S-TAP to monitor database traffic on a DB2 instance, `tinst1`.
3. In 5.4, "Enablement of workload capture and replay in the Workload Replay web console" on page 140, we enable workload capture and replay on a database and illustrate how to implement a security policy that restricts access to the capture, processing, and replay tasks.

Before you begin

Before you install S-TAP, configure and validate S-TAP:

- Review the S-TAP deployment plan.
- Complete the S-TAP configuration worksheet, as outlined in A.2.2, "S-TAP for Linux, UNIX, and Windows configuration worksheet" on page 316.
- Review the open ports requirements, as listed in A.2.2, "S-TAP for Linux, UNIX, and Windows configuration worksheet" on page 316.
- Download and prepare the required installation media, as described in A.1.2, "Downloading InfoSphere Workload Replay for DB2 for Linux, UNIX, and Windows installation media" on page 309.

S-TAP installation is typically performed by a system administrator who has root or sudo root privileges (on Linux and UNIX) or administrator privileges (on Windows platforms) on the database servers. Support from a network administrator is required if the deployment environment does not meet the open port requirements. S-TAP configuration is completed by a Workload Replay administrator in collaboration with database administrators.

5.2 Installing S-TAP

S-TAP is a lightweight software component that runs on a database server that monitors local and remote traffic that targets a database server.

The S-TAP installation process varies by platform. InfoSphere Workload Replay (and InfoSphere Guardium) provide several installation options. In 5.2.1, “Installing S-TAP using stand-alone installers” on page 115, we describe the installation process by using script-based installers (ideal for small and midsize deployments). In 5.2.2, “Installing S-TAP by using Guardium Installation Manager” on page 120, we describe an approach that is more suitable for large deployments.

For detailed S-TAP installation and configuration instructions for every platform, see the *Installing S-TAPs* section[1] of the IBM InfoSphere Guardium Knowledge Center[2]. The complete installation instructions are also available in PDF form in the product documentation, which is bundled with the installation media. For more information, see A.1.2, “Downloading InfoSphere Workload Replay for DB2 for Linux, UNIX, and Windows installation media” on page 309.

Upon completion of an S-TAP installation, S-TAP is running on the database but not actively monitoring any database traffic.

5.2.1 Installing S-TAP using stand-alone installers

We illustrate the stand-alone S-TAP installation process by using the DB2 system that runs on `hawk.itso.ibm.com`.

Before you begin

Complete the following tasks before the installation:

- Transfer the platform-specific S-TAP installation media to the database server and extract it in a temporary directory.
- Identify the host name or IP address of the main Workload Replay appliance that will be associated with the S-TAP.

Procedure

To install S-TAP on a Linux or UNIX database server by using a stand-alone installer, complete the following steps:

1. Log on to the database server as root (or sudo).
2. Navigate to the extracted S-TAP installation media, as shown in Figure 5-3 on page 116.

[1] http://www.ibm.com/support/knowledgecenter/SSMPHH_9.0.0/com.ibm.guardium.software.app.install.doc/topicsV90/stap_admin_install.html?lang=en

[2] http://www.ibm.com/support/knowledgecenter/SSMPHH/SSMPHH_welcome.html

```
# pwd
/download/stap_install/InfoSphere_Guardium_S-TAP_AIX_9.1_r62749
# ls
GIM_Packages              Shell_Installers
MD5SUMS                   UNIX_STAP_UPGRADER
Native_Installers         Unified_Shell_Installer
# _
```

Figure 5-3 The extracted S-TAP installation media includes shell and native installers

Note: A native installer ensures that S-TAP is registered in the operating system asset repository. If your company policy requires it, use a native installer, which is available for AIX, HP-UX, Linux, and Solaris. For details, see the *Installing an S-TAP with a native installer* topic in the Guardium Knowledge Center.

3. Navigate into the **Shell_Installers** directory. This directory contains operating system version-specific scripts. Identify the script that corresponds to the current operating system level. Figure 5-4 shows the contents of the `Shell_Installers` directory for the AIX platform.

```
# pwd
/download/stap_install/InfoSphere_Guardium_S-TAP_AIX_9.1_r62749
# ls
GIM_Packages              Native_Installers         UNIX_STAP_UPGRADER
MD5SUMS                   Shell_Installers          Unified_Shell_Instal
# cd Shell_Installers
# ls
guard-stap-9.0.0_r62749_v90_1-aix-5.3-aix-powerpc.sh
guard-stap-9.0.0_r62749_v90_1-aix-6.1-aix-powerpc.sh
guard-stap-9.0.0_r62749_v90_1-aix-7.1-aix-powerpc.sh
# 
```

Figure 5-4 Installation scripts are operating system version-specific

4. The installation script might be run in interactive or non-interactive mode. In interactive mode, the installer prompts you for required inputs as part of the installation process. In non-interactive mode, you provide the installation inputs by using command-line arguments. In our example, we use the non-interactive mode (`--ni`) and specify the required parameters as options:

```
# ./guard-stap-9.0.0_r62749_v90_1-aix-7.1-aix-powerpc.sh --ni -k
--tapip hawk.itso.ibm.com --dir /usr/local --sqlguardip
pine.itso.ibm.com --root --userinst
```

The command options indicate the following information:

- The **-k** option specifies that KTAP must be installed.
- The **tapip** parameter specifies the database server where the S-TAP will be installed. In our deployment, we install S-TAP on a pre-production database server named `hawk.itso.ibm.com`.
- The **dir** parameter specifies the installation directory.
- The **sqlguardip** parameter indicates the host name of the main Workload Replay appliance that S-TAP will connect to. In our deployment, the main Workload Replay appliance is `pine.itso.ibm.com`.
- The **root** option indicates to run S-TAP by using root. As part of the installation, the installation program creates a user ID guardium. It has the required permissions to run S-TAP on the database server. Optional: You can install and run as root or the built-in guardium user ID.

Note: A complete description of all command-line options is available in the *Install S-TAP from the Command Line* topic of the PDF product manual, which is included in the installation media.

Figure 5-5 shows the output that is displayed when the installation starts.

```
# ./guard-stap-9.0.0_r62749_v90_1-aix-7.1-aix-powerpc.sh --ni -k
 --tapip hawk.itso.ibm.com --dir /usr/local --sqlguardip pine.it
so.ibm.com --root --userinst
Verifying archive integrity... All good.
Uncompressing guard-stap.......................................
...........................
TARGET_TAG=9.0.0_r62749_v90_1 TARGET_PROCESSOR=powerpc BUILD_BUI
LD=62749
Script appears compatible with this system.
Installer is 9.0.0_r62749_v90_1-aix-7.1-powerpc
No ktap detected, proceeding with install
Please be patient... This might take more than a minute.
```

Figure 5-5 Start the S-TAP installation by using shell installer

Note (AIX only): All DB2 instances on the system must be restarted after the installation completes to finalize the setup. Use the **db2stop** and **db2start** commands to restart an instance. If an instance is not restarted after S-TAP is installed, its traffic might not be monitored.

Note (Linux only): You might get a message that the K-TAP loader cannot find a match for your operating system. Contact IBM Software support and request an updated InfoSphere Guardium S-TAP.

Note (Linux only): Certain database traffic can be tapped at the database server application level only, for example, because the database management system (DBMS) uses encryption or because of internal implementation details.

An optional component, A-TAP, monitors communication between internal database server components. A-TAP is required only if you are planning to capture shared memory (local) traffic.

If you deploy S-TAP in a Linux environment, A-TAP must be configured for each DB2 instance by using the **`guardctl`** utility. See 5.3.2, “Configuring S-TAP to monitor local DB2 instance traffic on Linux” on page 131.

5. Installation is complete.

Verifying that S-TAP is running and connected

Follow these steps to verify that S-TAP is running and connected to the main Workload Replay appliance:

1. Verify that the S-TAP process is running by using the following command:

   ```
   ps -ef | grep stap
   ```

   The `/usr/local/guardium/guard_stap/guard_stap` needs to be listed. You can now verify that S-TAP can communicate with the main Workload Replay appliance.

2. Open the Guardium web console on the main Workload Replay appliance `https://`*`guardium_hostname_or_ip`*`:8443/sqlguard`.

   Note: If you cannot open or connect to the web console, see 9.2.2, “Resolving Guardium web console connectivity issues” on page 287.

3. Log on as a privileged user. Figure 5-6 on page 119 shows an example of the Login window to the Guardium web console to verify that S-TAP is connected to the appliance.

Figure 5-6 Log in to verify that S-TAP connects to the appliance

4. Navigate to **Administration Console** → **Local Taps** → **S-TAP Control**, as shown in Figure 5-7.

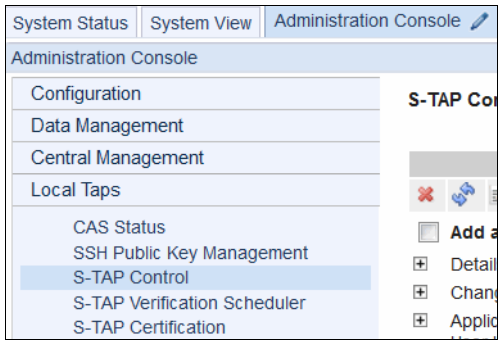


Figure 5-7 Open the S-TAP control page to review the list of connected S-TAPs

The S-TAP control window opens. An entry is displayed for the database server on which you installed S-TAP, as shown in Figure 5-8.

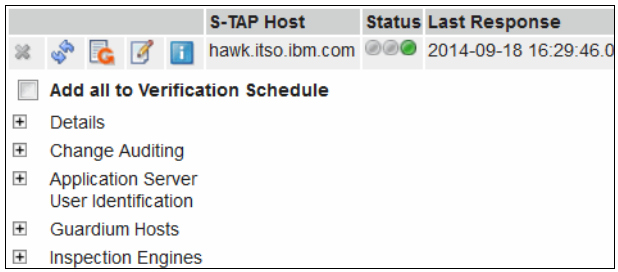


Figure 5-8 A green status light indicates that S-TAP is connected

> **Note:** If the installed S-TAP is not displayed in the list, see the troubleshooting information in 9.3, “Resolving S-TAP issues for a DB2 for Linux, UNIX, and Windows environment” on page 289.

You completed the first activity in the S-TAP deployment plan. Even though S-TAP is now running, it is not monitoring database traffic yet. To capture (or replay) workloads, you need to configure S-TAP. We describe the configuration process in 5.3, “Configuring S-TAP to monitor database traffic” on page 126.

5.2.2 Installing S-TAP by using Guardium Installation Manager

The Guardium Installation Manager (GIM) provides administrators with the ability to remotely install, configure, upgrade, and uninstall S-TAPs on database servers. We illustrate the GIM-based installation process by using the DB2 system running on `eagle.itso.ibm.com`.

Before you begin

Complete the following tasks before you start installation:

- Download the GIM client installation media and S-TAP installation media to your local machine.

> **Note:** If you plan to install the GIM client software on a DB2 v10.5 (or later) database server, it is not necessary to manually download the client installation media. During the DB2 installation, the DB2 installer places the GIM client installer files in path *<DB2 installation path>*/`guardium`.

- Verify that Perl is installed on the database server on which you want to install GIM.

Procedure

To take advantage of GIM, first install a GIM client on each database server. GIM clients register with the GIM server, which runs on the main Workload Replay appliance, check for updates, and perform management tasks, such as S-TAP installation, configuration, or upgrades.

The S-TAP installation that uses GIM is a two-step process:

- Upload the S-TAP GIM bundle to the main Workload Replay appliance and import it.
- Install S-TAP on the database server.

Installing the GIM client for the first time

Follow these steps to install the GIM client for the first time:

1. Upload the platform-specific GIM client installation media to the database server.
2. Log in as `root`.
3. Run the operating system version-specific installation script and specify the following parameters:
   - Installation directory
   - Host name (or IP address) of the database server
   - Host name (or IP address) of the main Workload Replay appliance

   ```
   ./guard-bundle-GIM-9.0.0_r65349_v90_1-aix-7.1-aix-powerpc.gim.sh
   --dir /usr/local/guardium --tapip eagle.itso.ibm.com --sqlguardip
   pine.itso.ibm.com
   ```
4. Review and accept the license agreement.
5. Verify that the GIM client is running:

   ```
   ps -ef | grep gim
   ```

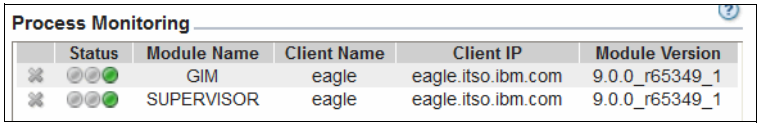
   Two Perl scripts must be running: **`guard_gimd.pl`** and **`gim_client.pl`**.

The GIM client automatically registers with the specified Workload Replay appliance.

Uploading the S-TAP GIM bundle

Complete the following steps to upload the S-TAP GIM bundle:

1. Log in to the Guardium web console on the main Workload Replay server as an administrator.
2. Navigate to **Administration Console** → **Module Installation** → **Process Monitoring** to verify that the database servers on which you installed the GIM clients are listed, as shown in Figure 5-9.



Process Monitoring

Status	Module Name	Client Name	Client IP	Module Version
	GIM	eagle	eagle.itso.ibm.com	9.0.0_r65349_1
	SUPERVISOR	eagle	eagle.itso.ibm.com	9.0.0_r65349_1

Figure 5-9 The GIM client on eagle is connected

3. Select **Administration Console** → **Module Installation** → **Upload** to open the Module Upload page.

4. Browse to the platform-specific S-TAP GIM module on your local machine and click **Upload,** as shown in Figure 5-10.

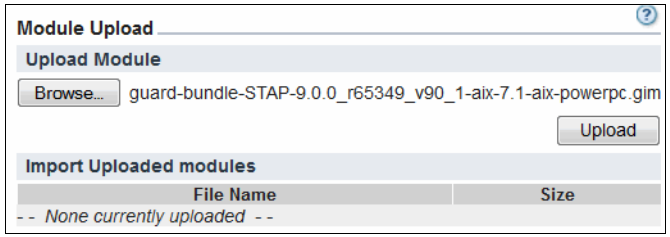


Figure 5-10 Upload the S-TAP GIM module

5. Import the S-TAP GIM module by clicking the check mark in front of the uploaded GIM module, as shown in Figure 5-11.

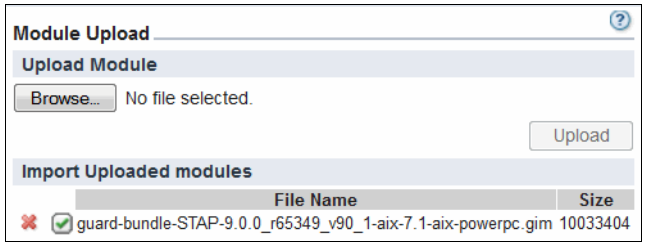


Figure 5-11 Import the uploaded S-TAP GIM module

6. You are now ready to install S-TAP on the database servers.

Installing S-TAP by using GIM

Complete the following steps to install S-TAP:

1. Navigate to **Administration Console** → **Module Installation** → **Setup By Module**.
2. Select the S-TAP module and click **Next**.
3. Select the database server (or servers) on which to install S-TAP and click **Next**, as shown in Figure 5-12.

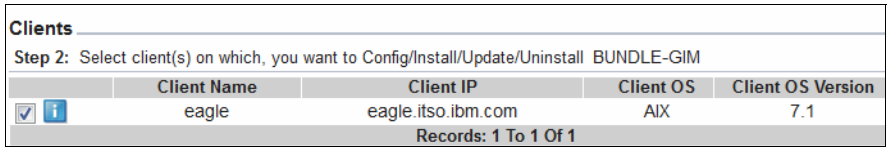


Figure 5-12 Select on which database servers to install S-TAP

Note: This list contains all database servers on which the GIM client is installed and associated with the main Workload Replay appliance that you are connected to.

4. On the Module Parameters page, select the database servers and click **Apply to Clients** and **Install/Update**, as shown in Figure 5-13.

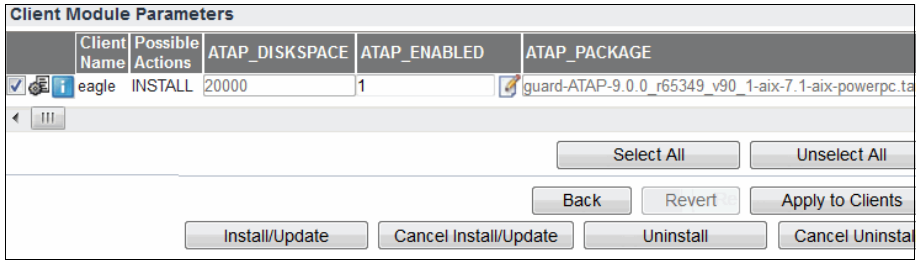


Figure 5-13 Start S-TAP installation

5. Enter **now** in the Schedule Date field and click **Apply**.

   The GIM client receives the request to install S-TAP, downloads the media from the main Workload Replay appliance, and starts the installation process.

Monitoring the S-TAP installation status

Use the following steps to monitor the S-TAP installation status:

1. Navigate to **Administration Console** → **Module Installation** → **Setup By Client**.
2. Select the blue information (i) icon to the left of the GIM client (or database server) name, as shown in Figure 5-14.

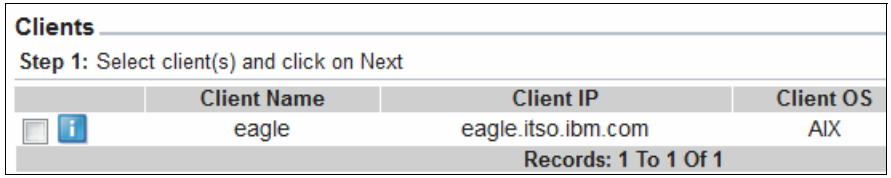


Figure 5-14 Review the S-TAP installation status

3. In the Installation Status window, wait until the S-TAP installation is complete, as shown in Figure 5-15 on page 124. Click **Refresh** to refresh the installation status if the status is PENDING.

Installation Status

Client: eagle

Module Name	Installed Version	Scheduled Version	Status
ATAP	9.0.0_r65349_1	9.0.0_r65349_1	INSTALLED
BUNDLE-GIM	9.0.0_r65349_1	9.0.0_r65349_1	INSTALLED
BUNDLE-STAP	9.0.0_r65349_1	9.0.0_r65349_1	INSTALLED
COMMON	9.0.0_r0_3	9.0.0_r0_3	INSTALLED
COMPONENTS	9.0.0_r65349_1	9.0.0_r65349_1	INSTALLED
GIM	9.0.0_r65349_1	9.0.0_r65349_1	INSTALLED
INIT	9.0.0_r65349_1	9.0.0_r65349_1	INSTALLED
KTAP	9.0.0_r65349_1	9.0.0_r65349_1	INSTALLED
STAP	9.0.0_r65349_1	9.0.0_r65349_1	INSTALLED
STAP-UTILS	9.0.0_r65349_1	9.0.0_r65349_1	INSTALLED

Figure 5-15 Installation Status window

Verifying that S-TAP is running and connected

To verify that S-TAP is running on the database server and connected to the main Workload Replay server, complete the following steps:

1. Navigate to **Administration Console** → **Local Taps** → **S-TAP Control**, as shown in Figure 5-16.

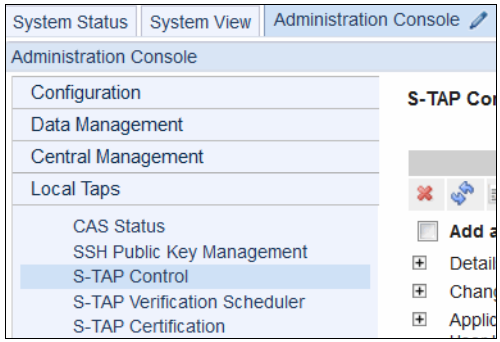


Figure 5-16 Open the S-TAP control page to review the list of connected S-TAPs

2. The S-TAP control window opens. An entry must be displayed for the database server on which you installed S-TAP, as shown in Figure 5-17 on page 125.

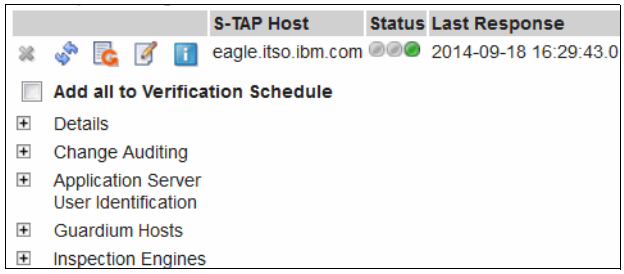


Figure 5-17 A green status light indicates that S-TAP is connected

Note: If the installed S-TAP is not displayed in the list, see the troubleshooting information in 9.3, “Resolving S-TAP issues for a DB2 for Linux, UNIX, and Windows environment” on page 289.

Note (AIX only): All DB2 instances on the system must be restarted after the installation completes to finalize the setup. Use the **`db2stop`** and **`db2start`** commands to restart an instance. If an instance is not restarted after S-TAP is installed, traffic monitoring might not occur.

Note (Linux only): Certain database traffic can be tapped at the database server application level only, for example, because the DBMS uses encryption or because of internal implementation details.

An optional component, A-TAP, monitors communication between internal database server components. A-TAP is required only if you are planning to capture shared memory (local) traffic.

If you deploy S-TAP in a Linux environment, A-TAP must be configured for each DB2 instance by using the **`guardctl`** utility. For more information, see 5.3.2, “Configuring S-TAP to monitor local DB2 instance traffic on Linux” on page 131.

5.3 Configuring S-TAP to monitor database traffic

After an S-TAP is installed, you must configure on which DB2 instances it needs to monitor and collect information about local and remote traffic. This configuration is performed by an administrator by using the Guardium web console on the main Workload Replay appliance that you associated with the S-TAP during installation.

In the following sections, we configure the S-TAP that we installed in 5.2, “Installing S-TAP” on page 114 to monitor the `tlinst` DB2 instance and enable multi-server support.

5.3.1 Configuring S-TAP to monitor DB2 instance traffic

This section provides step-by-step instructions for configuring an Inspection Engine on the InfoSphere Workload Replay Server, `pine.itso.ibm.com`, for the test database on `hawk.itso.ibm.com`.

Before you begin

Before you configure S-TAP to monitor DB2 instance traffic, verify that the S-TAP configuration worksheet is completed by the database administrators. For details, see A.2.2, “S-TAP for Linux, UNIX, and Windows configuration worksheet” on page 316.

Procedure

To configure an S-TAP installation to monitor a new DB2 instance, complete the following steps:

1. Open the Guardium web console on the main Workload Replay server:

   https://*guardium_hostname_or_ip*:8443/sqlguard

   > **Note:** If you cannot open or connect to the web console, see 9.2.2, “Resolving Guardium web console connectivity issues” on page 287.

2. Log on to the Guardium web console as a privileged user to configure S-TAP. Figure 5-18 on page 127 shows an example.

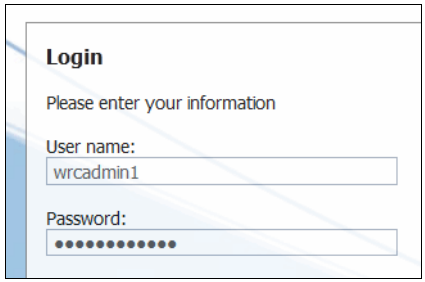


Figure 5-18 Log in to the Guardium web console as a privileged user

3. Navigate to **Administration Console** → **Local Taps** → **S-TAP Control**, as shown in Figure 5-19.

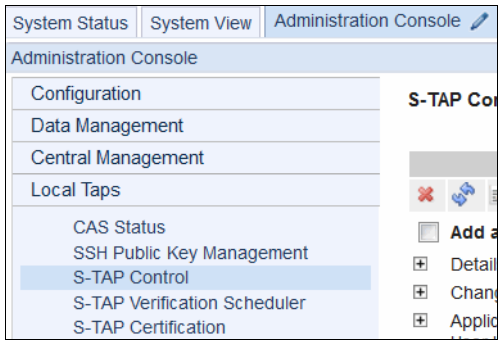


Figure 5-19 The S-TAP control page provides access to S-TAP configuration settings

4. The S-TAP control window opens. An entry is displayed for each database server on which an S-TAP is running that is associated with this appliance. In Figure 5-20, one entry is displayed for the S-TAP that we installed on `hawk.itso.ibm.com` in the pre-production environment.

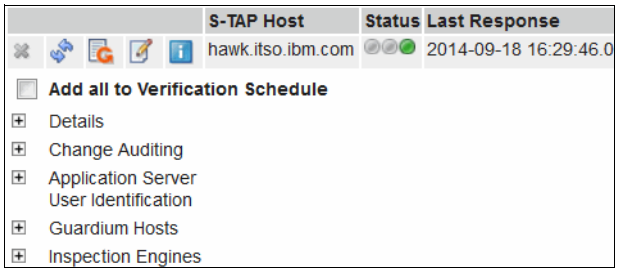


Figure 5-20 Database servers on which the S-TAP is running

5. Locate the entry of the S-TAP that you want to configure.

> **Note:** If no entry is displayed for the relevant S-TAP, see the troubleshooting information in 9.3, “Resolving S-TAP issues for a DB2 for Linux, UNIX, and Windows environment” on page 289.

6. Click the pencil icon to the left of the S-TAP host name to edit the configuration by using the information from your worksheet, as shown in Figure 5-21.

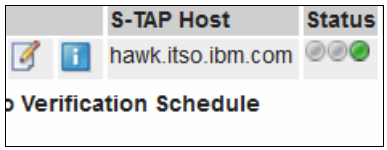


Figure 5-21 Click the pencil icon to edit the S-TAP configuration

When S-TAP is configured for the first time, no Inspection Engine is defined, which indicates that no DB2 instance is monitored.

7. Click **Add Inspection Engine** to define a new DB2 instance monitoring configuration, as shown in Figure 5-22.

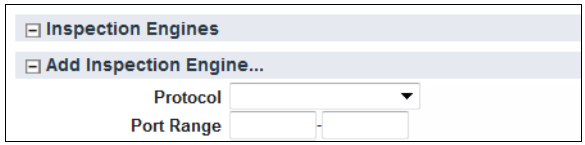


Figure 5-22 Define a monitoring configuration for DB2 instance tinst1

8. Complete the configuration parameters:
   - Select **DB2** as the Protocol.
   - For the Port Range and the KTAP DB Real Port, enter the value from your S-TAP configuration worksheet.
   - Enter a Client IP/Mask of `0.0.0.0/0.0.0.0`. This mask controls the clients from which to capture database traffic.

> **Note:** To capture both local and remote traffic, enter a value of `0.0.0.0/0.0.0.0`. If the IP address is the same as the database server and a mask of `255.255.255.255` is used, only local traffic is captured.

– Do not configure an Exclude Client IP/Mask. If used, this value sets the list of client IP addresses and masks to exclude when capturing traffic. If entered, this value excludes a certain client or subnet.

– Enter `127.0.0.1` for the Connect to IP value.

– Enter the DB2 instance's home directory as the DB Install Dir. Use the value from your S-TAP configuration worksheet.

– Enter the Process Name, including the full path to the binary. For details, see the S-TAP configuration worksheet.

– Enter the DB2 Shared Memory adjustment value from the S-TAP configuration worksheet.

– Enter the DB2 Shared Memory Client Position from the S-TAP configuration worksheet.

– Enter the DB2 Shared Memory Size from the S-TAP configuration worksheet.

– Do not check Encryption.

– Leave the Intercept Type field blank.

– Leave the Identifier field blank.

Figure 5-23 displays the example S-TAP (Inspection Engine) configuration for the pre-production DB2 instance `tlinst`.

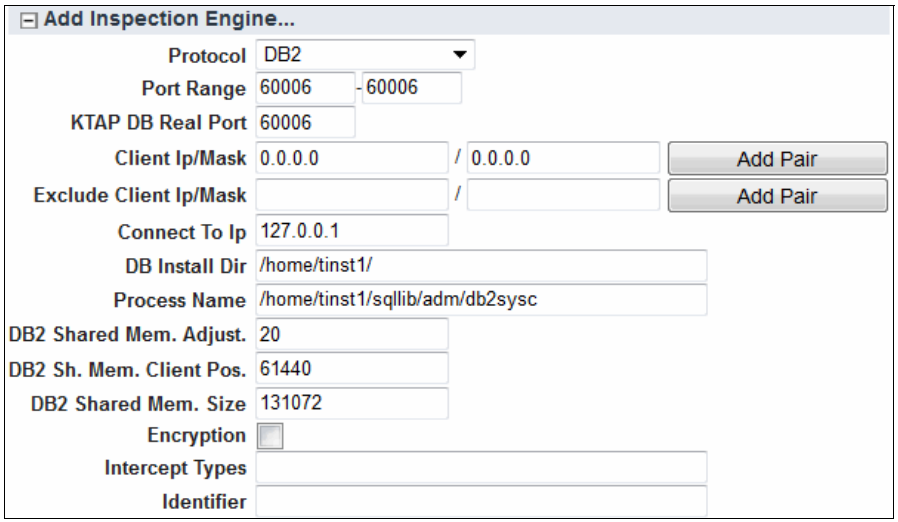


Figure 5-23 S-TAP on hawk is configured to monitor the DB2 instance tinst1

9. Click **Add** and then click **Save**.

10. Close the confirmation dialog.

    The appliance transmits the new DB2 instance monitoring configuration to S-TAP on the database server, where it is validated. While validation is in progress (and S-TAP is restarted), the traffic light status is displayed as synchronizing (yellow).

11. Refresh the S-TAP status view until S-TAP is online (green light) again.

12. Expand the Inspection Engines node for the configured S-TAP again and verify that the monitoring settings that you provided are accepted, as shown in Figure 5-24.

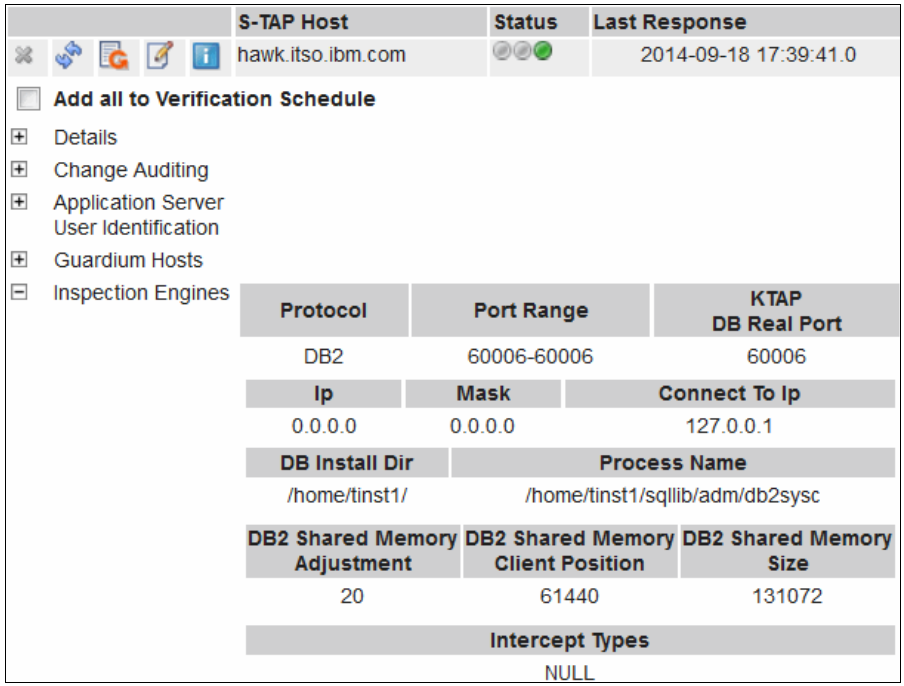


Figure 5-24 S-TAP configuration is complete

Note: If no configuration or an empty configuration is displayed, or a specified value is incorrect, troubleshoot the issue. For details about how to analyze S-TAP Inspection Engine configuration issues, see 9.3, “Resolving S-TAP issues for a DB2 for Linux, UNIX, and Windows environment” on page 289.

S-TAP is now actively monitoring database traffic for the selected DB2 instance. If additional DB2 instances on the database server need to be configured for monitoring, repeat these steps.

5.3.2 Configuring S-TAP to monitor local DB2 instance traffic on Linux

On Linux operating systems, an additional component, A-TAP, is required to capture SQL traffic on local (shared memory) connections. A-TAP is installed as part of the S-TAP installation but it must be configured or activated for each DB2 instance on which you plan to capture or replay workloads.

Before you begin

Perform these steps before you configure S-TAP to monitor DB2 instance traffic:

- Verify that the S-TAP configuration worksheet is completed by the database administrators. For details, see A.2.2, “S-TAP for Linux, UNIX, and Windows configuration worksheet” on page 316.
- Notify the database administrator that the DB2 instance must be restarted as part of the activation process.

Procedure

Follow these steps to configure A-TAP to monitor local connections on a DB2 instance on Linux:

1. Log in to the database server as root.
2. Navigate to the `<guardium_base>/bin` directory, where `<guardium_base>` is the InfoSphere Guardium installation directory. The default installation directory is `/usr/local/guardium`.
3. Create an instance configuration for A-TAP using the information from your worksheet by running the **guardctl** utility:

   ```
   /usr/local/guardium/bin/guardctl db_instance=<db2_instance_name>
   db_user=<instance_owner> db_type=db2
   db2_shmsize=<DB2_shared_memory_size>
   db2_c2soffset=<DB2_shared_memory_client_position>
   db2_header_offset=20 store-conf
   ```

   Note: The Italic font is used to indicate parameter values that must be replaced with the correct settings from your DB2 instance.

The following example creates a configuration for an instance named `db2inst1`:

/usr/local/guardium/bin/guardctl db_instance=db2inst1 db_user=db2inst1 db_type=db2 db2_shmsize=131072 db2_c2soffset=61440 db2_header_offset=20 store-conf

4. Verify that the configuration is saved:

   /usr/local/guardium/bin/guardctl list-configured

   In our example, the output is `db2inst1.conf`.

5. Authorize the instance owner to monitor database traffic:

   /usr/local/guardium/bin/guardctl authorize_user <*instance_owner*>

   In our example, **/usr/local/guardium/bin/guardctl authorize_user db2inst1** returns:

   ```
   Authorizing user 'db2inst1' to log traffic
   ```

6. Stop the DB2 instance.

7. Activate the Guard A-TAP mechanism for the instance:

   /usr/local/guardium/bin/guardctl db_instance=<*DB2_instance_name*> activate

   In our example, **/usr/local/guardium/bin/guardctl db_instance=db2inst1 activate** returns:

   ```
   Matching module found - db2 is supported by
   /usr/local/guardium/lib64/libguard-atap-db2-any
   Installing ATAP library
   /usr/local/guardium/lib64/libguard-atap-db2-any-64.so in /usr/lib64
   Creating permissions
   Matching module found - db2 is supported by
   /usr/local/guardium/lib64/libguard-atap-db2-any
   Set 453 bytes for 'executor/env' in file
   '/home/db2inst1/sqllib/adm/db2sysc-guard-executor'
   ```

8. Verify that A-TAP is successfully activated for the instance:

   /usr/local/guardium/bin/guardctl list-active

   In our example, the command returns `db2inst1`.

9. Start the DB2 instance.

S-TAP now monitors local and remote database connections. Repeat these steps for each DB2 instance on which you want to capture local traffic.

Note: For detailed information about A-TAP, see the *Help Book Guardium*. The help book is included in the InfoSphere Workload Replay installation media, as documented in A.1.2, “Downloading InfoSphere Workload Replay for DB2 for Linux, UNIX, and Windows installation media” on page 309.

5.3.3 Configuring multi-server support

In multi-server deployments, two or more Workload Replay appliances (one main Workload Replay server and one or more auxiliary Workload Replay servers) monitor and capture database traffic. To support this topology, S-TAP must be configured for load balancing, as shown in Figure 5-25 for the pre-production environment.

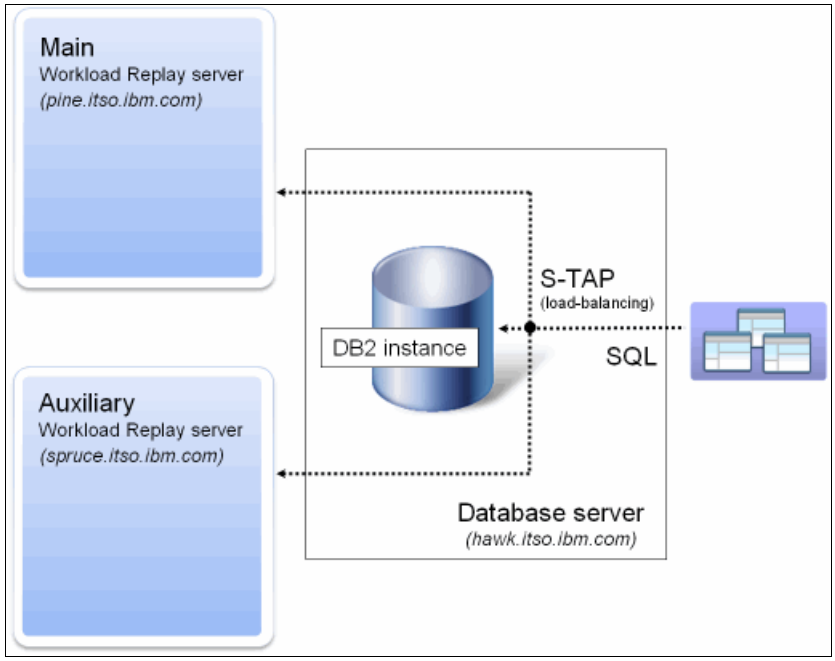


Figure 5-25 S-TAP load balancing distributes monitored traffic to multiple appliances

In our book scenario, two Workload Replay appliances are used to capture and replay workloads in the DB2 for Linux, UNIX, and Windows environments. The instructions in this section guide you through the process of enabling load balancing for two appliances for a single S-TAP installation.

Note: Special considerations are needed if an S-TAP will be used to capture or replay workloads and to perform Database Activity Monitoring (DAM) by using another InfoSphere Guardium appliance. For more information, see 2.4.2, “Planning DB2 for Linux, UNIX, and Windows deployments” on page 30.

Before you begin

Before you enable S-TAP load-balancing to support multi-server capture and replay, validate that the following tasks are completed:

- An S-TAP Inspection Engine configuration is defined for the DB2 instance on the main Workload Replay appliance (5.3.1, “Configuring S-TAP to monitor DB2 instance traffic” on page 126).
- The designated auxiliary servers are running and are associated with the main Workload Replay server.

Procedure

To configure S-TAP to distribute monitored traffic across multiple Workload Replay appliances, complete the following steps:

1. Open the Guardium web console on the main Workload Replay server:

   `https://guardium_hostname_or_ip:8443/sqlguard`

   Note: If you are having trouble opening the web console or connecting to it, see 9.2.2, “Resolving Guardium web console connectivity issues” on page 287.

2. Log on as a privileged user to configure S-TAP, as shown in Figure 5-26.

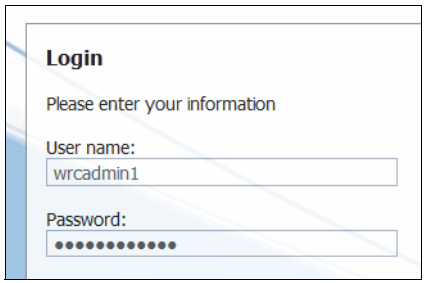


Figure 5-26 Log in to the Guardium web console as a privileged user

3. Navigate to **Administration Console** → **Local Taps** → **S-TAP Control**, as shown in Figure 5-27 on page 135 to open the S-TAP control panel in the Guardium web console to review and modify S-TAP configuration options.

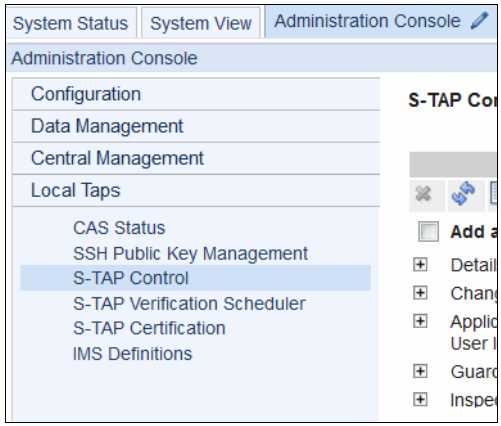


Figure 5-27 Open the S-TAP control panel in the Guardium web console

4. The S-TAP Control page opens. An entry is displayed for each database server on which an S-TAP is running that is associated with this appliance. In Figure 5-28, one entry is displayed for the S-TAP that we installed on `hawk.itso.ibm.com` in the pre-production environment.

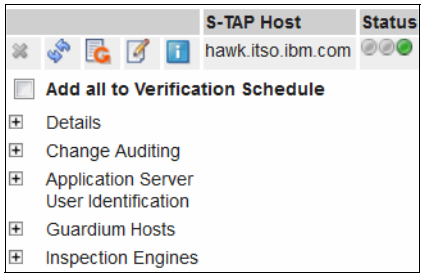


Figure 5-28 S-TAP Control page that displays the database server

5. Locate the entry of the S-TAP that you want to configure for load balancing.

> **Note:** If no entry is displayed for the relevant S-TAP, see the troubleshooting information in 9.3, “Resolving S-TAP issues for a DB2 for Linux, UNIX, and Windows environment” on page 289.

6. Click the pencil and paper icon to the left of the S-TAP host name to edit the S-TAP configuration, as shown in Figure 5-29 on page 136.

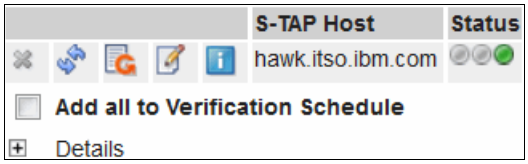


Figure 5-29 Click the pencil icon to edit the S-TAP configuration

> **Note:** If the pencil icon is disabled and more than one appliance is listed under the Guardium Hosts node, you logged in to the Guardium web console of an auxiliary Workload Replay server. To modify S-TAP configuration settings, you must be logged in to the Guardium web console of the main Workload Replay server.

7. Expand the Details node, as shown in Figure 5-30.

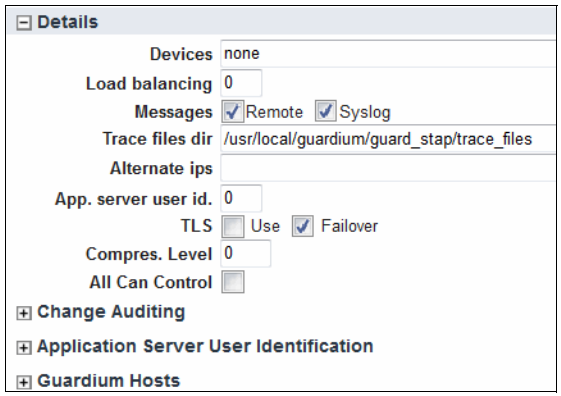


Figure 5-30 Load balancing is disabled by default

8. Locate the Load balancing configuration setting and change it from 0 to 1, as shown in Figure 5-31, to configure the S-TAP to load balance across multiple appliances.

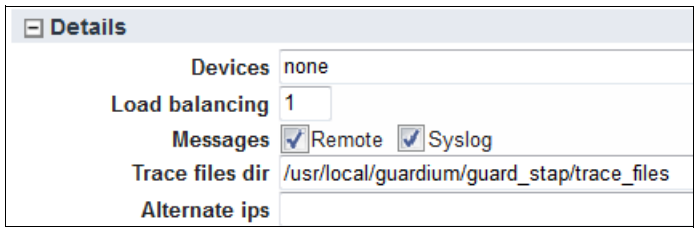


Figure 5-31 Modifying the Load balancing configuration setting

Note: The configuration setting *does not* indicate the number of appliances that will receive monitored traffic.

9. Expand the Guardium Hosts node, as shown in Figure 5-32. The main Workload Replay appliance's host name or IP address needs to be listed as active.

