Quest

Foglight® for Databases 5.9.5.10

Monitoring Database Systems

Deployment Guide

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 Databases Deployment Guide
Updated - December 2019
Software Version - 5.9.5.10

Contents

1

Deployment pre-requisites

Welcome to the *Foglight for Databases Deployment Guide*. This guide provides the pre-requisites for optimal deployment, to ensure the best user experience possible.

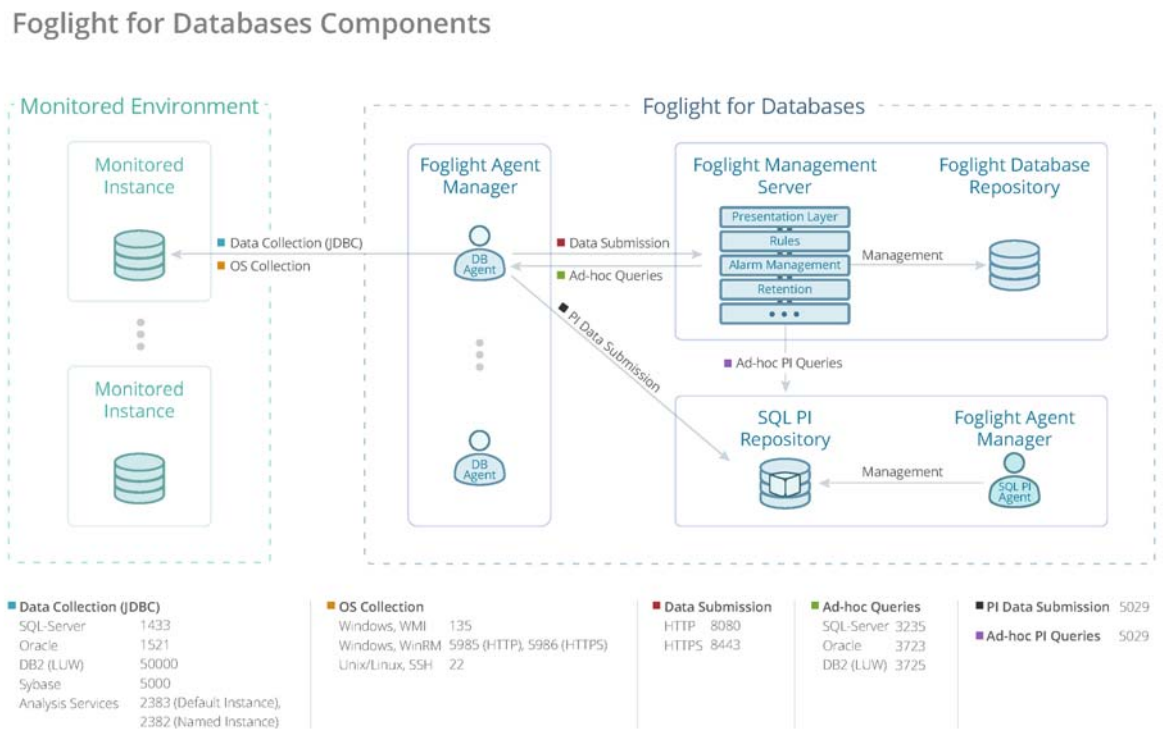
This section describes important deployment information required to monitor the leading RDBMS: Oracle®, SQL Server®, Sybase®, DB2 for LUW, and Azure® SQL.

Architecture

There are three main components:

- **Foglight Management Server** and **Foglight Database Repository** — Responsible for managing, alerting and viewing the collected data. Both components can be set to run on the same machine or reside on separate machines.
- **Agent Manager** — Hosts the monitoring database agents.
- **SQL PI Repository** — An embedded repository which stores the SQL PI data that the monitoring agents collect. Currently available on Oracle and SQL Server monitoring only.

Figure 1. Foglight for Databases Components



Deployment in Centralized vs Distributed

In monitoring environments that exceed a total of 20 agents, a distributed installation is necessary:

- The FMS should be installed on a dedicated server.
- External FglAMs should be used for DB Agents and with each installed on a dedicated server.
- Each instance of the SQL PI repository should be installed on a separate server.

In All-in-One installations on virtual machines (VMs), the machine must have all of the CPU and Memory requirements fully reserved.

