Quest

Foglight® for DB2 LUW 5.9.2.1

Monitoring DB2 LUW Database Systems:

Getting Started Guide

© 2020 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at www.quest.com/legal.

Trademarks

Quest, the Quest logo, Foglight, and Where next meets now are trademarks and registered trademarks of Quest Software Inc. in the U.S.A. and other countries. For a complete list of Quest Software trademarks, please visit our website at www.quest.com/legal. Red Hat, JBoss, the JBoss logo, and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. in the U.S. and other countries. CentOS is a trademark of Red Hat, Inc. in the U.S. and other countries. Fedora and the Infinity design logo are trademarks of Red Hat, Inc. Microsoft, .NET, Active Directory, Internet Explorer, Hyper-V, Office 365, SharePoint, Silverlight, SQL Server, Visual Basic, Windows, Windows Vista and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. AIX, IBM, PowerPC, PowerVM, and WebSphere are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Java, Oracle, Oracle Solaris, PeopleSoft, Siebel, Sun, WebLogic, and ZFS are trademarks or registered trademarks of Oracle and/or its affiliates in the United States and other countries. SPARC is a registered trademark of SPARC International, Inc. in the United States and other countries. Products bearing the SPARC trademarks are based on an architecture developed by Oracle Corporation. OpenLDAP is a registered trademark of the OpenLDAP Foundation. HP is a registered trademark that belongs to Hewlett-Packard Development Company, L.P. Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. MySQL is a registered trademark of MySQL AB in the United States, the European Union and other countries. Novell and eDirectory are registered trademarks of Novell, Inc., in the United States and other countries. VMware, ESX, ESXi, vSphere, vCenter, vMotion, and vCloud Director are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. Sybase is a registered trademark of Sybase, Inc. The X Window System and UNIX are registered trademarks of The Open Group. Mozilla and Firefox are registered trademarks of the Mozilla Foundation. IOS is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Apple, iPad, iPhone, Mac OS, Safari, Swift, and Xcode are trademarks of Apple Inc., registered in the U.S. and other countries. Ubuntu is a registered trademark of Canonical Ltd. Symantec and Veritas are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. OpenSUSE, SUSE, and YAST are registered trademarks of SUSE LCC in the United States and other countries. Citrix, AppFlow, NetScaler, XenApp, and XenDesktop are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. PostgreSQL is a registered trademark of the PostgreSQL Global Development Group. MariaDB is a trademark or registered trademark of MariaDB Corporation Ab in the European Union and United States of America and/or other countries. Intel, Itanium, Pentium, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries. Debian is a registered trademark of Software in the Public Interest, Inc. OpenStack is a trademark of the OpenStack Foundation. All other marks and names mentioned herein may be trademarks of their respective companies.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Foglight® for DB2 LUW Getting Started Guide
Updated - September 2020
Software Version - 5.9.2.1

Contents

Installing Foglight *for DB2 LUW* **4**
Installation Prerequisites 4
Supported Platforms 4
Required OS User Account Permissions and Programs 4
Required DB2 LUW User Account Privileges 6
Required DB2 LUW Monitor Switches 6
Installation Procedures 7
Installing Foglight *for DB2 LUW* using the executable installer 7
Installing the Foglight *for DB2 LUW* cartridge on a Management Server 7

Configuring Foglight for DB2 LUW **8**
Configuring Monitoring Agents 8
Monitoring DB2 HADR Environments 8
Monitoring IBM DB2 pureScale Environments 9

Permissions **10**

About us **12**
Technical support resources 12

Installing Foglight *for DB2 LUW*

The Getting Started Guide is a quick guide for the installation and use of Foglight for DB2 LUW, from the planning stage up to the actual monitoring of database instances. This document details the various privileges and permissions required for the successful operation of Foglight for DB2.

While installing and upgrade, Foglight will check for the required permissions, alert if any is missing and will provide a script to grant the missing permissions.

This guide is intended for IBM® DB2® Server database administrators.

Installation Prerequisites

Before installing Foglight *for DB2 LUW*, ensure that the following conditions are met.