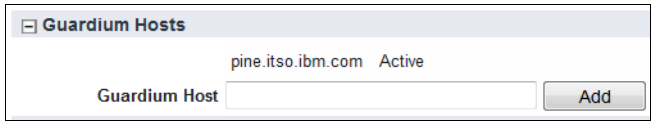


Figure 5-32 This S-TAP is associated to the main Workload Replay appliance

10. Enter the host name or IP address of the auxiliary Workload Replay appliance that you want to add to the load-balancing configuration, as shown in Figure 5-33.

Figure 5-33 Add an auxiliary Workload Replay appliance

11. Click **Add**.

    Figure 5-34 shows that `spruce.itso.ibm.com` was added as a secondary appliance to the load-balancing configuration.

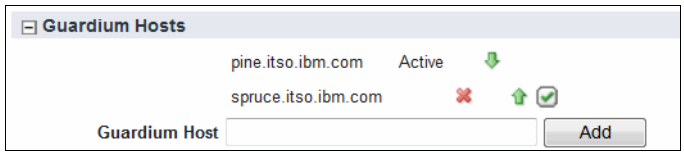


Figure 5-34 S-TAP can send traffic to multiple Workload Replay appliances

12. Repeat the previous two steps for each additional auxiliary Workload Replay server in your deployment topology.
13. Click **Save** to apply the changes. Close any confirmation messages.

    The appliance sends the new configuration information to the S-TAP host and the S-TAP status changes to yellow.
14. Wait until the S-TAP status changes to the green light (online). Figure 5-35 shows that the modified configuration settings are validated by S-TAP.

S-TAP is configured to forward monitored traffic to the main and auxiliary Workload Replay appliances.

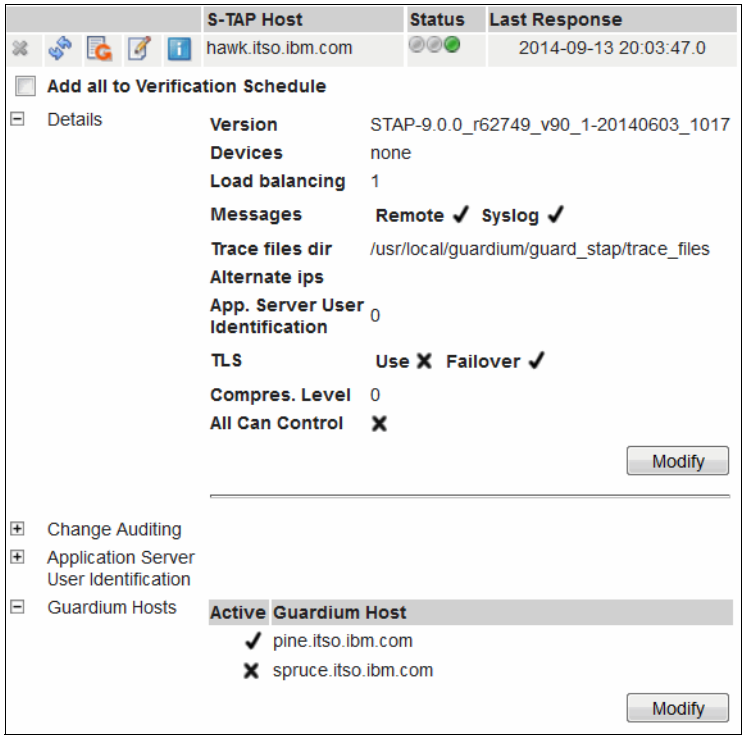


Figure 5-35 S-TAP configured to forward monitored traffic

You can now validate that S-TAP is connected to the auxiliary Workload Replay appliance.

15. Log out of the Guardium web console on the main Workload Replay appliance.
16. Open the Guardium web console on the auxiliary Workload Replay appliance:

    `https://guardium_hostname_or_ip:8443/sqlguard`

    Note: If you cannot open or connect to the web console, see 9.2.2, “Resolving Guardium web console connectivity issues” on page 287.

17. Log on as a privileged user to the Guardium web console on an auxiliary Workload Replay appliance to validate S-TAP connectivity after you configure load-balancing (Figure 5-26 on page 134).

Figure 5-36 Guardium web console login on an auxiliary Workload Replay appliance

18. Navigate to **Administration Console** → **Local Taps** → **S-TAP Control**, as shown in Figure 5-37, to open the S-TAP control panel on the auxiliary server's Guardium web console to validate the load-balancing configuration settings.

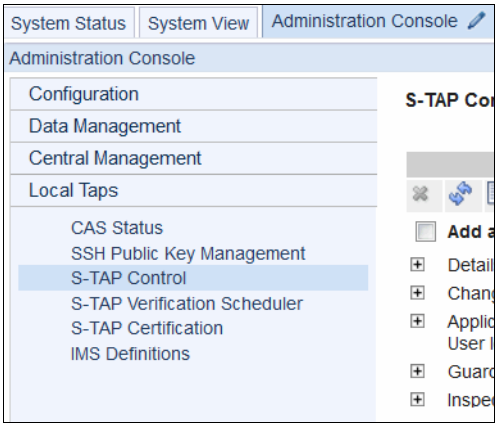


Figure 5-37 Open the S-TAP control panel on auxiliary server

19. Locate the S-TAP entry for the database server to verify that the status is green, and that the main and auxiliary Workload Replay appliances are listed under Guardium Hosts, as shown in Figure 5-38 on page 140. A green S-TAP status in the Guardium web console on an auxiliary Workload Replay appliance indicates that S-TAP is communicating as expected.

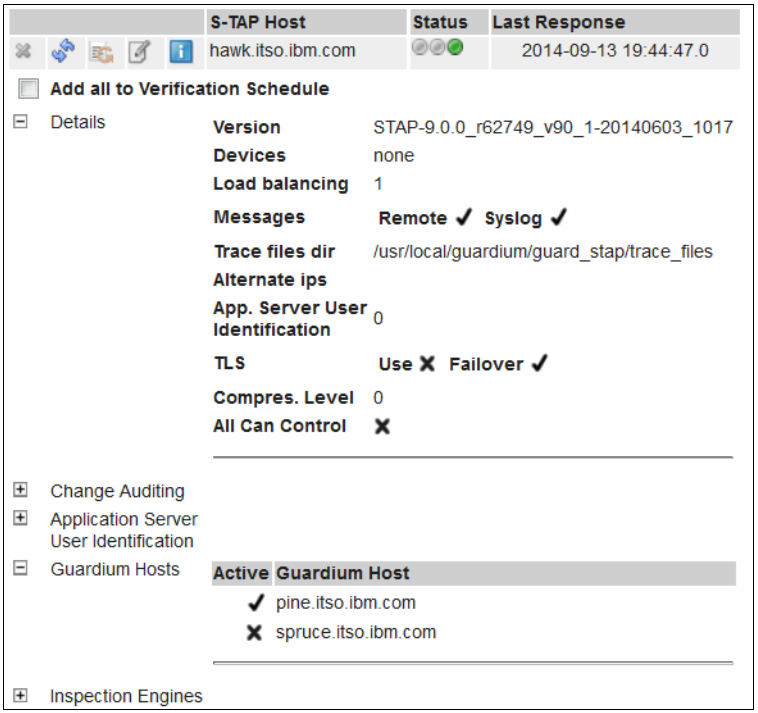


Figure 5-38 A green S-TAP status indicates that S-TAP is communicating

Note: By default, you can modify S-TAP configuration settings only on the main Workload Replay appliance.

S-TAP on this database server is now configured for load balancing. Repeat the steps in this section for each database server that requires a multi-server Workload Replay topology.

5.4 Enablement of workload capture and replay in the Workload Replay web console

Before privileged users or users can capture, process, or replay workloads on a database, a database connection profile must be created in the Workload Replay web console of the main Workload Replay server. This profile provides the appliance with access to the database that is required to perform housekeeping and authorization checking tasks.

In this section, we describe how to create a database connection profile and how to manage authorization for the workload replay tasks. The steps are illustrated by using the TESTDB database, which resides on the pre-production database server `hawk.itso.ibm.com`.

Before you begin

Before you can create a database connection profile, verify that the following tasks are completed:

- S-TAP is installed on the database server. (See 5.2, “Installing S-TAP” on page 114.)
- An S-TAP Inspection Engine configuration is defined for the DB2 instance on the main Workload Replay appliance. (See 5.3, “Configuring S-TAP to monitor database traffic” on page 126.)

Gather the following information:

- The database name
- The host name or IP address of the database server
- The port number
- The user ID and password of a DB2 user with at least authority to create user-defined functions on the database. (See A.4, “Workload Replay artifacts that reside in capture or replay databases or subsystems” on page 320.)

Note: Host and port information must match the S-TAP configuration.

Procedure

Follow these steps to create a database connection profile:

1. Open the Workload Replay web console on the main Workload Replay server:

   `https://`*`guardium_hostname_or_ip`*`:8443/dsweb/console/ocr/index.jsp`

   Note: If you cannot open or connect to the web console, see 9.2.1, “Resolving Workload Replay web console connectivity issues” on page 286.

2. As a privileged user, log on using the correct account, as shown in Figure 5-39 on page 142.

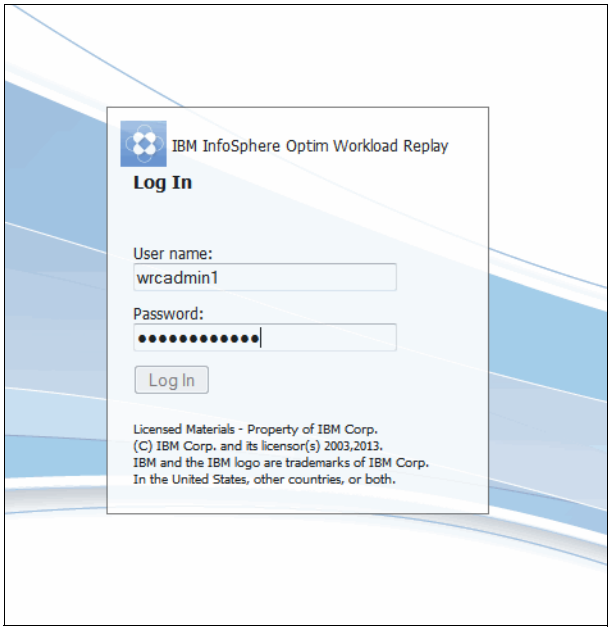


Figure 5-39 Log in to the Workload Replay web console as a privileged user account

3. Navigate to **Open** → **Administration** → **Databases**, as shown in Figure 5-40 on page 143.

   The Database Connections window opens and displays the currently defined database connection profiles. The database connection profiles provide the Workload Replay appliance access to DB2 for Linux, UNIX, and Windows databases or DB2 for z/OS subsystems.

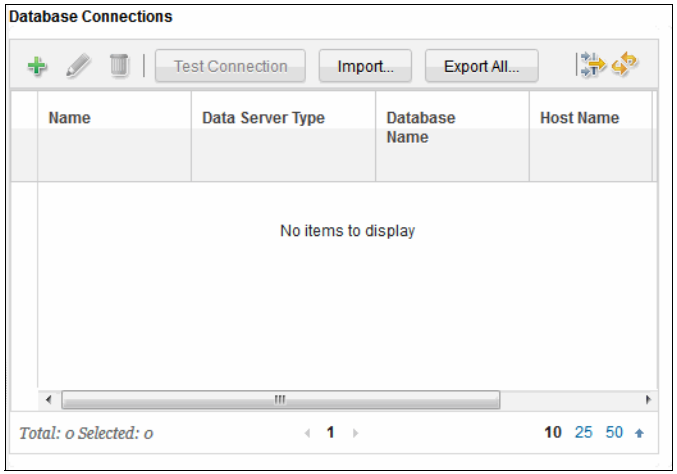


Figure 5-40 Database Connections window

4. Click the plus arrow in the upper-left corner to create a new database connection profile.

> **Note:** You can import database connection profiles that you created on other main Workload Replay servers.

5. Enter the database connection information to provide connectivity information for the database on which you want to capture or replay workloads:
   - Specify a unique database connection profile name that users can easily associate with the database.
   - Select **DB2 for Linux, UNIX, and Windows** as the data server type.
   - Enter the database name.
   - Specify the database's host name or IP address.
   - Specify the TCP/IP port number of the DB2 instance in which the database resides in the port number field.
   - Select **Clear text password** for Java Database Connectivity (JDBC) security.
   - Enter the user ID that will own this database connection profile in the user ID field.
   - Specify the password for user ID in the password field.

> **Note:** Mandatory fields are marked with an asterisk (*).

Figure 5-41 shows a completed example database connection profile for database TESTDB on `hawk.itso.ibm.com`.

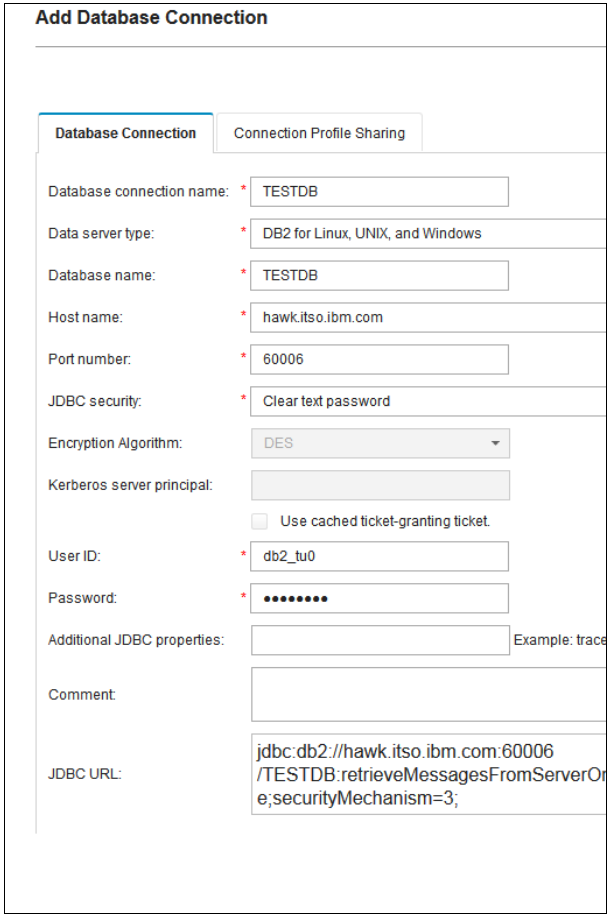


Figure 5-41 Connectivity details for the database where you capture or replay workloads

6. Click **Test Connection** to verify database connectivity.

   If the connection information was successfully verified, a message similar to Figure 5-42 on page 145 is displayed.

   a. Click **OK** to close the dialog window.

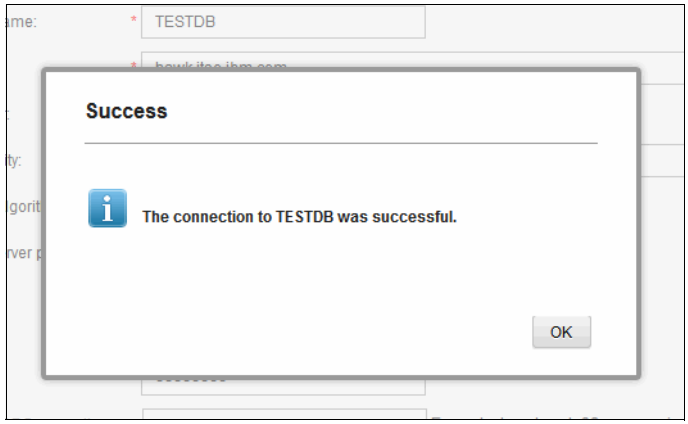


Figure 5-42 Connectivity to database TESTDB was successfully verified

7. Click **OK** in the Add Database Connection dialog to save the database connection profile.

> **Note:** When a database connection is created, a set of user-defined functions (UDFs) is created in the database. These UDFs control who can capture, process, or replay workloads on this database. For more information about the UDFs, see A.4, “Workload Replay artifacts that reside in capture or replay databases or subsystems” on page 320.

The new database connection profile is displayed. Figure 5-43 depicts the profile for TESTDB.

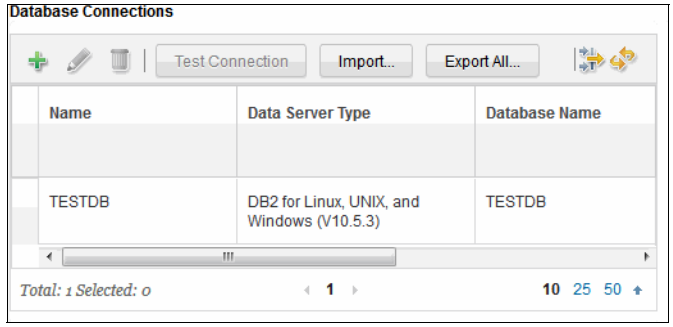


Figure 5-43 Review the new database connection profile

8. Repeat these steps for each capture or replay database on the configured DB2 instance.

Note: You must not create a database connection profile for a database whose DB2 instance is not monitored by S-TAP. No workloads can be captured or replayed on that database.

5.4.1 Managing access to capture and replay actions

When a privileged user creates a database connection profile, the default security policy is applied, restricting access to workload capture, processing, and replay actions. To perform an action, a privileged user or user must implicitly have the privileges that are listed in Table 5-1.

Table 5-1 Required privileges for workload capture, processing, and replay actions

Workload replay actions	Capture database	Replay database
Capture workload	Can capture workload	
Transform workload	Can capture workload	Can replay workload
Replay workload		Can replay workload
Review captured SQL	Can create report	
Review transformed SQL		Can create report
Review replayed SQL		Can create report
Compare two workloads	Can create report	Can create report
Delete captured workload	Can delete captured workload	
Delete transformed workload	Can delete captured workload	Can delete replayed workload
Delete replayed workload		Can delete replayed workload
Delete workload comparison report	Can delete report	Can delete report
Delete captured SQL report	Can delete report	
Delete transformed SQL report		Can delete report
Delete replayed SQL report		Can delete report
Export workload	Can export workload	
Import workload	Can import workload	

For example, assume that you want to introduce a security policy in a pre-production environment that allows a user (or group) to perform the following actions:

- Replay workloads
- Compare two workload executions
- Delete replayed workloads
- Delete workload comparison reports

To implement this policy, locate the actions that you want in Table 5-1 on page 146, note the required privileges, and grant them to the user (or group).

The following privilege list applies to this example scenario:

- On the capture database:
  - Can create report
  - Can delete report
- On the replay database:
  - Can replay workload
  - Can create report
  - Can delete replayed workload
  - Can delete report

Note: A security policy is implemented by InfoSphere Workload Replay through a set of UDFs that are created in each database for which a connection profile is added in the Workload Replay web console. For detailed information, see A.4, “Workload Replay artifacts that reside in capture or replay databases or subsystems” on page 320.

You *do not* need to grant specific privileges for any user IDs that are already authorized to run the UDFs (for example, a user ID with the authorities DBADM and DATAACCESS). These users have the required privileges to capture, replay, or create reports.

Before you begin

Identify the privileges that must be granted to a user or group on a database connection profile.

Procedure

To manage access to workload replay actions for a specific database, use these steps:

1. Open the Workload Replay web console on the main Workload Replay server:

   `https://guardium_hostname_or_ip:8443/dsweb/console/ocr/index.jsp`

   Note: If you cannot open or connect to the web console, see 9.2.1, “Resolving Workload Replay web console connectivity issues” on page 286.

2. As a privileged user, log on to the Workload Replay web console by using a privileged user account to manage access to workload capture, processing, and replay actions, as shown in Figure 5-39 on page 142.

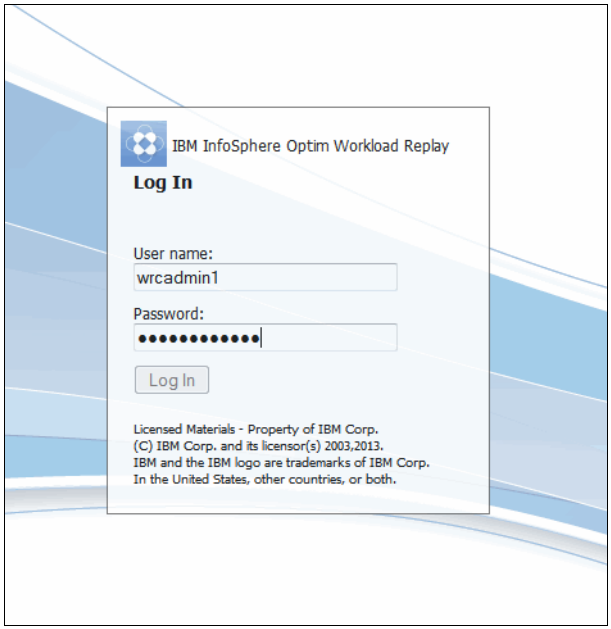


Figure 5-44 Log in to the Workload Replay web console as a privileged user account

3. Navigate to **Open** → **Administration** → **Manage Privileges**.

   The Manage Privileges tab opens, as shown in Figure 5-45.

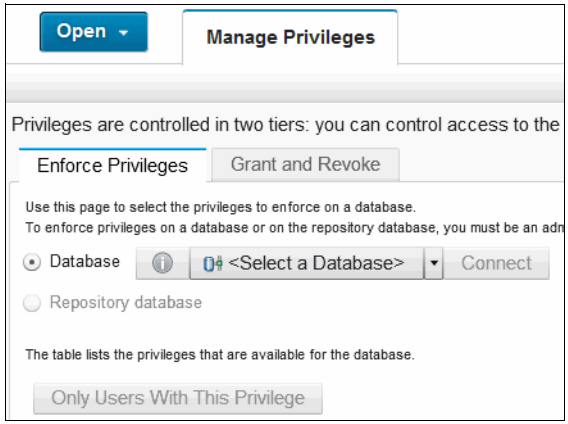


Figure 5-45 Open the security policy wizard

4. Select the **Grant and Revoke** tab (Figure 5-46).

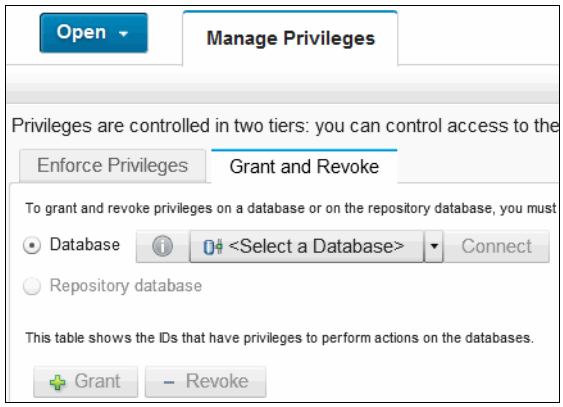


Figure 5-46 Access the policy management wizard

5. In the Database drop menu, click **<Select a Database>**. The dialog, as shown in Figure 5-47 on page 150, displays the currently defined database connection profiles. Select the database connection profile for which you will implement the security policy.

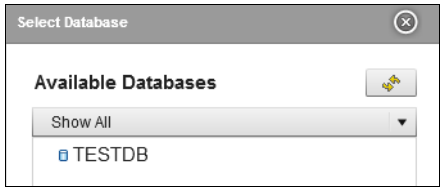


Figure 5-47 Select the database connection profile for the security policy

Note: Refresh the list if you cannot see the database connection profile that you want to manage.

Before you can modify the security policy, you must connect to the database, as shown in Figure 5-48.

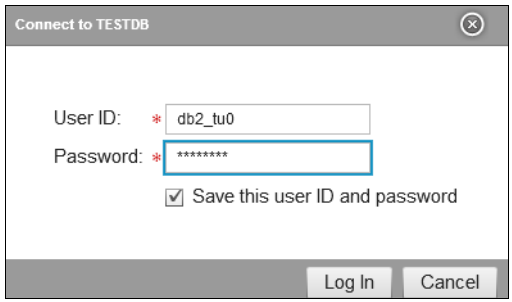


Figure 5-48 Connect to the database

6. Enter the credentials of a user that can modify the security policy and click **Log In**.

   The Workload Replay security policy for the selected database is displayed, as shown in Figure 5-49 on page 151. You can grant privileges to users, groups, or roles, or revoke them.

Grant Revoke

ID	ID Type	Privilege
DB2_TU0	USER	Can Capture Workload
DB2_TU0	USER	Can Replay Workload
DB2_TU0	USER	Can Import Workload
DB2_TU0	USER	Can Export Workload
DB2_TU0	USER	Can Delete Captured Workload
DB2_TU0	USER	Can Create Report
DB2_TU0	USER	Can Delete Report
DB2_TU0	USER	Can Delete Replayed Workload

Figure 5-49 Review the current security policy for this database

Note: By default, the owner of the database connection profile has all privileges.

7. To grant a privilege, click **Grant**.
8. In the dialog window, enter an ID and select the ID type (USER, GROUP, or ROLE). Figure 5-50 depicts an example, where we are granting members of group WR_TG1 the authority to replay workloads on this database.

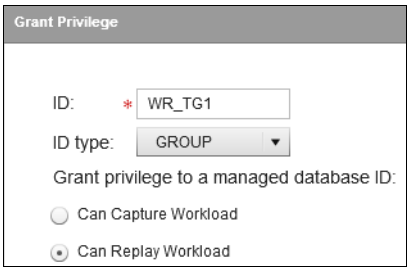


Figure 5-50 Grant a privilege to a group

9. Close any confirmation messages.

   The updated security policy is displayed, as shown in Figure 5-51 on page 152.

Grant Revoke

ID	ID Type	Privilege
DB2_TU0	USER	Can Capture Workload
DB2_TU0	USER	Can Replay Workload
DB2_TU0	USER	Can Import Workload
DB2_TU0	USER	Can Export Workload
DB2_TU0	USER	Can Delete Captured Workload
WR_TG1	GROUP	Can Replay Workload
DB2_TU0	USER	Can Create Report
DB2_TU0	USER	Can Delete Report
DB2_TU0	USER	Can Delete Replayed Workload

Figure 5-51 Review updated security policy

10. To revoke a privilege, select it and click **Revoke**.
11. Repeat the steps as needed to implement the security policy that you want.

6

Capturing and replaying workloads

This chapter describes the process of capturing and replaying workloads on your IBM InfoSphere Optim Workload Replay (InfoSphere Workload Replay) servers. In the chapter, we describe the following information:

- Content of a captured workload
- How to configure InfoSphere Workload Replay to capture the data that you want
- How to prepare your environment to successfully capture workloads
- How to prepare your test environment to successfully replay the captured workloads

We also describe how to export and move captured workloads between different InfoSphere Workload Replay servers, and how to use this export feature to archive captured workloads.

In this chapter, we assume that you installed and configured InfoSphere Workload Replay in your environment or environments, and that the workload replay components are installed and configured on your database servers.

Furthermore, to capture and replay workloads and create reports with InfoSphere Workload Replay, you must log in to the web console as a privileged user or a user with the `workload-replay-user` role or the `workload-replay-admin` role. For more information, see 7.1.6, “Creating a privileged user” on page 224 and 7.1.7, “Creating a user” on page 225.

In addition, you must have access to login credentials for user IDs that are granted the correct workload replay privileges on the databases on which you want to capture and replay workloads. For more information, for DB2 for z/OS, see 4.5.1, “Managing access to capture and replay actions” on page 104, and for DB2 for Linux, UNIX, and Windows, see 5.4.1, “Managing access to capture and replay actions” on page 146.

6.1 The workload capture and replay workflow

Capturing and replaying workloads with InfoSphere Workload Replay is a multi-step process that involves both web console driven steps and steps that are performed directly on the database servers.

Note: Except where noted, the terminology that is used in this chapter illustrates capturing and replaying workloads in a DB2 for Linux, UNIX, and Windows environment.

6.1.1 The basic workload replay steps

The capture and replay process consists of a sequence of steps; some of the steps are performed in the InfoSphere Workload Replay web console, and some steps must be performed outside the web console.

The following steps outline the recurring steps in a capture and replay workflow. The steps end with a comparison between the original captured workload and the same workload replayed on a different database.

The actual capture and replay process includes a set of basic steps that are performed in a set order:

1. Prepare the production environment for capturing.

   Before you capture a workload on your capture database, ensure that you have an up-to-date backup of the database. To successfully replay the workload on your test database, ensure that it is a good copy of the capture database.

2. Capture the workload.

   You use the InfoSphere Workload Replay web console to schedule or run the workload capture process.

3. Prepare the test environment for replaying the captured workload.

   Before you replay the captured workload, use your favorite backup or cloning tool to set up your replay database as a representative copy of the capture database that matches the state of the database at the start of the capture as much as possible.

You must also transform the captured workload into a replay-ready workload, which is a repackaged format that InfoSphere Workload Replay can use to run the SQL statements and transactions of the captured workload on a replay database. When you transform the captured workload, you select a replay database to replay it on. You can configure the workload to be replayed by using a default user ID for all SQL statement executions or you can map the captured user IDs to user IDs on the replay database. If necessary, you can also map the capture database schema to the replay database schema.

4. Replay the workload.

   When you replay the replay-ready workload on the replay server, the SQL data that was captured earlier is replayed in the correct sequence on the replay database. When you schedule or run the workload replay, you can set the replay speed to match the captured speed, or play it slower or faster to simulate different database loads.

   While the workload is replayed, InfoSphere Workload Replay performs another workload capture, this time on the replay database. This newly captured workload, which is called a *replayed workload* in the web console, can be compared to the original captured workload by creating a report to see any differences.

5. Compare and analyze.

   After you replay a captured workload on a test system, you can now create a comparison report to compare the execution of the workload on the two systems.

   You can use the reports to compare the accuracy at which the workloads replayed, based on criteria, such as how well the SQL statements and transactions matched and whether any SQL statements or transactions did not replay.

   In addition, you can compare the performance between the executions to see how SQL statement response times changed, and the number of SQL statements executed over time.

6.1.2 Iterative workload replay steps

One of the main usage scenarios for InfoSphere Workload Replay is to find and analyze changes in workload execution behavior when a database environment changes. With these changes identified, you can configure a modified environment to ensure that existing workloads replay successfully.

In this scenario, we use a workflow to help you understand how to modify the environment to successfully replay a baseline workload. The process includes an iterative cycle to fine-tune the replay environment.

The iterative steps are listed at a high level:

1. Create a baseline workload.

   A *baseline workload* is a workload that behaves well in the test environment and that can be used as a starting point when you test changes to the test environment.

   To create a baseline workload, you start with a captured workload. You replay this workload in the test environment and analyze the result by creating a comparison report.

   If the workload replayed with no issues and with the expected performance, the captured workload behaves as expected in the test environment and can be used as a baseline workload.

   If, however, differences exist in the behavior between the captured workload and the replayed workload, the test environment is not configured or behaving as expected.

   For example, if your test environment includes only a subset of the production data, some SQL statements and transactions that reference this data might replay incorrectly. You can then either include the data in the test database and replay and analyze the workload again, or exclude the SQL statements and transactions that reference this data and save the report as a new replay-ready workload that is now the new baseline candidate.

   Repeat this process until the workload that you replay behaves as expected. This workload is now your baseline workload.

   Figure 6-1 illustrates the process of creating a baseline workload.

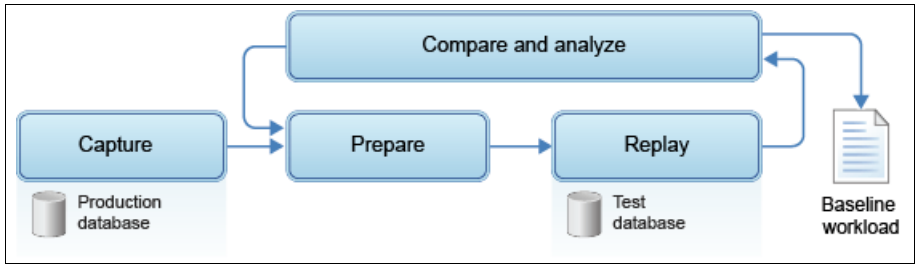


Figure 6-1 Create a baseline workload

2. Analyze the impact of changes on the workload execution.

   After you create the baseline workload, you can start modifying the replay database environment to test any changes that you plan to make in the production environment. You can, for example, update the database software, upgrade hardware or storage, create indexes or make other schema changes, or make any other changes.

   You then replay the workload on the modified database, capturing a new replayed workload in the process.

   You can now compare the newly replayed workload to the baseline workload in a new comparison report.

   Continue iterating until the workload execution characteristics for accuracy and performance meet your goals. Now, you can implement the same changes in the production environment confidently.

   Figure 6-2 illustrates the cycle of the iterative replay, report, and modify.

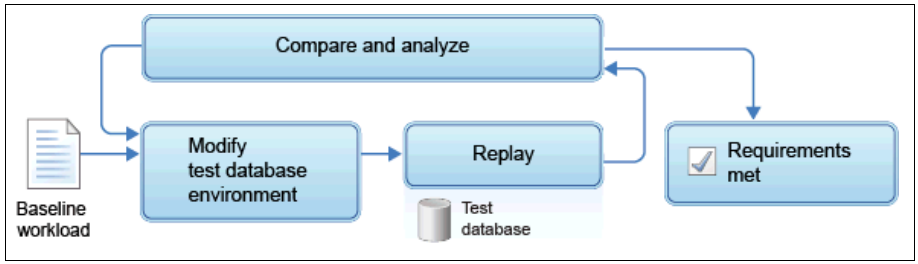


Figure 6-2 Iterative replay, report, and modify cycle

6.2 Planning

Before you start capturing and replaying workloads in your environment, depending on your type of database environment and the types of workloads that you plan to capture, a larger or smaller amount of planning might be required up-front before you connect to your database for the first workload capture.

For example, you need to determine the “what,” “when,” and “where” of the capture and replay process.

The following examples describe the capture and replay process:

- Capturing actual production workload data (what) from your production database (where) during peak hours (when) to use for stress testing requires precise timing of the workload capture.
- Capturing representative production database (where) workload data to cover a representative number of applications (what) for testing database software or hardware upgrades might require a longer workload capture (when).
- Capturing workload data in an isolated production environment (where) and replaying in a test environment (where) require you to move the captured workload between the two environments by exporting and importing the workloads. For information about replaying in isolated environments, see 6.5, “Moving workloads between servers” on page 200.

The requirements might also differ depending on your platform, see 6.2.2, “Capturing and replaying in a DB2 for z/OS environment” on page 160 and 6.2.3, “Capturing and replaying in a DB2 for Linux, UNIX, and Windows environment” on page 163.

6.2.1 General considerations

Before you start the workload capture and replay activities, consider the following general information.

Concurrent capture and replay activities

Only one workload capture or workload replay activity can be active at any time.

Connecting to your capture and replay databases

Before you can capture workloads from a database, you must first add a database connection profile for that database in the Workload Replay web console and grant the required capture and replay privileges to a user ID of that database. For details about adding database connections and granting privileges, for DB2 for z/OS, see 4.5, “Enablement of workload capture and replay in the Workload Replay web console” on page 98 and for DB2 for Linux, UNIX, and Windows, see 5.4, “Enablement of workload capture and replay in the Workload Replay web console” on page 140.

Cloning your capture database to your replay database

As part of the capture and replay cycle, you must also set up the replay database to be as close of a match to the original capture database as possible. For a workload to replay successfully, the database content must be the same. If the replay database content differs or is incomplete, the replayed workload might not yield the expected results.

To set up the replay database, use your favorite database tools to create a clone of the capture database to use when replaying. The clone does not have to contain the identical schema or user IDs. The schema or user IDs can be mapped as needed when you transform the captured workload for replaying. See “Mapping schemas” on page 171 and “Mapping user IDs” on page 173.

> **Tip:** To get a representative data set, it is a preferred practice to create the database clone to represent the capture database as closely as possible in time to the time when you plan to capture the workload. With InfoSphere Workload Replay, you can use stored procedures to run any database cloning or restore processes. You can create a data cloning method that runs before you capture or replay a workload. For more information, see 8.2.2, “Invoking external tools before workload capture or replay” on page 276.

6.2.2 Capturing and replaying in a DB2 for z/OS environment

The following features are available for DB2 for z/OS workload capture and replay only.

Filter out unwanted DB2 for z/OS SQL traffic

InfoSphere Workload Replay for DB2 for z/OS captures all SQL traffic on a stand-alone subsystem or active members in a data sharing group. Depending on how your environment is used, you might not be interested in all the SQL traffic from a capture and replay perspective. By using filters, you can filter out unwanted data during the capture phase. See Figure 6-3 on page 161.

Filters

You can add one or more filters to include or to exclude SQL statements during the workload capture process. An SQL statement is captured only if it fulfills the filtering condition that is set. You can base the filter conditions on criteria, such as authorization ID, connection type, or database table.

For example, if you are not interested in capturing SQL from the administration users `ADMIN1` and `ADMIN3`, use the following filter settings to remove workload traffic by the selected users:

- Filter type: Select **Authorization ID**.
- Operator: Select **not equal to one of list**.
- Operator value: Enter `ADMIN1`, `ADMIN3` separated by a comma.

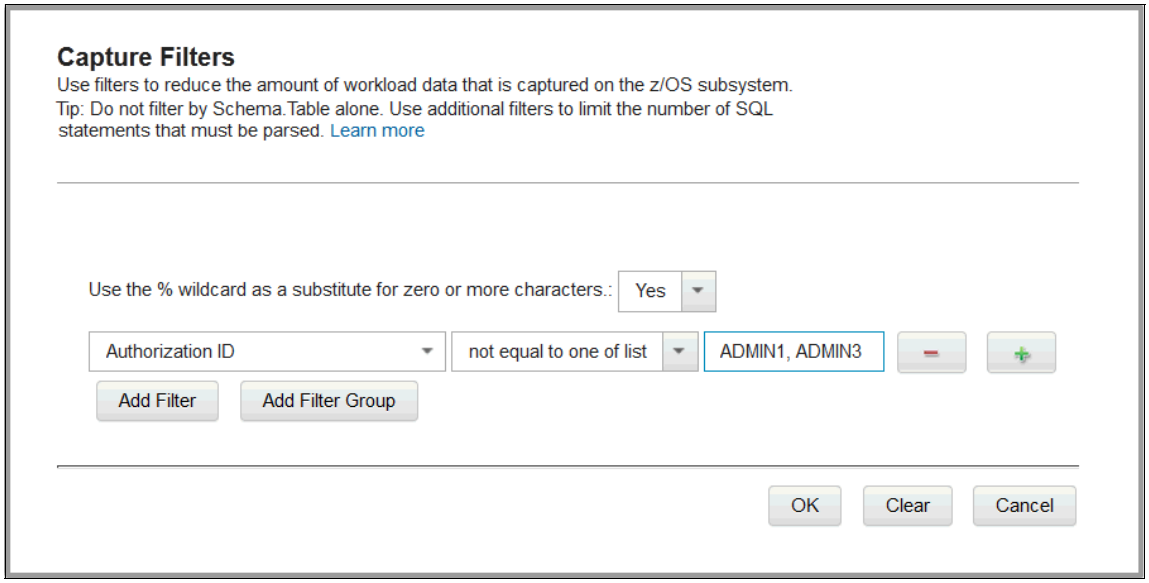


Figure 6-3 Filtering out authorization IDs

Filter groups

To build more complex filter rules, you can group separate filters together in one or more filter groups. With a filter group, an SQL statement is captured only if it meets the filtering conditions of the filters in at least one filter group.

For example, if you want to include SQL traffic from a specific authorization ID and one specific table, and also from another specific authorization ID and another table, you can set up two filter groups that define these filtering criteria. All SQL traffic that meets the requirement of at least one of the filter groups is captured.

Performance impact from filtering

The SQL statement filtering is performed directly on the DB2 for z/OS subsystem server by the Workload Replay S-TAP for DB2 on z/OS component. Depending on the complexity of your filters, more or fewer processor resources might be required to process the filtering criteria.

For example, a simple filter that specifies SQL traffic for a specific authorization ID might not increase processor usage much. However, if you filter by a specific database object, such as a table, the filtering process might require additional processing to identify the SQL statements to exclude or include. This requirement might increase the processor load for the filter.

Note: If you select a Schema.Table filter to capture SQL traffic for a specific database table, Workload Replay S-TAP for DB2 on z/OS must parse each SQL statement for the name of the table. To lower the processor load, you might consider including additional filters that reduce the number of SQL statements that must be parsed to identify the target tables. Filters are parsed in increasing complexity level order, with simple filter criteria, such as Authorization ID, being parsed before more complex filters, such as Schema.Table. For more information about InfoSphere Workload Replay for DB2 for z/OS performance considerations, see the following Techdocs Library white paper:

http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP102467

Capturing and replaying in a data sharing environment

If capturing a workload in a data sharing environment, by default SQL is captured on all active members that are associated with the location name or location alias. You can restrict on which members SQL is to be captured by deselecting members that are not to be included. See Figure 6-4.

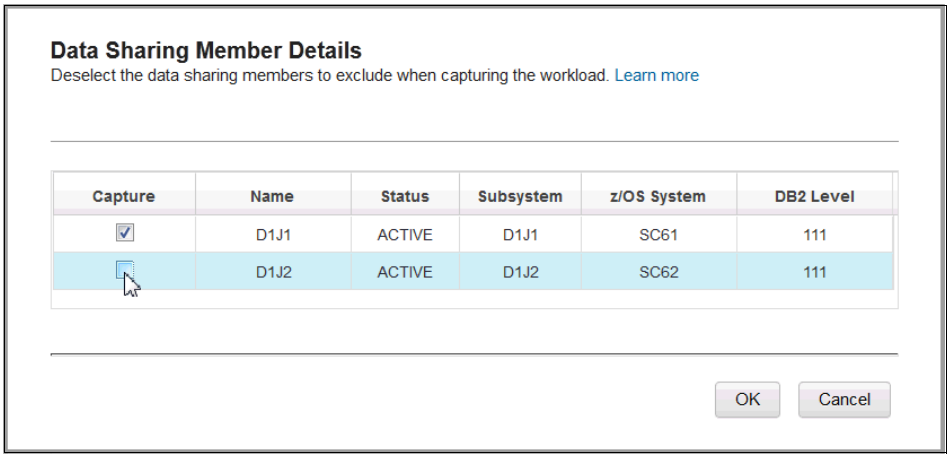


Figure 6-4 Deselecting a data sharing member

For example, if no SQL data is sent to the member while workload data is captured, you can exclude the member from the captured workload. This situation might be the result of using a data sharing member for load balancing.

Replaying workloads that are captured in data sharing environments

A workload that you captured in a data sharing environment can be replayed in either another data sharing environment or in a single subsystem environment. If you replay the workload in a data sharing environment, the workload is replayed on all active members of the replay data sharing group. To replay the workload on a subset of the members, you can create a location alias that represents the required subset of members. You can then use this location alias when you add the database connection for the data sharing environment.

6.2.3 Capturing and replaying in a DB2 for Linux, UNIX, and Windows environment

The following limitations are valid for DB2 for Linux, UNIX, and Windows workload capture and replay only.

Capturing and replaying workloads in DB2 DPF environments

InfoSphere Workload Replay can capture and replay SQL in database partitioning feature (DPF) environments if only a single coordinator node is used.

No support for DB2 pureScale capture and replay

InfoSphere Workload Replay Version 2.1.0.1 does not support DB2 pureScale.

Capturing and replaying workloads in high-availability environments

InfoSphere Workload Replay is, by default, not configured to capture or replay workloads that are executing on standby nodes if the primary database server fails. To capture or replay workloads on standby systems, you must create and use dedicated connection profiles for these systems.

6.3 Capturing and replaying workloads

In this section, we walk through the complete process of capturing and replaying workloads and creating reports with InfoSphere Workload Replay.

6.3.1 What is captured

A captured InfoSphere Workload Replay workload contains the SQL and metadata about the execution of the SQL statements and transactions. The captured SQL is replayed based on the metadata, and the resulting SQL workload is concurrently captured on the test system. The executions of the initial captured workload and the replayed workload can later be compared in a comparison report.