Once the total number of agents exceeds 20, All-in-One installations are no longer supported.

Hardware requirements

Identify your hardware requirements, which are determined by whether SQL PI is configured and by the number of monitoring agents.

- SQL PI configured
- SQL PI not configured

NOTE: The Numbers of agent refers to DB agents. The IC agents resources are calculated within the DB agents. Sizing requirements are exclusively for Foglight components and these resources should not compete with any other resources required for the OS or applications installed on the same system.

SQL PI configured

SQL PI is available only for Oracle, SQL Server and SQL Server BI (Analysis services). These tables define the Hardware requirements for each server based on the number of monitoring agents

After locating your hardware requirements in the tables, ensure that you complete the manual JVM Setting configuration as described in:

- Manual configuration required by all users

Foglight Management Server

Table 1. Foglight Management Server with SQL PI configured

Number of Agents	<5	<50	<100	<200	<400	<600	<800
CPUs (2.4GHz)*	2 cores	4 cores	4 cores	4 cores	4 cores	6 cores	8 cores
RAM*	6GB	8GB	8GB	10GB	12GB	16GB	18GB
JVM Settings**	4096MB	4096MB	4096MB	6144MB	8192MB	10240MB	14336MB
Hard Drive Space	10GB	100GB	200GB	400GB	800GB	1200GB	1600GB

CPUs (2.4GHz)* — for a virtual machine the CPU allocation must be reserved. The reservation is expressed in MHz

RAM*- for a virtual machine the memory allocation must be reserved.

Foglight Agent Manager

Table 2. Foglight Agent Manager

Number of Agents	<5	<50	<100	<200	<400	<600	<800
CPUs (2.4GHz)*	1 core	4 cores	8 cores	8 cores	10 cores	12 cores	14 cores
RAM*	2GB	8GB	12GB	16GB	20GB	26GB	34GB
JVM Settings**	1024MB	6144MB	8192MB	12288MB	16384MB	22528MB	30720MB
Hard Drive Space	2GB	5GB	10GB	20GB	40GB	60GB	80GB

IMPORTANT: If you are monitoring more than 70 agent running on Windows system, the monitored hosts should be configured to use WinRM.
Monitoring Analysis services is supported only on Agent Managers running on Windows which must have a version of .NET 3.5 installed.
One PI repository can only be attached by at most three Foglight Agent Managers at a time.

CPUs (2.4GHz)* — for a virtual machine the CPU allocation must be reserved. The reservation is expressed in MHz.

RAM*- for a virtual machine the memory allocation must be reserved.

SQL PI Repository

WARNING: Linux® is the recommended platform for both Oracle and SQL Server monitoring.
Exclude the SQL PI repository directory (named Infobright™) from real-time scanning (for example, Antivirus software). For a virtual machine the CPU and memory allocations must be reserved. Recommended configuration would be a separate FMS and FglAM where PI repository resides on and a separate FglAM where DB Agents resides on the different host machine.

Table 3. SQL PI Repository

Number of Agents	<5	<50	<100	<200	<400	<600	<800
CPUs (2.4GHz)*	1 core	4 cores	4 cores	6 cores	8 cores	12 cores	16 cores
RAM*	4GB	10GB	14GB	20GB	24GB	30GB	36GB
Hard Drive Space	10GB	100GB	200GB	400GB	800GB	1200GB	1600GB

CPUs (2.4GHz)* — for a virtual machine the CPU allocation must be reserved. The reservation is expressed in MHz

RAM*- for a virtual machine the memory allocation must be reserved.

SQL PI not configured

The table defines the Hardware requirements based on the number of monitoring agents.

After locating your hardware requirements in the tables, ensure that you complete the manual JVM Setting configuration as described in:

- Manual configuration required by all users

Foglight Management Server

Table 4. Foglight Management Server

Number of Agents	<5	<100	<200	<400	<600	<800
CPUs (2.4GHz)*	2 cores	4 cores	4 cores	4 cores	6 cores	8 cores
RAM*	6GB	8GB	10GB	12GB	16GB	18GB
JVM Settings**	4096MB	4096MB	6144MB	8192MB	10240MB	14336MB
Hard Drive Space	10GB	200GB	400GB	800GB	1200GB	1600GB

CPUs (2.4GHz)* — for a virtual machine the CPU allocation must be reserved. The reservation is expressed in MHz

RAM*- for a virtual machine the memory allocation must be reserved.