The following permissions must be granted **before** installation or upgrade begins:

- grant select on SYSIBMADM.PRIVILEGES
- grant select on syscat.views
- grant select on syscat.routines
- grant execute on function SYSPROC.AUTH_LIST_AUTHORITIES_FOR_AUTHID(VARCHAR(128),VARCHAR(1))

Supported Platforms

Review release notes for information about supported platforms.

- Foglight *for DB2 LUW* — System requirements and supported platforms are identical to those of Foglight Management Server. For details, see *Foglight System Requirements and Platform Support Guide*.
- DB2 LUW monitored instance — Review the *Foglight for DB2 LUW Release Notes* to ensure that your monitored environment versions are supported by this release.

Required OS User Account Permissions and Programs

Foglight agents require a DB2 LUW user account to monitor the operating system running the monitored DB2 instances. Some OS programs and settings are also required.

- Windows Systems
- UNIX Systems

NOTE: SYSMON role and privileges for OS user is not required but is recommended to enable installation to provide more information when discovering DB2 databases.

Windows Systems

The agent's OS user account requires:

- To monitor Windows Operating System metrics, access to WMI. Ensure that the WMI service is started before creating agents and monitoring the process metrics.

Permissions for monitoring Windows OS

Monitoring with WMI:

http://support.quest.com/technical-documents/foglight-agent-manager/5.9.2/foglight-agent-manager-guide/advanced-system-configuration-and-troubleshooting/configuring-windows-management-instrumentation-wmi

Monitoring with WinRM:

http://support.quest.com/technical-documents/foglight-agent-manager/5.9.2/foglight-agent-manager-guide/advanced-system-configuration-and-troubleshooting/configuring-windows-remote-management-winrm

UNIX Systems

The agent's OS user account requires:

- Access and execute permission to the following programs: df, du, awk, iostat, vmstat, uptime, hostname, netstat, sed, ps, uname
- Silent log-in — in particular, there must be no user-input required and no special login banners displayed
- For connection using SSH, the sshd daemon must be installed and running
- For connection using Telnet, a Telnet daemon must be installed and running

In addition to these general UNIX system requirements, the agent's user account requires additional privileges depending on the operating system, as specified in the following table.

Table 1. User account requirements by OS

OS	Additional OS user account requirements
Linux	• Access to the sysstat package, to permit the agent to get detailed disk I/O information • Access to the /proc filesystem • Access to the following programs: /proc/vmstat, /proc/net/dev, free, /proc/cpuinfo, getconf
Solaris	Access to the following programs: /usr/sbin/prtconf, mpstat, pagesize, psrinfo, db2ptree
AIX	• `setuid` permissions on vmstat and iostat • `setgid` permissions on PS • Access to the following programs: lsattr, lsdev, pagesize, bindprocessor, oslevel

Using Sudo

The sudo utility allows system administrators to grant specific users (or groups of users) the ability to run certain commands that require administrative privileges as the root, without having to log in as administrator.

If you intend for an agent to run UNIX commands with sudo permissions, check the /etc/sudoers file on the monitored host for the following line and comment it out:

```
Defaults requiretty
```

The programs that can be run using sudo are as follows:

- On all platforms: db2, du, df, grep, hostname, awk, iostat, vmstat, ps, uname, egrep
- On the Linux platform: free, /proc/cpuinfo, getconf

- On the Solaris platform: /usr/sbin/prtconf, xargs, pagesize, psrinfo, db2ptree
- On the AIX platform: lsattr, pagesize, bindprocessor, oslevel

Required DB2 LUW User Account Privileges

Foglight monitoring agents use DB2 LUW user accounts to access the monitored DB2 instances. *Before adding monitored instances*, ensure that the user accounts have at least the following privilege and permission set:

- **SYSMON** authority (enables monitoring)
- **AUTH_LIST_AUTHORITIES_FOR_AUTHID** permission (enables the wizard to verify and set permissions)
- **Select** permission on SYSIBMADM.PRIVILEGES, SYSCAT.VIEWS and SYSCAT.ROUTINES

When you add monitored instances, the Monitor DB2 Instance wizard checks that other required permissions exist and, if not, executes a script to grant any missing permissions. For a list of the required permissions granted by this script, see Permissions on page 10.