A captured workload includes the following types of SQL data:

- Dynamic SQL:
  - Statement text, for example:

    `SELECT item_number FROM item_table`
  - Time of SQL statement execution and response.
  - Execution count, for example:

    The SQL was executed 18,107 times
  - Information about database objects, such as names:

    The statement text was collected from `item_table`.
  - Information about data values that were passed in variables or data:
    - Literal values that are referenced in create, read, update, and delete (CRUD) statements (including CALL statements), for example:

      `SELECT item_number FROM item_table WHERE cid = “CID”`
    - Host variable values that are referenced in CRUD (including CALL statements), for example:

      `SELECT item_number FROM item_table WHERE cid = ?`

      Value of the host variable is “`CID`”.
    - XML or LOB data, for example, XML data:

      `“CUSTOMER SELECTED ITEM NUMBER 012345 to purchase”`
  - Data type information for host variables, for example:

    Column item_number is of type VARCHAR(19)

- Result set information.

  Apart from the number of rows returned or updated, no actual data values are saved, for example:

  `SELECT item_number FROM item_table WHERE cid = “CID”`

  When capturing the workload data, InfoSphere Workload Replay stores the information that a specific number of rows were returned but does not store the actual data (for example, `item_number = “012345”`).
- Return code and error message, if applicable.
- Isolation levels.
- Transaction information, such as commit and rollback processing.

► Static SQL (package, section information):

- Statement text
- Time of SQL statement execution and response
- Execution count
- Information about database objects
- Information about data values that are passed
- Result set information (no data values)
- Return code and error message, if applicable
- Isolation levels
- Transaction information, such as commit and rollback processing

► SQL commands, such as **SET**, that affect SQL execution behavior (by setting special register values), for example:

`SET CURRENT SCHEMA item_table_schema`

► User IDs:

- User IDs associated with database connections, for example:

  User JOE ran query `SELECT item_number FROM item_table`.
- No password information is stored.

6.3.2 Capturing an SQL workload

The first step in a workload capture and replay workflow is to capture a representative set of SQL statements and transactions on your production or capture database. Getting high-quality data in the workload capture is critical for the success of the subsequent workload manipulation and analysis steps: transforming, replaying, and reporting.

Capture the workload

To capture a workload, follow these steps:

1. Back up the capture database.

   Before you begin, back up the capture database so that you can configure the replay database to an identical state before you replay the workload. To clone the capture database onto the test database server that hosts your replay database, you can use a tool, such as IBM FlashCopy®, or backup so that you can restore and roll forward to a point in time. Replaying on a cloned database ensures that the workloads that you replay will more closely simulate the captured workload.

2. In the InfoSphere Workload Replay web console, open the capture wizard (Figure 6-5 on page 167):

   a. Log in to the InfoSphere Workload Replay web console of the main InfoSphere Workload Replay appliance at this website:

      `https://guardium_hostname_or_ip:8443/dsweb/console/ocr/index.jsp`

      For more information, see 7.1.1, “Roles and interfaces” on page 214.

   b. Select **Open** → **Capture and Replay**.

3. Provide the required information:

   – Folder: Select a folder to store the captured workload and all future workloads that are related to this captured workload.

   – Databases/location to capture: Select the database to capture from.

   – Aliases to capture: For Linux, UNIX, and Windows, include the database alias if you expect any connections to use aliases that are resolved at the server.

   – Capture filters: For DB2 for z/OS, use filters to include or to exclude SQL statements based on filtering criteria, such as authorization ID, connection type, or database table. An SQL statement is captured if it fulfills the filtering condition for the filter or the filter group.

   – LOB and XML data options: You can capture and replay large object (LOB) and XML workload data in two ways. Capture and replay the actual LOB and XML data, or capture the data length only, and then use generated data of the same length when the workload is replayed.

   – Start time and duration: Set the start time for the workload capture, and the duration.

   > **Note:** If you use a data cloning method, the start time is the time that the data cloning starts. The actual workload capture starts when the cloning is complete and continues for the scheduled duration.

– Data cloning method: You can create a data cloning method that calls a stored procedure on the database. If you select to clone the database with a data cloning method, at capture time the cloning procedure is run first and when it completes, the capture starts. For more information, see 8.2.2, “Invoking external tools before workload capture or replay” on page 276.

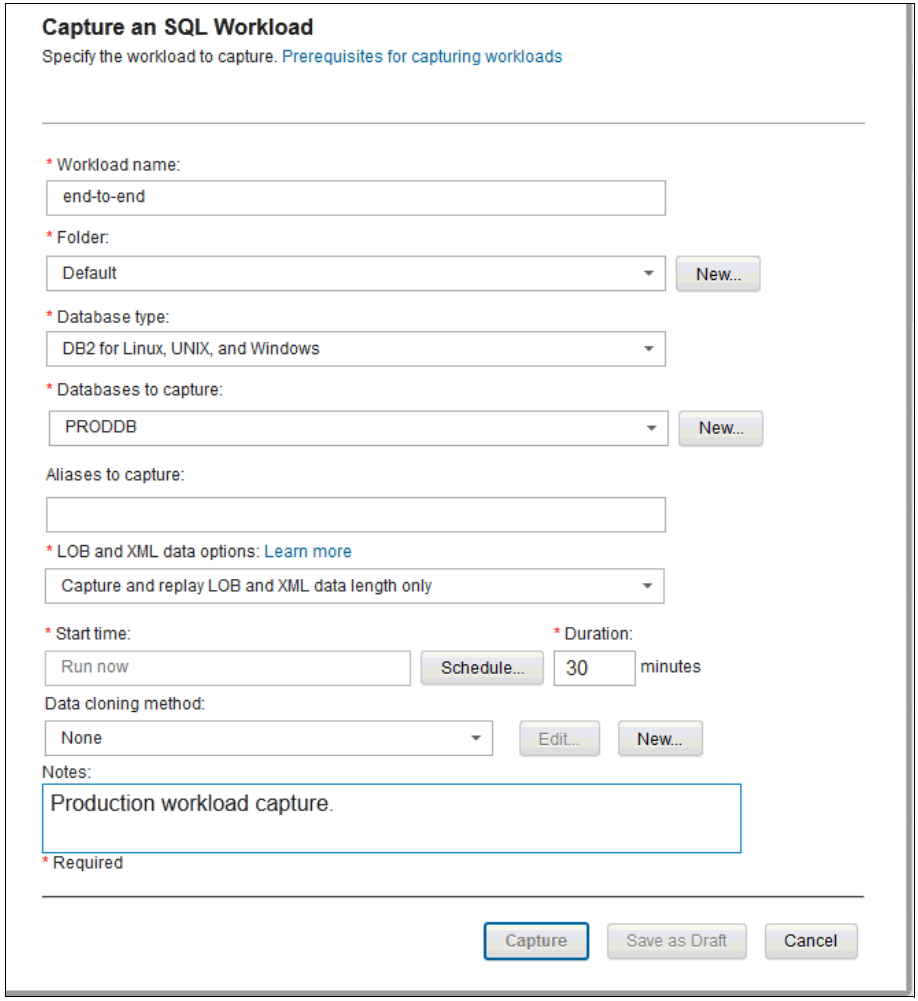


Figure 6-5 Capture an SQL workload wizard

4. Click **Capture**.
5. If prompted, authenticate with a capture database user ID with the Can Capture Workload privilege.

6. The capture status page opens.

   Use this page to monitor the progress of your workload capture.

   Note: You can stop the workload capture at any time to create a valid captured workload of a shorter than planned duration. A stopped workload capture is saved as a Completed workload in the grid, but the Capture Process Status details window shows the capturing workload data as *Stopped*, not Completed, as seen in Figure 6-6.

   The capture process continues in the background if you leave this page.

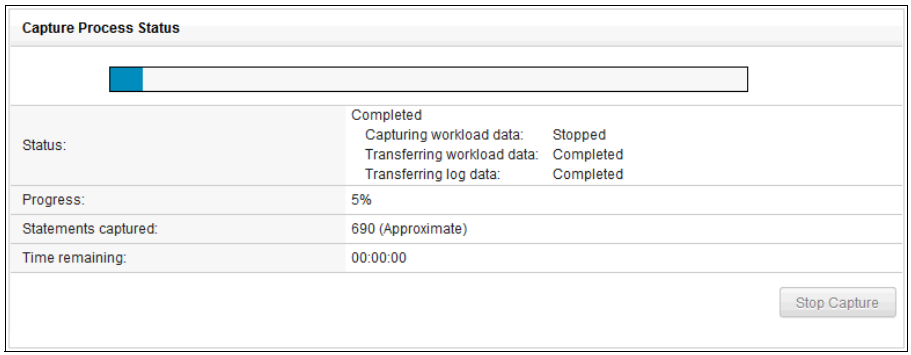
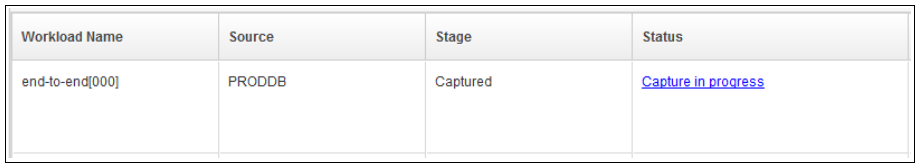


Figure 6-6 A stopped workload capture appears as completed with a Stopped status

7. When the workload capture is started, a new captured workload is added to the grid in the specified folder.

   At any time, you can log in to the web console and check the status of the ongoing workload capture from the SQL Workloads grid in the folder that you specified. You can click the status link for the workload to open the status page to see more details, and to access the capture log (Figure 6-7).



Workload Name	Source	Stage	Status
end-to-end[000]	PRODDB	Captured	Capture in progress

Figure 6-7 When the workload capture is started, a new captured workload is added

Reviewing a captured workload

When the capture process completes, review the capture log to ensure that workload data was successfully captured, and that no errors occurred.

If all seems well, you can also create a capture report to take a closer look at the workload data (SQL statements and transactions) that was captured. At this stage, if specific data was not captured or unwanted data was captured, you can go back and recapture the workload, as needed.

Creating a capture report

To create a capture report, follow these steps:

1. From the grid, right-click the captured workload and select **Report**.
2. Ensure that the **Capture Report** report type is selected.
3. Click **Create Report** to start the report generation process.
4. If prompted, authenticate with a capture database user ID with the Can Create Report privilege.
5. The web console opens to the report status page.
6. When the capture report process is complete, the report opens in the web console. See Figure 6-8 on page 170.

Analyzing the capture report

You can use the capture report to view the captured workload data before you transform the captured workload to a replay-ready workload. From the capture report page, you can look at overview information for the captured workload, and drill down into the captured SQL statements and transactions to verify that the workload data that you are interested in was captured and that no other unwanted SQL statements and transactions were captured.

Use the Captured SQL and Captured transactions tabs to get an overview of the captured workload data. You can drill down into the statement text for each unique SQL statement and each unique transaction.

The report shows the following headings:

- Statement Text
- Number of Executions
- Total Response Time
- Total Rows Returned
- Total Rows Updated
- Collection.Package.Section (Version)
- Current Schema
- Client Application
- Client User ID

- Client Workstation
- Client Accounting

> **Tip:** From the Captured SQL Statements tab or the Captured Transactions tab, you can export the report data to a delimited text file to analyze the data in your favorite tool. For more information, see 8.2.1, “Exporting SQL for analysis with third-party tools” on page 275.

Figure 6-8 shows the capture report.

Details | **Captured SQL Statements** | Captured Transactions

The SQL statements that were captured. Learn more

Report Metric	Unique	Executions	Description
Captured SQL Statements	25	4,226	All unique SQL statements in the captured

Export...

Capture C	Statement Text	Number of	Total Respon	Total Rows R	Total Rows U	Collection.Packag	Current Sche	Client Applic	Client User I
1	SELECT INST_NAME FROM SYSIBMADM.ENV_INST_INFO	1	00:00:00.0006	1	0				
2	select varchar_format (current timestamp, CAST (? AS VARCHAR(40))), current timezone from sysibm.sys	1	00:00:00.0000	1	0				
3	SELECT CU1.CUST_CODE, CUST_FIRST_NAME, CUST_LAST_NAME, CO1.CUST_TOTAL FROM GOSALESCT.CUST_CUSTOMER C	125	00:00:00.5826	0	0				
4	SELECT CU.CUST_CODE, CU.CUST_LAST_NAME, COH.CUST_ORDER_NUMBER, DATE(COH.CUST_ORDER_DATE) AS CUST_ORD	19	00:00:02.7400	30,134	0				

Figure 6-8 The capture report

6.3.3 Transforming a captured workload for replaying

Before you can replay a captured workload, you must transform it for use on the replay database. The captured workload contains information from the original workload that acted on the capture database, including connection information, schema information, and user ID information. To be able to replay the workload on a replay database, the information must be mapped for that database. You can create multiple replay-ready workloads from each captured workload to suit different scenarios for your environment.

Transforming the captured workload

To transform a captured workload, follow these steps:

1. In the grid, right-click a captured workload and then select **Transform**. You can also click **2. Transform** in the menu bar.
2. Select a replay database on which you want to replay the workload.

3. If needed, map the database schema from the capture to the replay database. See “Mapping schemas”.
4. DB2 for z/OS: Map any static SQL collection IDs from the capture to the replay database. See “DB2 for z/OS: Mapping static SQL collection ID” on page 172.
5. Click **Next**.
6. Add a default replay user ID that will replay the captured SQL statements on the database. The user ID must be authorized to execute all the captured SQL on the database.
7. Optional: Map the captured user IDs to user IDs on the replay database. See “Mapping user IDs” on page 173.
8. Click **Transform** to start the workload transformation.
9. When the workload transform is started, a new replay-ready workload is added to the grid in the specified folder.

   At any time, you can log in to the web console and check the status of the ongoing workload transform from the SQL Workloads grid in the folder that contains the initial captured workload. You can click the status link for the workload to open the status page to see more details, and to access the transform log.

Mapping schemas

For a workload to replay successfully, the schemas on the capture database and the replay database must match. Unmatched schemas might result in mismatched SQL statements when you replay the workload.

Schema mapping affects schema names in dynamic SQL statements with fully qualified table references only. Schema qualifiers for static statements are not modified by schema mapping.

> **Note:** If the captured workload statement that you want to map contains a delimited identifier, you must specify a value in quotations in the capture schema, for example:
>
> "Order" → "Order1" does not affect `select * from "order"."customer"`. But, order → order1 changes `select * from Order.customer` to `select * from order1.customer`.
>
> Depending on your database environment, schema mappings might be case-sensitive.

A preferred practice for comparing workloads is to clone the capture database before you capture the workload and then to replay the workload after you set the replay database to the same state that the capture database was in. If the replay database is an identical clone of the capture database, schema mapping is not required.

If the clone is not identical, or if statements in the workload contain schema information that does not correspond to the schema on the replay database, you must map mismatched schemas to allow the replay-ready workload to replay successfully.

Schema mapping issues can be identified in the comparison report. In the report, you find that certain SQL statements that contained explicit schema names did not run correctly. In the report, these statements are listed as SQL statement mismatches with SQL return codes, such as -204 or -206.

By analyzing the SQL statements that did not replay correctly, you find that error codes are caused by mismatches in the database schema. To resolve the mismatches, you can transform the captured workload again and add a schema mapping to correct for the mismatch in the new replay-ready workload.

Delete an entered value to reset an edited schema mapping to the captured schema.

DB2 for z/OS: Mapping static SQL collection ID

To successfully replay a workload that contains static SQL packages, any captured collection ID for the capture subsystem must have a matched collection ID on the replay subsystem. The dynamic collection IDs are replayed by using the job-completion checker (JCC) driver. The dynamic collection IDs are dynamically remapped, as needed.

If the replay subsystem is an identical clone of the capture subsystem, collection ID mapping is not required. If the clone is not identical, or if statements in the workload contain collection ID information that does not correspond to the collection IDs on the replay database, you must map mismatched collection IDs to allow the replay-ready workload to replay successfully.

Unmatched collection IDs might result in unmatched SQL statements in the replayed workload.

You can map static capture collection IDs to the replay subsystem by entering corresponding replay collection IDs. Delete an entered value to reset an edited collection ID to the captured collection ID.

Mapping user IDs

For a workload to replay successfully, each connect SQL statement must include a valid user ID and password for the replay database.

When a workload is captured, all user IDs that connected to the capture database are captured and included in the captured workload. To be able to replay the workload, each user ID that is included in the captured workload must be mapped to a user ID and its password on the replay database. You map the user IDs when you transform the captured workload.

Incorrectly mapped user IDs cause SQL statements to fail on the replay database, causing SQL statement mismatches.

You can map all captured users to a single default user ID. In addition to the default user ID, you can also map individual captured user IDs to corresponding user IDs.

The replay database user IDs that you specify must have the correct privileges on the database to complete the replayed tasks. For more information, for DB2 for z/OS, see 4.5.1, “Managing access to capture and replay actions” on page 104, and for DB2 for Linux, UNIX, and Windows, see 5.4.1, “Managing access to capture and replay actions” on page 146.

Reviewing replay-ready workloads

When the transform process completes, review the transform log to make sure that the workload data was successfully transformed, and that no errors occurred.

If all seems well, much like for a captured workload, you can create a transform report to take a closer look at the replay-ready workload data (SQL statements and transactions) that were transformed. At this stage, if it turns out that specific data was incorrectly transformed, you can go back and retransform or recapture the workload, as needed.

Creating a transform report

To create a transform report, follow these steps:

1. From the grid, right-click the replay-ready workload and select **Report**.
2. Select the **Transform Report** type of report.
3. Click **Create Report** to start the report generation process.
4. If prompted, authenticate with a replay database user ID with the Can Create Report privilege.
5. The web console opens to the report status page.

6. When the transform report process is complete, the report opens in the web console. See Figure 6-9.

Details | **Transformed SQL Statements** | Transformed Transactions

The SQL statements that will be replayed. Learn more

Report Metric	Unique	Executions	Description
Transformed SQL Statements	25	45,259	All unique SQL statements in the tran

Export...

Captur	Statement Text	Number of Executions	Total Rows Returned	Total Rows Updated	Collection.Package.Sect
1	SELECT INST_NAME FROM SYSIBMADM.ENV_INST_INFO	1	1	0	
2	select varchar_format (current timestamp, CAST (? AS VARCHAR(40))), current timezone from sysibm.sys	1	1	0	
3	SELECT CU1.CUST_CODE, CUST_FIRST_NAME, CUST_LAST_NAME, CO1.CUST_TOTAL FROM GOSALESCT.CUST_CUSTOMER C	1,300	0	0	

Figure 6-9 The transform report

6.3.4 Replaying workloads

When you replay a replay-ready workload on a replay database, InfoSphere Workload Replay takes the captured workload and replays it in the sequence in which it was captured. In addition, with InfoSphere Workload Replay, you can change certain settings to modify the way that the workload is replayed. For example, you can select to replay the workload faster or slower than the original captured workload to vary the SQL statement throughput and increase or decrease the load on the database server.

While the workload is replayed, InfoSphere Workload Replay simultaneously captures a workload on the replay database, capturing the SQL statements and transactions while they are replayed. The captured workload data is saved as a replayed workload that can later be compared with the original captured workload or another replayed workload to see how well the workload replayed in the test environment.

Replaying the replay-ready workload

To replay a replay-ready workload, follow these steps:

1. Reset the replay database.

   Before you begin, reset the replay database to a state that is similar to the capture database before you replay a workload. You can use a tool, such as FlashCopy, or backup so that you can restore and roll forward to a point in time to clone the capture database onto the database server that hosts your replay database. Replaying on a cloned database ensures that the workloads that you replay will more closely simulate the captured workload.

2. In the grid, right-click a replay-ready workload and then select **Replay**. You can also click **3. Replay** in the menu bar.

3. Validate that the replay user IDs and passwords are correctly set for your workload replay.

4. Select a start time for the workload replay. Either run the replay now or set a specific time.

5. Select the speed for the workload.

   You can select to run the workload at a different speed than the original captured workload. You can, for example, replay a workload at a faster speed to stress test an environment, or replay at a slower speed in a less powerful environment.

   When you change the replay rate, you decrease or increase the recorded wait time between SQL statements or transactions, which in turn decreases or increases the total elapsed time for the replayed workload.

6. Optional: Set a data reset method.

7. DB2 for z/OS: Optionally set a replay capture filter. For details, see “Filter out unwanted DB2 for z/OS SQL traffic” on page 160.

   Tips: No filter is selected, by default.

   If you select to retrieve the capture filters that were used during the workload capture, validate that the filters will apply in your replay environment, and modify them, as needed.

   For example, if you use a filter to include SQL traffic from a specific authorization ID only, and you map that user ID to a different user ID in the replay environment, you must modify the filter. The same type of modifications might be required if you mapped schemas or collection IDs, or if your capture and replay environments differ in other ways.

8. Click **Replay** to start or schedule the workload replay.

> **Important:** If you are using the built-in data cloning method to manage the cloning process, the actual workload replay starts when the cloning is complete, and continues for the scheduled duration.

9. When the workload replay is started, a new replayed workload is added to the grid in the specified folder.

   At any time, you can log in to the web console and check the status of the ongoing workload replay from the SQL Workloads grid in the folder that contains the initial captured workload. You can click the status link for the workload to open the status page to see more details, and to access the replay log and concurrent capture log.

> **Tip:** If the replay status page logs indicate that several replay issues, such as unmatched SQL statements or transactions, occur, perhaps the replay environment is incorrectly configured. In this case, you can cancel the workload replay. If you cancel the workload replay, an incomplete replayed workload is created.

Reviewing replayed workloads

When the replay process completes, review the replay and capture logs to ensure that workload data was successfully replayed and concurrently captured, and that no errors occurred.

If all seems well, similar to a transformed workload, you can create a replay report to look closely at the workload data (SQL statements and transactions) that were replayed. At this stage, if specific data was not correctly replayed, you can go back and replay the workload again, as needed.

Creating a replay report

To create a replay report, follow these steps:

1. From the grid, right-click the captured workload and select **Report**.
2. Select the **Replay Report** type of report.
3. Click **Create Report** to start the report generation process.
4. If you are prompted, authenticate with replay database user IDs with the Can Create Report privilege.
5. The web console opens to the report status page.
6. When the replay report process is complete, the report opens in the web console. See Figure 6-10 on page 177.

Details | Replayed SQL Statements | Replayed Transactions

The SQL statements that were captured while the workload was replayed. Learn more

Report Metric	Unique	Executions	Description
Captured SQL statements	25	45,224	All unique SQL statements in the

Export...

Capture	Statement Text	Number of Executions	Total Response Time	Total Rows Returned	Total Rows Updated
1	SELECT INST_NAME FROM SYSIBMADM.ENV_INST_INFO	1	00:00:00.219192	1	0
2	select varchar_format (current timestamp, CAST (? AS VARCHAR(40))), current timezone from sysibm.sys	1	00:00:00.017885	1	0
3	SELECT CU1.CUST_CODE, CUST_FIRST_NAME, CUST_LAST_NAME, CO1.CUST_TOTAL FROM GOSALESCT.CUST_CUSTOM C	1,300	00:00:06.260650	0	0

Figure 6-10 The replay report

6.3.5 Comparing workloads by creating comparison reports

After you replay a captured workload on a replay database, you can compare the way that the workloads behaved when they ran in their environments. InfoSphere Workload Replay stores data about the workload behavior when the workload was initially captured and when the workload was later replayed.

By creating a report, InfoSphere Workload Replay sets these workloads side-by-side and compares them, transaction by transaction and SQL statement by SQL statement.

InfoSphere Workload Replay uses the following attributes for comparison:

- SQL statement text (dynamic SQLs)
- Package information (static SQLs)
- Host variable SQL types
- Host variable values
- SQL return codes
- End unit of work (transactions, commit, or rollback)
- Rows returned (for SELECT SQLs)
- Rows updated (for user identifier (UID) SQLs, stored procedures, and static SQLs)

Depending on how well the workload replayed on the test database, and how similar the databases were, the workloads will differ more or less. A comparison report includes information about performance changes, missing and new SQL statements and transactions, and so on.

Note: To create and work with a comparison report, you must authenticate against the capture database and the replay database with user IDs that are granted the required privileges. For more information, for DB2 for z/OS, see 4.5.1, “Managing access to capture and replay actions” on page 104, and for DB2 for Linux, UNIX, and Windows, see 5.4.1, “Managing access to capture and replay actions” on page 146.

Creating the comparison report

To create a comparison report, follow these steps:

1. In the grid, right-click a captured or replayed workload and then select **Report**. You can also click **4. Report** in the menu bar. Figure 6-11 on page 179 shows the Create Report window.
2. Select the **Comparison Report** report type.
3. Select either a captured workload or a replayed workload for a baseline workload.
4. Select a replayed workload.
5. Optional: Click **Options** to set SQL statement grouping and masking criteria. For information, see “Optional: Grouping and masking SQL statements” on page 179.
6. Optional: Click **Advanced Options** to configure additional global report settings.
7. Click **Create Report** to start the report creation process, or click **Save as Draft** to save your current settings as a draft.

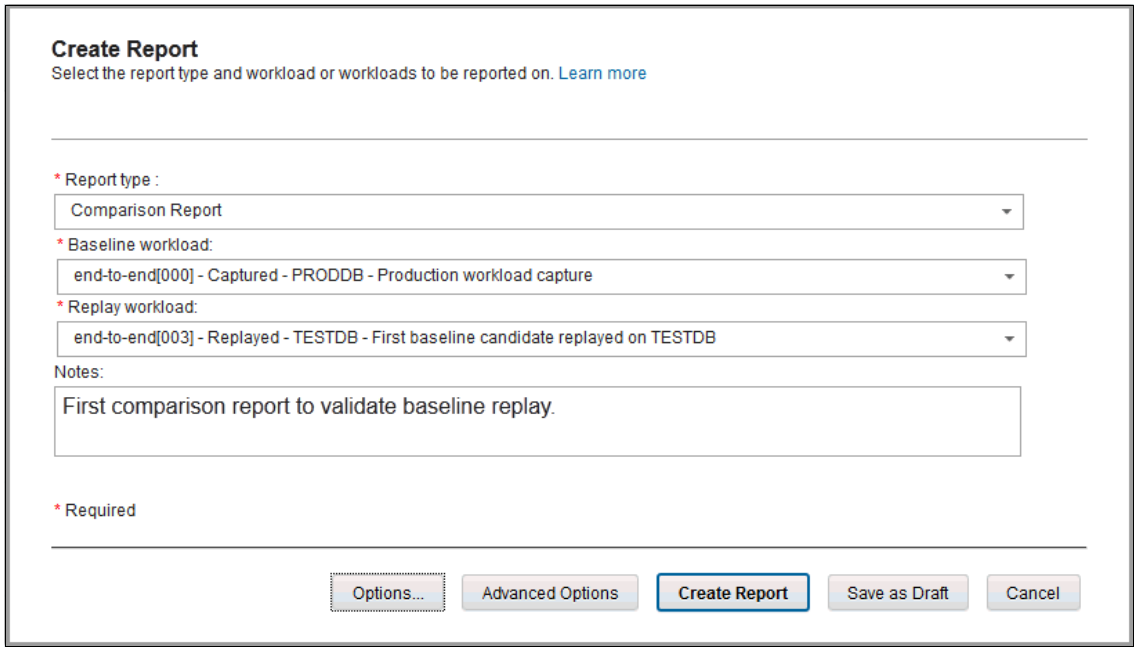


Figure 6-11 Create a report that compares a workload capture with a workload replay

Optional: Grouping and masking SQL statements

When you create a report, you can group SQL statements together as unique statements by specifying certain SQL attributes that are set as common for the unique SQL statement. In addition, if part of an attribute varies from one execution to another, you can use the masking to remove those characters from the grouping string.

The SQL statements can be aggregated to simplify comparing the execution count, total response time, and average response time. The statement grouping options are available in the Create Report wizard by clicking **Options**.

Figure 6-12 on page 180 shows the window for statement grouping and masking.

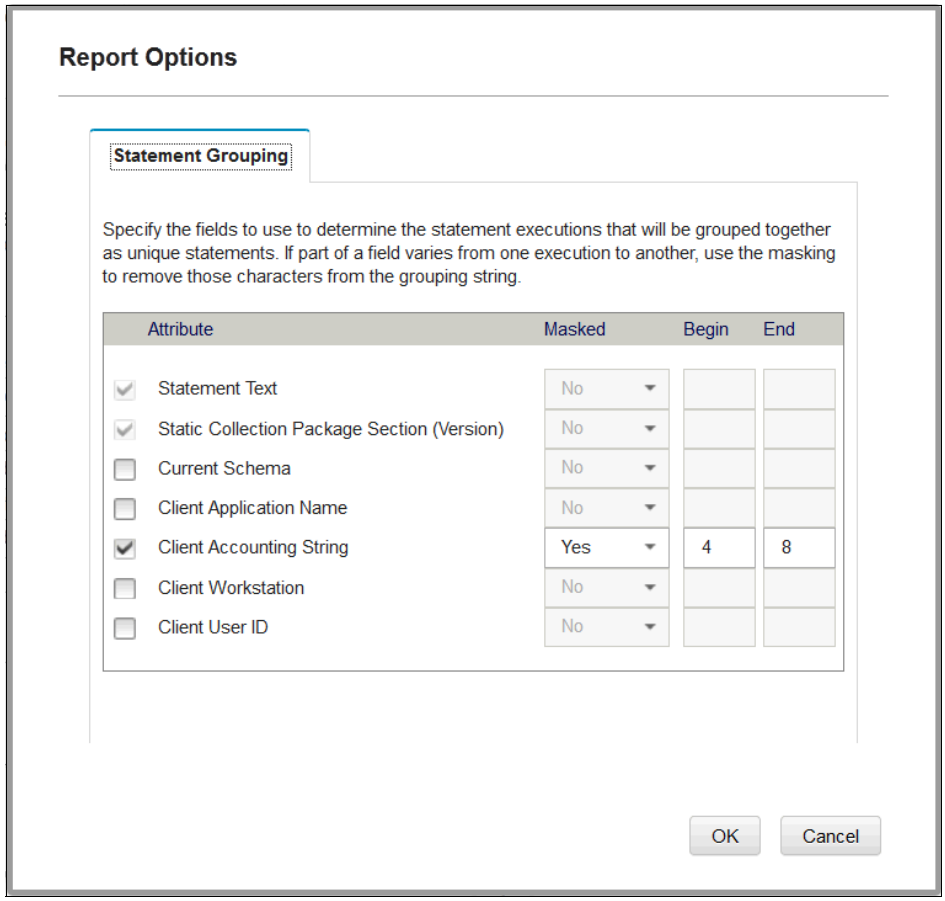


Figure 6-12 Statement grouping and masking

By default, the “Statement Text” for dynamic statements and the “Static Collection Package Section (Version)” for static statements are used as grouping attributes. The grouping attributes can also be masked with an asterisk (*) between the configured Begin and End indexes.

In addition, you can group by these attributes:

- Current schema
- Client application name
- Client accounting string
- Client workstation
- Client user ID

A client masking example is a client accounting string that is used by applications to tag transactions. The accounting string value might have keys that are specific to a transaction, such as Employee Code or Department Name. For example, “`Emp10012stock`”, “`Emp50013stock`”. To group all the Stock transactions into one transaction, the transaction-specific tags must be masked. In the report example that we created, the tags 10012 and 50013 can be masked with mask values of Begin as 4 and End as 8, which will result in a masked client account string value of “`Emp*****stock`”.

Optional: Configure global report settings

The report generation is controlled by a few user-modifiable settings. Access the report settings by clicking **Advanced Options** from the Create Report dialog or from the SQL Workloads page by clicking **More** → **Advanced options** → **Report Settings**. See Figure 6-13.

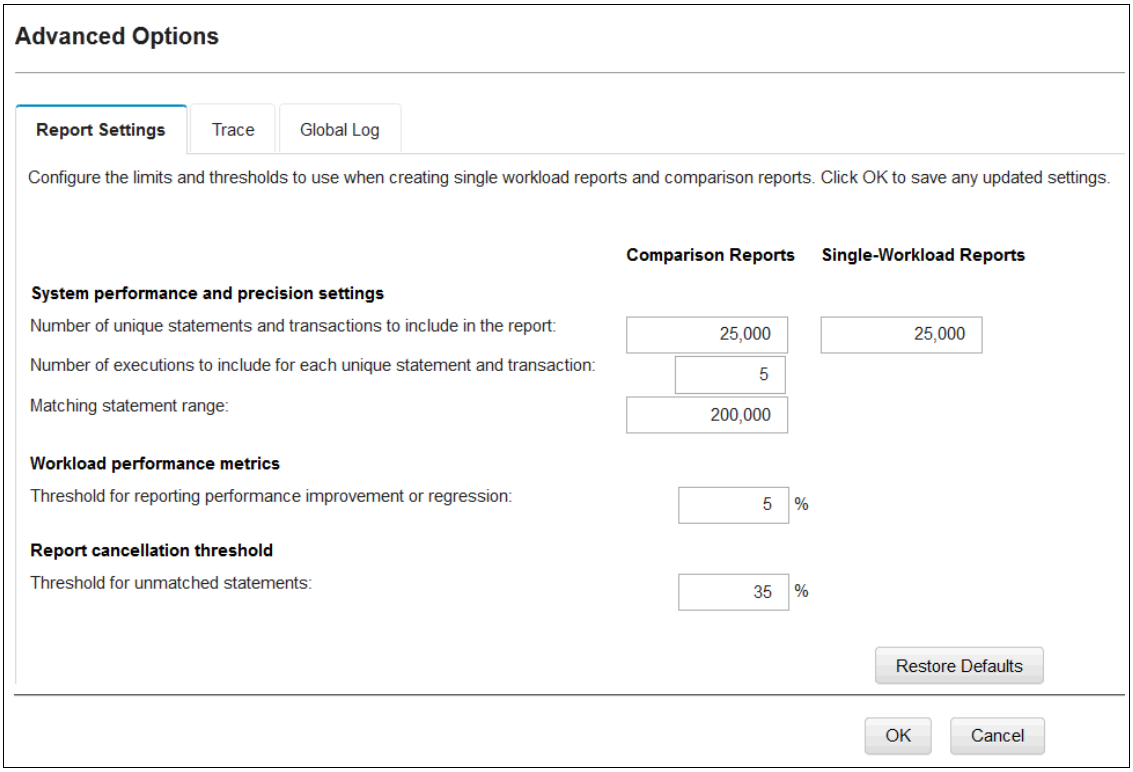


Figure 6-13 Report settings

The Report Settings options include the following categories:

- System performance and precision settings.
  - This option shows the number of unique statements and transactions to include in the report.

    The maximum number of unique statements and transactions to keep for each report.

    The default is 25,000.

    A higher value might affect the Java virtual machine (JVM) memory consumption and also performance.

    For example, the value is configured as 25,000 transactions (SQL statements), after comparison, the statements are aggregated by SQL text and only a maximum of 25,000 transactions are persisted and available in reports.
  - Number of executions to include for each unique statement and transaction.

    The maximum number of individual statement executions that are kept for each unique statement.

    The default is 5.

    The longest and shortest response time execution details that are listed for each statement include this number of executions.
  - Matching statement range.

    The maximum number of statements to allow between matching statements in the report.

    The default is 200,000.

    If a matching statement is identified but outside this range, the statement is considered a new SQL statement. A higher value might affect performance in terms of processing time. This value is adjusted by the system to optimize performance.

    For example, the value is configured as 200,000 statements. During the comparison, 200,000 captured statements are read and kept in the comparison cache. Then, the replay statements are read one at a time and matched against the captured statements in the comparison cache. This look ahead of 200,000 statements is always maintained in the comparison cache.

- Workload performance metrics

  Threshold for reporting performance improvement or regression (%). The percentage of change in performance that is needed to be reported as an improvement or regression for an SQL statement or transaction.

  The default is 5%.

  During the workload comparison, if the difference in performance metrics between baseline and replay is more than or equal to the value configured, those records are reported as an improvement or regression. This value applies to both SQL statements and transactions.

  For example, if the value is configured as 5%, any matched statement or transaction that is regressed or improved by at least 5% is reported.

- Report cancellation threshold

  Threshold for unmatched statements (%).

  The percentage of SQL statement mismatches between the baseline workload and the replay workload that will cancel the report.

  The default is 35%.

  Report generation tolerates the mismatch percentage to this configured value. If this threshold is reached, the report generation stops and the partial report is saved and available.

  For example, if at any time the unmatched statements go over 35%, the comparison is stopped and a partial report is generated.

6.3.6 How a comparison report is generated

During the comparison report generation, the SQL data that was originally captured in the baseline workload and the SQL data that was captured during a workload replay are compared.

The comparison process consists of the following high-level steps:

1. The SQL statements and transactions that were run and captured during the workload capture or an earlier replay (baseline) and the workload replay (replay) are processed. The workload details that are relevant for comparison are extracted for each SQL statement and transaction.

   During the records processing, InfoSphere Workload Replay identifies SQL statements that contain only literal values, and replaces these values with parameter markers. The SQL statement text is then aggregated to a unique SQL.

2. InfoSphere Workload Replay loads a batch of the baseline SQL statements and transactions into a comparison cache. The initial batch size is set by the “Matching statement range” report configuration value, which sets the maximum number of statements to allow between matching statements in the report. Even if a matching statement exists, but it is outside this range, the statement is considered a new SQL statement. For information, see “System performance and precision settings.” on page 182.
3. InfoSphere Workload Replay iteratively compares the cached records:
   a. The replayed SQL statements are read until an END_UOW (commit or rollback) record is encountered; in which case, the replayed record is processed as a transaction.
   b. InfoSphere Workload replay checks the replayed record against the cached baseline records to classify each record according to one of four states as shown in Table 6-1.

Table 6-1 Records matching state and criteria

State	Criteria
Matched	A baseline record exists with matching text, host variables, return code, and rows returned. InfoSphere Capture Replay uses the following attributes for comparison: ► SQL statement text (dynamic SQLs) ► Package Information (static SQLs) ► Host variable SQL types ► Host variable values. Some value difference is tolerated. See “Tolerated DB2 driver host variable differences” on page 185. ► SQL Return codes. Some value difference is tolerated. See “Tolerated SQL return code and rows returned differences” on page 187. ► End unit of work (transactions, commit, or rollback) ► Rows returned (for SELECT SQLs) ► Rows updated (for UID SQLs, stored procedures, and Static SQLs)
Unmatched	A baseline record exists with matching text and host variables but with unmatching return code, rows returned, and rows updated.
New	No baseline record with matching text and host variables exists.
Missing	At the end of the comparison report generation, any baseline records that were not marked as Matched or Unmatched after all the replayed records are compared are marked as Missing.

c. After the replayed record is marked, InfoSphere Workload Replay reads the next captured record into the cache and then compares the next replayed record.

   If all replayed statements are compared, the report creation is completed, and any remaining captured records are marked as Missing.

   Note: If the number of unmatched SQL statements or transactions exceeds the report setting “Threshold for unmatched statements”, the reporting process is stopped and a partial report is created. For information, see “Report cancellation threshold” on page 183.

Tolerated DB2 driver host variable differences

Different drivers might be used during the workload capture and the workload replay. The original capture driver might be any DB2 driver (command-line interface (CLI), Java Database Connectivity (JDBC), and so on) but the workload replay is always performed by using a JDBC driver. This driver difference means that certain data types might differ.

The matching algorithm treats the data types that are shown in Table 6-2 as equivalent.

Table 6-2 Capture and replay host variable SQL type differences that are tolerated

Capture host variable type	Replay host variable type
DB2_SQLTYPE_BINARY	DB2_SQLTYPE_VARBINARY
DB2_SQLTYPE_BLOB_LOCATOR	DB2_SQLTYPE_BLOB
DB2_SQLTYPE_CHAR	DB2_SQLTYPE_VARCHAR
DB2_SQLTYPE_CHAR	DB2_SQLTYPE_BLOB
DB2_SQLTYPE_CHAR	DB2_SQLTYPE_CLOB
DB2_SQLTYPE_CHAR	DB2_SQLTYPE_DBCLOB
DB2_SQLTYPE_CHAR	DB2_SQLTYPE_VARCHAR
DB2_SQLTYPE_CLOB	DB2_SQLTYPE_DBCLOB
DB2_SQLTYPE_CLOB	DB2_SQLTYPE_BLOB
DB2_SQLTYPE_CLOB	DB2_SQLTYPE_CLOB
DB2_SQLTYPE_CLOB	DB2_SQLTYPE_DBCLOB
DB2_SQLTYPE_CLOB	DB2_SQLTYPE_VARCHAR

Capture host variable type	Replay host variable type
DB2_SQLTYPE_CLOB_LOCATOR	DB2_SQLTYPE_CLOB
DB2_SQLTYPE_CSTR	DB2_SQLTYPE_VARCHAR
DB2_SQLTYPE_DATE	DB2_SQLTYPE_VARCHAR
DB2_SQLTYPE_DBCLOB_LOCATOR	DB2_SQLTYPE_DBCLOB
DB2_SQLTYPE_DECIMAL	DB2_SQLTYPE_DECIMAL_FLOAT
DB2_SQLTYPE_LONG	DB2_SQLTYPE_VARCHAR
DB2_SQLTYPE_LONG	DB2_SQLTYPE_BLOB
DB2_SQLTYPE_LONG	DB2_SQLTYPE_CLOB
DB2_SQLTYPE_LONG	DB2_SQLTYPE_DBCLOB
DB2_SQLTYPE_LONG	DB2_SQLTYPE_VARCHAR
DB2_SQLTYPE_TIME	DB2_SQLTYPE_VARCHAR
DB2_SQLTYPE_TIMESTAMP	DB2_SQLTYPE_TIMESTAMPTZ
DB2_SQLTYPE_VARBINARY	DB2_SQLTYPE_BLOB
DB2_SQLTYPE_VARBINARY	DB2_SQLTYPE_CLOB
DB2_SQLTYPE_VARBINARY	DB2_SQLTYPE_DBCLOB
DB2_SQLTYPE_VARBINARY	DB2_SQLTYPE_VARCHAR
DB2_SQLTYPE_VARCHAR	DB2_SQLTYPE_VARBINARY
DB2_SQLTYPE_VARCHAR	DB2_SQLTYPE_BLOB
DB2_SQLTYPE_VARCHAR	DB2_SQLTYPE_CLOB
DB2_SQLTYPE_VARCHAR	DB2_SQLTYPE_DBCLOB
DB2_SQLTYPE_VARGRAPH	DB2_SQLTYPE_VARCHAR
DB2_SQLTYPE_XML	DB2_SQLTYPE_DBCLOB
DB2_SQLTYPE_XML	DB2_SQLTYPE_BLOB
DB2_SQLTYPE_XML	DB2_SQLTYPE_CLOB
DB2_SQLTYPE_XML	DB2_SQLTYPE_DBCLOB
DB2_SQLTYPE_XML	DB2_SQLTYPE_VARCHAR

Tolerated SQL return code and rows returned differences

Because different drivers might be used in the capture environment and by the InfoSphere Workload Replay replay processes, different SQL return codes and rows returned values might be reported because of differences in driver prefetch behavior for cursor-related operations.

Because the resulting differences are an artifact of processing the SQL statement, specific discrepancies are tolerated by the comparison report. These discrepancies are shown in Table 6-3. SQL statements with the listed SQL return code and rows returned combination are classified as matching in the report, even though the SQL return codes and rows returned might differ in the report.

Table 6-3 Tolerated combinations of SQL return code and rows returned differences

Capture return code	Replay return code	Capture rows returned	Replay rows returned
0	100	N	>= N
0	0	N	> N

6.4 Analyzing comparison reports

This section describes how to interpret the InfoSphere Workload Replay comparison reports. A comparison report compares the execution of two workloads side by side so that you can compare the accuracy with which the workload replayed and any differences in performance between the two executions. You can compare a captured workload to a replayed workload, or a replayed workload to another replayed workload.

You can use a comparison report to determine how accurately a replayed workload represents a production workload by comparing a replayed workload to an original captured workload.

You can also use a comparison report to determine the impact of changes to a test system. In this case, you compare two replayed workloads to see performance similarities and differences when changes are made to the test system.

A comparison report consists of three tabs that collect the relevant workload comparison information:

- Details tab: High-level report details, log, and details of the baseline and replayed workloads.
- Replay Results tab: Details about how accurately the SQL statements and transactions were replayed. This tab opens, by default, when you open a completed report.
- Response Time tab: Details about performance improvements and regressions between the baseline and replay workloads.