Foglight Agent Manager

Table 5. Foglight Agent Manager

Number of Agents	<5	<100	<200	<400	<600	<800
CPUs (2.4GHz)*	1 core	2 cores	4 cores	4 cores	6 cores	8 cores
RAM*	1GB	4GB	6GB	10GB	14GB	18GB
JVM Settings**	256MB	2048MB	4096MB	8192MB	12288MB	16384MB
Hard Drive Space	2GB	5GB	10GB	20GB	30GB	40GB

IMPORTANT: If you are monitoring more than 70 agent running on Windows system, the monitored hosts should be configured to use WinRM.

CPUs (2.4GHz)* — for a virtual machine the CPU allocation must be reserved. The reservation is expressed in MHz

RAM*- for a virtual machine the memory allocation must be reserved.

Manual configuration required by all users

Foglight Management Server, JVM Settings **

Edit the *server.config* file located under the <*Foglight installation directory*>*config directory*.

For 4096MB, add the following lines:

```
server.vm.option0 = "-Xms4096m";
server.vm.option1 = "-Xmx4096m";
```

Foglight Agent Manager, JVM Settings **

Edit the *baseline.jvmargs.config* file located under the <*Agent Manager installation directory*>*state**default**config*\ *directory*

For 2048MB, add the following lines:

```
vmparameter.0 = "-Xms2048m";
vmparameter.1 = "-Xmx2048m";
```

Other settings

For number of agents > 50, edit these settings:

- **Data submission channel** — edit the *fglam.config.xml* file located under the <*Agent Manager installation directory*>*state**default**config*\ directory

  Alter the following lines:

  ```
  config:upstream attribute max-disk-space="102400"
  ```

  ```
  config:downstream attribute max-disk-space="102400"
  ```

- **Number of OS connections** — edit the *baseline.jvmargs.config* file located under the <*Agent Manager installation directory*>*state**default**config*\ directory

  Increase the number of allowed OS connections:

```
vmparameter.2 = “-Dcom.quest.connection.regulator.maxActiveConnectionsCap=1024”;
```

Supported monitoring platforms

Supported Platforms for the Foglight Management Server

http://support.quest.com/technical-documents/foglight/5.9.5/system-requirements-and-platform-support-guide/supported-platforms/supported-platforms-for-the-management-server

Supported Platforms for Foglight Agent Manager

http://support.quest.com/technical-documents/foglight/5.9.5/system-requirements-and-platform-support-guide/supported-platforms/supported-platforms-for-the-agent-manager

Supported Platforms for Foglight Agent Manager with PI Configured

Refer to Table 6 Supported Platforms for SQL PI Repository.

Supported Platforms for SQL PI Repository

- **WARNING:** Linux® is the recommended platform for both Oracle and SQL Server monitoring. Exclude the SQL PI repository directory (named Infobright™) from real-time scanning (for example, Antivirus software). For a virtual machine the CPU and memory allocations must be reserved.

Table 6. Supported Platforms for SQL PI Repository

Operating System	Version	OS Architecture	32-bit	64-bit
CentOS™ Linux®	6.x	x86-64		+
	7.x	x86-64		+
Red Hat® Enterprise Linux	6.x	x86-64		+
	7.x	x86-64		+
SUSE Linux	11	x86-64		+
	12	x86-64		+
	13	x86-64		+
	14	x86-64		+
Microsoft® Windows®	Windows Server 2003, 2008, 2012, and 2016	x86-64		+
		x86-64		+

IMPORTANT: Microsoft Visual C++ 2010 Package needs to be installed on the Foglight Management Server and Agent Manager host to enable PI on a Windows platform.