Required DB2 LUW Monitor Switches

To monitor DB2 instances below version 9.7, ensure that the following monitored switches are turned on:

- **UOW**
- **STATEMENT**
- **LOCK**
- **SORT**
- **TABLE**
- **BUFFERPOOL**
- **TIMESTAMP**

To monitor DB2 instances of version 9.7 and above, ensure that the following monitoring configuration parameters are set to base level (at least):

- **MON_REQ_METRICS**
- **MON_ACT_METRICS**
- **MON_OBJ_METRICS**

When you add monitored instances, the Monitor DB2 Instance wizard checks that the monitoring configuration parameters are set correctly. If not, it prompts you to set them.

The switches can be turned on or off manually by updating the database manager configuration. Enabled switches may cause additional overhead on the database manager.

For additional information, see *http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp?topic=/com.ibm.db2.luw.admin.mon.doc/doc/c0005719.html System Monitor Switches* and http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/index.jsp?topic=%2Fcom.ibm.db2.luw.wn.doc%2Fdoc%2Fc0054153.html on IBM's DB2 InfoCenter web site.

Or, review the information in at *http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp?topic=/com.ibm.db2.luw.common.doc/doc/r0008264.htm DB2 System Monitor Guide and Reference Redbook*

Installation Procedures

Foglight *for DB2 LUW* runs on the Foglight Management Server, which is its operation framework. Therefore, Foglight Management Server must be installed before installing the cartridge. The installation of Foglight *for DB2 LUW* can be carried out using either of the following scenarios:

- Installing both Foglight *for DB2 LUW* and Foglight Management Server. For more information, see Installing Foglight *for DB2 LUW using the executable installer* on page 7.
- Installing Foglight *for DB2 LUW* as a cartridge from within an existing Foglight Management Server. For more information, see Installing the Foglight *for DB2 LUW cartridge on a Management Server* on page 7.

Installing Foglight *for DB2 LUW* using the executable installer

A single executable file allows installing Foglight Management Server together with Foglight *for DB2 LUW*.

To run the combined installation file:

1 Copy the installation file appropriate to the operating system and the bit level (32-bit or 64-bit) to a temporary directory on the requested host.

NOTE: The combined installation file is named using the following convention: Foglight-<version_number>-DB2-install_<operating system>-<instruction set><bit level><.exe/.bin>. For example: Foglight-5_6_4-DB2-install_windows-x86_64.exe or Foglight-5_6_4-DB2-install_solaris-x86_64.bin.

2 If planning to use an external database for the Foglight Management Server Installation, ensure that this database is running.

3 Follow the on-screen installation instructions.

Installing the Foglight *for DB2 LUW* cartridge on a Management Server

Ensure that the pre-existing Foglight license that is being used allows cartridge installation. If a license that does not allow cartridge installation is used, the installation wizard cannot proceed beyond the Foglight Management Server License screen, which requires specifying the type of license to be installed.

To install Foglight for DB2 LUW as a cartridge:

1 Copy the cartridge's car file (DB_DB2-VersionNumber.car; for example, DB_DB2-5_6_4.car), which is included in the installation media, to your local computer.

2 Log in to the Foglight browser interface.

3 In the browser interface, on the navigation panel, click **Dashboards** > **Administration** > **Cartridges** > **Cartridge Inventory**.

4 On the Cartridge Inventory dashboard, click **Browse** to find the car file on your local computer.

5 Click **Install Cartridge**.

Configuring Foglight for DB2 LUW

The next step is to configure agents to monitor your DB2 instances.

NOTE: This section assumes that you have a Foglight Agent Manager installed with capacity to host Foglight for DB2 LUW monitoring agents. Agent Managers host agents, manage agent lifecycle (such as start, stop, and restart), manage the agent connection to the Management Server, and provide centralized services to agents. To determine the capacity of an Agent Manager to host agents, see the Foglight for DB2 LUW Hardware Sizing Guide.