6.4.1 The report details

The Details tab contains information about the workloads that were compared and the report log for report troubleshooting.

Figure 6-14 shows the report Details tab.

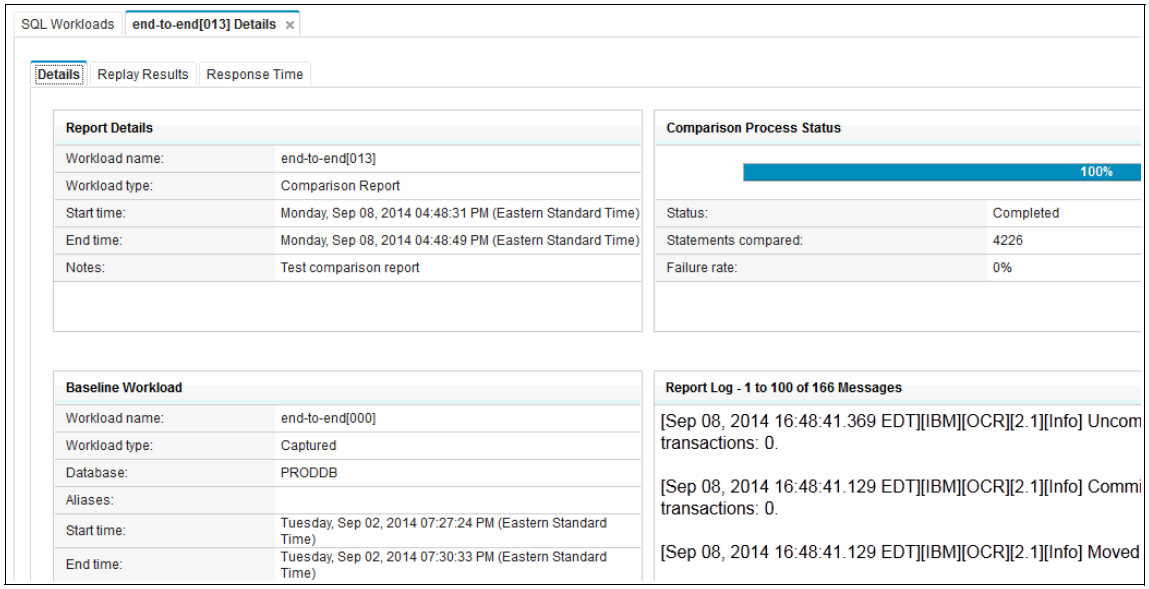


Figure 6-14 The report Details tab

6.4.2 The replay results report

By default, the comparison report opens on the Replay Results tab, which provides an easy to digest overview of the accuracy at which the replayed workload compared to the baseline workload. A highly accurate workload replay results in a high percentage of matched SQL statements and transactions and few to no SQL statements and transactions that were not matched or that are new.

This first report layer shows aggregated information from the comparison of two workloads. This layer shows high-level summaries, such as the number of mismatched SQL statements, SQL statements that did not replay, and new SQL statements that were executed while a workload replay was in progress but that did not exist in the original captured workload.

Figure 6-15 shows the report replay results.

Details | **Replay Results** | Response Time

This report shows the accuracy with which the workload was replayed for the SQL statements

SQL Replay Comparison Metric	Unique	Executions	Percentage
Baseline SQL	56	8,277,947	
Matched SQL replays	50	8,270,435	99.91%
Unmatched SQL replays	6	1,520	0.02%
Different return code	5	922	0.01%
Different number of rows returned	1	598	0.01%
Different number of rows updated	3	900	0.01%

Figure 6-15 The report replay results

Interpreting the replay result metrics

Use the accuracy metrics overview to get a basic understanding of why a replayed workload did not match the baseline workload.

Table 6-4 on page 190 lists the SQL replay comparison metrics and provides a description of how to interpret the metrics.

Tip: A transactions replay comparison metric is also included in the report, and the interpretation of transactions is similar to the interpretation of SQL statements.

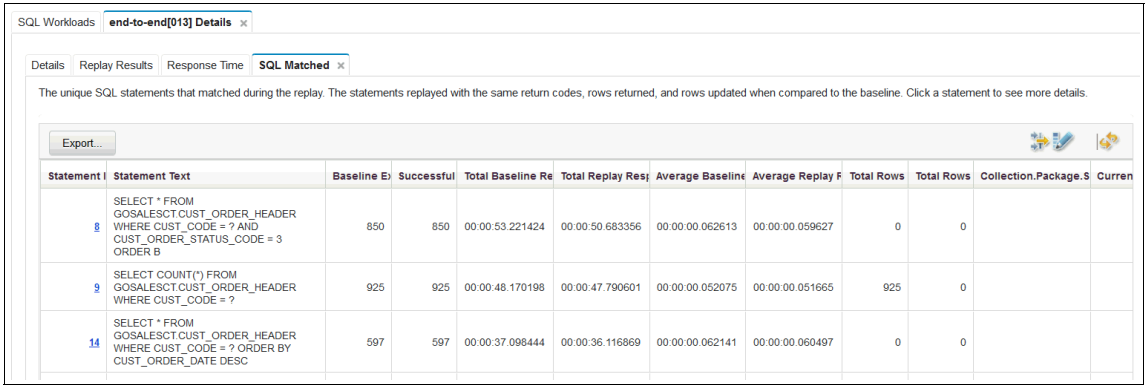
Table 6-4 Interpreting the SQL replay result metrics

Metric	Description	Interpretation
Baseline SQL	All SQL statements in the baseline workload	The number of unique SQL statements and the total number of executions of these statements in the baseline workload.
Matched SQL replays	SQL statements with the same return codes, rows returned, and rows updated in the baseline and replayed workload	If the number of matched SQL statements corresponds closely to the total number of captured SQL statements, your workload replayed with good accuracy.
Unmatched SQL replays	SQL statements with different return codes, rows returned, and rows updated in the baseline and replayed workload	Many unmatched SQL statements mean that your workload did not replay with good accuracy. Click the unmatched subcategories to drill down to and troubleshoot the unmatched SQL statements.
Unmatched SQL replay - Different return code	SQL statements that replayed with different return codes	Many SQL statements with different return codes compared to the captured SQL statements might mean that the replay database is missing database objects. Another possibility is that the user ID to replay the workload has insufficient privileges.
Unmatched SQL replay - Different number of rows returned	SQL statements that replayed with a different number of rows returned	Many SQL statements with a different number of rows returned might mean that the replay database data is not identical to the capture database data. Verify that your replay database is a good copy of the captured database and that you reset the replay database before you started replaying the workload.

Metric	Description	Interpretation
Unmatched SQL replay - Different number of rows updated	SQL statements that replayed with a different number of rows updated	Many SQL statements with different number of rows updated might mean that the replay database data is not identical to the capture database data. Verify that your replay database is a good copy of the captured database and that you reset the replay database before you started replaying the workload.
SQL statements that did not replay	SQL statements that were in the baseline workload but that were not replayed	Many SQL statements that did not replay might mean that the workload replayed out-of-synch with the captured workload. Try increasing the “Maximum range to check for matching statements” report parameter and create a new report to see whether the number decreases.
New SQL statements	SQL statements that were not in the baseline workload, but that were identified in the replayed workload	Many new SQL statements might indicate that additional database activity took place on the replay database while the workload was replaying. Another possibility is that the report settings need to be modified to be less restrictive. Report settings that are too restrictive can cause some SQL statements that replay correctly to be reported as new transactions. For example, filter conditions on z/OS might be too restrictive and not reflect differences in replay behavior, such as user ID mapping and connection type.

Metrics detailed window

From the replay results page, you can click a metrics link to see more information about the metric. Figure 6-16 on page 192 shows the report metric detailed window.



Statement I	Statement Text	Baseline E	Successful	Total Baseline Re	Total Replay Resp	Average Baseline	Average Replay F	Total Rows	Total Rows	Collection.Package.S	Curren
8	SELECT * FROM GOSALESCT.CUST_ORDER_HEADER WHERE CUST_CODE = ? AND CUST_ORDER_STATUS_CODE = 3 ORDER B	850	850	00:00:53.221424	00:00:50.683356	00:00:00.062613	00:00:00.059627	0	0		
9	SELECT COUNT(*) FROM GOSALESCT.CUST_ORDER_HEADER WHERE CUST_CODE = ?	925	925	00:00:48.170198	00:00:47.790601	00:00:00.052075	00:00:00.051665	925	0		
14	SELECT * FROM GOSALESCT.CUST_ORDER_HEADER WHERE CUST_CODE = ? ORDER BY CUST_ORDER_DATE DESC	597	597	00:00:37.098444	00:00:36.116869	00:00:00.062141	00:00:00.060497	0	0		

Figure 6-16 The report metric drill-down

This second layer shows the data that is associated with a single metric that was selected from the comparison metrics layer. From this layer of the report, you can see the SQL statements and transactions that differ between the two workloads. Each row lists a specific unique SQL statement, and it includes basic information, such as the number of baseline and replay executions, total and average response time, and rows returned and updated.

To see execution details for a specific SQL statement, you can click the statement identifier to open a third layer of details.

> **Tip:** From the metrics detailed layer, you can select and remove unmatched statements, and save the workload as a new replay-ready workload. For more information, see 6.4.4, “Creating a new replay-ready workload from a comparison report” on page 198.

Statement details

This third layer shows all the metrics and data points for a specific SQL statement or transaction that was selected from the metrics detailed layer.

Figure 6-17 on page 193 shows the report execution details.

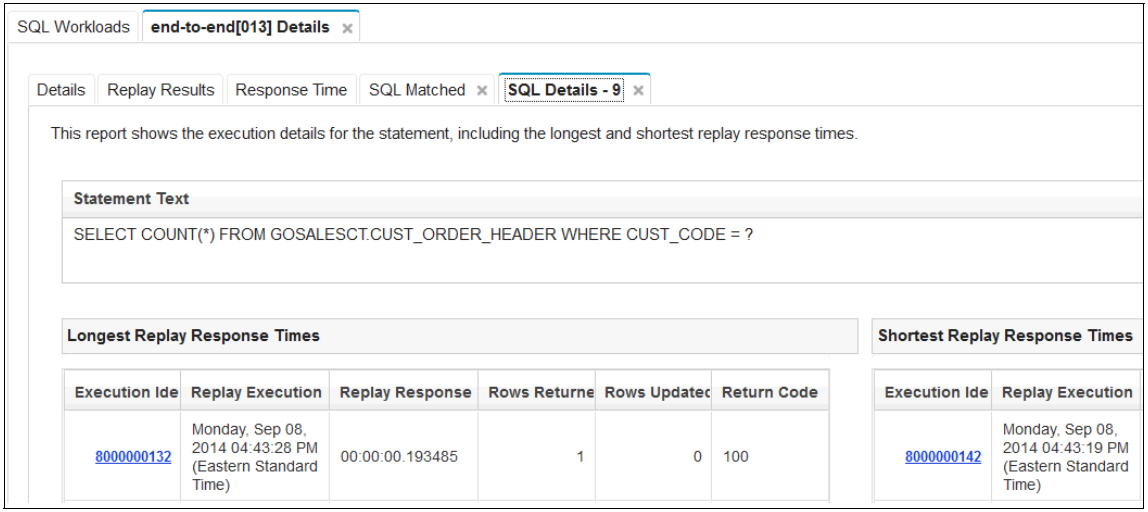


Figure 6-17 The report execution details

> **Tip:** You can set the number of individual executions to keep and display by changing the “Number of individual statement executions to keep for each unique statement” field in the report settings. From the SQL Workloads page, select **More** → **Advanced Options** → **Report Settings**.

To see the execution details for an individual execution, click the execution identifier.

Figure 6-18 on page 194 shows an individual execution example.

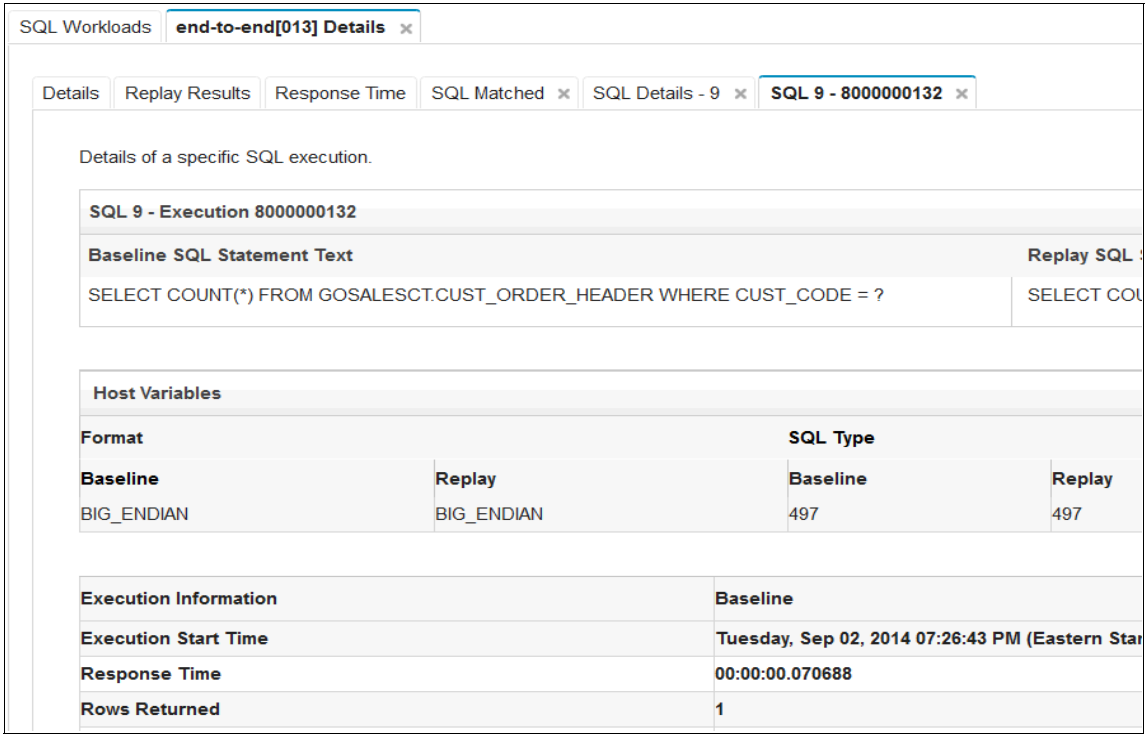


Figure 6-18 Individual execution details

6.4.3 The response time report

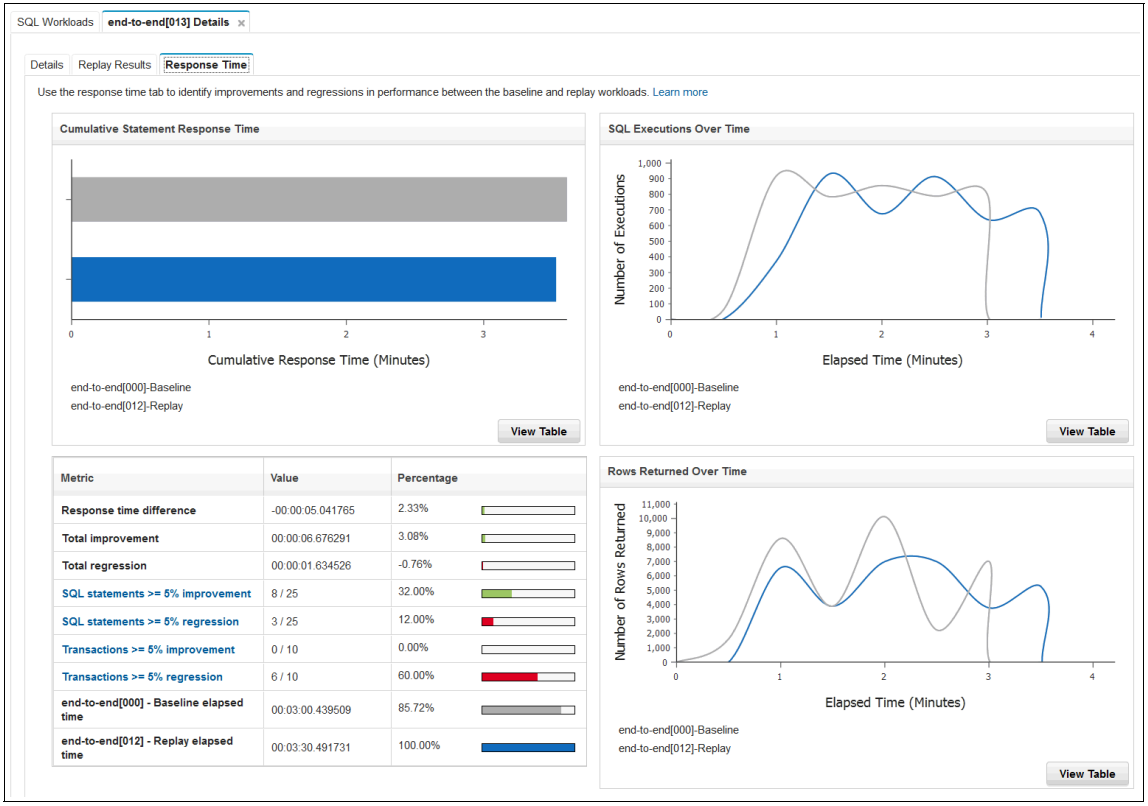
The third tab of the comparison report identifies improvements and regressions in performance between the baseline and replay workloads.

Three graphs provide a side-by-side comparison of the total cumulative SQL response time, number of SQL executions, and number of rows returned for the baseline workload and for the replayed workload that you compared to when you created the report.

> **Note:** The report metrics do not include any information about SQL executions that were not captured because a replay capture filter was used for a DB2 for z/OS workload replay.

In addition, a metrics table outlines main performance metric differences between the workloads.

Figure 6-19 on page 195 shows the report Response Time tab.



Metric	Value	Percentage
Response time difference	-00:00:05.041765	2.33%
Total improvement	00:00:06.676291	3.08%
Total regression	00:00:01.634526	-0.76%
SQL statements >= 5% improvement	8 / 25	32.00%
SQL statements >= 5% regression	3 / 25	12.00%
Transactions >= 5% improvement	0 / 10	0.00%
Transactions >= 5% regression	6 / 10	60.00%
end-to-end[000] - Baseline elapsed time	00:03:00.439509	85.72%
end-to-end[012] - Replay elapsed time	00:03:30.491731	100.00%

Figure 6-19 Report Response Time tab

Cumulative statement response time

The cumulative statement response time graph provides an overview of the relative performance improvement between the replayed SQL statements that exist in both the baseline and the replayed workload and that yielded the same results.

The cumulative statement response time might be longer than the total elapsed time because it adds all statement response times while statements might be running in parallel, being executed at the same time in the actual workload.

The cumulative response time is the sum of all statement response times, as though they were run back-to-back. Because the cumulative statement response time does not include wait times, it might indicate a significant execution improvement even though the actual elapsed time increased as though they were run back-to-back, but with resource contention.

In the example in Figure 6-20, the last statement for connection 3 represents a response time regression, and it is solely responsible for the longer elapsed time of the replayed workload.

Figure 6-20 shows a cumulative response time calculation.

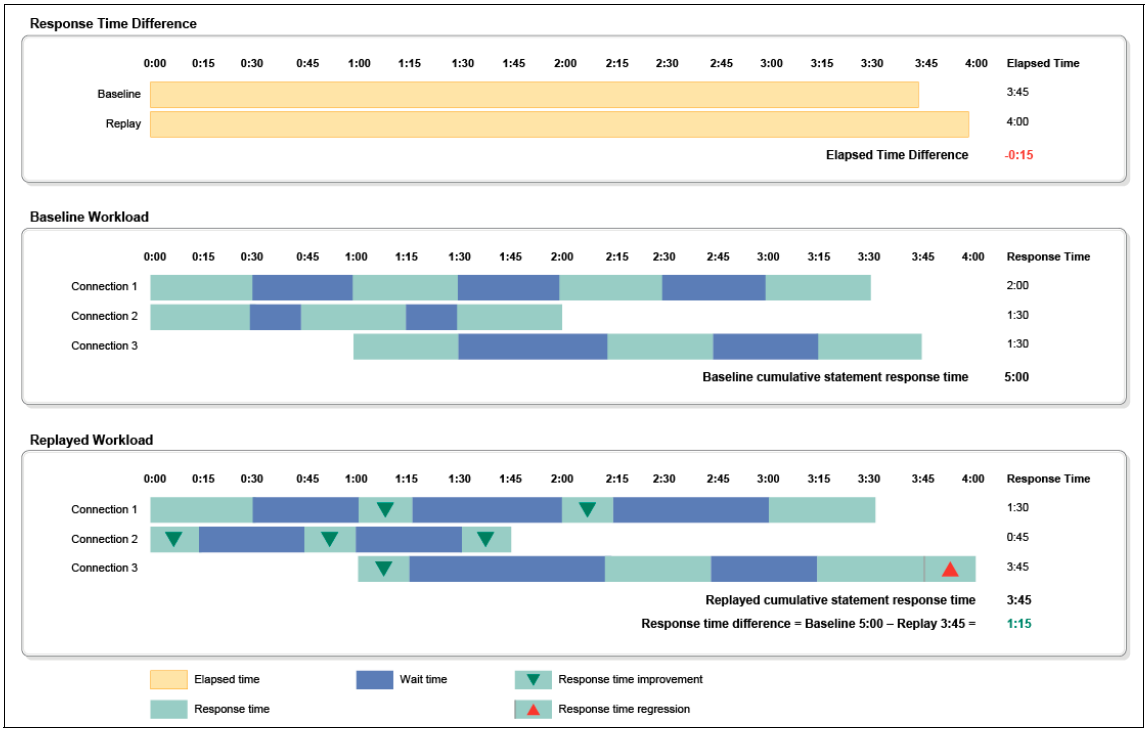


Figure 6-20 Cumulative response time calculation

SQL executions over time

This graph shows a comparison between the number of SQL executions over time. In this comparison, all SQL executions, such as unmatched and new executions, are included. This graph provides an overview of the relative difference in execution speed between the baseline and the replayed workload.

> **Note:** The SQL executions over time metric does not include any information about SQL executions that were not captured because a replay capture filter was used for a DB2 for z/OS workload replay.

Rows returned over time

This graph shows a comparison between the number of rows returned over time. In this comparison, all SQL executions, such as non-matching, failed, and new executions, are included. This graph provides an overview of the relative precision difference between the baseline and the replay.

Note: The rows returned over time metric does not include any information about SQL executions that were not captured because a replay capture filter was used for a DB2 for z/OS workload replay.

Metrics

The overview page also provides a list of critical metrics, as described Table 6-5.

Table 6-5 Interpreting the SQL replay result metrics

Metric	Description	Usage and interpretation
Total response time difference	The total cumulative change in response time for all matched SQL statements and transactions	Use this metric to understand the general behavior of the replayed SQL statements. Because this metric adds all statement response times, it might be longer than the total elapsed time. In the actual workload, statements might execute and run in parallel. A low total response time difference combined with high total improvements and regressions might indicate replay issues.
Total improvements	The cumulative improvement in response time for all matched SQL statements and transactions	Use this metric to gauge the performance improvement of the SQL statements in the workload.
Total regressions	The cumulative regression in response time for all matched SQL statements and transactions	Use this metric to gauge the performance regression of the SQL statements in the workload.
SQL and transaction improvement and regression	The total number of SQL statements or transactions that improved or regressed equal to or larger than the threshold	Click the metrics titles to drill down to list the actual improved and regressed SQL statements. Use the report setting “Threshold for reporting performance improvement or regression” to set the precision level for improvements and regressions.

Metric	Description	Usage and interpretation
Baseline and replay elapse time	The total elapsed time for the workloads	The total elapsed time values represent the actual period that the workloads ran from start to end, including all statements, and including any wait time between statements. The total elapsed time might differ from the cumulative statement response time. The cumulative response time adds all statement response times while, in the actual workload, statements might run in parallel.

6.4.4 Creating a new replay-ready workload from a comparison report

If the report indicates unmatched SQLs or transactions that are unwanted or unexpected, you can remove those entries from the report detailed pages and save the workload as a new replay-ready workload. You can then replay the newly created replay-ready workload and analyze the new replay by creating a comparison report. The new report lists the SQL statements and transactions that were removed as missing instead of unmatched.

If a specific SQL statement is removed from a report, InfoSphere Workload replay also removes the transaction to which the SQL statement belongs. If the removed aggregated SQL statement consists of multiple executions of an SQL statement, all the transactions that correspond to these individual executions are removed from the workload.

The option to remove SQL statements is available only in the unmatched SQL statement and unmatched transactions report types.

To create new replay ready workload, follow these steps:

1. From the replay results tab, open one of the following subreports:
   - Unmatched SQL replays:
     - Different Return Code
     - Different Rows Returned
     - Different Rows Updated
   - Unmatched transaction replays:
     - Transaction - Different Return Codes
     - Transaction - Different Rows Returned
     - Transaction - Different Rows Updated

2. Mark statements for removal.

   In the subreport, select one or more statements to remove, then click **Remove Selected**.

   > **Tip:** All the records that are removed from a report are stored in a temporary list and are hidden from the grid temporarily until you complete the process by clicking **Save as New Replay-Ready Workload**. A current list of removed statements is displayed in the report window.

   If multiple report pages are opened at the same time, you can switch between pages and mark records for removal simultaneously. For each report type, you can click **Undo** to restore any removed SQL statements.

3. Submit the removal of records and create a new replay-ready workload.

   After all selections are complete, click **Save as New Replay-Ready workload**.

   Add any relevant notes that describe the new workload, and click **OK**.

   The transformation progress details page opens and a new replay-ready workload is added in the workload grid.

6.4.5 Exporting workloads for analysis in InfoSphere Optim Query Workload Tuner

From a comparison report, you can export the captured workloads as XML in the InfoSphere Optim Query Workload Tuner schema. You can then import the XML to InfoSphere Optim Query Workload Tuner to analyze the workload and update your test environment according to any recommendations. You can then replay the baseline workload to verify that the changes improve the performance of the SQL statements. For more information, see 8.1, “Integration with Query Workload Tuner” on page 270.

To export SQL statements as an XML file, follow these steps:

1. Open the comparison report and drill down to any of the following reports:
   - Replay Results

     Matched SQL replays
   - Response Time:
     - Improved SQL Statements
     - Regressed SQL Statements

2. Click **Export** to select the number of SQL statements to export.

> **Tip:** If you select fewer than the total number of SQL statements in the report, the statements with the longest response time are exported first.

3. The XML file opens in your default web browser. Save the XML file to your local disk.

6.5 Moving workloads between servers

In a decentralized (“Decentralized deployments” on page 12) InfoSphere Workload Replay environment, you capture workloads in one environment and replay them in another environment. These environments might reside in isolated networks, making it impossible to capture and replay from the same InfoSphere Workload Replay server.

In situations where the production environment on which you capture production data is isolated from the test environment, you can set up two InfoSphere Workload Replay servers, one in each environment, and use one server to capture workloads and the other server to replay and analyze the workloads.

After you capture a workload, you can then export the captured workload as a compressed file, use the CLI to upload it to an intermediate Secure Copy Protocol (SCP) or FTP server, and then download and import it to the second InfoSphere Workload Replay environment.

> **Important:** The export and import feature supports captured workloads only, and it does not export and import any other workload type.

6.5.1 Associated database for an imported workload

All workloads are associated with a capture database in the environment where they are captured, but when you import a workload to a new environment, that specific capture database might not exist in that environment. At import time, you must therefore associate the imported workload with a database in the test environment.

Note: To be able to process the imported workload as a captured workload, this associated database must include a user ID that is granted the required privileges. For more information for DB2 for z/OS, see 4.5.1, “Managing access to capture and replay actions” on page 104, and for DB2 for Linux, UNIX, and Windows, see 5.4.1, “Managing access to capture and replay actions” on page 146.

6.5.2 Export and import process

When you export a workload, InfoSphere Workload Replay packages the workload as a password-protected and encrypted file on the InfoSphere Workload Replay server. Use the InfoSphere Guardium command-line interface (CLI) to access and upload the workload file to an FTP or SCP server. You then use the CLI on a second InfoSphere Workload Replay appliance to download the workload file to that server. Figure 6-21 on page 202 illustrates the flow of this process.

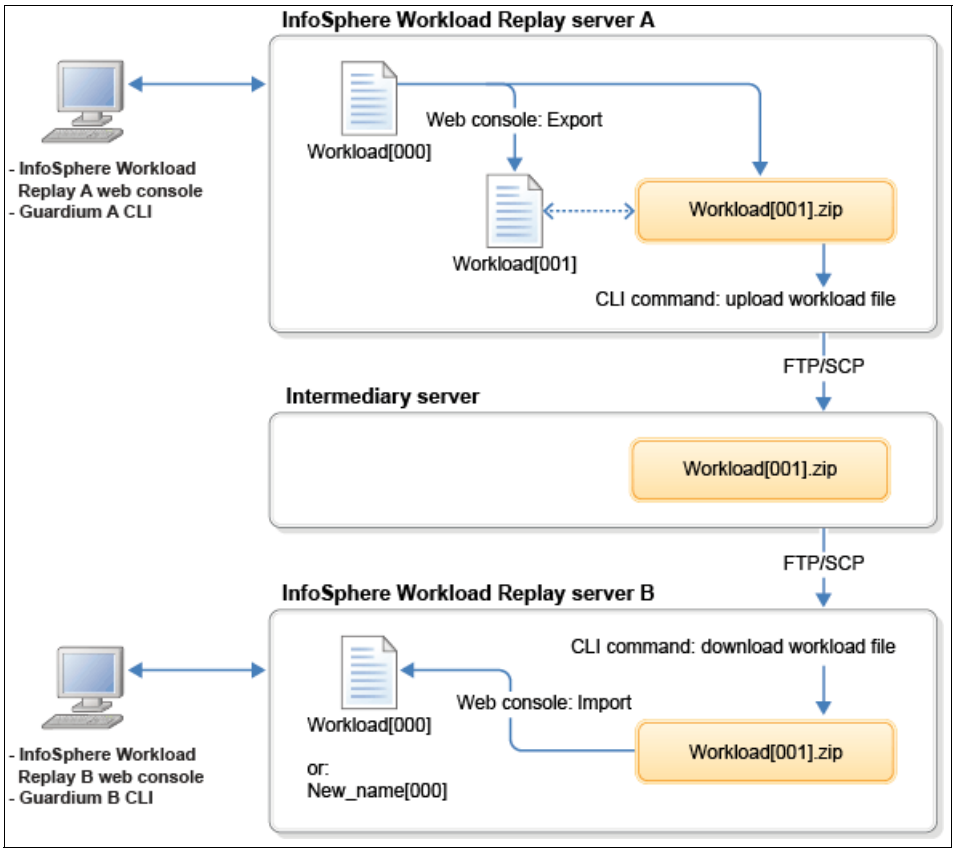


Figure 6-21 Exporting and importing processes

You can use this feature if your production environment and test environment are on isolated networks, or use it to archive your captured workloads on a server other than the InfoSphere Workload Replay server on which they were captured.

Exporting a workload

To export a workload and upload a workload to an intermediary server, complete the following steps:

1. From the SQL Workloads page of your InfoSphere Workload Replay production server (Server A in Figure 6-21), right-click the captured workload that you want to export, and select **Export** (Figure 6-22 on page 203).

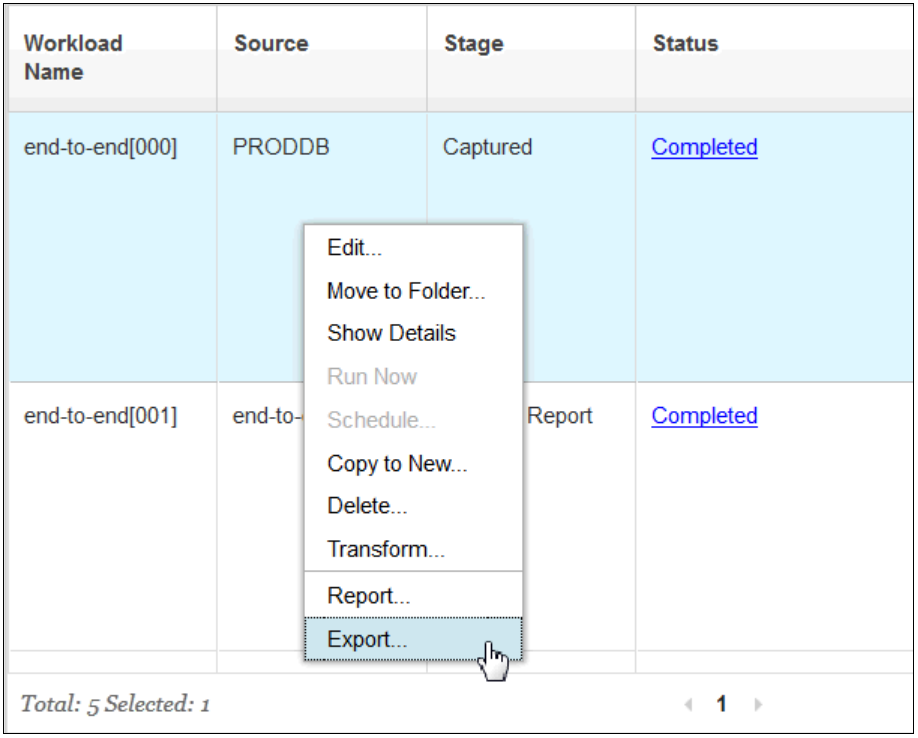


Figure 6-22 Selecting Export

2. In the Export a Workload wizard (Figure 6-23 on page 204), enter a workload password to secure the encrypted workload file. This password is required to import the workload to the pre-production InfoSphere Workload Replay server (Server B in Figure 6-21 on page 202). The workload is packaged into an encrypted file and stored in the InfoSphere Workload Replay server file system.

> **Note:** Depending on the size of the workload, the packaging process might take time. Use the Export Process Status information in the workload details page to monitor the export process.

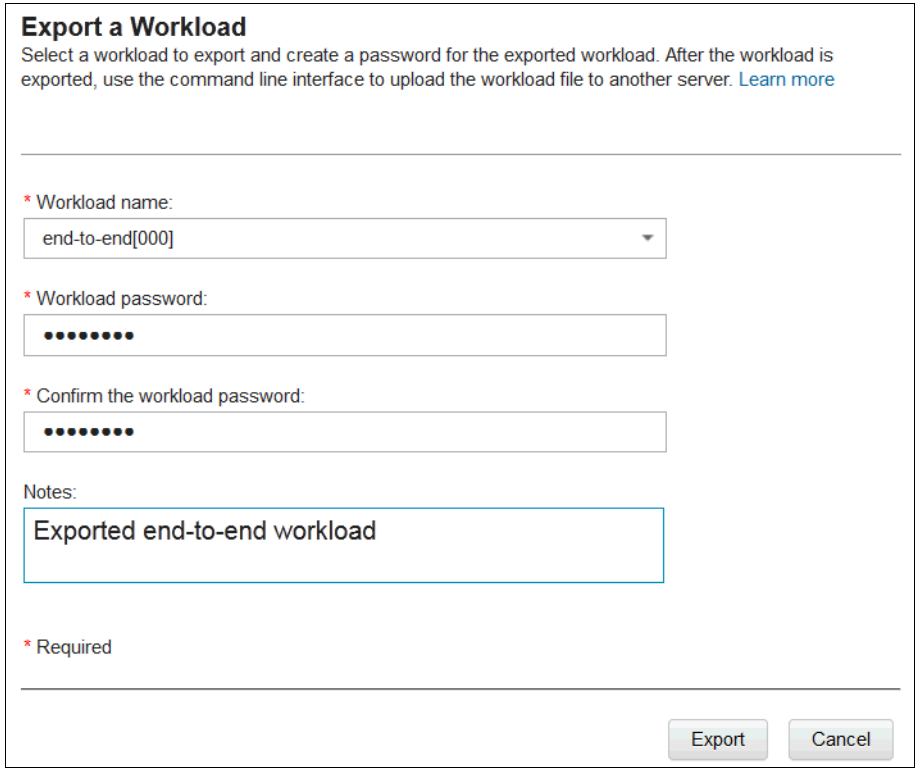


Figure 6-23 Exporting a workload

3. When the workload is packaged, use the production InfoSphere Workload Replay server CLI to upload the workload to an intermediary server:

   a. Log in to the CLI as an administrator or privileged user on the main InfoSphere Workload Replay appliance.

   > **Tip:** You can log on to the CLI on the InfoSphere Workload Replay server system console or access the server through Secure Shell (SSH) on port 22. For more information, see 7.1.1, “Roles and interfaces” on page 214.

   b. Enter the following CLI command to upload the workload to an intermediary server (Figure 6-24 on page 205):

   ```
   upload ocr_workload_file
   ```

Follow the CLI prompts to specify the following parameters:

- Transfer protocol: FTP or SCP.
- User ID: A user ID on the target system with at least write privileges on the target directory.
- Password: The password of the user.
- Server address: Server name or IP address of the target server.
- Target directory: Enter the absolute path to the target directory.
- Workload file: Select the workload file to upload to the target server.

```
pine.itso.ibm.com> upload ocr_workload_files

Select the transfer protocol by entering the corresponding number (q to quit):
        1. SCP
        2. FTP

2

Enter the FTP port. Enter "0" or press "Enter key" to use the default port:

Enter the server name or IP address of the target server: 9.12.5.103

Enter a user ID that has write privileges on the target directory: ftproot

Enter the password for the selected user:

Enter the absolute path to the FTP target directory: /FTP_ROOT/exported_workload
s

Select the workload file to upload by entering the corresponding number:
1. end-to-end[005].zip [196K]

Select the workload file to upload by entering the corresponding number: 1
Type Y to upload the end-to-end[005].zip file to the 9.12.5.103 FTP server. Type
 N to cancel and exit. The file size is 196K.
y

The workload file is being uploaded. Depending on the size of the file, this mig
ht take some time. You can monitor the file upload progress on your FTP server.


194014 bytes transferred
File uploaded successfully.
ok
pine.itso.ibm.com>
```

Figure 6-24 Uploading an exported workload file to an FTP or SCP server

Note: The file upload runs as a background process. Depending on the size of the workload file, the process might take time to complete.

c. On the target FTP or SCP server, verify that the file uploaded successfully (Figure 6-25 on page 206).

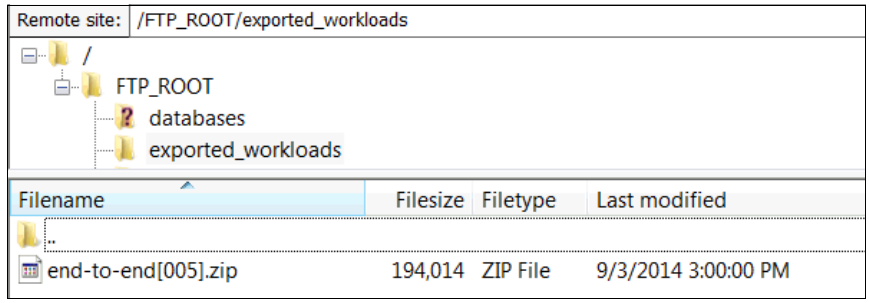


Figure 6-25 Verify that the exported workload file uploaded

The exported workload is on the intermediary server, and it can now be imported to another InfoSphere Workload Replay server.

Importing a workload

To download a workload from an intermediary server and import it to your pre-production InfoSphere Workload Replay server, complete these steps:

1. On the pre-production InfoSphere Workload Replay server, log in to the InfoSphere Guardium CLI to download the workload from the intermediary server:

   a. Log in to the CLI as an administrator or privileged user on the main InfoSphere Workload Replay appliance.

   > **Tip:** You can log on to the CLI on the InfoSphere Workload Replay server system console or access the server through SSH on port 22. For information, see 7.1.1, “Roles and interfaces” on page 214.

   b. Enter the following CLI command to download the workload file from an intermediary server (Figure 6-26 on page 207):

   ```
   download ocr_workload_file
   ```

   Follow the CLI prompts to specify the following parameters:

   - Transfer protocol: FTP or SCP.
   - User ID: A user ID on the target system with at least read privileges on the target directory.
   - Password: The password of the user.
   - Server address: Server name or IP address of the target server.
   - Target directory: Enter the absolute path to the target directory.

- Workload file: Enter the name of the workload file to download from the target server.

```
pine.itso.ibm.com> download ocr_workload_file

Select the transfer protocol by entering the corresponding number (q to quit):
        1. SCP
        2. FTP

2

Enter the FTP port. Enter "0" or press "Enter key" to use the default port:

Enter the server name or IP address of the source server: 9.12.5.103

Enter a user ID that has read privileges on the source directory: ftproot

Enter the password for the selected user:

Enter the absolute path to the FTP source directory: /FTP_ROOT/exported_workload
s

Enter the file name of the workload file to download: end-to-end[005].zip


The workload file is being downloaded, and will be available for import in the w
eb console when the download is complete. Depending on the size of the file, thi
s might take some time. Enter the 'show ocr_workload_files' command to see a lis
t of the workloads on your server and to monitor the current download progress..

Connected to 9.12.5.103
Login successful as user ftproot
Proceeding to download our file, this might take a few minutes...

end-to-end[005].zip transferred

ok
pine.itso.ibm.com>
```

Figure 6-26 Download the workload file

2. From the SQL Workloads page of the second InfoSphere Workload Replay server, click **More** → **Import**.
3. In the Import an SQL Workload window (Figure 6-27 on page 208), select the workload file that you want to import, and enter the password for the file.

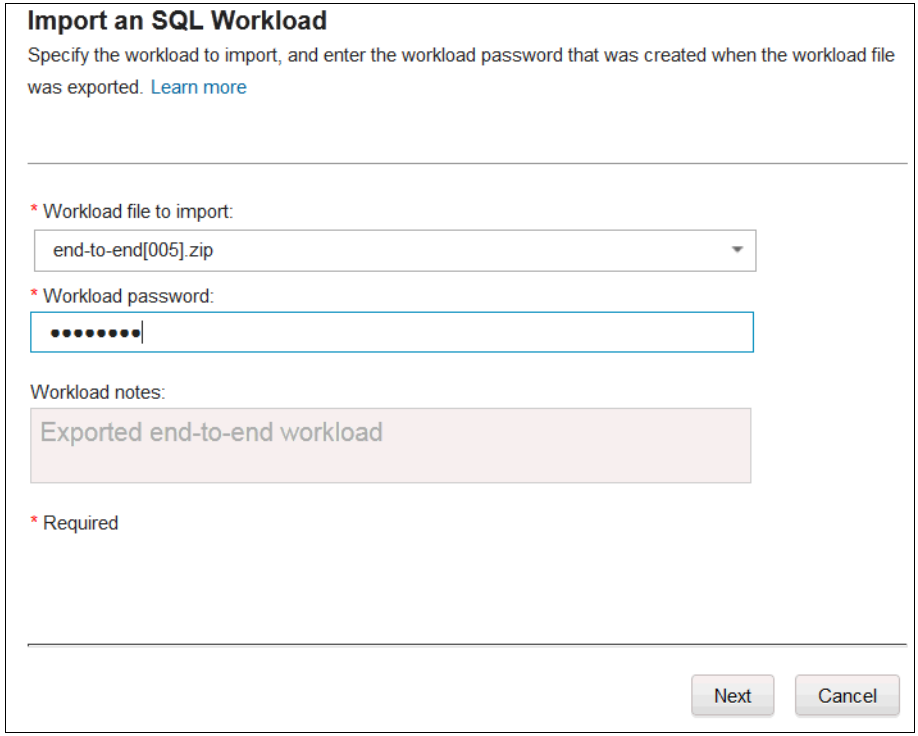


Figure 6-27 Import an SQL Workload

4. Enter a unique workload name, select a folder, and select a database to associate the workload with (Figure 6-28 on page 209).