Supported monitored databases

Table 7. Supported Monitored Databases

Oracle®	SQL Server®	Sybase®	DB2 for LUW
Oracle Database 10g* Oracle Database 11g Oracle Database 12c Oracle Database 18c Oracle Database 19c	Microsoft® SQL Server 2005 Microsoft SQL Server 2008 Microsoft SQL Server 2008 R2 Microsoft SQL Server 2012 Microsoft SQL Server 2014 Microsoft SQL Server 2016 Microsoft SQL Server 2017 for Windows Microsoft SQL Server 2019 for Windows Microsoft SQL Server 2017 for Linux Microsoft SQL Server 2019 for Linux Microsoft SQL Server 2012 on Amazon RDS Microsoft SQL Server 2014 on Amazon RDS Microsoft SQL Server 2016 on Amazon RDS Microsoft SQL Server 2017 on Amazon RDS	Adaptive Server Enterprise: 12.5.1 through 16.0 Replication Server: 12.1, 12.5, 12.6, 15.0, 15.1, 15.2	DB2 version 9.5, 9.7, 10.1, 10.5, 11.1

Oracle Database 10g* — SQL PI supports version 11g and later

Operating Systems — All operating systems supported by the vendor.

Supported Editions — All editions supported by the vendor. Except for Sybase Edge and Runtime editions.

NOTE:
1. The SQL Server Azure managed instance is supported.
2. For the Amazon RDS SQL Server, only Standard and Enterprise version are supported.

Supported monitored BI services

- The same user monitoring the SQL Server database engine must be used to monitor the Integration and Reporting Services.
- The login ID used to monitor the Integration Service must be a user on the SSISDB database. This user ID is created while applying the “Grant permissions” script.
- The ID used to monitor the Integration Services on the database needs to have:
  - the `ssis_admin` role in order to gather all needed information for its collections.
  - the `db_datareader` role on the SSISDB database.
- Monitoring Analysis Services requires system administrator permissions on the Analysis Services instance.
- Monitoring Analysis Services is supported only on Agent Managers running on Windows which must have a version of .Net 3.5 installed.
- No additional permissions are required to monitor the Reporting Services.

Table 8. Supported Monitored BI Services

Integration Services*	Reporting Services*	Analysis Services
Microsoft® SQL Server® 2012	Microsoft SQL Server 2008	Microsoft SQL Server 2008
Microsoft SQL Server 2014	Microsoft SQL Server 2008 R2	Microsoft SQL Server 2008 R2
Microsoft SQL Server 2016	Microsoft SQL Server 2012	Microsoft SQL Server 2012
Microsoft SQL Server 2017 for Windows	Microsoft SQL Server 2014	Microsoft SQL Server 2014
Microsoft SQL Server 2019 for Windows	Microsoft SQL Server 2016	Microsoft SQL Server 2017 for Windows
	Microsoft SQL Server 2017 for Windows	Microsoft SQL Server 2019 for Windows
	Microsoft SQL Server 2019 for Windows	

*SQL Server instance must be monitored to be able to monitor the service.

Operating Systems — All operating systems supported by the vendor.

Supported Editions — All editions supported by the vendor.

PI aggregation and retention

PI manages data using an internal time pyramid; the roll-up process runs every 15 minutes.

Table 9. Time pyramid table

Time resolution	Retention period
1 minute	6 hours
15 minutes	3 days
1 hour	2 weeks
6 hours	30 days
1 day	90 days
1 week	2 years

Permissions for monitored databases

Ensure that you set the permissions required, based on which database you are using:

- Permissions for Oracle databases
- Permissions for SQL Server databases
- Permissions for Sybase databases
- Permissions for DB2 for LUW databases
- Permissions for Azure SQL Database

Permissions for Oracle databases

If you are using Oracle®, ensure that these permissions are set.

Grant **Select** on the following dictionary views:

NOTE: For Oracle 12c, replace all the dba_* dictionary views with the cdb prefix (cdb_*)