Configuring Monitoring Agents

A wizard guides you through the process of configuring agents. You are prompted to specify connection details for the DB2 host, instances, and databases. As you go, you can validate log in credentials, database and instance connectivity, and host connectivity. You can correct issues by granting database permissions, setting monitoring switches, and configuring parameters.

To monitor DB2 instances:

1. In the navigation panel, under **Homes**, click **Databases**.

   On a fresh installation, no instances are listed for DB2 in the Databases dashboard.

2. In the instances table, click **Monitor more instances** and select **Add one DB2**.

   The Monitor DB2 Instance wizard opens.

3. Follow the online prompts to configure an agent to monitor the DB2 host, instance, and databases. For help with options, click .

Monitoring DB2 HADR Environments

A DB2 high availability disaster recovery (HADR) environment has two or more databases:

- Primary Database — This is the active database.
- Standby Database — Data from the primary database is propagated to standby databases.

A standby database can be opened in read-only mode and used for reporting. Running the standby database in reporting mode eases the load on the primary (production) database.

NOTE: The HADR read on Standby option is available in DB2 version 9.7.1 or later and is subject to licensing. As of version 10, you can have more than one standby database for each primary database.

We recommend creating agents to monitor each of the instances with databases that participate in the HADR environment. This approach ensures that there is no loss of monitoring in a failover scenario.

For the primary database and for the standby databases that are in read-only mode, you create agents as usual to monitor their DB2 instances. For standby databases that are not in read-only mode, you can define the settings for its DB2 instance, but the wizard is unable to verify database connectivity. To resolve this issue, run the Grant Permissions script for the monitoring user on the standby database.

To monitor databases in a DB2 HADR environment:

1. Configure agents to monitor the instances that host the primary database and standby databases. See Configuring Monitoring Agents on page 8.
2. When selecting a standby database that is not in read-only mode, the wizard's validate database connectivity step shows a message indicating the connection could not be verified. Installation can proceed but it is recommended that you click **View grant script** and make sure that the Foglight user has the required permissions on the standby database.

Monitoring IBM DB2 pureScale Environments

IBM DB2 pureScale® offers high availability and scalability through clustering technology. To monitor instances in a pureScale environment, ensure that the Permissions for DB2 pureScale Environments are set and then configure monitoring agents as usual. Foglight automatically reports on the pureScale cluster cache facility (CF) component, buffer pools and caches, locks, and request time breakdown.

The following pages and views contain monitoring data for pureScale:

- Databases dashboard — The instance's Host is identified as pureScale.
- Instances home page — See the *Additional Information* and *PureScale CF* panes.
- Instances home page > Memory — See the *Primary CF* and *Backup CF* tabs.
- Database home page — See the *Balance Criterion* and *Memory* panes.
- Database home page > Activity > Locks — See the *PureScale Lock Time* tab.
- Database home page > Memory > Buffer Pools — See the *GBP Hit Ratio* tab.
- Member (History) home page — See the *Request Time Breakdown* pane.
- Member (Real Time) home page — See the *Request Time Breakdow*n pane.
- Member (*either*) home page > Activity > Locks — See the *PureScale Lock Time* tab.
- Member (*either*) home page > Memory > Buffer Pools — See the *GBP Hit Ratio* tab.

3

Permissions

Foglight monitoring agents use DB2 LUW user accounts to access monitored DB2 instances. The user accounts need to have the privilege and permission listed in Required DB2 LUW User Account Privileges on page 6. When these conditions are met, the Monitor DB2 Instance wizard checks that the rest of the required permissions exist and, if not, enables you to run the Grant Permissions script to grant missing permissions.

The Grant Permissions script verifies and sets the following general and pureScale-specific permissions.