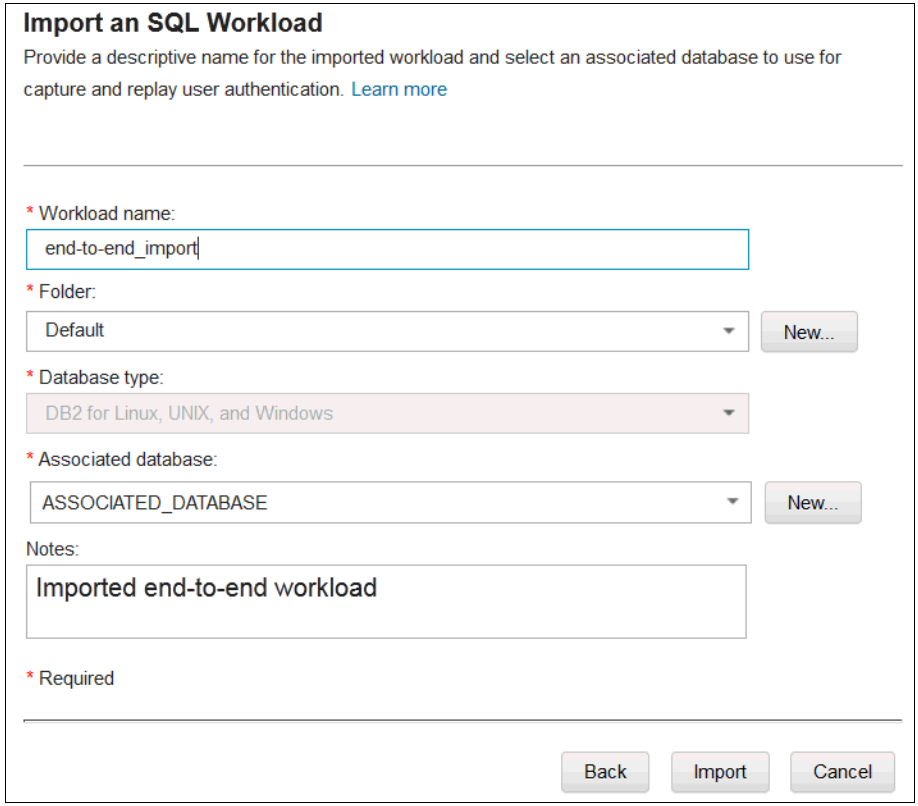
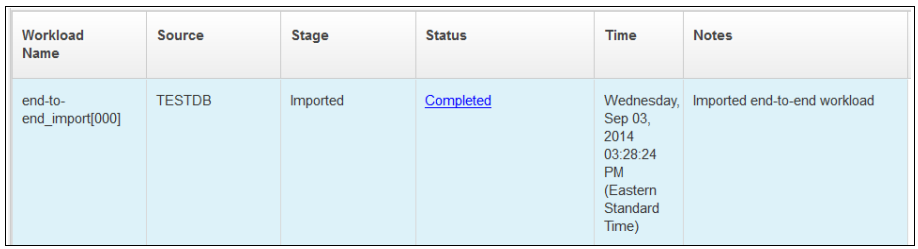


Figure 6-28 Associate a database

5. If prompted, enter the credentials of a user ID with Can Import Workload privileges.
6. The workload is imported and now appears in the SQL Workloads grid (Figure 6-29).



Workload Name	Source	Stage	Status	Time	Notes
end-to-end_import[000]	TESTDB	Imported	Completed	Wednesday, Sep 03, 2014 03:28:24 PM (Eastern Standard Time)	Imported end-to-end workload

Figure 6-29 Imported workload in the grid

You can now use the imported workload as a normal captured workload by transforming it and replaying it in the test environment.

6.5.3 Using the export feature to archive captured workloads

In addition to exporting and importing for direct capture and replay use, you can export captured workloads for archiving. Use the export feature and then upload the exported captured workload files to an FTP or SCP server to create a library of your captured workloads.

> **Note:** The export feature supports only captured workloads, and it does not export any other workload type. To back up your workload replay environment completely, including all workload types, perform a full system backup from the CLI. For the backup procedure, see 7.5, “Backup and recovery” on page 249.

6.5.4 Removing exported and imported workload files from the server

The exported workload files and the downloaded workload files are not automatically removed from the InfoSphere Workload Replay servers after you upload or import the file. You must manually remove these exported workload files and the downloaded workload files to make space available, if needed.

To remove an exported workload and the exported workload file, use the following steps:

1. From the SQL Workloads page of the InfoSphere Workload Replay server, right-click the exported workload and select **Delete** (Figure 6-30).

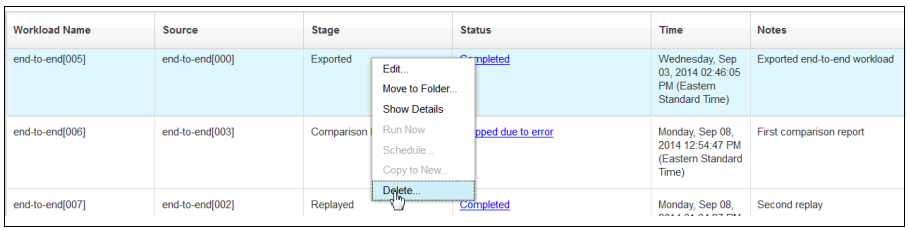


Figure 6-30 Delete exported workload

2. When prompted, enter the credentials of a user ID with Can Delete Captured Workload privileges.
3. The workload and the exported workload file are deleted from the server.

To remove a downloaded workload file, use the following steps:

1. Log in to the CLI as an administrator or privileged user on the main InfoSphere Workload Replay appliance.
2. Enter the following CLI command to delete the workload file from the InfoSphere Workload Replay server (Figure 6-31):

   `delete ocr_workload_file`

   Perform these tasks when you are prompted:

   a. Select the workload file to delete.

   b. Confirm that you want to delete the file.

```
maple.itso.ibm.com> delete ocr_workload_file
Select the workload file to delete by entering the corresponding number:
1. end-to-end[005].zip [196K]

Select the workload file to delete by entering the corresponding number: 1
Type Y to delete the end-to-end[005].zip file from the server. Type N to cancel
and exit. The file size is 196K.
Y

The workload file is being deleted. Depending on the size of the file, this migh
t take some time. Enter the 'show ocr_workload_files' command to see a list of t
he workloads on your server.
File deleted successfully.ok
maple.itso.ibm.com>
```

Figure 6-31 Delete downloaded workload file

3. The downloaded workload file is deleted from the InfoSphere Workload Replay server.

7

Ongoing operations

This chapter describes, in detail, common IBM InfoSphere Optim Workload Replay administration and maintenance tasks. We cover the following topics:

- Access management
- Appliance health monitoring
- S-TAP health monitoring
- Backup and recovery
- Appliance maintenance and upgrades
- Stopping and starting services

7.1 Access management

In 2.6.1, “Assigning Workload Replay server roles” on page 36, we define the security administrators, administrator, privileged user, and user roles, the interfaces they use, and their privileges.

In this section, we describe how to implement security on an InfoSphere Workload Replay appliance by using the following tasks:

- Configuring general account and password settings
- Creating and maintaining user accounts for the security manager, administrator, privileged user, and user roles

Each security administrator, administrator, privileged user, and user accesses the InfoSphere Workload Replay user interfaces by using an account. Several default accounts, such as admin, accessmgr, cli, and guardcli1-5, are created during product installation. You can create additional accounts, as needed, to implement appliance security according to your company’s policy.

In the first section, we describe how to access the user interfaces. In later sections, we outline how a security administrator can perform the following tasks:

- Configure appliance-wide account settings
- Create an account
- Customize an account for a security administrator
- Customize an account for an administrator
- Customize an account for a privileged user
- Customize an account for a user
- Unlock an account
- Delete an account

7.1.1 Roles and interfaces

In 1.2.3, “Roles and responsibilities” on page 13, we define the administrator, security administrator, privileged user, and user types that are commonly used in an InfoSphere Workload Replay deployment.

Whether a single user can perform the duties of two or more roles is governed by your company’s security policy and the size of your InfoSphere Workload Replay deployment.

Table 7-1 on page 215 recaps the user interfaces by user type.

Table 7-1 User types that require access to Workload Replay interfaces

Workload Replay user types	Guardium web console	Workload Replay web console	CLI
Administrator	Yes	No	Yes
Security administrator	Yes	No	No
Privileged user	Yes	Yes	Yes
User	No[a]	Yes	No

a. Access is only required to change the account password.

Accessing the Guardium web console

To access the Guardium web console, go to the following web address:

`https://guardium_hostname_or_ip:8443/sqlguard`

The *guardium_hostname_or_ip* is the host name or IP address of a main Workload Replay appliance or an auxiliary Workload Replay appliance.

If you encounter any issues accessing this web console, see 9.2.2, “Resolving Guardium web console connectivity issues” on page 287.

Accessing the Workload Replay web console

To access the Workload Replay web console, go to the following web address:

`https://guardium_hostname_or_ip:8443/dsweb/console/ocr/index.jsp`

The *guardium_hostname_or_ip* is the host name or IP address of a main Workload Replay appliance.

If you encounter issues accessing this web console, see 9.2.1, “Resolving Workload Replay web console connectivity issues” on page 286.

Note: You can access the Workload Replay web console only on the main Workload Replay server; there is no Workload Replay web console for the auxiliary servers.

Accessing the CLI

To access the command-line interface (CLI) on a main or auxiliary Workload Replay appliance, complete the following steps:

1. Open your Secure Shell (SSH) client to port 22 on *guardium_hostname_or_ip*.
2. If you are an administrator, log in by using the default cli account, as shown in Figure 7-1 on page 216.

```
login as: cli

IBM InfoSphere Guardium, Command Line Interface (CLI)

cli@pine.itso.ibm.com's password:
Last login: Thu Sep 11 20:12:44 2014 from catnap.usca.ibm.com

=================================================================
IBM InfoSphere Guardium

Unauthorized access is prohibited
=================================================================


Welcome cli - your last login was Thu Sep 11 20:12:45 2014
pine.itso.ibm.com>
```

Figure 7-1 Log in to the CLI as an administrator

3. If you are a privileged user, log in by using your assigned guardcli account, as shown in Figure 7-2.

```
login as: guardcli1

IBM InfoSphere Guardium, Command Line Interface (CLI)

guardcli1@pine.itso.ibm.com's password:
Last login: Mon Sep 15 12:55:20 2014 from catnap.usca.ibm.com

=================================================================
IBM InfoSphere Guardium

Unauthorized access is prohibited
=================================================================

Welcome guardcli1 - your last login was Thu Sep 11 16:55:03 2014
pine.itso.ibm.com>
```

Figure 7-2 Log in to the CLI as a privileged user

4. Associate your login session with a user ID for auditing reasons.

   Before you can issue any commands, you must enter the following command to associate your login session with a user ID:

   set guiuser ***<privileged user's account name>***

   or

   set guiuser ***<privileged user's account name>*** **password** ***<password>***

Specify the account that the security administrator created for you, as shown in Figure 7-3.

```
Welcome guardcli1 - your last login was Mon Sep 15 13:20:57 2014
pine.itso.ibm.com> set guiuser wrcadmin1
Enter current password:
ok
pine.itso.ibm.com> com
add inspection-engines
aggregator backup keys file
```

Figure 7-3 Privileged users must authenticate before they run any CLI commands

Tip: Enter **com** or **com** ***<string>*** to display a list of available commands. For example, to display a list of all Workload Replay commands, enter **com ocr**.

7.1.2 Configuring account settings

You can customize general account settings with the **store account** CLI commands. To review the current setting, use the equivalent **show account** commands.

Configuring account lockout settings

You can configure the following account lockout settings by using the **store account** CLI command:

- Enable or disable the automatic account lockout feature, which disables a user account after a specified number of login failures:

  store account lockout <on or **off>**

- Set the number of failed login attempts in the configured strike interval before you disable the account:

  store account strike count ***<maximum number of failed login attempts>***

- Set the number of seconds during which the configured number of failed login attempts must occur to disable the account:

  store account strike max ***<seconds>***

- Set the maximum number of failed login attempts to be allowed for an account over the life of the server before the account is permanently disabled:

  store account strike max ***<maximum number of failed login attempts>***

Configuring password settings

You can configure password settings by using the **store password** CLI commands. To review the current setting, use the equivalent **show password** commands:

- Set the number of days after which a CLI or web console password expires. The default is 90 days. Use **-1** to disable password expiration.

  ```
  store password expiration cli <number of days>
  store password expiration gui <number of days>
  ```

- Set the number of days after which an inactive account is disabled. The default is 0; therefore, accounts will not be disabled due to inactivity.

  ```
  store password disable <number of inactive days>
  ```

- Enable or disable the hardened password validation rules. By default, hardened password validation is enabled.

  ```
  store password validation on
  ```

> **Note:** When password validation is enabled, the password must be eight or more characters in length, and must include at least one uppercase alphabetic character (A - Z), one lowercase alphabetic character (a - z), one digit (0 - 9), and one special character. When disabled (not recommended), any length or combination of characters is allowed.

7.1.3 Creating an account

Table 7-1 on page 215 mapped the system administrator, administrator, privileged user, and user types to user interfaces. Before you implement a user type in your environment, review Table 7-2 to determine on which appliances you must create accounts.

Table 7-2 Not every user type requires access to every appliance

Workload Replay user type	Access required to main Workload Replay appliance	Access required to auxiliary Workload Replay appliances
Administrator	Yes	Yes
Security administrator	Yes	Yes
Privileged user	Yes	Yes
User	Yes	No

Procedure

To create an account, complete the following steps:

1. Open the Guardium web console on the Workload Replay server that you want by using the following web address:

   `https://guardium_hostname_or_ip:8443/sqlguard`

   > **Note:** If you cannot open the web console or connect to it, see 9.2.2, “Resolving Guardium web console connectivity issues” on page 287.

2. Log on as a security administrator to create or manage accounts, as shown in Figure 7-4.

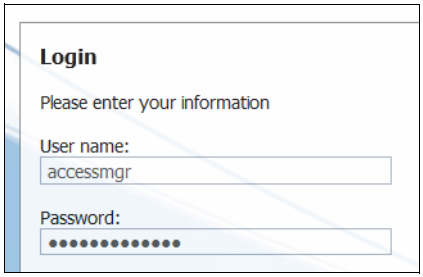


Figure 7-4 Log in to the Guardium web console

The User Browser opens, as shown in Figure 7-5, displaying the account list.

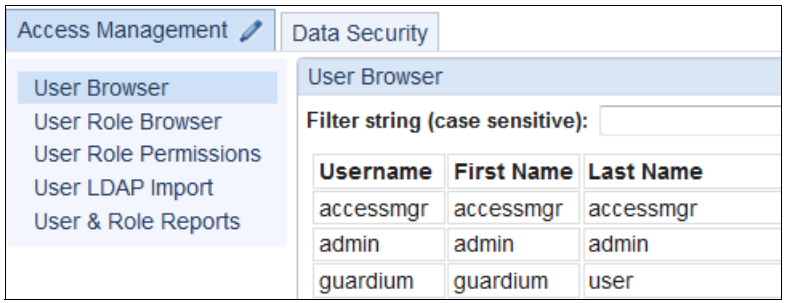


Figure 7-5 The User Browser displays all accounts

3. Click **Add User** to create an account.
4. Complete the User Form, as shown in Figure 7-6 on page 220. Clear **Disabled**.

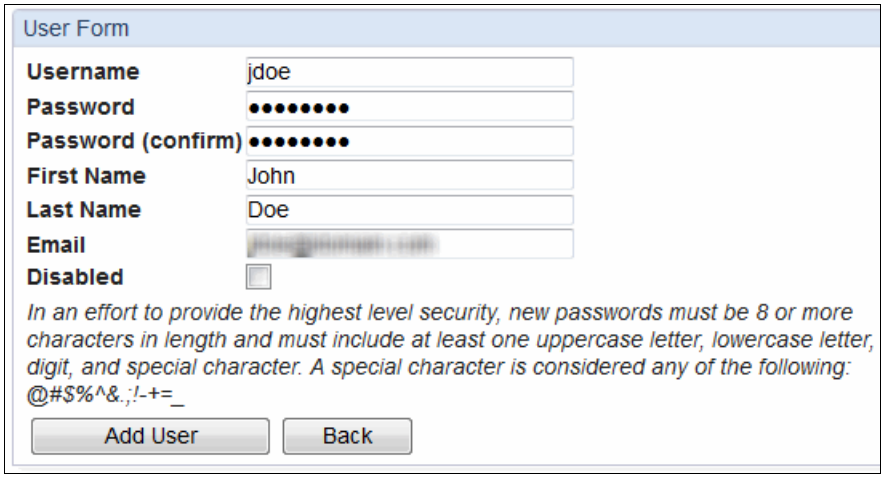


Figure 7-6 Enter basic account information

Note: Specify the default password for this account. The user is prompted to change the password during the first login to the Guardium web console.

5. Click **Add User** to save the account.

   The updated account list is displayed, as shown in Figure 7-7.

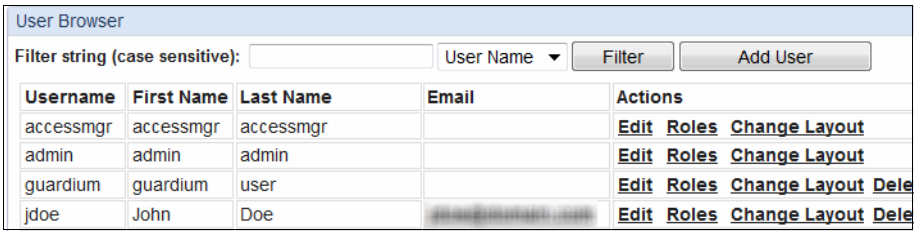


Figure 7-7 John Doe has now an account on this appliance

6. Click **Roles** next to the account entry to review the currently assigned roles. The User Role Form opens, as shown in Figure 7-8 on page 221, displaying John Doe's roles on this appliance.

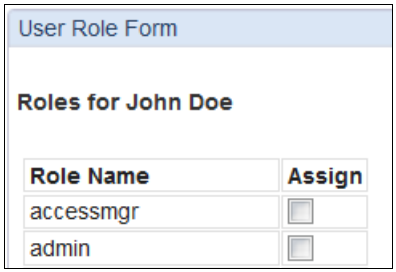


Figure 7-8 Review the default roles of a new account holder

Note: A role is granted (or revoked) by selecting the correct check box next to the account.

Note: Certain roles are mutually exclusive. An error message is displayed if an invalid combination is selected.

7. Do not change the default. Click **Back** to return to the User Browser.

Repeat these steps on each appliance, as needed.

Follow the applicable instructions in the following sections to assign the correct roles to the account.

7.1.4 Creating a security administrator

A security administrator manages access to a Workload Replay appliance.

During the product installation, a default account that is named accessmgr is created. This account has only limited access to the Guardium web console and no access to the Workload Replay web console or the CLI.

You can create additional security administrator accounts and grant them the accessmgr role.

Before you begin

Create an account as described in 7.1.3, “Creating an account” on page 218 or identify an existing account for the new security administrator.

Procedure

To grant the security administrator privileges to an existing account, complete the following steps:

1. Open the Guardium web console on the Workload Replay server that you want by using the following web address:

   `https://guardium_hostname_or_ip:8443/sqlguard`

2. Log on as a security administrator.
3. In the User Browser, click **Roles** next to correct account name.
4. Select the **accessmgr** role.
5. Clear the **user** role.

   > **Important:** Select the **cli** role if the security administrator must be able to configure account settings, as described in 7.1.2, “Configuring account settings” on page 217.

6. Click **Save** to return to the User Browser.
7. Click **Change Layout** next to correct account name, click **Reset**, and select **OK**.

Repeat these steps on each applicable main Workload Replay appliance and auxiliary Workload Replay appliance.

Communicate the following information to the owners of the security administrator accounts that you set up:

- The URLs of the Guardium web consoles:

  `https://guardium_hostname_or_ip:8443/sqlguard`

- The account name and temporary password (if a new account). The account owner is prompted to change their password the first time that they log in to the Guardium web console.

7.1.5 Creating an administrator

An administrator manages Workload Replay appliances by using the Guardium web console and the CLI.

During the appliance installation, several default accounts are created for administrative purposes:

- The admin account provides access to administrative features in the Guardium web console.
- The cli account provides access to the CLI.
- The guardcli1, guardcli2, guardcli3, guardcli4, and guardcli5 accounts also provide access to the CLI. These accounts are unique because they are shared accounts that require an additional authorization check before any CLI commands can be run. For details, see “Accessing the CLI” on page 215.

Note: Limit the use of the default admin and cli accounts for auditing reasons. Whenever appropriate, create a custom account and grant the required roles, as described in this chapter.

We suggest that you create additional accounts and grant them the admin and cli roles.

Before you begin

Create an account as described in 7.1.3, “Creating an account” on page 218 or identify an existing account.

Procedure

To assign the admin and cli roles to an existing account, complete the following steps:

1. Open the Guardium web console on the Workload Replay appliance that you want by using the following web address:

   `https://guardium_hostname_or_ip:8443/sqlguard`

2. Log on as a security administrator.
3. In the User Browser, click **Roles** next to correct account name.
4. Select the following roles: **admin** and **cli**.
5. Clear the **user** role.
6. Click **Save** to return to the User Browser.
7. Click **Change Layout** next to correct account name, select **Reset**, and click **OK**.

Repeat these steps on each applicable main Workload Replay appliance and auxiliary Workload Replay appliance.

Communicate the following information to the owners of the accounts that you set up:

- The URLs of the Guardium web consoles:

  `https://guardium_hostname_or_ip:8443/sqlguard`

- The CLI connectivity information:

  `guardium_hostname_or_ip port 22`

- The account name and temporary password (if a new account). The account owner is prompted to change their password the first time that they log in to the Guardium web console.
- The designated guardcli account (1 - 5) and password.

7.1.6 Creating a privileged user

No default account is created for the Workload Replay user role during the product installation.

Before you begin

Create an account as described in 7.1.3, “Creating an account” on page 218 or identify an existing account.

Procedure

To assign admin, cli, and workload-replay-admin roles to an existing account, complete the following steps:

1. Open the Guardium web console on the Workload Replay appliance that you want by using the following web address:

   `https://guardium_hostname_or_ip:8443/sqlguard`

2. Log on as a security administrator with the accessmgr role.
3. In the User Browser, click **Roles** next to correct account name.
4. Select the following roles: **admin**, **cli**, and **workload-replay-admin**.
5. Clear the **user** role.
6. Click **Save** to return to the User Browser.
7. Click **Change Layout** next to correct account name, select **Reset**, and click **OK**.

Repeat these steps on each correct main Workload Replay appliance and auxiliary Workload Replay appliance.

Communicate the following information to the owners of the accounts that you set up:

- The URLs of the Guardium web consoles:

  `https://guardium_hostname_or_ip:8443/sqlguard`

- The URLs of the Workload Replay web consoles:

  `https://guardium_hostname_or_ip:8443/dsweb/console/ocr/index.jsp`

- The CLI connectivity information:

  `guardium_hostname_or_ip port 22`

- The account name and temporary password (if a new account). The account owner is prompted to change their password the first time that they log in to the Guardium web console.
- The designated guardcli account (1 - 5) and password.

7.1.7 Creating a user

No default account is created for the Workload Replay user role during product installation.

Before you begin

Create an account as described in 7.1.3, “Creating an account” on page 218 or identify an existing account.

Procedure

Follow these steps to assign user and workload-replay-user roles to an existing account:

1. Open the Guardium web console on the Workload Replay appliance that you want by using the following web address:

   `https://guardium_hostname_or_ip:8443/sqlguard`

2. Log on as a security administrator.
3. In the User Browser, click **Roles** next to correct account name.
4. Select the following roles: **user** and **workload-replay-user**.
5. Click **Save** to return to the User Browser.
6. Click **Change Layout** next to correct account name, click **Reset**, and select **OK**.

Repeat these steps on each main Workload Replay appliance.

Communicate the following information to the owners of the accounts that you set up:

- The URLs of the Guardium web consoles:

  `https://guardium_hostname_or_ip:8443/sqlguard`

- The URLs of the Workload Replay web consoles:

  `https://guardium_hostname_or_ip:8443/dsweb/console/ocr/index.jsp`

- The account name and temporary password (if a new account). The account owner is prompted to change their password the first time that they log in to the Guardium web console.

7.1.8 Unlocking accounts

Account settings on each appliance enforce the locking policy that is enforced by the system.

Unlocking the default accessmgr account

If the default accessmgr account is locked on an appliance, use the following steps to unlock the account:

1. Log in to the CLI.
2. Run these commands:

   ```
   unlock accessmgr
   support reset-password accessmgr random
   ```

3. Provide the output from the support command to IBM Software Support.
4. IBM Software support gives you a temporary password.

Unlocking the default admin account

If the default admin account is locked on an appliance, use the following steps to unlock the account:

1. Log in to the CLI.
2. Run these commands:

   ```
   unlock admin
   restart gui
   ```

3. Log out of the CLI.
4. Log in to the Guardium web console as the security administrator (the default accessmgr account or an account with the accessmgr role):

   `https://guardium_hostname_or_ip:8443/sqlguard`

5. In the User Browser, locate the admin account and click **Edit**.
6. Enter and confirm the new temporary password.
7. Notify the account owner (administrator or authorized user of the admin account) that the account is unlocked and a new temporary password is set. The account owner can change the password during the next login attempt on the Guardium web console.

Unlocking privileged user and user accounts

If the account of a privileged user or user is locked on an appliance, use the following steps to unlock the account:

1. Log in to the Guardium web console as a security administrator (the default accessmgr account or a user with the accessmgr role):

   `https://guardium_hostname_or_ip:8443/sqlguard`

2. In the User Browser view, find the locked user account. Locked (or disabled) accounts are crossed out, as shown in Figure 7-9.

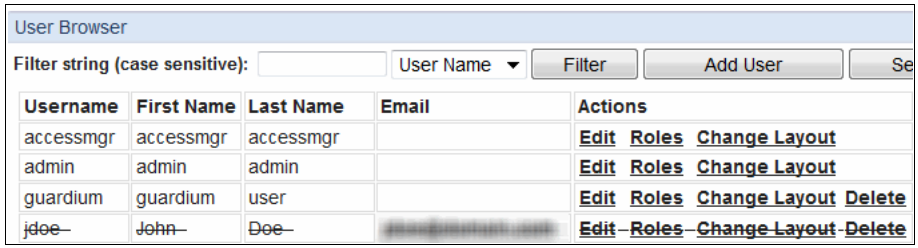


Figure 7-9 John Doe's account is locked

3. Click **Edit** to change the user's settings.
4. In the User Form for the locked account, clear **Disabled** and change the password, if necessary, as shown in Figure 7-10 on page 228.

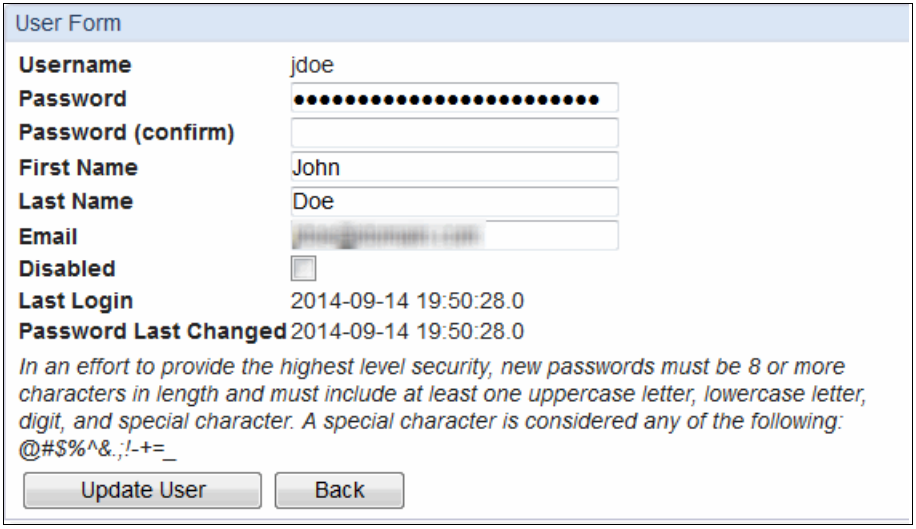


Figure 7-10 Unlock an account by clearing the disabled box

5. Notify the account owner that the account was unlocked and that a new temporary password was set. The account owner can change the password during the next login attempt on the Guardium web console.

7.1.9 Deleting accounts

A security administrator can delete all accounts except the default accessmgr and admin accounts. To delete an account, use the following steps:

1. Log in to the Guardium web console as a security administrator (the default accessmgr account or an account with the accessmgr role).
2. In the User Browser view, locate the account.
3. Click **Delete** and select **Confirm the deletion**.

The account is deleted.

7.1.10 Changing passwords

This section describes the procedure to change the password for various accounts.

Changing CLI passwords

To change the password of the cli or guardcli account, use these steps:

1. Log in to the CLI.
2. Enter `store user password` and follow the prompts, as shown in Figure 7-11.

```
pine.itso.ibm.com> store user password
Changing password for 'cli'.
Enter current password:
```

Figure 7-11 Change the cli or guardcli passwords

Changing Guardium web console and Workload Replay web console passwords

To change an account password on an appliance, use these steps:

1. Log in to the Guardium web console:

   `https://guardium_hostname_or_ip:8443/sqlguard`

2. Click **Edit Account: <*account name*>**, as shown in Figure 7-12.

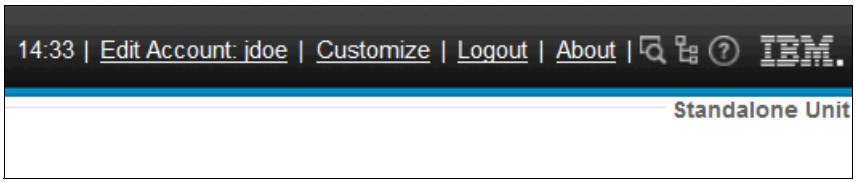


Figure 7-12 Click Edit Account to change your password

3. In the Edit your account details window, enter your old password and the new password, as shown in Figure 7-13 on page 230.

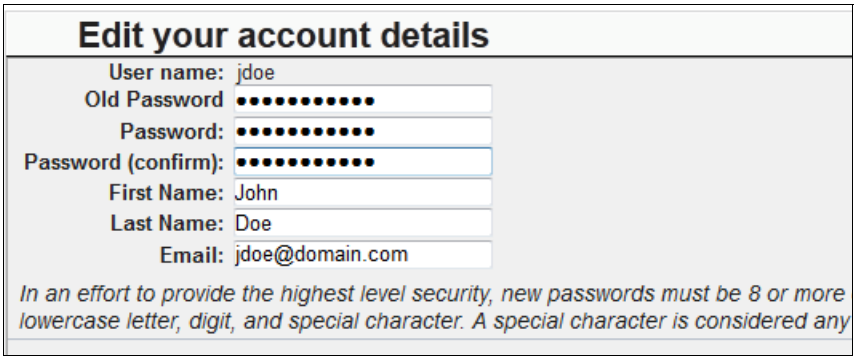


Figure 7-13 Entering the old and new passwords

4. Click **Save**.

> **Note:** A security administrator (accessmgr account or role) can assign a new temporary password to an account by completing these steps:
>
> 1. Log in to the Guardium web console.
> 2. Locate the account and click **Edit**.
> 3. Enter and confirm the new temporary password.

7.2 Appliance health monitoring

In this section, we describe methods to monitor the capacity, disk usage, and performance of a Workload Replay appliance.

7.2.1 Monitoring disk utilization

Captured, processed, and replayed workloads are permanently stored on the appliance in single-server deployments and on the main appliance in multi-server deployments. Auxiliary appliances store workload information only temporarily while a workload capture or replay is in progress.

> **Note:** Disk space is reserved for the operating system, InfoSphere Guardium software, and InfoSphere Workload Replay software, therefore reducing the amount of storage that is available for workload files.
>
> You can increase the initial disk space allocation only by rebuilding the appliance.

Monitoring the disk usage

To monitor the disk usage on an appliance, use these steps:

1. Log in to the Guardium web console as an administrator or a privileged user.
2. Select **Guardium Monitor** → **Buffer Usage Monitor**.
3. The current disk usage for `/root` (reserved for the operating system) is displayed in the System Root Disk Usage column. The current disk usage for `/var` (used by InfoSphere Guardium and Workload Replay) is displayed in the System Var Disk Usage column. The information is updated every minute.

Creating a high disk usage alert

InfoSphere Guardium can generate alerts that are based monitoring information that is collected on the appliance or by S-TAPs. To take advantage of alerting, you must enable the alerter service by following the instructions in 7.4.1, “Enabling the alerting service” on page 248.

In the following example, we create an alert that is triggered if the `/var` file system usage exceeds 50% at least one time during a 24-hour period. To create this alert, complete the following steps:

1. Log in to the Guardium web console as an administrator or a privileged user.
2. Create a query that retrieves the current `/var` disk usage:
   a. Select **Tools** → **Report Building** → **Sniffer Buffer Usage Tracking**.
   b. Select **Sniffer Buffer Usage** as the Main Entity, as shown in Figure 7-14, and click **New**.

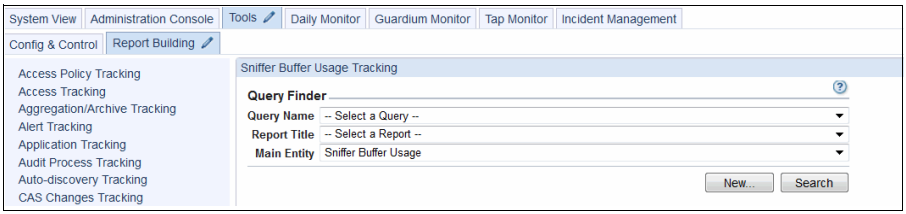


Figure 7-14 Sniffer Buffer Usage Tracking

   c. Enter `High VAR disk usage` for the query name, and select **Sniffer Buffer Usage**, as the Main Entity, as shown in Figure 7-15 on page 232.

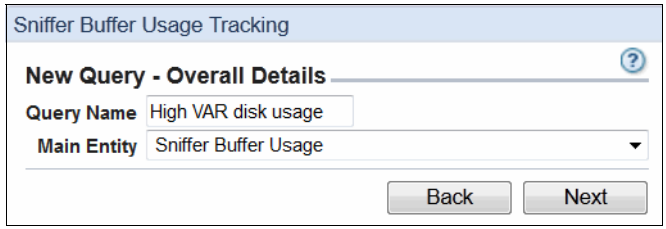


Figure 7-15 Create a query to see whether VAR disk usage exceeds a threshold

d. Click **Next** to define the query output and condition.

e. In the Entity List, expand the **Sniffer Buffer Usage** node.

f. Add **Timestamp** and **System Var Disk Usage** as the query fields and add **System Var Disk Usage** as a query condition, as shown in Figure 7-16.

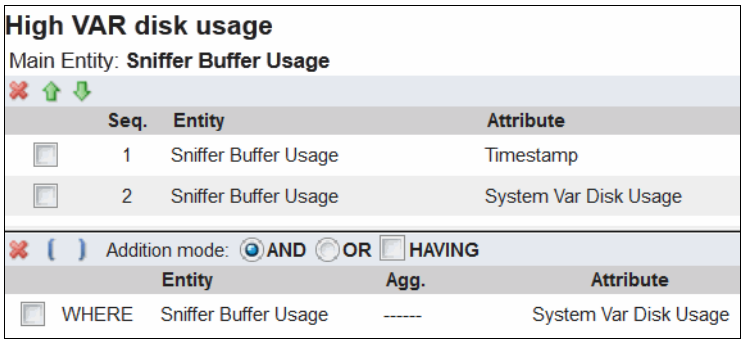


Figure 7-16 Define the query output and query condition entity

g. Under Query Conditions, select the greater than (>) operator. You can compare the selected entity with a constant, a runtime parameter, or another entity. For illustration, we will compare the current `/var` disk usage with a runtime parameter.

h. Select **Parameter** and enter `var_disk_utilization_level` as the parameter name, as shown in Figure 7-17.

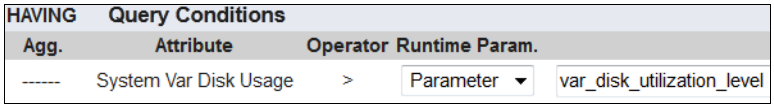


Figure 7-17 Define the disk usage alert threshold

i. Click **Save** to save the query.

3. Create the alert:
   a. Navigate to **Tools** → **Config and Control** → **Alert Builder**.
   b. Click **New** to create a new alert.
   a. Enter or select the following information for your environment:
      - Name: `High VAR disk usage`
      - Description: `VAR disk usage exceeded 50% at least once during the past 24 hours`
      - Severity: **MED**
      - Run frequency: `15` (indicates how frequently, in minutes, the query is run to retrieve the current `/var` disk usage)
      - Query: **High VAR disk usage**
      - Query parameters: `50` (This value is passed as a parameter to the selected query, therefore determining whether the current `/var` disk usage exceeds 50%)
      - Accumulation interval: `1440` (indicates the time interval, in minutes, for which the query results are evaluated)
      - Threshold: `1` (indicates how many times during the specified time interval the condition must be met before an alert is triggered)
      - Alert when value is: **>=**
      - Notification frequency: `60` (indicates how frequently, in minutes, an alert notification is generated)

      Note: Click the help icon in the Alert Builder pane to learn more about the input fields.

   b. Click **Apply**.

   Figure 7-18 on page 234 depicts the completed disk usage alert. This alert is triggered if the `/var` file system usage on the appliance reaches 50% during a 24-hour period.

Alert Builder

Name: High VAR disk usage
Description: VAR disk usage exceeded 50% at least once during
Category:
Classification:
Recommended Action:
Message Template: Threshold Default Template Edit message
Severity: MED
Run frequency: 15 (minutes)
Active: ☑
Log policy violation: ☐

Alert Definition

Query: High VAR disk usage

Query Parameters

var_disk_utilization_level String 50

Accumulation interval: 1440 (minutes)
Note: Alerts run on aggregators will be based only on data
Log full query results: ☑
Column: (optional)

Alert Threshold

Threshold: 1
Alert when value is >= threshold
Threshold Evaluated: per report / per line
Threshold Used: As absolute limit / As percentage change within period:
From
To
As percentage change for the same "Accumulat
Ending at

Notification

Notification frequency: 60 (minutes)

Figure 7-18 Triggers alert if /var disk usage on appliance reaches 50% in 24 hours

4. Assign an alert receiver:
   a. Click **Add Receiver**.
   b. Select one:
      - SMTP: The Simple Mail Transfer Protocol (SMTP) (outgoing email) server. The alerter passes standard email messages to the SMTP server for which it is configured.
      - SNMP: The Simple Network Management Protocol (SNMP) (network information and control) server. When SNMP is selected for an alert notification, the alerter passes all alert messages of that type to the single trap community for which the alerter is configured.
      - Syslog: The alert is written to syslog on the Guardium appliance, which can be configured by the Guardium Administrator to write syslog messages to a remote system.
      - Custom: A user-written Java class to handle alerts. The alerter passes an alert message and time stamp to the custom alerting class. Multiple custom alerting classes can exist, and one custom alerting class can be an extension of another custom alerting class.
5. Click **Save** to save the alert.

Note: Ensure that the alerter service is running, as described in 7.4.1, “Enabling the alerting service” on page 248.

Reviewing workload disk usage

To determine the workload disk footprints, use the following steps:

1. Log in to the CLI as an administrator or a privileged user.
2. Run the following command:

   ```
   show ocr_profile_size
   ```

   The command lists the disk footprints for each workload. Figure 7-19 on page 236 depicts the output of this command for a workload that is transformed one time and replayed eight times. The total disk footprint for this workload is about 26 GB. cw43 represents the original captured workload. gw43 represents the transformed workload. Each rw43 entry represents every time that the workload is replayed. ocrtemp is used when you are building a report. Figure 7-19 on page 236 shows the replayed workloads that are deleted to make space available because we no longer want to compare and analyze them.

```
pine.itso.ibm.com> show ocr_profile_size
cw43 26G
  gw43_1_0 8.2G
  rw43_1_0_1 31M
  rw43_1_0_2 24M
  rw43_1_0_3 7.0M
  rw43_1_0_4 12M
  rw43_1_0_5 9.2M
  rw43_1_0_6 14M
  rw43_1_0_7 7.0G
  rw43_1_0_8 5.6G
ocrtemp 25G
  rc1383706499819 237M
  rd1373267814441 8.0K
```

Figure 7-19 Replayed workloads that are deleted to free space

7.2.2 Monitoring the connection status of Workload Replay services

The InfoSphere Workload Replay components in a single-server or multi-server deployment communicate with each other through controllers. If these controllers are not running or unable to connect, your ability to capture or replay workloads might be restricted.

Follow these steps to monitor the controller connection status:

1. In a single-server deployment, open the appliance's Workload Replay web console (in multi-server deployments, open the main Workload Replay appliance's web console) and log in as a privileged user or user.

   Note: The Workload Replay web console is not available on auxiliary appliances.

2. Navigate to the System Status page by selecting **Open** → **Administration** → **System Status**.

   Each connected service is displayed in the Workload Replay controller grid. Figure 7-20 on page 237 shows the main Workload replay server for the z/OS book deployment.

Main workload replay server:

Host Name	IP Address	Version
maple.itso.ibm.com	9.12.5.27	2.1.348

Workload replay contro:

Host Name	IP Address	Type	ID	Status
maple.itso.ibm.com	9.12.5.27	Controller for auxiliary server	1451365446	Connected
oak.itso.ibm.com	9.12.5.104	Controller for auxiliary server	1451375097	Connected
wtsc61.itso.ibm.com	9.12.4.32	CQZSERV	IOQCRSERVER	Connected
wtsc62.itso.ibm.com	9.12.4.34	CQZSERV	IOQCRSERVER	Connected

Figure 7-20 All services are connected as expected on maple.itso.ibm.com

In a fully operational deployment, the following controllers need to be connected to the appliance:

- A controller for the auxiliary server for the Workload Replay appliance that you are accessing (Row 1 in Figure 7-20).
- A controller for the auxiliary server for each auxiliary Workload Replay appliance that is assigned to the main Workload Replay appliance in multi-server deployments (Row 2 in Figure 7-20).
- A CQZSERV for each z/OS logical partition (LPAR) on which you configured S-TAP for a subsystem (Rows 3 and 4 in Figure 7-20).

7.2.3 Monitoring CPU utilization

You can monitor current or historical CPU utilization and create an alert to be notified if CPU utilization on an appliance breaches a predefined threshold.

Monitoring system CPU utilization

The CLI versions of the UNIX **`top`** command provide a real-time view of the processor activity on an appliance. The **`top`** command displays a listing of the most CPU-intensive tasks on the system.

To monitor the current CPU utilization on an appliance, use these steps:

1. Log in to the CLI as an administrator or a privileged user.
2. Run the following commands:

```
support show top cpu
support show top memory
support show top time
```

To review the historical CPU utilization, use the following steps:

1. Log in to the Guardium web console as an administrator or a privileged user.
2. Select **Guardium Monitor** → **Buffer Usage Monitor**.
3. The system CPU utilization is displayed in the System CPU Load column. The information is updated in 1 minute intervals.

> **Note:** Sort the System CPU Load column in descending order to identify periods of high CPU usage quickly.

Creating a System CPU utilization alert

InfoSphere Guardium can generate alerts based on monitoring information that is collected on the appliance or by S-TAPs. To take advantage of alerting, you must enable the alerter service by following the instructions in 7.4.1, “Enabling the alerting service” on page 248.

In the following example, we create an alert that is triggered if the system CPU load on the appliance exceeds 75% at least 10 times during a 24-hour period. Follow these steps to create this alert:

1. Log in to the Guardium web console as an administrator or a privileged user.
2. Create a query that retrieves the current system CPU load:
   a. Select **Tools** → **Report Building** → **Sniffer Buffer Usage Tracking**.
   b. Select **Sniffer Buffer Usage** as the Main Entity, as shown in Figure 7-21, and click **New**.