Table 10. Oracle views requiring Select permission

Dictionary view	Dictionary view	Dictionary view
dba_constraints	gv_$session	v_$logfile
dba_data_files	gv_$session_wait	v_$open_cursor
dba_db_links	gv_$sort_segment	v_$osstat
dba_directories	gv_$spparameter	v_$parameter
dba_extents	gv_$sql	v_$pgastat
dba_free_space	gv_$sysstat	v_$pq_sysstat
dba_indexes	gv_$temp_extent_pool	v_$process
dba_jobs	gv_$undostat	v_$recovery_file_dest
dba_jobs_running	obj$	v_$resource
dba_libraries	recyclebin$	v_$result_cache_statistics
dba_objects	ts$	v_$rman_status
dba_profiles	uet$	v_$rowcache
dba_role_privs	user$	v_$segstat
dba_roles	v_$archive_dest	v_$segment_statistics
dba_rollback_segs	v_$archived_log	v_$sess_time_model
dba_scheduler_jobs	v_$asm_disk	v_$session
dba_scheduler_running_jobs	v_$asm_disk_stat	v_$session_wait
dba_segments	v_$asm_diskgroup	v_$sesstat
dba_sequences	v_$asm_diskgroup	v_$sga
dba_sequences	v_$asm_diskgroup_stat	v_$sga_dynamic_components
dba_synonyms	v_$asm_operation	v_$sgainfo
dba_sys_privs	v_$asm_template	v_$sgastat
dba_tab_columns	v_$cell	v_$spparameter
dba_tab_privs	v_$controlfile	v_$sql
dba_tables	v_$database	v_$sql_plan
dba_tablespaces	v_$datafile	v_$sqlarea
dba_temp_files	v_$dataguard_status	v_$sqltext_with_newlines
dba_temp_free_space	v_$dbfile	v_$standby_log
dba_undo_extents	v_$dispatcher	v_$statname
dba_users	v_$enqueue_stat	v_$sysmetric
dba_views	v_$enqueue_statistics	v_$sysstat
dba_recyclebin	v_$event_name	v_$system_event
fet$	v_$filestat	v_$system_parameter
file$	v_$fixed_table	v_$tablespace
gv_$archive_dest	v_$flash_recovery_area_usage	v_$temp_extent_pool
gv_$archived_log	v_$instance	v_$temp_space_header
gv_$instance	v_$instance_cache_transfer	v_$tempfile
gv_$instance_cache_transfer	v_$iostat_file	v_$tempstat
gv_$lock	v_$librarycache	v_$transaction

Table 10. Oracle views requiring Select permission

Dictionary view	Dictionary view	Dictionary view
gv_$pq_sysstat	v_$lock	v_$memory_target_advice
gv_$rman_configuration	v_$log	v_$pga_target_advice
gv_$rman_output	v_$log_history	v_$sga_target_advice
	v_$undostat	v_$sql_shared_cursor
gv_$archive_dest_status	v_$flashback_database_log	v_$backup_set_details
gv_$dataguard_stats	v_$dataguard_config	v_$session_event
gv_$dataguard_status		v_$services

Additional configurations for Amazon Oracle RDS instances

There are two user credential options for monitoring Amazon Oracle RDS instances:

- **Master predefined user** that comes as part of Amazon Oracle RDS instance

  Or

- **Separate user** who has either of the following:
  - *SELECT_CATALOG_ROLE* or *SELECT ANY TABLE* system privilege
  - Grant additional permissions by manually executing the following commands from the master user:
    - ```
      EXEC RDSADMIN.RDSADMIN_UTIL.GRANT_SYS_OBJECT(p_obj_name=>'FET$',p_grantee =>'TEST', p_privilege => 'SELECT');
      ```
    - ```
      EXEC RDSADMIN.RDSADMIN_UTIL.GRANT_SYS_OBJECT(p_obj_name=>'UET$',p_grantee =>'TEST', p_privilege => 'SELECT');
      ```
    - ```
      EXEC RDSADMIN.RDSADMIN_UTIL.GRANT_SYS_OBJECT(p_obj_name=>'FILE$',p_grantee =>'TEST', p_privilege => 'SELECT');
      ```
    - ```
      EXEC RDSADMIN.RDSADMIN_UTIL.GRANT_SYS_OBJECT(p_obj_name=>'OBJ$',p_grantee =>'TEST', p_privilege => 'SELECT');
      ```
    - ```
      EXEC RDSADMIN.RDSADMIN_UTIL.GRANT_SYS_OBJECT(p_obj_name=>'TS$',p_grantee =>'TEST', p_privilege => 'SELECT');
      ```
    - ```
      EXEC RDSADMIN.RDSADMIN_UTIL.GRANT_SYS_OBJECT(p_obj_name=>'USER$',p_grantee =>'TEST', p_privilege => 'SELECT');
      ```
    - ```
      EXEC RDSADMIN.RDSADMIN_UTIL.GRANT_SYS_OBJECT(p_obj_name=>'RECYCLEBIN$',p_grantee =>'TEST', p_privilege => 'SELECT');
      ```

Permissions for SQL Server databases

If you are using SQL Server®, ensure that these permissions are set.
      ```

NOTE: Monitoring mirroring requires sysadmin privileges. Foglight user needs to be created on every database within the instance, otherwise it cannot be monitored. New databases created after Foglight agent installation needs to be added either by running the permission script again or manually using CREATE USER <Foglight User> under the new database.