General Permissions

An agent needs to be able to select and run from the following SYSPROC table functions and procedures:

- AUTH_LIST_AUTHORITIES_FOR_AUTHID (for DB2 version 9.5 or later)
- ADMIN_CMD
- DB_PARTITIONS
- DB2_GET_INSTANCE_INFO (for DB2 version 9.8 or later)
- ENV_GET_PROD_INFO
- ENV_GET_SYS_INFO
- ENV_GET_SYSTEM_RESOURCES (for DB2 version 9.7.0.1 or later)
- PD_GET_DIAG_HIST (for DB2 version 10 or later)
- MON_FORMAT_XML_TIMES_BY_ROW (for DB2 version 9.7.0.1 or later)
- MON_GET_PKG_CACHE_STMT (for DB2 version 9.7.0.1 or later)
- MON_GET_SERVICE_SUBCLASS_DETAILS (for DB2 version 9.7.0.1 or later)
- SNAP_GET_APPL
- SNAP_GET_APPL_INFO
- SNAP_GET_BP
- SNAP_GET_BP_PART
- SNAP_GET_DB_V91, or SNAP_GET_DB (for DB2 version 10 or later)
- SNAP_GET_DBM
- SNAP_GET_DBM_MEMORY_POOL
- SNAP_GET_DYN_SQL_V91, or SNAP_GET_DYN_SQL (for DB2 version 10 or later)
- SNAP_GET_FCM_PART
- SNAP_GET_HADR
- SNAP_GET_LOCKWAIT
- SNAP_GET_STMT
- SNAP_GET_STORAGE_PATHS
- SNAP_GET_SWITCHES
- SNAP_GET_TAB_V91, or SNAP_GET_TAB (for DB2 version 10 or later)

- SNAP_GET_TBSP_V91, or SNAP_GET_TBSP (for DB2 version 10 or later)
- DB2_GET_INSTANCE_INFO (for DB2 version 10 or later)
- MON_FORMAT_XML_TIMES_BY_ROW(for DB2 version 9.7.0.1 or later)
- MON_FORMAT_LOCK_NAME (for DB2 version 9.7.0.1 or later)
- MON_GET_CONNECTION (for DB2 version 9.7.0.1 or later)
- MON_GET_UNIT_OF_WORK (for DB2 version 9.7.0.1 or later)
- WLM_GET_SERVICE_CLASS_AGENTS_V97 (for DB2 version 9.7.0.1 or later), or WLM_GET_SERVICE_CLASS_AGENTS (for DB2 version 10 or later), or MON_GET_AGENT (for DB2 version 10.5 or later)
- MON_GET_WORKLOAD(for DB2 version 9.7.0.1 or later)
- MON_GET_BUFFERPOOL(for DB2 version 9.7.0.1 or later)
- MON_GET_FCM_CONNECTION_LIST(for DB2 version 9.7.0.1 or later)
- MON_GET_TABLESPACE(for DB2 version 9.7.0.1 or later)
- MON_GET_TABLE(for DB2 version 9.7.0.1 or later)
- ADMIN_GET_STORAGE_PATHS(for DB2 version 10 or later)
- MON_GET_TRANSACTION_LOG(for DB2 version 10 or later)
- MON_GET_DATABASE(for DB2 version 10.5 or later)
- MON_GET_INSTANCE(for DB2 version 10.5 or later)
- ENV_GET_DB2_SYSTEM_RESOURCES (for DB2 version 9.7.0.1 or later)
- SNAP_GET_CONTAINER_V91(for DB2 version below 9.7), or MON_GET_CONTAINER (for DB2 version 9.7 or later)

An agent also needs to be able to select from the following SYSIBMADM administrative views:

- DBPATHS (for version 9.7.0.1 or later)
- REG_VARIABLES
- BP_HITRATIO
- DBCFG
- ENV_INST_INFO
- MON_LOCKWAITS (for version 9.7.0.1 or later)
- SNAPDBM
- SNAPFCM
- SYSIBMADM.ENV_PROD_INFO

Permissions for DB2 pureScale Environments

In addition to the General Permissions, an agent requires permission to run the following table functions for pureScale environments:

- MON_GET_CF
- MON_GET_GROUP_BUFFERPOOL

An agent also needs to be able to select from the following pureScale views:

- ENV_CF_SYS_RESOURCES
- SNAPDB
- SYSIBMADM.DB2_MEMBER

About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit https://www.quest.com/.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.