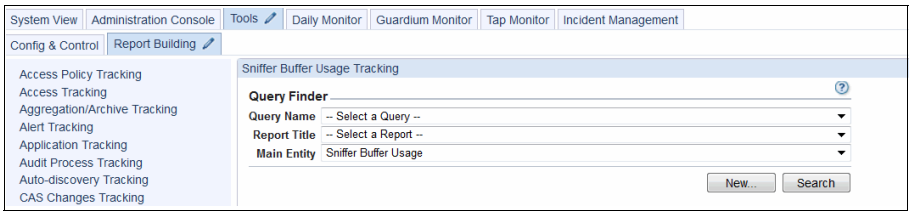


Figure 7-21 Navigate to the Sniffer Buffer Usage Tracking pane

c. Enter **CPU Utilization** as Query Name and select **Sniffer Buffer Usage** as Main Entity, as shown in Figure 7-22.

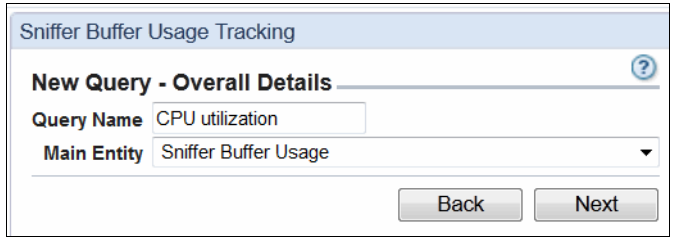


Figure 7-22 Create a query for the alert

d. Click **Next** to define the query output and condition.

e. In the Entity List, expand the **Sniffer Buffer Usage** node.

f. Add **Timestamp** as a Query Field and add **System CPU Load** as a Query Condition, as shown in Figure 7-23.

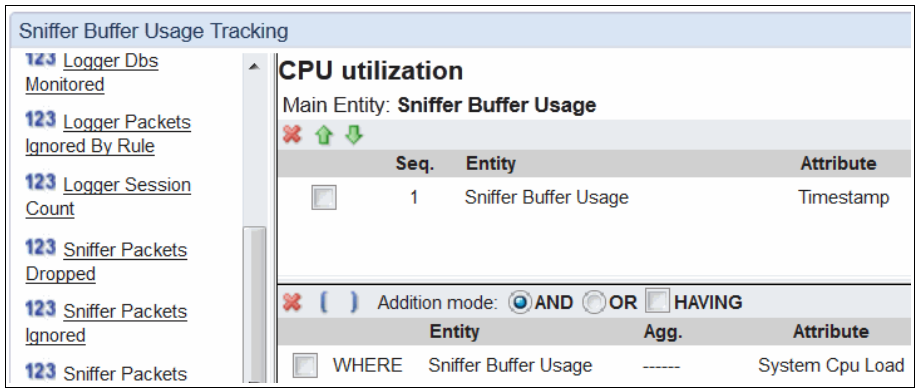


Figure 7-23 Create the alert query

g. Under Query Conditions, select the greater than (>) operator. You can compare the selected entity with a constant, a runtime parameter, or another entity. For illustration, we compare the current CPU load with a constant value.

h. Enter the CPU load threshold that you want in a percentage (%), such as 75, as shown in Figure 7-24 on page 240.

( ) Addition mode: AND OR HAVING **Query Conditions**

	Entity	Agg.	Attribute	Operator	Runtime Param.	
WHERE	Sniffer Buffer Usage	------	System Cpu Load	>	Value	75

Figure 7-24 Specify the CPU load threshold that you want

i. **Save** the query.

3. Create the alert:

   a. Navigate to **Tools** → **Config and Control** → **Alert Builder**.

   b. Click **New** to create a new alert.

   c. Enter or select the following based on your environment:

   - Name: `High system CPU load`
   - Description: `CPU load exceeded 75% at least 10 times during the past 24 hours`
   - Severity: **HIGH**
   - Run frequency: `15` (indicates how frequently, in minutes, the query is run to retrieve the current system CPU load)
   - Query: `CPU utilization`
   - Accumulation interval: `1440` (indicates the time interval, in minutes, for which the query results are evaluated)
   - Threshold: `10` (indicates how many times during the specified interval the condition must be met before an alert is triggered)
   - Alert when value is: **>=**
   - Notification frequency: `10` (indicates how frequently, in minutes, an alert notification is generated)

   Note: Click the help icon in the Alert Builder pane to learn more about the input fields.

   d. Click **Apply**.

   Figure 7-25 on page 241 depicts the completed alert definition. This alert is triggered if CPU utilization exceeds 75% at least 10 times during a 24-hour period.

Alert Builder

Description: CPU load exceeded 75% at least 10 times during the past 24 ho
Category:
Classification:
Recommended Action:
Message Template: Threshold Default Template — Edit message templates
Severity: HIGH
Run frequency: 15 (minutes)
Active: ☑
Log policy violation: ☐

Alert Definition

Query: CPU utilization
Accumulation interval: 1440 (minutes)
Note: Alerts run on aggregators will be based only on data within the de
Log full query results: ☑
Column: (optional)

Alert Threshold

Threshold: 10.0
Alert when value is: >= threshold
Threshold Evaluated: per report / per line
Threshold Used: As absolute limit / As percentage change within period: / As percentage change for the same "Accumulation Period" c
From
To
Ending at

Notification

Notification frequency: 10 (minutes)

Figure 7-25 Triggers alert if CPU utilization exceeds 75% at least 10 times in 24 hours

4. Assign an alert receiver:
   a. Click **Add Receiver**.
   b. Select one:
      - SMTP: The SMTP (outgoing email) server. The alerter passes standard email messages to the SMTP server for which it was configured.

- SNMP: The SNMP (network information and control) server. When SNMP is selected for an alert notification, the alerter passes all alert messages of that type to the single trap community for which the alerter is configured.
- Syslog: The alert is written to syslog on the Guardium appliance, which can be configured by the Guardium Administrator to write syslog messages to a remote system.
- Custom: A user-written Java class to handle alerts. The alerter passes an alert message and time stamp to the custom alerting class. Multiple custom alerting classes can exist, and one custom alerting class can be an extension of another custom alerting class.

5. Click **Save** to save the alert.

> **Note:** Ensure that the alerter service is running, as described in 7.4.1, “Enabling the alerting service” on page 248.

7.3 S-TAP health monitoring

The database server components play a critical role in an InfoSphere Workload Replay deployment. To avoid availability or performance issues, monitor their health periodically.

> **Note:** For more information about S-TAP performance optimization and tuning, see 7.1.1 “S-TAP optimization and tuning” in the *Deployment Guide for InfoSphere Guardium*, SG24-8129, which you can download from the following website:
>
> http://www.redbooks.ibm.com/abstracts/sg248129.html

7.3.1 Monitoring connection status on DB2 for Linux, UNIX, and Windows database servers

Use these steps to monitor the connection status on DB2 for Linux, UNIX, and Windows database servers:

1. Log in to the Guardium web console as an administrator or a privileged user.
2. Select **Administration Console** → **Local Taps** → **S-TAP Control**.

3. You need to see the S-TAP status as green, as shown in Figure 7-26. If not, see 9.3, “Resolving S-TAP issues for a DB2 for Linux, UNIX, and Windows environment” on page 289.

Figure 7-26 S-TAP status for DB2 for Linux, UNIX, and Windows

Note: The Last Response time indicates when this S-TAP last communicated with the appliance that you are connected to.

7.3.2 Monitoring S-TAP health and performance on DB2 for Linux, UNIX, and Windows database servers

InfoSphere Guardium provides facilities that you can use to monitor S-TAP health and performance in the Guardium web console. Before you can monitor the collected information, you must enable S-TAP statistics collection, which is disabled by default, and create a statistics report.

Enabling S-TAP statistics

Follow these steps to enable S-TAP statistics collection on a database server:

1. Log in to the database server as the owner (typically root) of the S-TAP process.
2. Edit the S-TAP configuration `guard_tap.ini` file.

   Note: To locate the configuration file easily, run **`ps -ef | grep stap`** on Linux and UNIX servers. The configuration file name (including the full path to it) is displayed as the first parameter of the `guard_stap` process.

3. Locate the stap_statistics configuration setting, which is set to `0` (disabled), by default.
4. Change the collection interval. A negative value indicates a duration in minutes. A positive value indicates a duration in hours. For example, setting stap_statistics to `-20` instructs S-TAP to collect and transmit statistics about every 20 minutes to its associated Workload Replay appliances.

> **Note:** Use a collection interval of 1 hour for normal operation, unless advised by IBM Software Support to use a shorter interval for troubleshooting.

5. Save the configuration file and recycle the S-TAP process. You can cancel the pid that is associated with the stap process to re-create it.

   S-TAP statistics are now transmitted. They can be queried by using an S-TAP statistics report in the Guardium web console.

Creating an S-TAP statistics report

Follow these steps to create an S-TAP statistics report after you enable statistics collection on each database server:

1. Log in to the Guardium web console as an administrator or a privileged user.
2. Select **Tools** → **Report Building** → **Stap Statistics Tracking**, as shown in Figure 7-27.

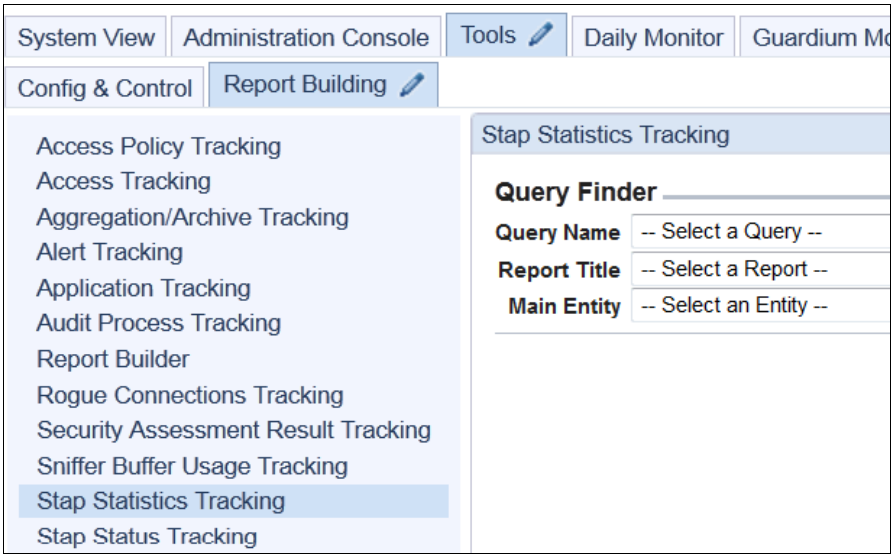


Figure 7-27 Navigate to the Stap Statistics Tracking report builder

3. In the Stap Statistics Tracking pane, click **New** to create a report.
4. Enter `Monitor S-TAP health` as the query name and select **Stap Statistics** as Main Entity. Click **Next**.
5. In the Entity List, expand the **Stap Statistics** node.

6. Click each of the following entities and select **Add Field** from the context menu to add them to the report:
   - Timestamp
   - Software Tap Host
   - System CPU Percent
   - Stap CPU Percent
   - Buffer Recycled

   The selected entities are displayed in the Query Fields pane, as shown in Figure 7-28.

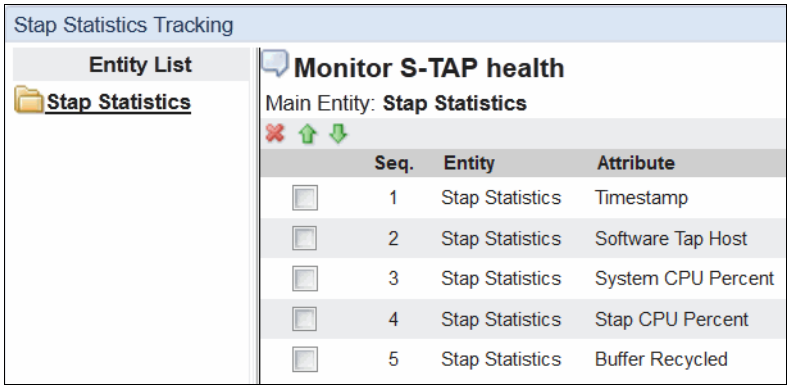


Figure 7-28 Select the statistics information to include in the health report

7. Click **Save** to save the Monitor S-TAP health query.
8. Click **Add to Pane** and choose the **Tap Monitor** → **S-TAP** pane, as shown in Figure 7-29.

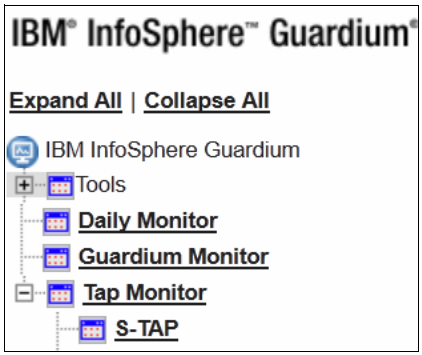


Figure 7-29 Select the pane in which the report is stored

You can now monitor S-TAP health by using the S-TAP statistics report that you created.

Monitoring S-TAP health

Follow these steps to review the collected S_TAP statistics:

1. Log in to the Guardium web console as an administrator or a privileged user.
2. Select **Tap Monitor** → **S-TAP** → **Monitor S-TAP health**, as shown in Figure 7-30.

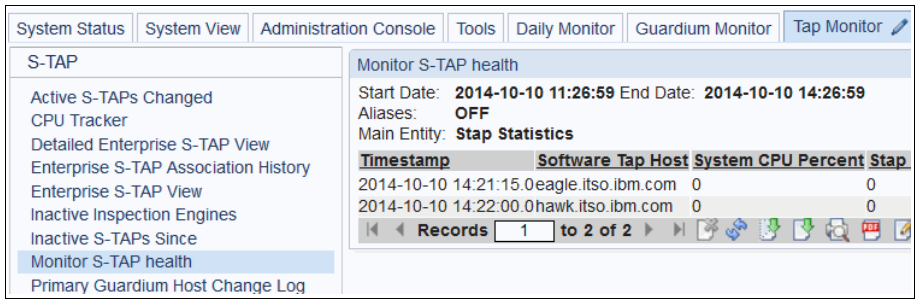


Figure 7-30 Access the S-TAP statistics report

> **Note:** Your navigation steps differ if you assigned a different name to the report or saved it in a different pane.

The S-TAP statistics are displayed for each database server on which S-TAP statistics collection is enabled, as shown in Figure 7-31.

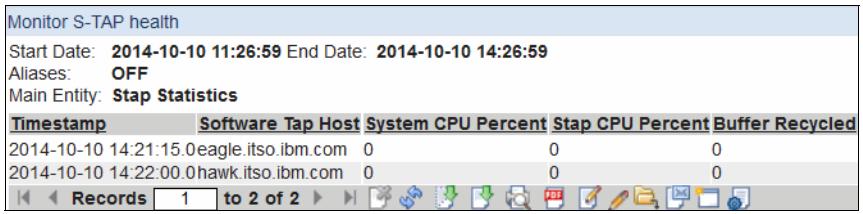


Figure 7-31 Monitor CPU utilization for each database server

3. Review the displayed statistics:
   - Timestamp: Indicates when the statistics were collected.
   - Software Tap Host: The database server where the statistics were collected.
   - System CPU Percent: Total CPU utilization in a percentage (%) on the database server. A high number indicates a busy system.
   - Stap CPU Percent: S-TAP CPU utilization in a percentage (%) on the database server. At the time of writing this book, the S-TAP process runs single-threaded and can therefore at most consume 100% of one core. To estimate the CPU % for one core, multiply the displayed number with the number of cores on the database server. For example, if the reported CPU utilization is 2% and the database server runs on 24 cores, S-TAP is consuming about 48% of one core. If the value approaches 100%, performance degradation is likely, resulting in loss of data.
   - Buffer Recycled: The number of times that the S-TAP buffer overflowed. A nonzero value is a strong indication of a performance issue. If S-TAP is unable to send the collected database traffic to Workload Replay appliances fast enough, the internal buffer might be exhausted and data is dropped. Two main reasons exist for buffer overflows:
     - Insufficient network bandwidth exists between the database server and the associated Workload Replay appliances.
     - The designated Workload Replay appliances are overloaded and are unable to process transmitted data in a timely manner.

     Note: If buffer overflows are reported, check the CPU utilization on the associated appliances for the selected interval. You can increase buffer_file_size to `2000` by editing the `guard_tap.ini` file.

4. Customize the report display, as needed. By default, statistics for the past three hours are displayed. Click the pencil icon on the right to modify the “Enter Period From” and “Enter Period To” runtime parameters to display statistics for the interval that you are interested in.

7.3.3 Monitoring the connection status on DB2 for z/OS LPARs

Use the following steps to monitor the connection status on DB2 for z/OS LPARs:

1. Log in to the Guardium web console as an administrator or a privileged user.
2. Select **Administration Console** → **Local Taps** → **S-TAP Control**.

3. You need to see the S-TAP status in green, as shown in Figure 7-32. Remember that no inspection engines are defined for DB2 for z/OS S-TAPs. The z/OS S-TAP Collector is only active when capture is running. Therefore, it is normal for the S-TAP status to not appear green when no active capture or replay is running.

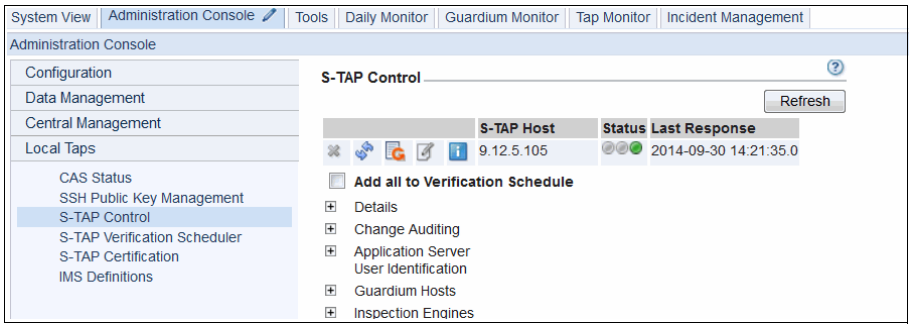


Figure 7-32 S-TAP status for DB2 for z/OS

7.4 Managing alerts

InfoSphere Guardium provides alerting mechanisms to send notifications about specific events to users.

7.4.1 Enabling the alerting service

The alerting service is disabled, by default. To enable it on a main or auxiliary Workload Replay appliance, complete the following steps:

1. Log in to the Guardium web console as an administrator or a privileged user.
2. Select **Administration Console** → **Alerter**, as shown in Figure 7-33.

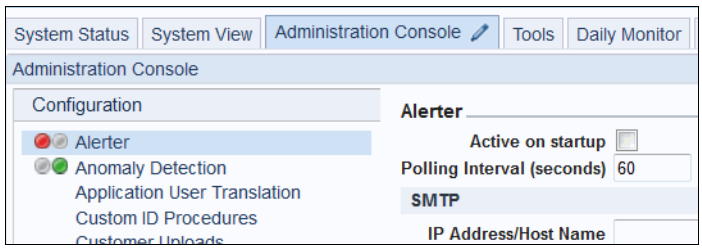


Figure 7-33 Alerter

3. Check **Active on startup** to enable automatic startup.

4. Enter the correct SMTP or SNMP information for your environment.
5. Click **Apply**.
6. Click **Restart**. The alerter status changes from red to green, as shown in Figure 7-34.

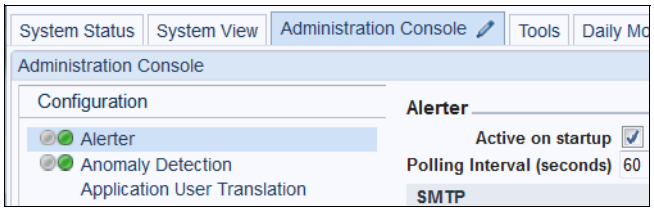


Figure 7-34 The alerter is running

7.5 Backup and recovery

This section describes how you can perform a system backup and recovery of a Workload Replay appliance. Remember that you must back up the data and the configuration separately and restore both the data and the configuration.

7.5.1 System backup and restore

A system backup is a full backup of the internal repository database and selected configuration files from the appliance. It is used to restore the appliance in a hardware failure. Therefore, it is not necessary to keep more than three rolling copies. The backup is written to a single compressed and encrypted file. The backup is sent to the specified destination by using the transfer method that is configured for backups on the appliance.

A system backup saves the system data and the configuration settings as two compressed backup files with file names of the following format:

- `2014****-SQLGUARD_DATA-9.0.tgz`
- `2014****-SQLGUARD_CONFIG-9.0.tgz`

The backup files contain all workloads and reports and also all database connection profiles and accounts that are stored on the appliance. A backup can be restored to the same system or to a different system.

Creating a system backup

To back up a Workload Replay appliance, complete the following steps:

1. Log in to the CLI as an administrator.
2. Back up the Workload Replay system data by running the following command:

   `backup system`

   Choose the **DATA** backup option.
3. Follow the prompts:
   - Transfer type. (Choose **SCP** for a secure copy file transfer.)
   - Backup host name.
   - Backup host user name.
   - Destination directory on backup host.
   - Password for <*backup host user name*>.
   - SCP port number if you need to use a non-default port. Press Enter to use the default port.

   The system backs up the Workload Replay data to a backup file in the destination directory that you specify. Depending on the amount of data to back up, this process might take time. There is no progress indication.
4. Confirm that the backup completed successfully. A message similar to the following message displays at the command prompt:

   ```
   Backup done.
   File=/destination/directory/2014****-SQLGUARD_DATA-9.0.tgz using=SCP
   ok
   ```
5. Back up the Workload Replay configuration data by running the following command:

   `backup system`

   Choose the **CONFIGURATION** backup option.

6. Follow the prompts:
   - Transfer type. (Choose **SCP** for a secure copy file transfer.)
   - Backup host name.
   - Backup host user name.
   - Destination directory on backup host.
   - Password for <*backup host user name*>.
   - SCP port number if you need to use a non-default port. Press Enter to use the default port.

   The system backs up the Workload Replay configuration to a backup file in the destination directory that you specify. Depending on the amount of data to back up, this process might take time. There is no progress indication.
7. Confirm that the backup completes successfully. A message similar to the following message displays at the command prompt:

   ```
   Backup done.
   File=/destination/directory/2014****-SQLGUARD_CONFIG-9.0.tgz
   using=SCP
   ok
   ```
8. Verify that the backup files were created on the destination host in the backup directory that you specified.

Restoring a system backup

To restore a Workload Replay appliance from a backup, complete the following steps:

1. Rebuild the appliance on which you want to restore the system backup.

   > **Note:** You *must* install the prerequisite patches (9997, GPU 200, 1033, and 3990) and the Version 2.1.0.1 Workload Replay software patch (3423) before you restore a system backup.

2. Log in to the CLI as an administrator.
3. Restore the Workload Replay system data by running the following command:

   ```
   restore system
   ```

4. Follow the prompts:
   - Transfer type. (Choose **SCP** for a secure copy file transfer.)
   - Backup host name.
   - Backup host user name.
   - Backup directory on backup host.
   - Backup file name:

     `/destination/directory/2014****-SQLGUARD_DATA-9.0.tgz`
   - Password for <*backup host user name*>.
   - SCP port number if you need to use a non-default port. Press Enter to use the default port.
   - Select normal recovery type.
5. The system restores the Workload Replay data from the backup file in the backup directory.
6. Verify that the system data restore process completes successfully. A message similar to the following message displays at the command prompt:

   ```
   Data recovery complete
   Proceeding to startup services
   Safekeeping xregs
   Recovery procedure was successful.
   ok
   ```
7. Restore the Workload Replay system configuration by running this command:

   `restore system`
8. Follow the prompts:
   - Transfer type. (Choose **SCP** for a secure copy file transfer.)
   - Backup host name.
   - Backup host user name.
   - Backup directory on backup host.
   - Backup file name:

     `/destination/directory/2014****-SQLGUARD_CONFIG-9.0.tgz`
   - Password for <*backup host user name*>.
   - SCP port number if you need to use a non-default port. Press Enter to use the default port.
   - Select normal recovery type.

9. The system restores the Workload Replay system configuration from the backup file in the backup directory.
10. Verify that the system configuration restore process completes successfully. A message similar to the following message displays at the command prompt:

    ```
    Data recovery complete
    Proceeding to startup services
    Safekeeping xregs
    Recovery procedure was successful.
    ok
    ```

11. Restart the Workload Replay appliance by entering this command:

    `restart system`

    Follow the prompts.
12. Wait for the system to come back online.
13. Log in to the CLI as an administrator.
14. Start the Workload Replay services by running the following commands:

    `restart ocr_capture_manager`
    `start ocr_aux_controller`
15. Verify that you can access the Workload Replay console as a privileged user or a user that was defined on the backed up system:

    `https://`*`guardium_hostname_or_ip`*`:8443/dsweb/console/ocr/index.jsp`

7.5.2 Workload backup and restore

You can back up captured workloads to an FTP or SCP server for archiving or disaster recovery. Archive files are a password-protected and encrypted. Workload backup and restore operations are typically performed by privileged users.

Backing up captured workloads

The workload backup process consists of two steps: export and upload to intermediary storage.

To export a workload and upload a workload to an intermediary server, complete the following steps:

1. In a single-server deployment, open the appliance's Workload Replay web console (in multi-server deployments, open the web console of the main Workload Replay appliance) and log in as a privileged user.
2. From the SQL Workloads page (**Open** → **Capture and Replay**), right-click the captured workload that you want to export, and select **Export**, as shown in Figure 7-35.

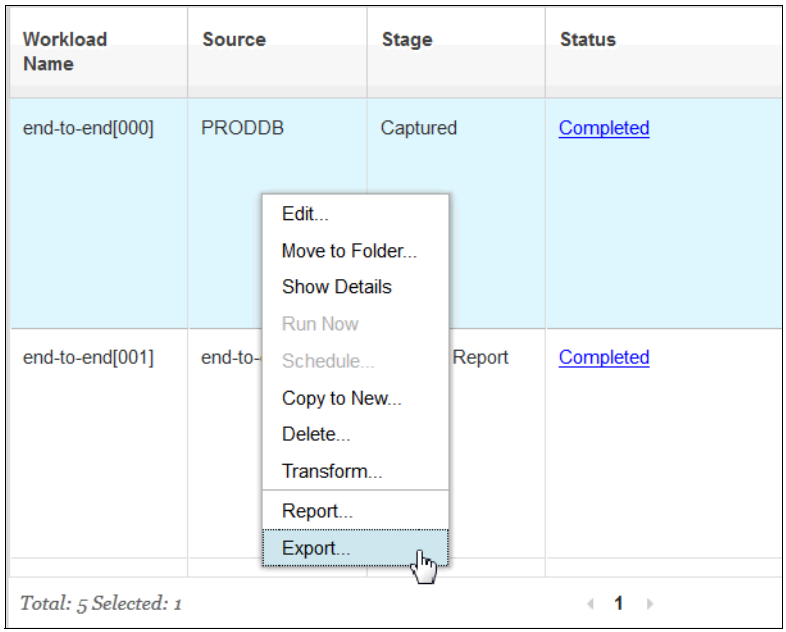


Figure 7-35 Select Export to create a workload backup

In the Export a Workload wizard (Figure 7-36 on page 255), enter a workload password to secure the encrypted workload file. This password is required to restore the workload on the same or another Workload Replay server. The workload is packaged into an encrypted file and stored in the Workload Replay server file system.

Note: Depending on the size of the workload, the packaging process might take time. Use the Export Process Status information in the workload details page to monitor the export process.

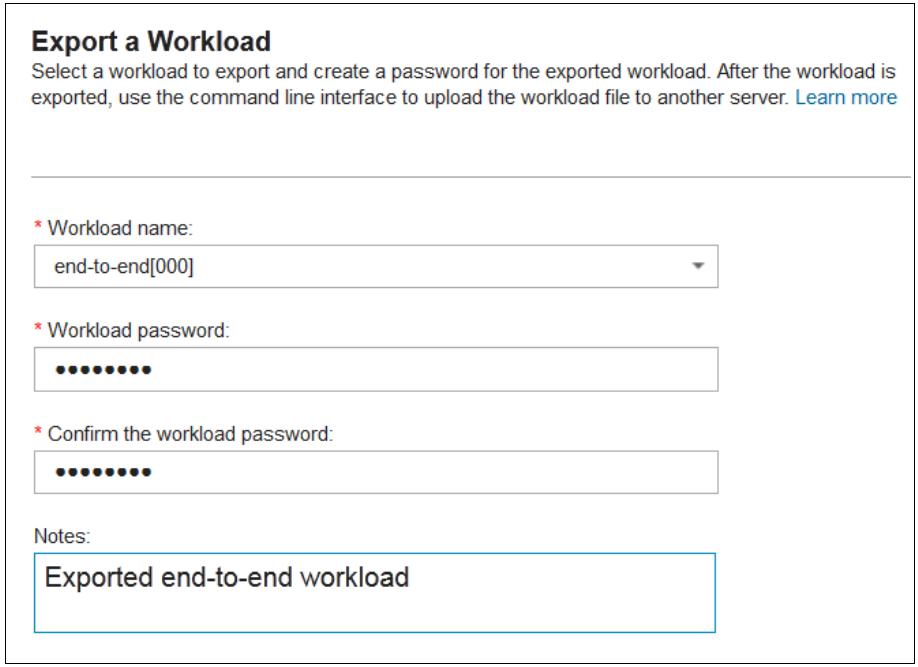


Figure 7-36 Protect workload archives by using a password

3. When the workload is packaged, use the CLI to upload the workload to the backup server:
   a. Log in to the CLI as a privileged user.
   b. Enter the following CLI command to upload the workload to an intermediary FTP or SCP server (Figure 7-37 on page 256):

      `upload ocr_workload_files`

      Follow the prompts to provide connectivity information for the backup server:

      - Transfer protocol: FTP or SCP.
      - User ID: A user ID on the target system with at least write privileges on the target directory.
      - Password: The password of the user.
      - Server address: Server name or IP address of the backup server.
      - Target directory: Enter the absolute path to the target directory.
      - Workload file: Select the workload file to upload to the backup server.

```
pine.itso.ibm.com> upload ocr_workload_files

Select the transfer protocol by entering the corresponding number (q to quit):
        1. SCP
        2. FTP

2

Enter the FTP port. Enter "0" or press "Enter key" to use the default port:

Enter the server name or IP address of the target server: 9.12.5.103

Enter a user ID that has write privileges on the target directory: ftproot

Enter the password for the selected user:

Enter the absolute path to the FTP target directory: /FTP_ROOT/exported_workload
s

Select the workload file to upload by entering the corresponding number:
1. end-to-end[005].zip [196K]

Select the workload file to upload by entering the corresponding number: 1
Type Y to upload the end-to-end[005].zip file to the 9.12.5.103 FTP server. Type
 N to cancel and exit. The file size is 196K.
y

The workload file is being uploaded. Depending on the size of the file, this mig
ht take some time. You can monitor the file upload progress on your FTP server.


194014 bytes transferred
File uploaded successfully.
ok
```

Figure 7-37 Transfer a workload backup to an FTP or SCP server

Note: The file upload runs as a background process. Depending on the size of the workload file, the process might take time to complete.

c. On the target backup server, verify that the file uploaded successfully.

Restoring captured workloads

A backed-up workload can be restored on the same appliance where the backup was created or on another appliance:

1. In a single-server deployment, open the appliance's CLI (in multi-server deployments, open the CLI of the main Workload Replay appliance) and log in as a privileged user.
2. Enter the following CLI command to download the workload file from an intermediary server (Figure 7-38 on page 258):

   ```
   download ocr_workload_files
   ```

   Follow the CLI prompts to specify the following parameters:

   – Transfer protocol: FTP or SCP.
   – User ID: A user ID on the backup system with at least read privileges on the target directory.
   – Password: The password of the user.
   – Server address: The server name or IP address of the target server.
   – Target directory: Enter the absolute path to the target directory.
   – Workload file: Enter the name of the workload file to download from the backup server.

   Figure 7-38 on page 258 shows a download of the archived captured workload to a main Workload Replay appliance.

```
pine.itso.ibm.com> download ocr_workload_file

Select the transfer protocol by entering the corresponding number (q to quit):
        1. SCP
        2. FTP

2

Enter the FTP port. Enter "0" or press "Enter key" to use the default port:

Enter the server name or IP address of the source server: 9.12.5.103

Enter a user ID that has read privileges on the source directory: ftproot

Enter the password for the selected user:

Enter the absolute path to the FTP source directory: /FTP_ROOT/exported_workload
s

Enter the file name of the workload file to download: end-to-end[005].zip


The workload file is being downloaded, and will be available for import in the w
eb console when the download is complete. Depending on the size of the file, thi
s might take some time. Enter the 'show ocr_workload_files' command to see a lis
t of the workloads on your server and to monitor the current download progress..

Connected to 9.12.5.103
Login successful as user ftproot
Proceeding to download our file, this might take a few minutes...

end-to-end[005].zip transferred

ok
pine.itso.ibm.com>
```

Figure 7-38 Download archived captured workload

3. In a single-server deployment, open the appliance's Workload Replay web console (in multi-server deployments, open the web console of the main Workload Replay appliance) and log in as a privileged user.
4. From the SQL Workloads page (**Open** → **Capture and Replay**), click **More** → **Import**.
5. In the Import an SQL Workload dialog (Figure 7-39 on page 259), select the workload backup that you want to import, and enter the password for the file.

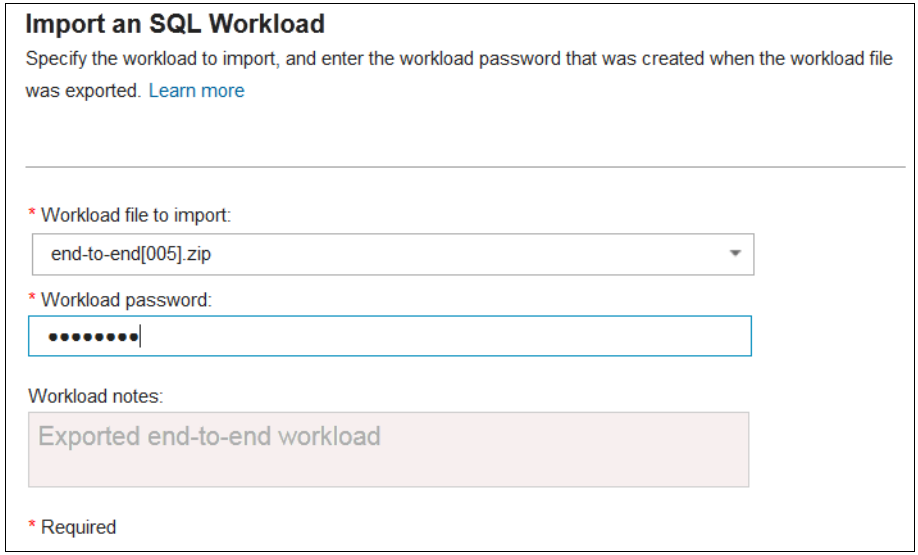


Figure 7-39 A password is required to decrypt backup files

6. Enter a unique workload name, select a folder, and select the database connection profile to associate the workload with. Figure 7-40 shows the association of the restored workload with an existing database connection profile.

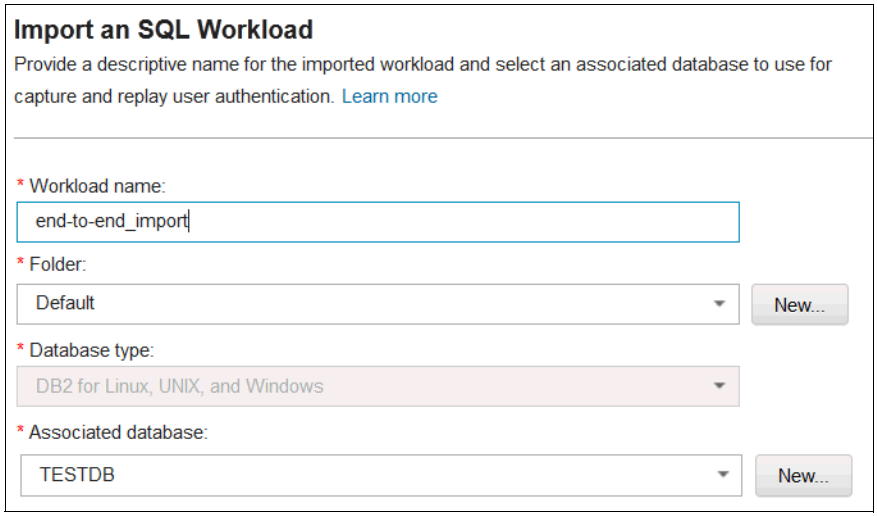


Figure 7-40 Associate restored workload with existing database connection profile

> **Note:** You can restore workloads only on the same DB2 platform where the backup was created.

7. If you are prompted, enter the credentials of a user ID with Can Import Workload privileges.
8. The imported workload displays in the SQL Workloads grid. The imported workload can be used like a captured workload.

7.6 Maintenance and upgrades

IBM periodically releases maintenance patches for InfoSphere Guardium and InfoSphere Workload Replay. We describe the following topics:

- How to determine the patches that are installed on an appliance
- How to download patches from the IBM website
- How to install patches

7.6.1 Determining the appliance patch level

To determine the patches that are installed on a Workload Replay appliance, follow the CLI or Guardium web console instructions that are listed in this section.

Determining the current patch level by using the CLI

To determine the current patch level by using the CLI, complete the following steps:

1. Log in to the CLI as an administrator.
2. Run the following command to display the list of installed patches (Figure 7-41 on page 261):

```
show system patch installed
```

```
pine.itso.ibm.com> show system patch installed
P#      Who       Description                     Request Time
Status
50      CLI       Guardium Patch Update (GPU) for 2014-08-28 09:46:57
DONE: Patch installation Succeeded.
9997    CLI       Health Check for GPU and Upgrad 2014-08-29 02:31:29
DONE: Patch installation Succeeded.
200     CLI       Guardium Patch Update (GPU) for 2014-08-29 02:34:27
DONE: Patch installation Succeeded.
1033    CLI       Patch 1 for Optim Capture and R 2014-08-29 02:56:07
DONE: Patch installation Succeeded.
3990    CLI       Pre-req to setup Aux server     2014-08-29 03:05:19
DONE: Patch installation Succeeded.
3423    CLI       IOWR Install 2.1.348 2014_08_06 2014-09-17 16:07:46
DONE: Patch installation Succeeded.
ok
```

Figure 7-41 Display the installed patches by using the CLI

Note: Patches are not necessarily displayed in the order that they were installed. If a patch is installed multiple times, the time stamp of the most recent installation is shown.

3. Run the following command to display a list of patches that were uploaded but not yet installed in the appliance:

   `show system patch available`

   After a patch is installed, it no longer displays as available.

Determining the current patch level by using the Guardium web console

To determine the current patch level by using the Guardium web console, complete the following steps:

1. Log in to the Guardium web console as an administrator or a privileged user.
2. Navigate to **Guardium Monitor** → **Installed Patches** to review the list, as shown in Figure 7-42 on page 262.

Installed Patches

Aliases: **OFF**
Main Entity: **Available Patch**

Patch Number	Guardium Version	Patch Description	Patch Dependencies	Creation Date	Upload Date	Installed By
1033	9.0	Patch 1 for Optim Capture and Replay Development	200	2014-08-05 12:27:53.0	2014-08-29 03:01:50.0	CLI
200	9.0	Guardium Patch Update (GPU) for Version 9.0	9997	2014-04-03 15:16:42.0	2014-08-29 02:43:31.0	CLI
3423	9.0	IOWR Install 2.1.348 2014_08_06_20_49	1033	2014-08-06 20:49:48.0	2014-08-29 03:13:51.0	CLI
3990	9.0	Pre-req to setup Aux server		2014-06-02 16:20:30.0	2014-08-29 03:05:54.0	CLI
9997	9.0	Health Check for GPU and Upgrade installations		2014-01-22 13:54:53.0	2014-08-29 02:33:15.0	CLI

Figure 7-42 Display installed patches by using Guardium web console

Note: The list includes patches that are installed and patches that are being installed. If you installed a patch more than once, you will see only a single entry with a time stamp that corresponds to the most recent installation.

3. Navigate to **Guardium Monitor** → **Available Patches** to display a list of patches that are uploaded but not yet installed in the appliance. After a patch is installed, it no longer displays as available.

7.6.2 Accessing product updates

IBM periodically releases maintenance for InfoSphere Workload Replay appliances and S-TAP. For details, see A.1.1, “Downloading InfoSphere Workload Replay for DB2 for z/OS installation media” on page 302 and A.1.2, “Downloading InfoSphere Workload Replay for DB2 for Linux, UNIX, and Windows installation media” on page 309.

7.6.3 Installing maintenance on an appliance

InfoSphere Guardium and InfoSphere Workload Replay patches can be installed from your local system or from any FTP or SCP server that is accessible from the appliance. Before you install patches, you might want to create a backup profile.

Creating a backup profile before patch installation

With a backup profile, you can recover from a patch installation failure.

To create a backup profile and store it on an SCP host, follow these steps:

1. Log in to the CLI of the correct appliance as an administrator.
2. Run the following command and follow the prompts to create a backup profile:

   store backup profile

3. Run the following command to determine whether a backup profile exists:

   show backup profile

Installing patches from a local file system

To install a patch that is on your local machine, you upload the patch to the appliance, invoke the patch installation, and monitor installation progress.

Complete these steps to install patches from a local file system:

1. Log in to the CLI of the correct appliance as an administrator.
2. Issue the **fileserver** command and specify the IP address of your local machine (Figure 7-43):

   fileserver <*client_ip_address*>

```
pine.itso.ibm.com> fileserver 9.55.156.227
Creating the index file.

Starting the file server. You can find it at
http://pine.itso.ibm.com
The timeout has been set to 3600 seconds and it may timeout
during the uploading.

The upload will only be accessible from the IP you are logged in
from: 9.55.156.227

Press ENTER to stop the file server.
```

Figure 7-43 Start the file server

Note: If you connect to the appliance by using a proxy, specify the proxy server's IP address instead of your local IP address.

Note: The file server automatically terminates all connections after a customizable amount of time passes after the server was started, regardless of whether a file upload or download is in progress. The default timeout is 600 seconds. You can increase the timeout to a maximum of 3600 seconds.

To display the current timeout value, issue the following CLI command:

```
show timeout fileserver_session
```

To increase the timeout, run the following CLI command:

```
store timeout fileserver_session <time_in_seconds>
```

3. Open a web browser to the URL that is returned by the **`fileserver`** command and click **Upload a patch**, as shown in Figure 7-44.

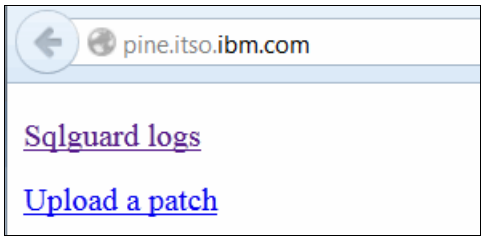


Figure 7-44 Navigate to the upload a patch page

4. On the upload page, click **Browse** to open the File Upload dialog, as shown in Figure 7-45. Browse to the InfoSphere Guardium or InfoSphere Workload Replay patch.

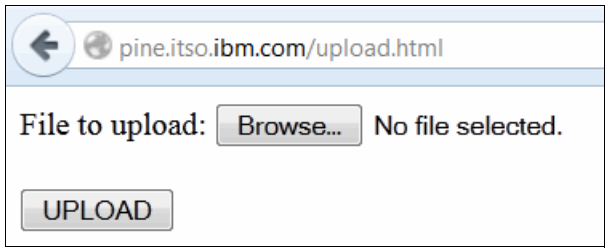


Figure 7-45 Browse to the InfoSphere Guardium or Workload Replay patch

5. Select the patch file to upload and click **Open**.
6. Click **UPLOAD**, as shown in Figure 7-46 on page 265.

Figure 7-46 Uploading the file

7. Wait for the upload to complete.
8. Repeat the steps if multiple patches need to be uploaded.
9. Close the browser window.
10. Stop the file server in the CLI by pressing Enter.

> **Note:** We suggest that you create a backup profile as described in "Creating a backup profile before patch installation" on page 263 before you proceed with the installation.

11. Install the uploaded patches by using the following command and follow the prompts:

```
store system patch install sys
```

> **Note:** You can schedule the installation of several patches by entering multiple patch numbers, such as `1,2,3`. Patches are installed in the order specified.

12. Monitor the patch installation status by using the following command until the status changes to complete:

```
show system patch installed
```

> **Note:** Patch installation might take time. Certain patches automatically restart the appliance after the patch installation completes.

13. Log out of the CLI.

Installing patches from an FTP or SCP server

To install a patch that is on an FTP or SCP server, invoke the patch installation and monitor the installation progress.

Note: We suggest that you create a backup profile as described in “Creating a backup profile before patch installation” on page 263 before you start with the installation.

To install patches from an FTP or SCP server, use the following steps:

1. Log in to the CLI of the correct appliance as an administrator.
2. Upload the patch by issuing the following command:

   ```
   store system patch install [scp | ftp]
   ```

3. Specify the host name, user, and full path to the patch.

   Note: You can use wildcards to retrieve multiple patches at the same time.

4. Enter non-default SCP or FTP port numbers, if needed, or accept the defaults. The patch files are transferred to the appliance.
5. If you previously installed the same patch, you are asked if you want to install it again.

   Note: You can select multiple patches to install by specifying the number that is associated with the patch in the correct sequence. If you attempt to install patches in the wrong sequence, patch installation stops and an error displays that indicates that prerequisite patches are missing.

6. Monitor the patch installation status by using the following command until the status changes to complete:

   ```
   show system patch installed
   ```

   Note: Patch installation might take time. Certain patches automatically restart the appliance after patch installation completes.

7. Log out of the CLI.

7.7 Deciding when to start and stop services

On each appliance, the capture manager and the controller for the auxiliary server services must be running before you can capture or replay workloads.

You must manually start one or both services in the following scenarios:

- You restarted an appliance.
- You want to assign an auxiliary Workload Replay appliance to a different main Workload Replay appliance.
- You want to enable or disable the controller for auxiliary server traces.

7.7.1 Restarting a Workload Replay appliance

To restart an appliance cleanly, follow these steps:

1. Log in to the CLI of the correct appliance as an administrator.
2. Issue the following command and follow the prompts:

   ```
   restart system
   ```

3. Wait until the appliance comes back online.
4. Log in to the CLI of the appliance as an administrator.
5. Start the Workload Replay services by running the following commands:

   ```
   restart ocr_capture_manager
   start ocr_aux_controller
   ```

6. Log out of the CLI.

7.7.2 Associating an auxiliary Workload Replay appliance with a different main Workload Replay appliance

When you configure an auxiliary Workload Replay appliance, you associate it with a main Workload Replay appliance.

If you want to later associate the auxiliary appliance with a different main Workload Replay appliance, complete these steps:

1. Log in to the CLI of the auxiliary appliance as an administrator.
2. Issue the following commands:

   ```
   store ocr_aux_controller ocr_server_IP <guardium_ip>
   stop ocr_aux_controller
   start ocr_aux_controller
   ```

   Replace *<guardium_ip>* with the IP address of the new main Workload Replay appliance.
3. Log out of the CLI.

7.7.3 Enabling and disabling the controller for auxiliary server traces

IBM support might request controller for auxiliary server traces to assist with problem determination. Tracing is enabled, by default, on the auxiliary server. If you must disable and enable trace, follow these instructions:

1. Log in to the CLI of the auxiliary appliance as an administrator.
2. Issue the following commands to disable trace:

   ```
   store ocr_aux_controller trace off
   stop ocr_aux_controller
   start ocr_aux_controller
   ```

   Or, issue these commands to enable trace:

   ```
   store ocr_aux_controller trace on
   stop ocr_aux_controller
   start ocr_aux_controller
   ```
3. You can then issue this command to collect traces on the auxiliary server:

   ```
   support must_gather ocr_issues
   ```

7.7.4 When you might need to restart capture manager

If you changed the configuration on either the main or auxiliary servers and you do not see any captured statements, try to restart the capture manager by using this CLI command:

```
restart ocr_capture_manager
```

8

Integration with other tools

IBM InfoSphere Optim Workload Replay captures information about running SQL statements and transactions while a workload capture or a workload replay is in progress. This information is used to compile overview and detail reports that highlight performance improvements or regressions between two workload executions.

In this chapter, we describe how you can export some of this information for processing by IBM tools, third-party applications, and even in-house developed applications.

8.1 Integration with Query Workload Tuner

IBM InfoSphere Optim Query Workload Tuner for DB2 for Linux, UNIX, and Windows and IBM InfoSphere Optim Query Workload Tuner for DB2 for z/OS provide advanced visualization and tuning capabilities for single SQL statements and sets of SQL statements. Use the tooling in Query Workload Tuner for the following reasons:

- To determine the referenced tables to offload to the DB2 Analytics Accelerator for z/OS
- To determine the referenced tables to enable for DB2 with BLU Acceleration to improve the performance of analytical applications that run on DB2 for Linux, UNIX, and Windows
- To analyze how query performance can be improved through advanced statistics collection, indexes, and so on.

We describe how to export sets of SQL statements, import them into Query Workload Tuner, and link to resources that explain the tuning steps in detail.

Note: Entitlement for Query Workload Tuner is not included in the InfoSphere Workload Replay license.

8.1.1 Exporting SQL from the Workload Replay web console

The Workload Replay web console displays SQL performance information that is automatically collected while workloads are captured or replayed.

To export SQL to a Query Workload Tuner compatible format, complete these steps:

1. In a single-server deployment, open the appliance's Workload Replay web console (in multi-server deployments, open the web console of the main Workload Replay appliance), and log in as a privileged user or user.
2. Open the SQL Workloads page (**Open** → **Capture and Replay**).
3. Open the workload comparison report that you want.
4. Open one of the following workload comparison detail reports:
   - Replay Results → SQL Matched
   - Response Time → SQL Improvements
   - Response Time → SQL Regressions
5. Click **Export** and follow the prompts, as shown in Figure 8-1 on page 271.

Details | Replay Results | Response Time | **SQL Matched**

The unique SQL statements that matched during the replay. The statements replayed w

Export...

Statement I	Statement Text	Baseline E)	Successful
11	SELECT COH.CUST_ORDER_NUMBER, COH.CUST_ORDER_DATE, COH.CUST_ORDER_STATUS_CODE, P.PRODUCT_NAME, COD.C	256	256
13	SELECT COH.CUST_ORDER_NUMBER, COH.CUST_ORDER_DATE, COH.CUST_ORDER_STATUS_CODE, P.PRODUCT_NAME, COD.C	256	256

Figure 8-1 Export SQL from accuracy or performance reports

The exported workload is displayed in your web browser, as shown in Figure 8-2.

Tip: If the web browser displays an error message that indicates that a pop-up window is blocked, confirm the exception and repeat the export steps.


```
- <workload desc="OQCR - Fri Sep 19 21:47:10 EDT 2014" dbtype="DB2LUW">
  - <source name="Matched Aggregated Statements">
    - <statement num_executions="256">
      - <statement_text default_schema="">
          SELECT COH.CUST_ORDER_NUMBER, COH.CUST_ORDER_DATE, COH.CUST_ORDER_STATUS_CO
          GOSALESCT.CUST_ORDER_DETAIL COD, GOSALES.PRODUCT_NAME_LOOKUP P WHERE COH.CU
          COD.PRODUCT_NUMBER = P.PRODUCT_NUMBER
        </statement_text>
        <statement_runtime stmt_exec_time="16.907009"/>
      </statement>
    - <statement num_executions="256">
      - <statement_text default_schema="">
          SELECT COH.CUST_ORDER_NUMBER, COH.CUST_ORDER_DATE, COH.CUST_ORDER_STATUS_CO
          GOSALESCT.CUST_ORDER_DETAIL COD, GOSALES.PRODUCT_NAME_LOOKUP P WHERE COH.CU
          COD.PRODUCT_NUMBER = P.PRODUCT_NUMBER AND P.PRODUCT_LANGUAGE = ?
        </statement_text>
        <statement_runtime stmt_exec_time="15.477355"/>
      </statement>
    - <statement num_executions="206">
      - <statement_text default_schema="">
          SELECT CU.CUST_CODE, CU.CUST_LAST_NAME, COH.CUST_ORDER_NUMBER, DATE(COH.CUST_
          GOSALESCT.CUST_CUSTOMER AS CU, GOSALESCT.CUST_ORDER_HEADER AS COH, GOSALESCT.
          CU.CUST_CODE=COH.CUST_CODE AND COH.CUST_ORDER_NUMBER = COD.CUST_ORDER_NUMI
        </statement_text>
        <statement_runtime stmt_exec_time="12.47691"/>
      </statement>
```


Figure 8-2 Review the exported workload

The exported workload file includes the statement text, execution count, and total elapsed time for each unique SQL.

6. Save the exported workload by clicking your browser's **Save Page** feature.

> **Note:** Do not copy and paste the content of the web browser window if you plan to import the workload into Query Workload Tuner. The import operation might fail, indicating that the file is corrupted.

7. Close the browser window.

8.1.2 Importing SQL workloads into Query Workload Tuner

Optim Query Workload Tuner can capture SQL from various sources:

- DB2 database, for example, dynamic statement cache, EXPLAIN tables, or catalog tables
- Performance monitors, such as DB2 Query Monitor for z/OS and Optim Performance Manager
- Administration and development tools, for example, IBM Data Studio
- Files

Follow these steps to import files that were exported:

1. Open the IBM Data Studio client.
2. Open the **Tune Queries** perspective.
3. If needed, create a database connection profile for the database (or subsystem) on which you want to analyze the workload.
4. Create a Query Tuner project (click **File** → **New** → **Query Tuner Project**) and associate it with the correct database connection profile.
5. Select **Non-DB2 Sources** → **XML File** in the Query Tuner Workflow Assistant, as shown in Figure 8-3 on page 273.

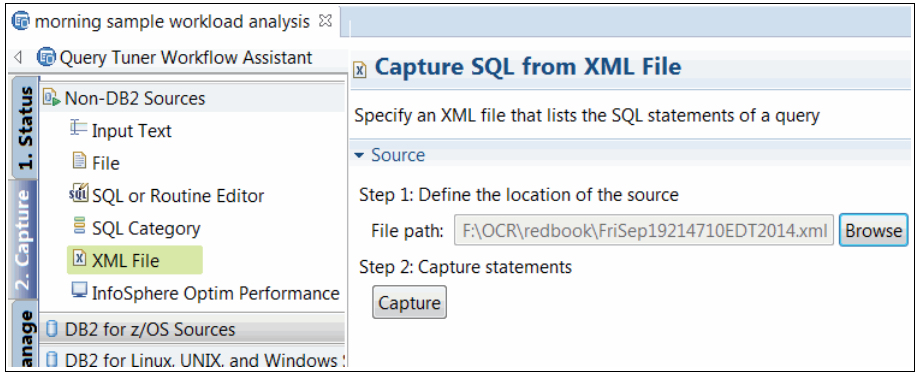


Figure 8-3 Import exported workload file in Query Workload Tuner

6. Browse to the exported workload file and click **Capture**. The captured SQL is displayed, as shown in Figure 8-4.

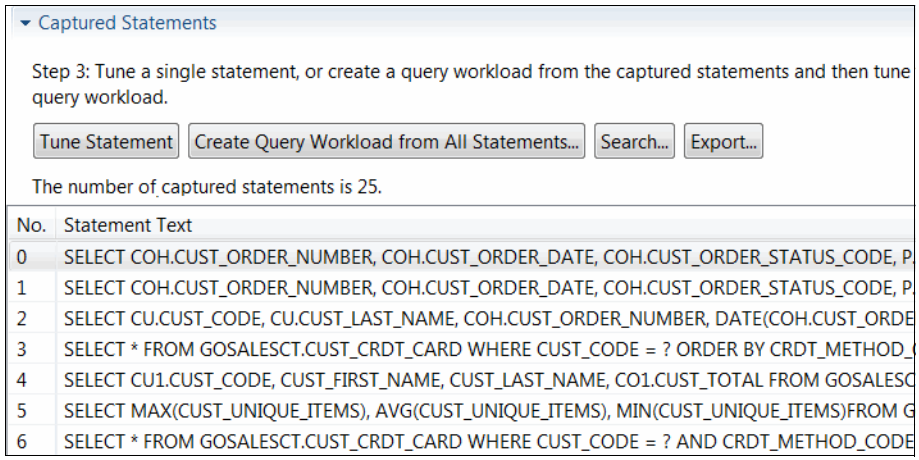


Figure 8-4 Save workload to invoke workload advisors or tune individual statements

7. Click **Create Query Workload from All Statements** to save the workload. The workload is displayed, as shown in Figure 8-5 on page 274. You can now process the workload by using the platform-specific advisors.

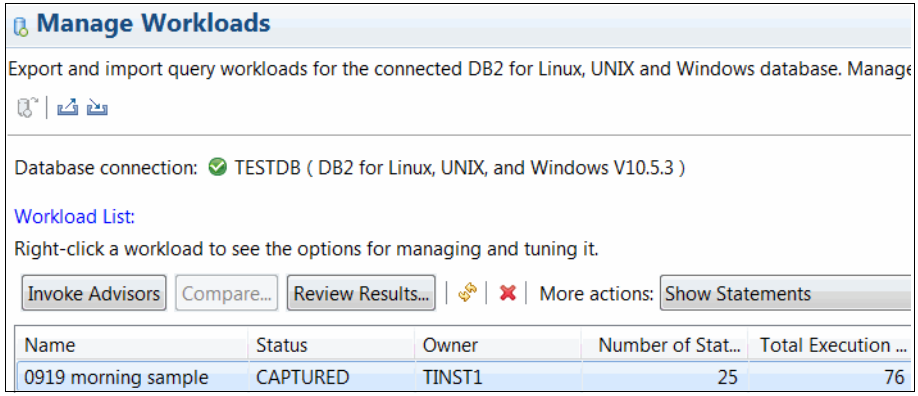


Figure 8-5 Invoke advisors to tune the captured workload

8.1.3 Processing imported workloads

It is beyond the scope of this book to describe how you can use Query Workload Tuner for DB2 for Linux, UNIX, and Windows and Query Workload Tuner for DB2 for z/OS. For in-depth scenario descriptions and step-by-step instructions, see the following publications.

DB2 Analytics Accelerator for z/OS

For information about how to use Query Workload Tuner to identify tables to offload to the accelerator, see the following documents:

- "*Accelerate queries with IBM DB2 Analytics Accelerator for z/OS by using InfoSphere Optim Query Workload Tuner*". You can access this article on IBM developerWorks at the following web address:

  http://www.ibm.com/developerworks/data/library/techarticle/dm-1403queryaccel

- *Optimizing DB2 Queries with IBM DB2 Analytics Accelerator for z/OS*, SG24-8005. You can download this IBM Redbooks publication at the following web address:

  http://www.redbooks.ibm.com/abstracts/sg248005.html?Open

DB2 with BLU Acceleration

For information about how to use Query Workload Tuner to identify BLU Acceleration table candidates, see Chapter 3 "Optim Query Workload Tuner and BLU Acceleration" in *Architecting and Deploying DB2 with BLU Acceleration*, SG24-8212.

You can download this IBM Redbooks publication at the following web address:

http://www.redbooks.ibm.com/abstracts/sg248212.html?Open

DB2 workload tuning

For information about how to use Query Workload Tuner to tune single queries or entire workloads, see Chapter 5, “Getting to know InfoSphere Optim Query Workload Tuner” in *Performance Management: Using IBM InfoSphere Optim Performance Manager and Query Workload Tuner*, SG24-8111. You can download this IBM Redbooks publication at the following web address:

http://www.redbooks.ibm.com/abstracts/sg248111.html?Open

8.2 Integration with other tools

This section describes how you can export captured, transformed, and replayed SQL statements or transactions for offline analysis and how you can invoke a stored procedure before you capture or replay a workload.

8.2.1 Exporting SQL for analysis with third-party tools

You can export captured, transformed, or replayed unique SQL statements (or unique transactions) as delimited text files for processing by third-party tools, that, for example, parse the SQL text and visualize database object dependencies.

To export captured, transformed, or replayed SQL or transactions to a comma-delimited file, use the following steps:

1. In a single-server deployment, open the appliance’s Workload Replay web console (in multi-server deployments, open the web console of the main Workload Replay appliance) and log in as a privileged user or user.
2. Open the SQL Workloads page (**Open** → **Capture and Replay**).
3. Create a single workload report, such as a Capture report, Transform report, or Replay report, by selecting a workload in the captured, replay-ready, or replayed stage, right-clicking it, and selecting **Report** from the menu.
4. Choose the report type tab (SQL or transaction) that you want, as shown in Figure 8-6 on page 276 for the Captured SQL Statements report.

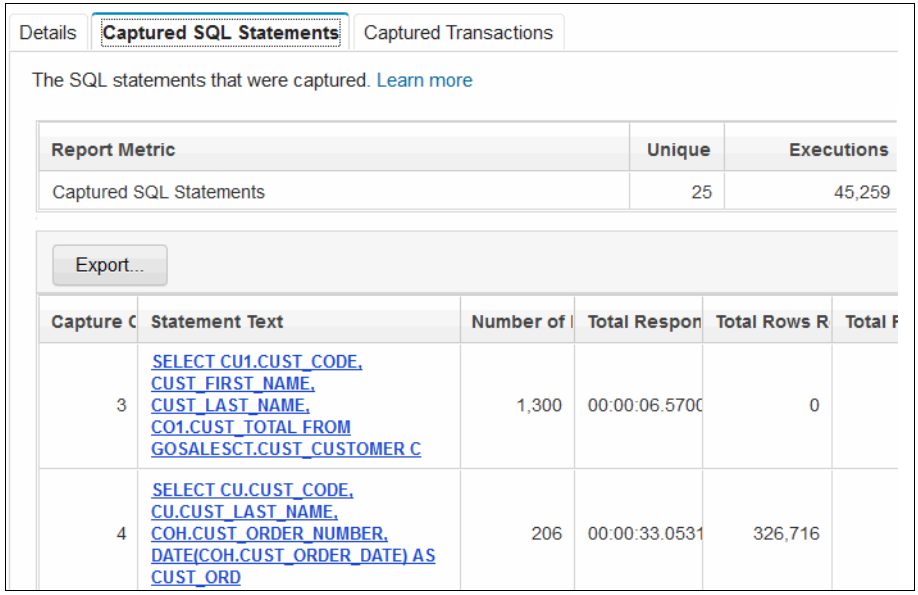


Figure 8-6 Export captured, transformed, or replayed SQL to a comma-delimited file

5. Click **Export** and follow the prompts. The exported file contains a header that describes the exported information.

8.2.2 Invoking external tools before workload capture or replay

Before you run a workload capture or a workload replay, InfoSphere Workload Replay can invoke a user-provided stored procedure, that, for example, can perform housekeeping tasks. Before a workload is captured or replayed, the stored procedure is invoked and the return code is evaluated. The workload capture or replay action is only performed if a positive success code is returned, providing you with the ability to perform conditional workload captures or replays.

> **Note:** The original intent of the stored procedure exits is to invoke a data cloning method before you perform a workload capture or a data reset method before you perform a workload replay. However, you can invoke any type of stored procedure that meets the stated signature guidelines.

To invoke a stored procedure before you capture or replay a workload, complete the following steps:

1. In a single-server deployment, open the appliance's Workload Replay web console (in multi-server deployments, open the web console of the main Workload Replay appliance) and log in as a privileged user or user.
2. Open the SQL Workloads page (**Open** → **Capture and Replay**).
3. Open the workload capture or replay dialog.
4. Select **New** under Data cloning method in the capture dialog (or Data Reset Method in the replay dialog), as shown in Figure 8-7.

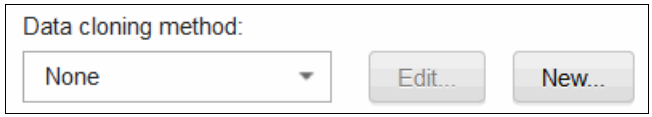


Figure 8-7 Data cloning reset methods invoke stored procedures

> **Note:** If a data cloning method or a data reset method was already defined, you can select it and proceed with step 8 on page 278).

5. Assign a name and specify the fully qualified stored procedure name, as shown in Figure 8-8. On this window, you define a new cloning or reset method that maps to an existing stored procedure.

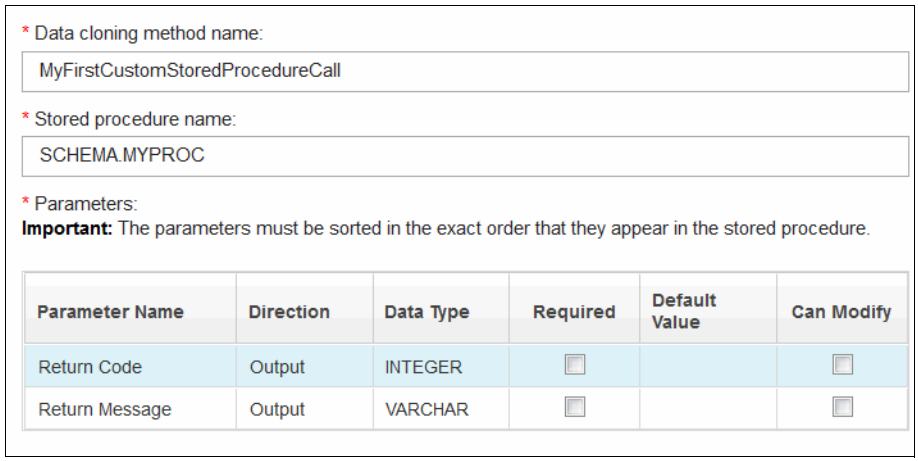


Figure 8-8 Define a cloning or reset method to map to an existing stored procedure

The stored procedure signature must include two output parameters: a return code and a return message. The return code is evaluated after the stored procedure call completes and the workload capture or replay starts if a zero code was returned. The capture or replay action is canceled otherwise.

6. Specify additional input or output parameters to match the signature of your existing stored procedure, as shown in Figure 8-9.

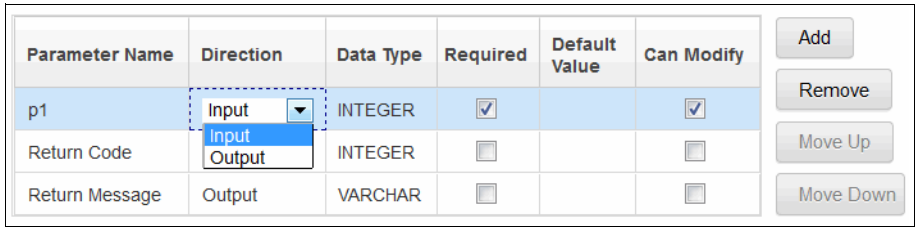


Figure 8-9 Customize the parameter list to match the stored procedure signature

Tip: If an input parameter is tagged as modifiable, the default value can be overridden before you invoke the stored procedure.

7. Save the cloning or reset method.
8. Customize the stored procedure call by specifying the database connection profile of the database (or subsystem) on which the stored procedure will be run and provide all mandatory input parameters, as shown in Figure 8-10.

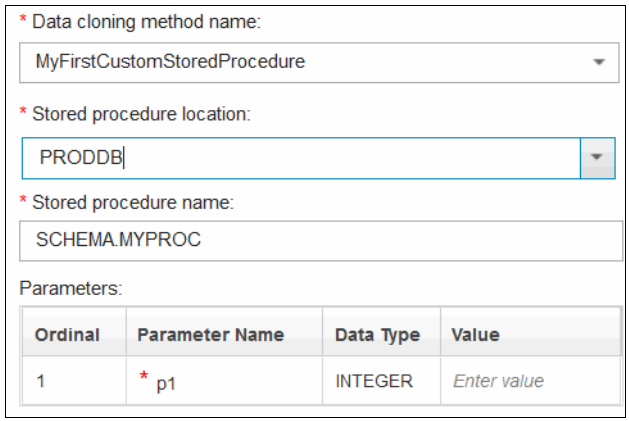


Figure 8-10 Specify the runtime parameters of the stored procedure call

Tip: You can call a stored procedure that resides in any database (or subsystem). You are not limited to the capture or replay systems.

Before you run the workload capture or replay, you are prompted to provide the credentials of a user that is authorized to execute the stored procedure.

Note: If the stored procedure call returns an error message, the message text is displayed and the workload capture or replay is not started.

9

Troubleshooting

This chapter describes common error scenarios that pertain to installation, connectivity, workload capture and replay, and how to address these scenarios. We also explain how to collect diagnostic information for IBM Software Support.

9.1 Troubleshooting SQL capture and replay issues

During workload capture or workload replay, IBM InfoSphere Guardium S-TAP for DB2 collects and streams information about locally or remotely executed SQL statements to the IBM InfoSphere Optim Workload Replay for DB2 appliances. The following sections provide guidance about how to investigate unexpected results. Wherever necessary, we provide platform-specific details.

9.1.1 SQL capture or replay fails to start with an error

InfoSphere Workload Replay appliances use several services to capture SQL. These services must be running when you start a workload capture or replay, or the operation will fail.

The following error messages relate to this issue:

- **"`Controller for auxiliary server is not running`"** (`CDOCR0300E`)

  To address this error, start the controller for auxiliary server, as described in 7.7, "Deciding when to start and stop services" on page 267.

- **"`Capture manager is not running`"** (`CDOCR0010E`)

  To address this error, start the capture manager as described in 7.7, "Deciding when to start and stop services" on page 267.

DB2 for z/OS

When a DB2 for z/OS database is chosen, Workload Replay invokes a stored procedure (shipped by DB2 for z/OS) that is used to discover the information that is needed to run the capture or replay. This information includes the logical partition (LPAR) where DB2 is running, whether the location name that is provided is a location alias or a data sharing group, and if applicable, the active members of a data sharing group. Errors that are encountered during discovery processing are recorded in the Global Log. Location aliases, where you can limit the capture or replay to a certain subset of members in a data sharing group, are supported during capture and replay.

In z/OS environments, an additional controller, which coordinates between S-TAP and the Workload Replay appliance, is running on each LPAR:

- **"`Controller for auxiliary server is not running`"** (`CDOCR0300E`)

  To address this error, check the controller connectivity on the specified LPAR (7.2.2, "Monitoring the connection status of Workload Replay services" on page 236).

- **“**`The Capture Replay Controller cannot be found`**”** (`CDOCR0161E`)

  To address this error, verify that the Capture Replay Controller for z/OS (CQZSERV) procedure is active on the DB2 for z/OS subsystem.

- **“**`No suitable dispatcher was found`**”** (`CDOCR0040E`)

  To address this error, ensure that the Capture Replay Controller for z/OS (CQZSERV) has RACF permission to connect to the local DB2 for z/OS subsystem.

9.1.2 No SQL is collected during SQL capture or replay

If after a workload capture or replay completes, an empty capture is reported, review the following troubleshooting tips:

- Verify that you are running the workload on the database (or subsystem) that you are capturing.
- Verify that the required services are running on each appliance and that the associated auxiliary appliances are connected to the main Workload Replay appliance (7.2, “Appliance health monitoring” on page 230).
- Verify that the Workload Replay appliances were configured correctly:
  - The DB2-to-DB2 policy is installed (3.4.2, “Installing the DB2-to-DB2 policy” on page 60).
  - The Workload Replay license is applied, and Replay is one of the licensed applications (3.4.1, “Installing the InfoSphere Workload Replay license” on page 56).
  - The listed unit type includes Sink (3.5.1, “Verifying the installation” on page 70).
- Ensure that the ports that are listed in A.3, “Open port requirements” on page 318 are not blocked by a firewall.
- Check the workload capture log file in the Workload Replay web console for any unexpected runtime exceptions.

If you determine that the behavior is likely not caused by an issue with the appliances, review the platform-specific database server analysis steps.

DB2 for z/OS

If no SQL is captured, verify the following items:

- The filter condition that you specified during workload capture or replay does not exclude any relevant SQL (“Filter out unwanted DB2 for z/OS SQL traffic” on page 160).
- S-TAP is customized to monitor the DB2 subsystem traffic. Therefore, SQL activity is collected for the database on which the workload is run (4.3.1, “Customize InfoSphere Workload Replay S-TAP for DB2 for z/OS” on page 86).

DB2 for Linux, UNIX, and Windows

If no SQL is captured, verify the following items:

- S-TAP is configured to monitor the DB2 instance traffic. Therefore, SQL activity is collected for the database on which the workload is run (5.3.1, “Configuring S-TAP to monitor DB2 instance traffic” on page 126).
- The S-TAP process runs on the database server and it can connect to the main Workload Replay appliance and auxiliary appliances in multi-server deployments (“Verifying that S-TAP is running and connected” on page 118).
- If you are trying to capture local traffic on the Linux platform, ensure that you activated ATAP (5.3.2, “Configuring S-TAP to monitor local DB2 instance traffic on Linux” on page 131).
- If you are trying to capture traffic on the AIX platform, ensure that you restarted DB2 after you configured the STAP (5.2.1, “Installing S-TAP using stand-alone installers” on page 115).

9.1.3 Not all expected SQL is collected during SQL capture or replay

If you reviewed a captured or replayed workload and determined that some (but not all) SQL is missing, use the following tips for this issue.

Multi-server deployments

Verify that the required services are running on each appliance and that the associated auxiliary appliances are connected to the main Workload Replay appliance (7.2.2, “Monitoring the connection status of Workload Replay services” on page 236).

DB2 for z/OS

If not all SQL is captured, verify the following items:

- The filter condition that you specified during workload capture or replay does not exclude any relevant SQL.

  > **Note:** Review the replay capture filter. If you are reusing the original capture filter, ensure that the filter conditions are applicable in your replay environment. For example, you might capture SQL that pertains to user ID `wolli` but mapped that user ID during workload transformation to `wilvi`. If you reuse the original filter condition, and that condition includes traffic that is associated with user `wolli` only, no replayed SQL that is associated with user ID `wilvi` will be captured.

- In data sharing environments, you captured (or replayed) on all members that process the SQL workload.

9.1.4 Replay is slow to progress or appears to be stuck

If the progress bar in the replay status window does not seem to progress, check the following areas:

- Monitor DB2 activity.

  Are there any long running queries that are fetching lots of data? Keep in mind that DB2 settings, such as the Workload Manager (WLM) policy, affect SQL processing in a way that differs from the original environment where the SQL was executed.

- Check for messages in the DB2 server logs.
- DB2 for z/OS: Check whether workloads are local or distributed.

  SQL statements that run locally when they are originally captured are replayed by using the job-completion checker type-2 (JCC T2) z/OS driver regardless of how they were issued during Capture.

9.2 Resolving Workload Replay connectivity issues

Before you contact IBM Software Support to report Workload Replay appliance connectivity issues, review the solutions that are provided next.

9.2.1 Resolving Workload Replay web console connectivity issues

The Workload Replay web console provides privileged users and users access to Workload Replay tasks. If you are unable to connect or log in, review the following troubleshooting tips.

Unable to connect to the Workload Replay web console

If your web browser is unable to connect to the Workload Replay web console (Figure 9-1), verify the following information:

- Verify that you specified a valid main Workload Replay web console URL:

  `https://guardium_hostname_or_ip:8443/dsweb/console/ocr/index.jsp`

- Verify that you can ping *guardium_hostname_or_ip*.
- Verify that access to port 8443 is not blocked. For a list of ports that are used by the InfoSphere Workload Replay appliance, see A.3, “Open port requirements” on page 318.

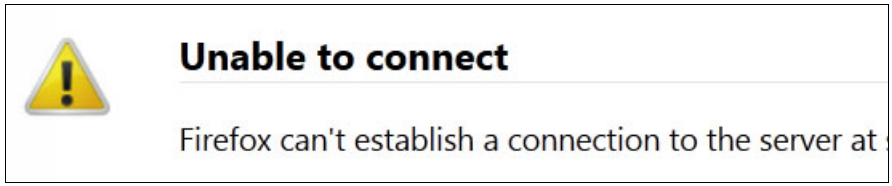


Figure 9-1 Cannot connect to Workload Replay web console

Unable to open the Workload Replay web console

If you are unable to open the Workload Replay web console in your web browser (`https://guardium_hostname_or_ip:8443/dsweb/console/ocr/index.jsp`), verify the following information:

- Verify that you specified the `HTTPS` protocol in the URL and not HTTP (Figure 9-2).

Figure 9-2 Invalid HTTP protocol

- Verify that you specified the URL of a main Workload Replay web server. The Workload Replay web console does not run on InfoSphere Workload Replay auxiliary servers. Figure 9-3 shows the error message.

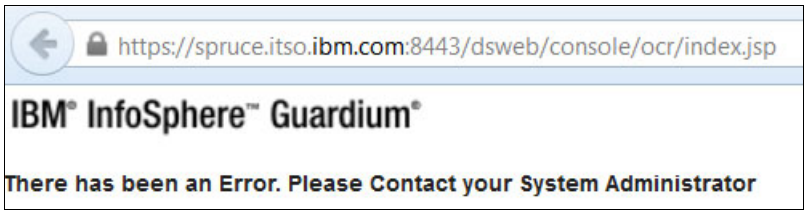


Figure 9-3 Invalid URL specified

Unable to log in to the Workload Replay web console

If you are unable to log in to the Workload Replay web console (Figure 9-4), verify the following information:

- Verify the ID and password that you entered.
- Ask your security administrator to verify that your Workload Replay web console account has the workload-replay-admin or workload-replay-user role. For information about how to check an account's roles, see 7.1, "Access management" on page 214.

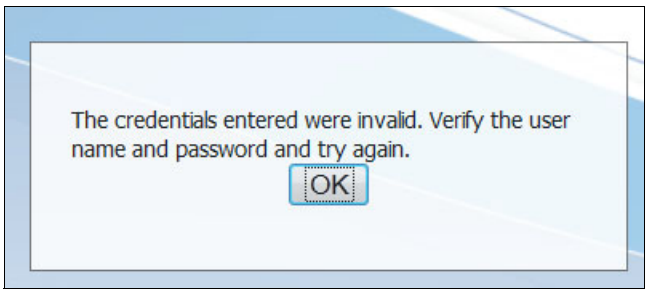


Figure 9-4 Cannot log in to the web console

9.2.2 Resolving Guardium web console connectivity issues

The Guardium web console `https://guardium_hostname_or_ip:8443/sqlguard` provides security administrators, administrators, and privileged users access to Workload Replay appliance tasks. If you are unable to connect or log in to the web console, review the following troubleshooting tips.

Unable to connect to the Guardium web console

If your web browser is unable to connect to the Guardium web console, verify the following information:

- You specified a valid Guardium web console URL:
- `https://guardium_hostname_or_ip:8443/sqlguard`
- You can ping *guardium_hostname_or_ip* from the machine where your web browser is running.
- The required port 8443 is not blocked by a firewall. For a list of ports that are used by the InfoSphere Workload Replay appliance, see A.3, “Open port requirements” on page 318.

Unable to log in to the Guardium web console

If you are unable to log in to the Guardium web console, ask your security administrator to verify that your Workload Replay web console account has a role that implies access authority to the Guardium web console. For information about how to check the roles of an account, see 7.1, “Access management” on page 214.

If your account is locked, contact your security administrator.

Unable to connect to the Guardium file server

The Guardium file server provides authorized users with the ability to upload and download files. If you are unable to open the file server web page, verify the following information:

- The file server was started on the appliance.
- You are connecting to the file server from the IP address that was specified when the file server was started.

Note: If you connect to the Workload Replay appliance through a proxy server, specify the host name or IP address of the proxy server.

9.2.3 Resolving CLI connectivity issues

The command-line interface (CLI) provides secure administrative access to Workload Replay appliances. For information about how to connect, see “Accessing the CLI” on page 215.

Unable to connect to the CLI

If you are unable to connect to the Guardium CLI by using a Secure Shell (SSH) client, verify the following information:

- Verify that you can ping the appliance.
- Verify that access to port 22 is not blocked. For a list of ports that are used by the Workload Replay appliance, see A.3, “Open port requirements” on page 318.

Unable to log in to the CLI

If you are unable to log in to the Guardium CLI by using an SSH client, verify that you are using the correct login process, as described in “Accessing the CLI” on page 215.

Unable to run a command at the CLI

If you logged in by using the correct login process, as described in “Accessing the CLI” on page 215, contact your security administrator. Your account might not have the privilege to use the CLI. See 7.1, “Access management” on page 214 for details.

9.3 Resolving S-TAP issues for a DB2 for Linux, UNIX, and Windows environment

S-TAP plays a vital role in a Workload Replay deployment. S-TAP issues typically have a fundamental impact on your ability to capture or replay workloads but they do not affect workload processing activities, such as transformation or reporting.

9.3.1 Connectivity issues

The current S-TAP status can be determined in the Guardium web console by clicking **Administration Console** → **Local Taps** → **S-TAP Control**, as shown in Figure 9-5 on page 290.

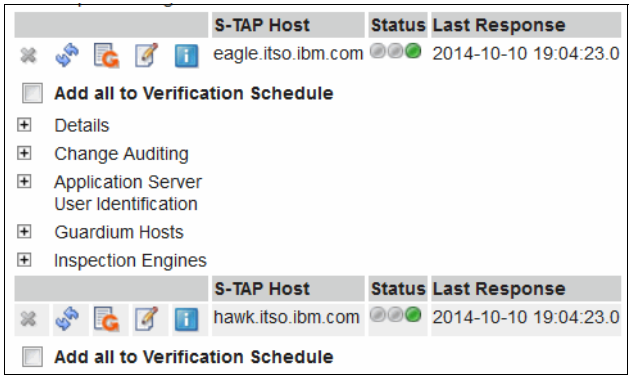


Figure 9-5 S-TAP status can be monitored in the Guardium web console

The status is displayed by using the traffic light pattern (green, yellow, or red):

- Green: STAP is running and connected to the appliance.
- Yellow (not synchronized): Configuration changes were sent to the S-TAP, but the S-TAP did not acknowledge that the changes were applied. If the light remains yellow for an extended period, you can assume that the S-TAP did not accept the new configuration. When that situation happens, S-TAP attempts to restart by using the last good configuration. In this case, you must fix the error and restart the S-TAP.
- Red (offline): S-TAP previously connected to the appliance but it is not currently connected. Verify the following information:
  - Verify that the S-TAP process is running on the database server:
    - i. Log in as `root` on the database server.
    - ii. Verify that the guard_stap process is running by using the following command:

      ```
      ps -ef | grep stap
      ```
  - Verify that no firewall is blocking the communication between S-TAP and the appliance. The open port requirements are listed in A.3, “Open port requirements” on page 318.
  - Verify that the Sniffer is running.

    The Sniffer, which is also referred to as the *inspection core*, is a core component on the appliance that monitors and parses database traffic as it is received from the network interface. If the Sniffer is not running, S-TAP can be reported as disconnected.

To restart the Sniffer, complete these steps:

i. Log in to the CLI of the correct Workload Replay appliance as an administrator or a privileged user.

ii. Issue the **`restart inspection-core`** command.

If the S-TAP status is displayed as offline, review the event log. This log can be accessed by clicking the information icon, as shown in Figure 9-6.

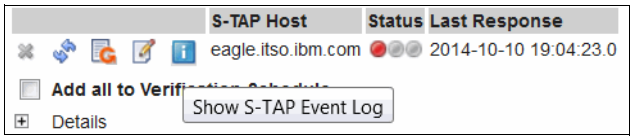


Figure 9-6 Review the event log if a problematic status is displayed

In Figure 9-7, the event log indicates that S-TAP did not start because a host name was not resolved.

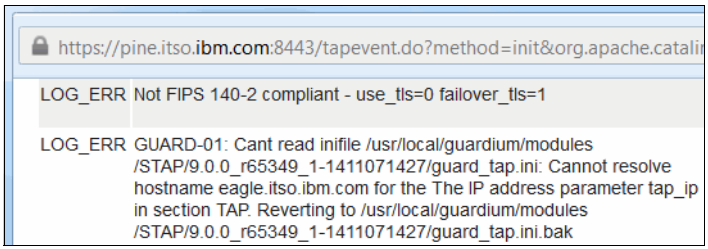


Figure 9-7 The event log contains useful troubleshooting information

Note: Not every LOG_ERR event entry indicates a problem.

If an S-TAP is not listed for a database server host, it never connected to the appliance. Verify the following information:

- The S-TAP software was installed on the database server machine. It is associated with the appliance that you are connected to (5.2, “Installing S-TAP” on page 114). An S-TAP entry is only displayed if S-TAP connected at least one time to the associated Workload Replay appliance.
- The S-TAP process is running:

  a. Log in as `root` on the database server.

  b. Verify that the `guard_stap` process is running by using the following command:

  ```
  ps -ef | grep stap
  ```

- The K-TAP process is running:
  a. Log in as `root` on the database server.
  b. Verify that K-TAP is active by running the following platform-specific commands:
     - AIX: **`genkex | grep tap`**
     - Solaris: **`modinfo | grep tap`**
     - Linux: **`lsmod | grep tap`**
     - HP_UX: **`lsdev | grep tap`**
- Verify that no critical errors are logged in the S-TAP log file:
  a. Log in as `root` on the database server.
  b. Review the `/tmp/guard_stap.stderr.txt` log file.

9.3.2 S-TAP buffer overflow errors

The workload capture or workload replay log file might contain an error message that advises you to check for S-TAP buffer overflows. An S-TAP overflow can occur if S-TAP is unable to send monitored database traffic fast enough to a Workload Replay appliance. This issue results in a loss of data if the internal buffers are exhausted.

To determine whether a buffer overflow occurred, use the following steps:

1. Log in as `root` on the database server.
2. Search for the string "`NO enough space`" in S-TAP log file `/tmp/guard_stap.stderr.txt`.

Buffer overflows might occur under the following conditions:

- High SQL throughput
- Database server CPU constraints

  For information about how to investigate database server CPU constraints, see 7.3.2, "Monitoring S-TAP health and performance on DB2 for Linux, UNIX, and Windows database servers" on page 243.
- Workload Replay appliance overload

  For information about how to investigate Workload Replay appliance overload, see "Monitoring system CPU utilization" on page 237.
- Inadequate network bandwidth

9.4 Collecting diagnostic information for IBM support

To facilitate the problem analysis process, IBM Software Support might request collection of additional diagnostic information. The following sections outline how to collect the requested information.

9.4.1 Collecting must_gather diagnostic information

Follow these instructions to package and download the requested information to your local machine:

1. Log in to the CLI as an administrator or privileged user by using an SSH client.

   Note: For details about how to log in, see “Accessing the CLI” on page 215.

2. Enter the **`support must_gather ocr_issues`** CLI command to collect diagnostic information, as shown in Figure 9-8.

```
pine.itso.ibm.com> support must_gather ocr_issues


This operation may take several minutes to complete.

Created file
/var/log/guard/must_gather/oqcr_logs/ocr.201409082001.tgz.enc.
ok
```

Figure 9-8 Running the support must_gather CLI command

3. Log out of the CLI.
4. Log in to the Guardium web console as an administrative user or a privileged user.
5. Navigate to **Administration Console** → **Configuration** → **Support Information Results** (Figure 9-9 on page 294).

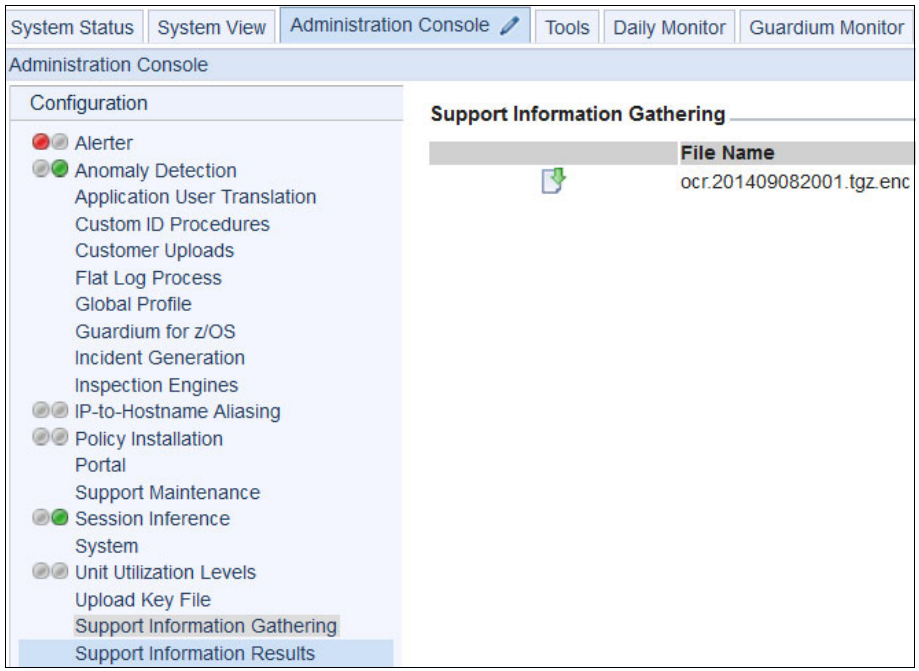


Figure 9-9 Download the must_gather output by using the Guardium web console

6. Download the encrypted diagnostic archive.
7. Log out of the Guardium web console.

> **Note:** Guardium retains a rolling set of diagnostic archives only and deletes the oldest archive, as needed.

8. Provide the available archive to your assigned IBM support specialist.

> **Note:** Occasionally, IBM requests that you collect diagnostic information that relates to other areas, such as `patch_install_issues` and `sniffer_issues`. Follow a similar procedure to the process that you used to provide `ocr_issues`.

9.4.2 Collecting problem-specific trace files

To investigate deviations from expected behavior, IBM Software Support might request additional trace information that is not collected during normal operation.

Use the following steps to collect trace data:

1. Collect the trace information:
   a. Log in to the web console on the main Workload Replay server.
   b. Navigate to **Open** → **Capture and Replay** → **More** → **Advanced Options**, as shown in Figure 9-10.

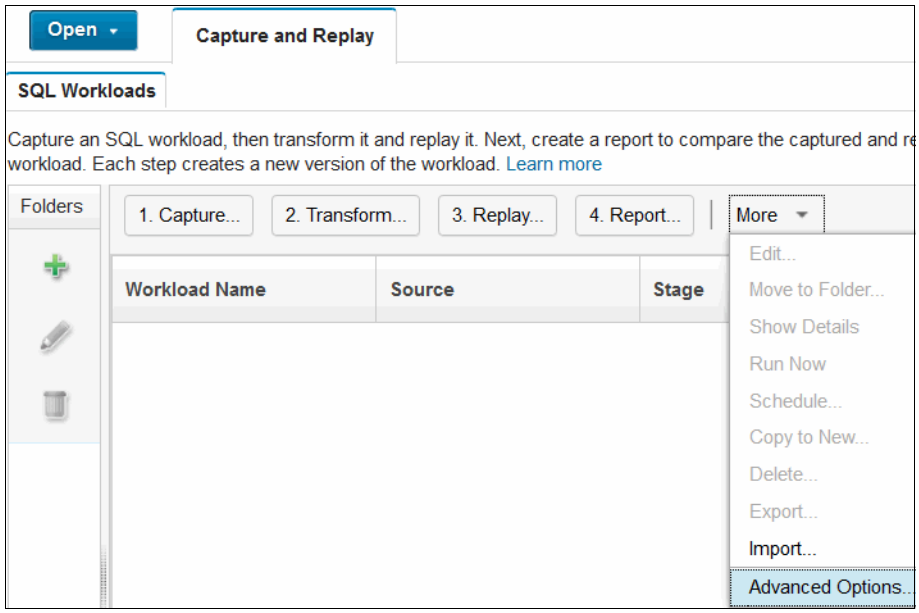


Figure 9-10 Open the advanced options to enable or disable Workload Replay trace

   c. On the Trace tab, click **Start Trace**, as shown in Figure 9-11 on page 296.

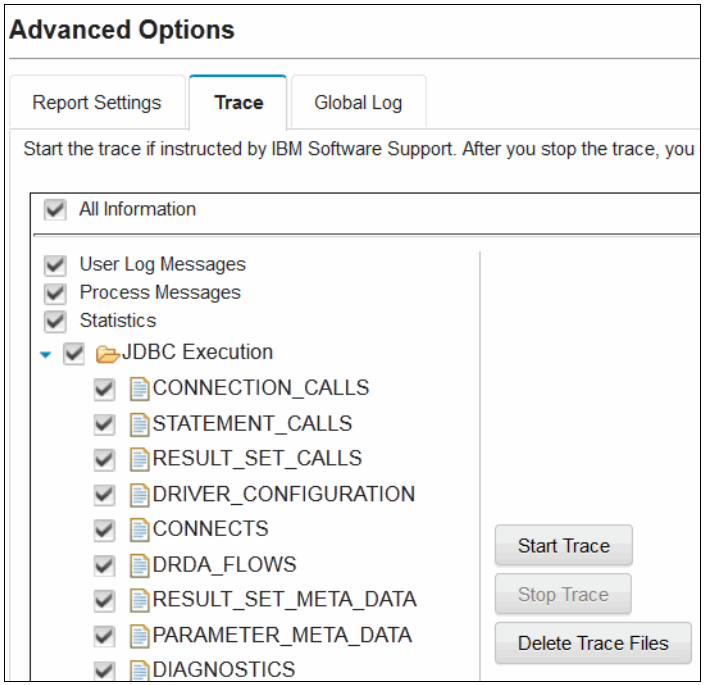


Figure 9-11 Enable trace to collect Workload Replay diagnostic information

Note: Document the trace ID.

d. Follow the instructions that IBM Software Support provided to re-create the issue.

e. In the Workload Replay web console, navigate to **Open** → **Capture and Replay** → **More** → **Advanced Options**.

f. On the Trace tab, click **Stop Trace**.

2. Follow the instructions in 9.4.5, “Downloading diagnostic information from an appliance” on page 298 to download the encrypted trace file from the `secureTraces` directory, as shown in Figure 9-12.

Date	Permissions	Path
Sep 17 17:16:31 2014	rwxrwxr-x	/var/log/guard
Sep 17 17:14:42 2014	rwxr-xr-x	secureTraces
Sep 17 17:14:42 2014	rw-r--r--	secureTraces/td1410988427229traceData.zip.enc

Figure 9-12 Download the Workload Replay trace from the secureTraces directory

3. Remove the trace archive from the appliance:
   a. In the Workload Replay web console, navigate to **Open** → **Capture and Replay** → **More** → **Advanced Options**.
   b. On the Trace tab, click **Delete Trace Files**.
4. Provide the archive to your assigned IBM Software support specialist.

9.4.3 Collecting SLON traces by using the diag utility

The SLON traces are sometimes necessary to ensure that data is processed by the Workload Replay appliance. The SLON traces are not included as part of the `support must_gather sniffer_issues` command.

Follow these steps to collect the SLON trace information:

1. Log in to the CLI as an administrator or privileged user by using an SSH client.

   Note: For details about how to log in, see “Accessing the CLI” on page 215.

2. Run the `diag` command.
3. Click **3 System Interactive Queries** → **12 SLON Utility** → **m to Dump Tap Message Data**.
4. Enter the time in seconds to collect trace information, for example, `120`.
5. Start the SLON trace.
6. Run a workload capture or replay for the specified time.
7. After the trace collection finishes, return to the Main menu.
8. Select **1 Output management** in the Main menu.
9. Select **1 End and pack current session** in the Output redirection menu.
10. Select **3 Export recorded files** in the Output redirection menu.
11. Select the **diag_session_<*todays_date*>.tgz** file.
12. Upload the diagnostic archive to an FTP server or Secure Copy Protocol (SCP) server. If you do not have access to an FTP or SCP server, follow the file server download instructions in 9.4.5, “Downloading diagnostic information from an appliance” on page 298 to download the file, as shown in Figure 9-13 on page 298.

Size	Date	Permissions	Path
4096	Wed Sep 17 16:58:17 2014	rwxrwxr-x	/var/log/guard
4096	Wed Sep 17 16:57:25 2014	rwxrwxr-x	diag/depot
4388	Wed Sep 17 16:53:44 2014	rw-r--r--	diag/depot/diag_session_17_9_1653.tgz

Figure 9-13 Download the SLON trace from the diag/depot directory

9.4.4 Collecting z/OS specific trace files

Follow these steps to collect the z/OS trace files:

1. If you are running local workloads on the z/OS server, and you started traces from the user interface (UI), you will see z/OS local replay dispatcher traces in the location that is specified in the `OcrServerTraceDir` property in the configuration file (default name is `IOQCRSERVER.properties`). The default location is under `/var/ioqcr/traces/gmxx_`*`xx_xx_xx`* where `gmxx_`*`xx_xx_xx`* represents the IP address of the Guardium machine.

   Important: These z/OS local replay dispatcher traces are not part of the compressed encrypted file that you can download through the file server.

2. Follow these steps if you are asked to collect traces for Workload Replay Controller for z/OS (CQZSERV):

   a. Turn on trace by setting `OcrServerTraceLevel=-1` in the configuration file `IOQCRSERVER.properties`.

   b. Stop and Start the Workload Replay Controller for z/OS (CQZSERV).

   c. Re-create the problem.

   d. You can then forward the traces from the location that is specified in the `OcrServerTraceDir` property (default location is `/var/ioqcr/traces/ocrtrc`) to IBM support.

9.4.5 Downloading diagnostic information from an appliance

To download one or more trace files from an appliance, follow these steps:

1. Log in to the CLI as an administrator or privileged user by using an SSH client.

   Note: For details about how to log in, see “Accessing the CLI” on page 215.

2. Enter the **`fileserver`** command and specify the IP address of your local machine, as shown in Figure 9-14.

```
pine.itso.ibm.com> fileserver 9.55.156.227
Creating the index file.

Starting the file server. You can find it at
http://pine.itso.ibm.com
The timeout has been set to 3600 seconds and it may timeout
during the uploading.

The upload will only be accessible from the IP you are
logged in from: 9.55.156.227

Press ENTER to stop the file server.
```

Figure 9-14 Start the file server to download diagnostic information from an appliance

> **Note:** If you are connecting to the appliance by using a proxy, specify the proxy server's IP address instead of your local IP address.

3. Open a web browser to the specified URL, as shown in Figure 9-15.

Figure 9-15 Go to the sqlguard_logs directory

> **Note:** Use HTTP, not HTTPS as the protocol. The file server connection is not secured.

4. Navigate to the **sqlguard_logs** directory and download the correct diagnostic files.
5. Close the web browser.
6. Stop the file server in the CLI by pressing Enter.
7. Close the CLI session.

A

Worksheets and references

Throughout the previous chapters, we referred to various worksheets and references that simplify product planning and deployment. In this appendix, we cover the following topics:

- Electronic installation media access

  Outlines how to access the installation media for IBM InfoSphere Optim Workload Replay for DB2 for z/OS and InfoSphere Optim Workload Replay for Linux, UNIX, and Windows

- Worksheets

  Provides a collection of deployment worksheets, including several platform-specific worksheets

- Open port requirements

  Lists the ports that are used during the workload capture and replay operation

- Workload Replay artifacts that reside in capture or replay databases or subsystems

  Documents the artifacts that are created in each capture or replay database (or subsystem)

A.1 Electronic installation media access

InfoSphere Optim Workload Replay for Linux, UNIX, and Windows and InfoSphere Optim Workload Replay for DB2 for z/OS installation media can be downloaded from a password-protected IBM website. For details, see the following sections:

- A.1.1, “Downloading InfoSphere Workload Replay for DB2 for z/OS installation media”
- A.1.2, “Downloading InfoSphere Workload Replay for DB2 for Linux, UNIX, and Windows installation media” on page 309

A.1.1 Downloading InfoSphere Workload Replay for DB2 for z/OS installation media

InfoSphere Workload Replay for DB2 for z/OS installation media is available as a download on ShopZ or physical media.

Downloading the base installation media from ShopZ

To download the base installation media from ShopZ, use the following steps:

1. Open the ShopZ website at the following web address and log in:

   `https://www.software.ibm.com/webapp/ShopzSeries/ShopzSeries.js`

2. Locate your InfoSphere Workload Replay for DB2 for z/OS v 2.1 order:

   a. Navigate to **My orders** → **In process**, as shown in Figure A-1 on page 303.

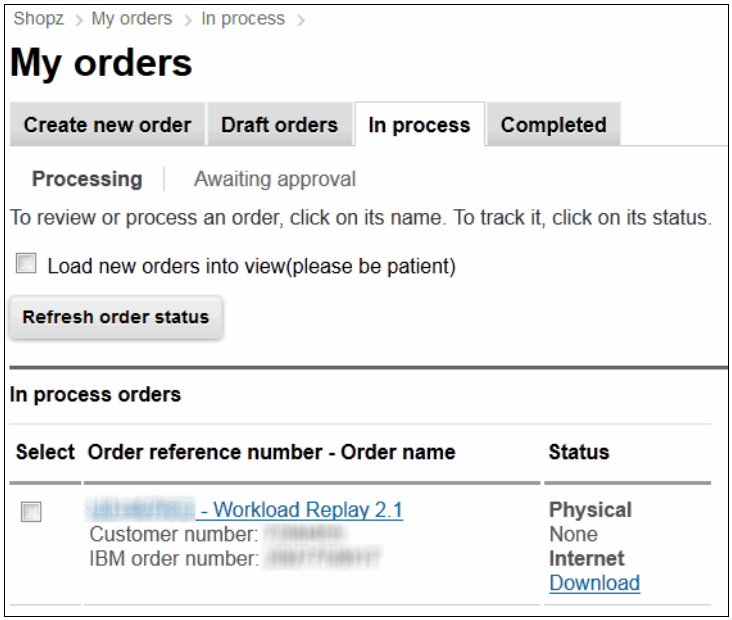


Figure A-1 Locate your Workload Replay for DB2 for z/OS order in ShopZ

b. Click the **Download** link. Figure A-2 on page 304 depicts the installation media download options for the z/OS media files and non z/OS media files that are used to build appliances.

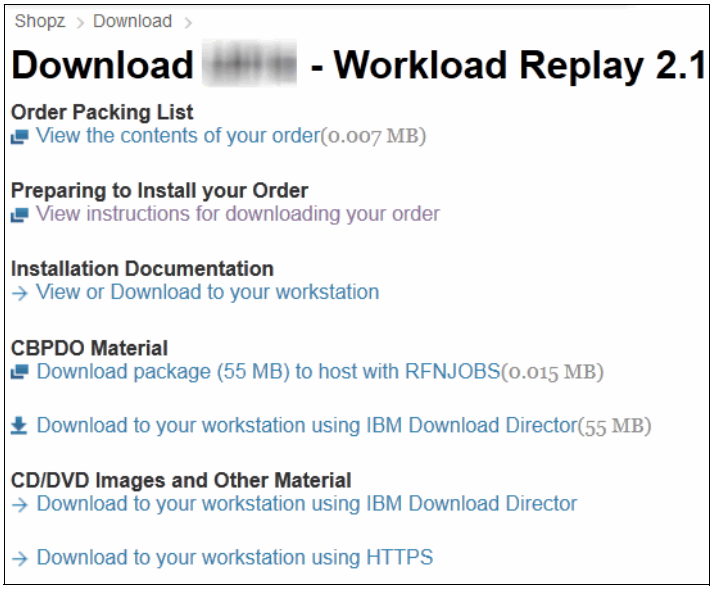


Figure A-2 Review the media download options

3. Download the z/OS installation media (**CBPDO Material**) to your host system:

   a. If your host system can access the Internet, download the supplied **RFNJOBS JCL**, transfer it to your host, customize it, and run it to download the SMP/E for z/OS files.

   b. If your host system cannot access the Internet, download the SMPE files to your workstation and transfer them manually to your host system.

   These media files are used during the installation and configuration of the z/OS database server components. The installation and configuration are described in Chapter 4, “IBM InfoSphere Optim Workload Replay for DB2 for z/OS installation and configuration” on page 77.

4. Download the installation documentation and Workload Replay appliance installation media (CD/DVD Images and Other Material) by using IBM Download Director (preferred) or your web browser:

   a. Click the correct link for your download option of choice.

      The appliance installation media is delivered as a set of ISO 9660 CD-ROM image files. Download and review the media preparation instructions, as shown in Figure A-3 on page 305.

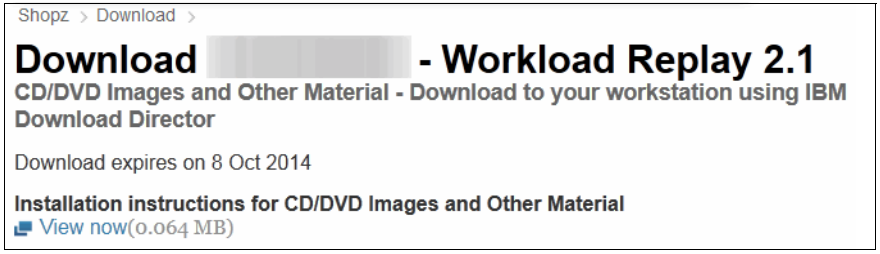


Figure A-3 Review the media preparation instructions

b. Download all appliance installation media files to your local machine by using Download Director or your browser, as shown in Figure A-4.

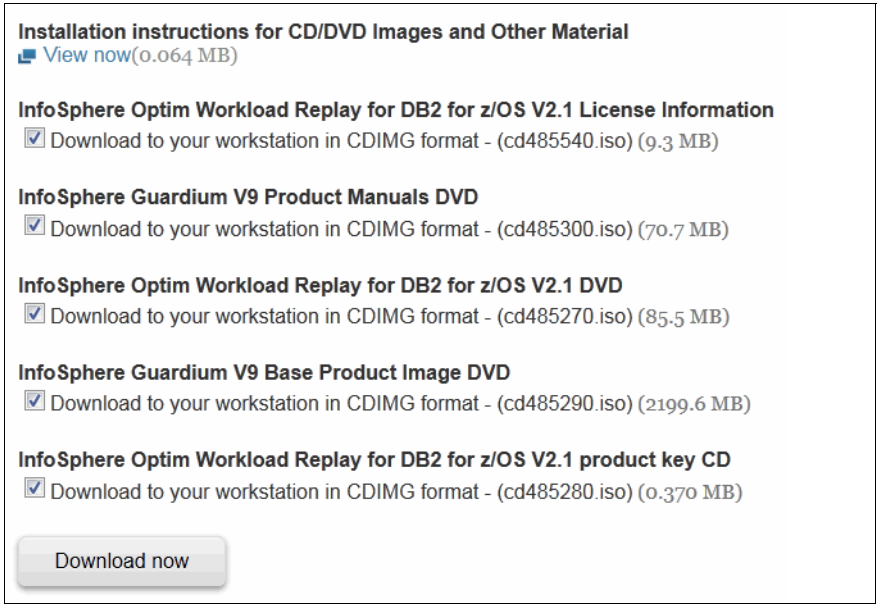


Figure A-4 Download the appliance installation media files

c. Follow the media file preparation instructions.

> **Note:** If you plan to deploy physical InfoSphere Workload Replay appliances, burn a DVD by using the `cd4852980.iso` file. This DVD contains the Guardium installation files from which the appliance must be started during the initial setup.

Table A-1 on page 306 lists the content and purpose of the media files.

Table A-1 Review the content of the media file

V2.1 media file name on ShopZ	Content	Purpose
cd485270.iso	Appliance patch files	This file contains InfoSphere Workload Replay V2.1 installation and uninstallation patches. For details about how to install a patch on an appliance, see 3.4.3, “Installing the prerequisite patches” on page 63. This patch is unnecessary if you are planning to install newer patches, such as a V2.1.0.1 patch.
cd485280.iso	License key text file	This file contains the InfoSphere Workload Replay license key. For information about how to apply the license key on an appliance, see “Installing a license by using the CLI” on page 58.
cd485290.iso	Bootable Red Hat Linux OS-based InfoSphere Guardium installation media	This file contains the InfoSphere Guardium installation image. For details about how to build an appliance by using this image, see 3.3, “Installing and configuring the InfoSphere Guardium software” on page 44.
cd485300.iso	PDF files	This file contains the InfoSphere Guardium product manuals.

V2.1 media file name on ShopZ	Content	Purpose
cd485540.iso	PDF files	This file contains license agreement information. *This file does not contain the license key.* Review the license information before you install the product.

Note: Media file names are subject to change in each major release.

These media files are used during the installation and configuration of the InfoSphere Workload Replay appliances. The installation and configuration are described in Chapter 3, “Installing and configuring IBM InfoSphere Optim Workload Replay appliances” on page 41.

Identifying prerequisite patches

Each version of InfoSphere Workload Replay for DB2 for z/OS requires that you install prerequisite patches on the appliances before the InfoSphere Workload Replay software can be installed. For major releases, such as Version 2.1, these patches are included in the installation media that you download from IBM ShopZ. For minor releases, such as V2.1.0.1, new prerequisite patches must be downloaded from IBM Fix Central. Obtain a complete prerequisite patch list for Version 2.1.0.1 with download information at the following web address:

http://www.ibm.com/support/docview.wss?uid=swg27039922

Note: The InfoSphere Workload Replay for DB2 for z/OS information roadmap[a] contains a link to the document for the current product release under **Installing** → **Required Maintenance Levels for InfoSphere Optim Workload Replay for DB2 for z/OS**.

a. http://www.ibm.com/developerworks/data/roadmaps/roadmap_caprep_21_zos.html

Downloading InfoSphere Guardium patches

InfoSphere Workload Replay for DB2 for z/OS patches require a minimum Guardium Patch Update (GPU) level, which at the time of writing this book is GPU 200. You can obtain an up-to-date list of prerequisite patches in the IBM InfoSphere Workload Replay Knowledge Center.

Complete the following steps to download the InfoSphere Guardium patches:

1. Open the IBM Fix Central web page at the following web address:

   http://www.ibm.com/support/fixcentral

   Note: A no-charge IBM ID is required to download software from IBM Fix Central.

2. On the Select product tab, choose the value for the following fields:
   - Product Group: **Information Management**
   - Product: **InfoSphere Guardium**
   - Version: **9.0** at the time of writing this book
   - Platform: **Linux**
3. Browse to the maintenance media, for example, Guardium Patch Update 200 if you are installing InfoSphere Workload Replay Version 2.1.0.1. Choose a download option (Download Director or FTP) or your browser.
4. Download the InfoSphere Guardium patch media to your local desktop or notebook.

For more information about how to install Guardium patches on an appliance, see 3.3, “Installing and configuring the InfoSphere Guardium software” on page 44.

Downloading InfoSphere Workload Replay server patches

A Workload Replay server patch is a special Guardium patch that delivers enhancements or addresses opportunities for growth.

Complete the following steps to download the InfoSphere Workload Replay server patches:

1. Open the IBM Fix Central web page at the following web address:

   http://www.ibm.com/support/fixcentral
2. On the Select product tab, choose the value for the following fields:
   - Product Group: **Information Management**
   - Product: **InfoSphere Optim Workload Replay for DB2 for z/OS**
   - Version: **2.1.0.1** at the time of writing this book
   - Platform: **All**
3. Browse to the maintenance media and choose a download option (Download Director or FTP) or use your browser.

4. Download the current Workload Replay server patch media to your local desktop or notebook.

> **Note:** Unless explicitly stated otherwise in patch readme files, InfoSphere Workload Replay patches are cumulative. Therefore, you can install, for example, the V2.1.0.1 patch without having to install the V2.1 (base) patch. An InfoSphere Workload Replay patch might require a Guardium patch; otherwise, the installation fails.

For information about how to install InfoSphere Workload Replay for DB2 for z/OS patches on an appliance, see 3.4, “Preparing for the InfoSphere Workload Replay software installation” on page 56.

A.1.2 Downloading InfoSphere Workload Replay for DB2 for Linux, UNIX, and Windows installation media

InfoSphere Workload Replay installation media is only available as electronic download. If you install the product for the first time, download the base installation media and the latest maintenance for all product components.

Downloading the base server installation media

The appliance’s base installation media consists of the 64-bit InfoSphere Guardium product image, the InfoSphere Workload Replay software, a license key, and supporting documentation.

To download the base server installation media, use the following steps:

1. Open the IBM Passport Advantage® web page at the following web address:

   `http://www.ibm.com/software/passportadvantage`

2. Locate the eAssembly media by part number. The part number of Version 2.1 is `CRQ74EN`.

   > **Note:** You can also locate the media by searching for “InfoSphere Workload Replay”.

3. Download the media to your local machine.

   Figure A-5 on page 310 shows the InfoSphere Workload Replay installation media files on IBM Passport Advantage. Review the InfoSphere Workload Replay installation media files on IBM Passport Advantage.

IBM InfoSphere Optim Workload Replay 2.1 Multiplatform English eAssembly (CRQ74EN)
Size 7 Images (4,217Mb)
Date posted 13 Dec 2013

Select All (or use check boxes below to select image(s) to download)

IBM InfoSphere Optim Workload Replay 2.1 Quick Start and Installation Guide English (CIS2NEN)
Size 5Mb
Date posted 13 Dec 2013
License agreement Download estimate → eAssembly

IBM InfoSphere Optim Workload Replay 2.1 Multiplatform Multilingual (CIUD9ML)
Size 87Mb
Date posted 13 Dec 2013
License agreement Download estimate → eAssembly

IBM InfoSphere Optim Workload Replay 2.1 Product Key Multiplatform Multilingual (CIX9GML)
Size 0.5Mb
Date posted 7 Mar 2014
License agreement Download estimate → eAssembly

IBM InfoSphere Guardium STAPs Locator ReadMe (CIHE7EN) - View details
Size 0.5Mb
Date posted 15 Feb 2013
License agreement Download estimate → eAssembly

IBM InfoSphere Guardium - Product Image V9.0 - 64 Bit Multiplatform Multilingual (CILW9ML)
Size 4,070Mb
Date posted 2 Aug 2013
License agreement Download estimate → eAssembly

IBM InfoSphere Guardium - Software Applicance Activation Kit V9.0 English (CIC2XML)
Size 2Mb
Date posted 11 Oct 2012
License agreement Download estimate → eAssembly

IBM InfoSphere Guardium V9.0 - Product Manuals Multiplatform Multilingual (CIC2YML)
Size 52Mb
Date posted 11 Oct 2012
License agreement Download estimate → eAssembly

Figure A-5 Passport Advantage InfoSphere Workload Replay installation media

Table A-2 on page 311 lists the media files, their content, and their purpose.

Table A-2 Review the media files content

V 2.1 part number on Passport Advantage	Content	Purpose
CIS2NEN[a]	PDF files	InfoSphere Workload Replay Quick Start and Installation Guides. The content of these guides is covered in more detail in this book.
CIUD9ML[b]	Appliance patch files	This file contains the InfoSphere Workload Replay v2.1 installation and uninstallation patches. For details about how to install a patch on an appliance, see 3.4.3, “Installing the prerequisite patches” on page 63 for details. This patch is unnecessary if you are planning to install newer patches, such as a V2.1.0.1 patch.
CIX9GML[c]	License key text file	This file contains the InfoSphere Workload Replay license key. For information about how to apply the license key on an appliance, see 3.4.1, “Installing the InfoSphere Workload Replay license” on page 56.
CIHE7EN[d]	PDF file	This file contains the S-TAP download information document. The content of this document is covered in “Downloading the current S-TAP installation media” on page 314.
CILW9ML[e]	Bootable Red Hat Linux OS-based Guardium installation media	This file contains the InfoSphere Guardium installation image. For details about how to build an appliance by using this image, see 3.5, “Installing a main Workload Replay appliance” on page 68 and 3.6, “Installing an auxiliary Workload Replay appliance” on page 71.
CIC2XML[f]	PDF files	This file contains InfoSphere Guardium appliance requirements and installation instructions. Review these documents before you deploy an appliance.
CIC2YML[g]	PDF files	This file contains the InfoSphere Guardium product help manual.

a. IS_Optim_WorkloadReplay_2.1_QSG_MP.zip
b. IS_Optim_WorkloadReplay_2.1.zip
c. ISO_WR_2.1_PRODUCTKEY_MP_EN.zip
d. STAPs_Locator_README.pdf
e. IS_GD_PRODUCT_IMAGE_9.0_64bit.zip
f. InfoSphere_Guardium-VM_Activation_Kit_9.0.zip
g. IS_GD_-_PRODUCT_MANUALS_9.0.zip

Note: Part numbers and file names are subject to change in each major release.

4. Extract the compressed files. You will use their content to install the Workload Replay appliances.

Note: The downloaded CILW9ML part (`IS_GD_PRODUCT_IMAGE_9.0_64bit.zip`) contains two ISO files: `InfoSphere_Guardium_Image_V90-64_DVD.iso` and `InfoSphere_Guardium_Image_V90-64_DVD_auto.iso`. We suggest that you use `InfoSphere_Guardium_Image_V90-64_DVD.iso` during product installation because it provides access to advanced installation options that are not available in the other image.

Identifying prerequisite patches

Each version of InfoSphere Workload Replay requires that you install prerequisite patches on appliances. For major releases, such as Version 2.1, these patches are included in the installation media that you download from IBM Passport Advantage. For minor releases, such as V2.1.0.1, new prerequisite patches must be downloaded from IBM Fix Central. A complete prerequisite patch list for Version 2.1.0.1 with download information is at the following web address:

http://www.ibm.com/support/docview.wss?uid=swg24035897

Note: The InfoSphere Workload Replay for Linux, UNIX, and Windows information roadmap[a] contains a link to the document for current product release. Click **Installing** → **Download document**.

a. http://www.ibm.com/developerworks/data/roadmaps/roadmap_caprep_21.html

Downloading InfoSphere Guardium patches

To download the prerequisite Guardium patches, complete the following steps:

1. Open the IBM Fix Central web page at the following web address:

   http://www.ibm.com/support/fixcentral

   > **Note:** A no-charge IBM ID is required to download software from IBM Fix Central.

2. On the Select product tab, select the value for the following fields:
   - Product Group: **Information Management**
   - Product: **InfoSphere Guardium**
   - Version: The current version (**9.0** at the time of writing this book)
   - Platform: **Linux**
3. Browse to the maintenance media, for example, Guardium Patch Update 200 if you are installing InfoSphere Workload Replay Version 2.1.0.1. Choose a download option (Download Director or FTP) or use your browser.
4. Download the InfoSphere Guardium patch media to your local desktop or notebook.

For more information about how to install Guardium patches on an appliance, see 7.6.3, “Installing maintenance on an appliance” on page 262.

Downloading Workload Replay server patches

A Workload Replay server patch is a special Guardium patch that delivers enhancements or addresses opportunities for growth.

Complete the following steps to download Workload Replay server patches:

1. Open the IBM Fix Central web page at the following web address:

   http://www.ibm.com/support/fixcentral

2. On the Select product tab, choose the value for the following fields:
   - Product Group: **Information Management**
   - Product: **InfoSphere Optim Workload Replay for Linux, UNIX, and Windows**
   - Version: The current version (**2.1.0.1** at the time of writing this book)
   - Platform: **All**

3. Browse to the maintenance media and choose a download option (Download Director or FTP) or use your browser.
4. Download the Workload Replay server media to your local desktop or notebook.

For more information about how to install InfoSphere Workload Replay patches on an appliance, see 7.6.3, “Installing maintenance on an appliance” on page 262.

Downloading the current S-TAP installation media

InfoSphere Guardium and InfoSphere Workload Replay share the S-TAP installation media. To download the installation files for your database servers, use the following steps:

1. Open the IBM Fix Central web page at the following web address:

   http://www.ibm.com/support/fixcentral

2. On the Select product tab, choose the value for the following fields:
   - Product Group: **Information Management**
   - Product: **InfoSphere Guardium**
   - Version: The current compatible version (**9.0** at the time of writing this book)
   - Platform: The operating system of your database server
3. Locate the current fix pack. Select the command-line installation media for small deployments or the Guardium Installation Manager media for large-scale deployments.
4. Browse to the installation media and choose a download option (Download Director or FTP) or use your browser.
5. Download the S-TAP installation media to your local desktop or notebook.

For more information about how to install S-TAP on a database server, see 5.2, “Installing S-TAP” on page 114.

A.2 Worksheets

Throughout the deployment process, you must collect environment information. Use the following worksheets to document the details.

A.2.1 Appliance configuration worksheet

Collect the following configuration information for each main and auxiliary appliance that you plan to deploy.

InfoSphere Guardium configuration

Collect the following information for the InfoSphere Guardium configuration:

- Primary system IP address: The primary static IP address of the ETH0 connection of the appliance on which you are installing InfoSphere Guardium.

  Note: Throughout the documentation, *guardium_hostname_or_ip* refers to this IP address or the fully qualified host name of the appliance.

- Subnet mask: The map that identifies the subnet to which the IP address belongs.
- Default router IP address: The IP address of the gateway or router that the InfoSphere Guardium computer uses to communicate with other networks.
- DNS server IP addresses: The IP address of at least one Domain Name System (DNS) server to be used by the appliance to resolve host names and IP addresses.
- Host name for the appliance: This name needs to match the host name that is registered for the appliance in the DNS server.
- Domain name for the appliance: The domain in which the host resides.
- Network Time Protocol (NTP) server host names.

  Note: In a multi-server deployment, ensure that all your InfoSphere Workload Replay servers are configured to use the same NTP servers.

- Time zone: The time zone in which the physical or virtual appliance resides.

  Note: In a multi-server deployment, ensure that all your InfoSphere Workload Replay servers are configured to use the same time zone settings.

InfoSphere Workload Replay configuration

Collect the appliance types. An appliance can be designated as a main Workload Replay server or an auxiliary Workload Replay server.

A.2.2 S-TAP for Linux, UNIX, and Windows configuration worksheet

S-TAP must to be configured to monitor a DB2 instance before workloads that are running on the instance's databases can be captured or replayed. Collect the following configuration information:

- DB2 instance home directory: On the Linux and UNIX operating systems, this directory is the instance owner's home directory. On the Windows operating systems, the home directory is the location where the DB2 database product was installed, for example:

  ```
  $ echo $DB2INSTANCE
  tinst1
  $ whoami
  tinst1
  $ echo $INSTHOME
  /home/tinst1
  ```

  In this example, the DB2 instance home directory needs to be set to `/home/tinst1`.

- TCP/IP port number: S-TAP monitors this port for SQL activity. To determine the port number, query the instance's TCP/IP service name (`SVCENAME`) configuration value. If the value represents a service name instead of a port number, look up the service name mapping, for example:

  ```
  $ echo $DB2INSTANCE
  tinst1
  $ db2 get dbm cfg | grep "(SVCENAME)"
   TCP/IP Service name (SVCENAME) = DB2_tinst1
  $ grep  DB2_tinst1  /etc/services
  DB2_tinst1      60006/tcp
  DB2_tinst1_1    60007/tcp
  DB2_tinst1_2    60008/tcp
  DB2_tinst1_3    60009/tcp
  DB2_tinst1_4    60010/tcp
  DB2_tinst1_END  60011/tcp
  ```

  In this example, the TCP/IP port number needs to set to `60006`.

- Process name: On the Linux and UNIX operating systems, the value is the full path name of `$INSTHOME/sqllib/adm/db2sysc`. On the Windows operating systems, the value is `SDB2SYSCS.EXE`, for example:

  ```
  $ echo $DB2INSTANCE
  tinst1
  $ ls $INSTHOME/sqllib/adm/db2sysc
  /home/tinst1/sqllib/adm/db2sysc
  ```

In this example, the process name needs to be set to `/home/tinst1/sqllib/adm/db2sysc`.

- DB2 shared memory adjustment: On the Linux and UNIX operating systems, the value is `20`. On the Windows operating systems, the value is `80`.
- DB2 shared memory client position: Query the instance's application support layer heap size (ASLHEAPSZ) configuration parameter. The DB2 shared memory client position is calculated by multiplying the value of ASLHEAPSZ with 4096, for example:

```
$ echo $DB2INSTANCE
tinst1
$ db2 get dbm cfg | grep "ASLHEAPSZ" | awk '{print $9 * 4096}'
61440
```

  In this example, the DB2 shared memory client position needs to be set to `61440`.

- DB2 shared memory size: Query the instance's application support layer heap size (ASLHEAPSZ) configuration parameter. The DB2 shared memory size is calculated by using the following formula: `(ASLHEAPSZ + 1) * 8192`. The exact size can be determined by running the commands that are shown in the example for AIX:

```
$ echo $DB2INSTANCE
tinst1
$ ipcs -ma | sort -n -2 +3 > /tmp/o.txt
$ db2 connect to TESTDB
   Database Connection Information

   Database server        = DB2/AIX64 10.5.3
   SQL authorization ID   = TINST1
   Local database alias   = TESTDB

$ ipcs -ma | sort -n -2 +3 > /tmp/t.txt
$ db2 terminate
DB20000I  The TERMINATE command completed successfully.
$ diff /tmp/o.txt /tmp/t.txt | awk '{if ($10 == 2) print $11}'
131072
```

  In this example, the DB2 shared memory size needs to be set to `131072`.

A.2.3 Workload Replay appliance user mapping worksheet

Use Table A-3 and Table A-4 to map employees to user types for each main and auxiliary Workload Replay appliance. After the appliance is installed and configured, create the correct accounts on each appliance, as described in 7.1, “Access management” on page 214.

For illustration, we added two example entries for the Linux, UNIX, and Windows deployment that we performed. `Silvi W.` manages the two appliances and captures, processes, and replays workloads. `Pat K.` only captures, processes, and replays workloads.

Table A-3 Main Workload Replay appliance user mapping

Employee	Main appliance	Administrator?	Security administrator?	Privileged user?	User?
Silvi W.	pine.itso.ibm.com	Yes	Yes	Yes	No
Pat K.	pine.itso.ibm.com	No	No	No	Yes

Table A-4 Auxiliary Workload Replay appliance user mapping

Employee	Auxiliary appliance	Administrator?	Security administrator?	Privileged user?
Silvi W.	spruce.itso.ibm.com	Yes	Yes	Yes

Note: Non-privileged users do not require access to auxiliary appliances.

A.3 Open port requirements

InfoSphere Workload Replay appliances communicate with each other with their associated S-TAPs. They are accessed by using remote user interfaces. Review Table A-5 on page 319 shows the communication between the Linux, UNIX, and Windows database server machines and the Workload Replay appliance. Table A-6 on page 319 shows the communication between the z/OS logical partitions (LPARs) and the Workload Replay appliance. Table A-7 on page 320 lists the open port requirements for z/OS and Linux, UNIX, and Windows deployments.

Table A-5 Linux, UNIX, and Windows database servers and Workload Replay appliance

Port number	Protocol	Applicable database server platform	Comment
8075	User Datagram Protocol (UDP)	Windows	Heartbeat
9500	TCP	Windows	S-TAP not encrypted (default)
9501	Transport Layer Security (TLS)	Windows	S-TAP encrypted
16016	TCP	Linux and UNIX	S-TAP not encrypted (default)
16018	TLS	Linux and UNIX	S-TAP encrypted
Custom	TCP	All	Monitored DB2 instance TCP/IP port

Table A-6 Communication between z/OS LPARs and the Workload Replay appliance

Port number	Protocol	Applicable database server platform	Comment
16016	TCP	z/OS	S-TAP not encrypted
40000	TCP	z/OS	Controller
40001	TCP	z/OS	Controller
Custom	TCP	z/OS	DB2 Distributed Relational Database Architecture (DRDA) port (default 446)

Table A-7 Ports used for communication between appliances and external interfaces

Port number	Protocol	Comment
22	TCP	Secure Shell (SSH) access to the command-line interface (CLI)
80	TCP	Temporary HTTP access to the file server (to upload patches, download trace files, and so on)
8443	TCP	HTTPS access to Guardium web console and Workload Replay web console
40000	TCP	Inter-appliance communication in multi-server deployments
40001	TCP	Inter-appliance communication in multi-server deployments
Custom	FTP	Temporary FTP access to upload or download external files (outgoing only, default port number 21)
Custom	SCP	Temporary SCP access to upload or download external files (outgoing only, default port number 22)

A.4 Workload Replay artifacts that reside in capture or replay databases or subsystems

Workload action security policies are implemented through a set of user-defined functions (UDFs), as shown in Table A-8 on page 321, that are maintained by InfoSphere Workload Replay in the capture and replay databases or subsystems. These UDFs are created when a privileged user creates a database connection profile in the Workload Replay web console, as described in 4.5, “Enablement of workload capture and replay in the Workload Replay web console” on page 98 for DB2 for z/OS and 5.4, “Enablement of workload capture and replay in the Workload Replay web console” on page 140 for DB2 for Linux, UNIX, and Windows.

Table A-8 Security UDFs that are created on a database or subsystem

UDF	Privilege
OCR.CAN_CAPTURE_WORKLOAD	Can Capture workload
OCR.CAN_EXPORT_WORKLOAD	Can Export Workload
OCR.CAN_IMPORT_WORKLOAD	Can Import Workload
OCR.CAN_REPLAY_WORKLOAD	Can Replay Workload
OCR.CAN_CREATE_REPORT	Can Create Report
OCR.CAN_DELETE_CAPTURED_WORKLOAD	Can Delete Captured Workload
OCR.CAN_DELETE_REPLAYED_WORKLOAD	Can Delete Replayed Workload
OCR.CAN_DELETE_REPORT	Can Delete Report

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book.

IBM Redbooks

The following IBM Redbooks publications provide additional information about the topic in this document. Note that some publications referenced in this list might be available in softcopy only.

- *Architecting and Deploying DB2 with BLU Acceleration,* SG24-8212:

  http://www.redbooks.ibm.com/abstracts/sg248212.html

- *Reliability and Performance with IBM DB2 Analytics Accelerator V4.1,* SG24-8213:

  http://www.redbooks.ibm.com/redpieces/abstracts/sg248213.html

- *Deployment Guide for InfoSphere Guardium,* SG24-8129:

  http://www.redbooks.ibm.com/abstracts/sg248129.html

- *Optimizing DB2 Queries with IBM DB2 Analytics Accelerator for z/OS*, SG24-8005:

  http://www.redbooks.ibm.com/abstracts/sg248005.html

- *Performance Management: Using IBM InfoSphere Optim Performance Manager and Query Workload Tuner*, SG24-8111:

  http://www.redbooks.ibm.com/abstracts/sg248111.html?Open

You can search for, view, download or order these documents and other Redbooks, Redpapers, Web Docs, draft and additional materials, at the following website:

ibm.com/redbooks

Online resources

These websites are also relevant as further information sources:

- Download InfoSphere Optim Workload Replay Version 2.1.0.1:

  http://www-01.ibm.com/support/docview.wss?uid=swg24035897

- Current Maintenance Levels for InfoSphere Optim Workload Replay for DB2 for z/OS:

  http://www-01.ibm.com/support/docview.wss?uid=swg27039922

- IBM InfoSphere Guardium Knowledge Center:

  http://www-01.ibm.com/support/knowledgecenter/SSMPHH/SSMPHH_welcome.html

- IBM InfoSphere Optim Query Capture and Replay for DB2 on z/OS version 1.1.x compatibility report:

  http://www-01.ibm.com/support/docview.wss?uid=swg27036808

- System requirements for IBM InfoSphere Optim Workload Replay Version 2.1.x:

  http://www-01.ibm.com/support/docview.wss?uid=swg27039781

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Getting Started with IBM InfoSphere Optim Workload Replay for DB2

(0.5” spine)
0.475”<->0.875”
250 <-> 459 pages

Getting Started with IBM InfoSphere Optim Workload Replay for DB2

Describes planning, installation, configuration, and usage details

Covers UNIX, Linux, Windows, and z/OS platforms

Introduces tools integration

This IBM Redbooks publication will help you install, configure, and use IBM InfoSphere Optim Workload Replay (InfoSphere Workload Replay), a web-based tool that lets you capture real production SQL workload data and then replay the workload data in a pre-production environment. With InfoSphere Workload Replay, you can set up and run realistic tests for enterprise database changes without the need to create a complex client and application infrastructure to mimic your production environment.

The publication goes through the steps to install and configure the InfoSphere Workload Replay appliance and related database components for IBM DB2 for Linux, UNIX, and Windows and for DB2 for IBM z/OS. The capture, replay, and reporting process, including user ID and roles management, is described in detail to quickly get you up and running.

Ongoing operations, such as appliance health monitoring, starting and stopping the product, and backup and restore in your day-to-day management of the product, extensive troubleshooting information, and information about how to integrate InfoSphere Workload Replay with other InfoSphere products are covered in separate chapters.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-8221-00 ISBN 0738440396