Table 11. SQL Server Permissions

Instance Level		Database Level	
VIEW ANY DEFINITION VIEW SERVER STATE ALTER TRACE	Granted for: Tracing a Session Deadlocks monitoring PI Change-Tracking	Map Foglight Login to a database user* db_datareader db_ddladmin CREATE USER**	Granted for: Running DBCC commands for indexes

* Creation of a new user is not required if a domain group with the appropriate permissions is used.

** It's permission for SQL Server databases on Amazon RDS.

Grant **Execute** on these *master* database objects:

Table 12. Master database objects requiring Execute permission

xp_enumerrorlogs xp_readerrorlog	Granted for Error log monitoring

Grant **Select** on these *msdb* database objects:

Table 13. MSDB database objects requiring Select permission

log_shipping_monitor_primary	Granted for Log Shipping monitoring
log_shipping_monitor_secondary	
log_shipping_primaries	
log_shipping_secondaries	
log_shipping_primary_secondaries	
syscategories	
sysjobactivity	Granted for Jobs and Replication monitoring
sysjobs	
sysjobhistory	
dbm_monitor_data	Granted for Mirroring monitoring
dbm_monitor	
sysalerts	Granted for Agent alerts and services
agent_datetime	

NOTE:
1. For SQL Server databases on Amazon RDS, msdb database fixed database role of SQLAgentUserRole is needed.
2. For SQL Server databases on Amazon RDS, Master user should have access to all databases in the instance.

Permissions for Sybase databases

If you are using Sybase®, ensure that these permissions are set.

Permission required — Sybase MDA Agent requires mon_role

In case the agent is created with a non-*sa* user, procedures need to be manually created on the monitored instance. This is achieved by executing the scripts available at the following directory:

<Agent Manager installation directory>\agents\SybaseCartridge\<version#>\config\Sybase\scripts

Permissions for DB2 for LUW databases

If you are using DB2 LUW, ensure that these permissions are set.

Set Account **Privileges** on:

- SYSMON authority

Grant **Select privilege** on:

- SYSIBMADM.PRIVILEGES
- SYSIBMADM.SNAPADM
- SYSCAT.VIEWS
- SYSCAT.ROUTINES

Grant **Execute** on:

- AUTH_LIST_AUTHORITIES_FOR_AUTHID

Required Monitor Switches

Table 14. Required Configurations

Monitor switches for version 9.5 to 9.7	Monitoring parameters for version 9.7.0.1 or above*
UOW	MON_REQ_METRICS
STATEMENT	MON_ACT_METRICS
LOCK	MON_OBJ_METRICS
SORT	
TABLE	
BUFFERPOOL	
TIMESTAMP	

*Should be set to at least the base level.

Permissions

Table 15. Permissions — All versions

General
ADMIN_CMD
ENV_GET_PROD_INFO
DB_PARTITIONS
ENV_GET_SYS_INFO
SNAP_GET_APPL_INFO
SNAP_GET_BP
SNAP_GET_APPL
SNAP_GET_BP_PART
SNAP_GET_DBM
SNAP_GET_HADR
SNAP_GET_DBM_MEMORY_POOL
SNAP_GET_FCM_PART
SNAP_GET_STMT
SNAP_GET_LOCKWAIT
SNAP_GET_SWITCHES
SNAP_GET_STORAGE_PATHS
PD_GET_DIAG_HIST

Table 16. Permissions — Version-specific

9.5	9.7.0.1	10.1
SNAP_GET_DB_V91	ENV_GET_SYSTEM_RESOURCES	ENV_GET_SYSTEM_RESOURCES
SNAP_GET_TAB_V91	MON_GET_PKG_CACHE_STMT	MON_GET_PKG_CACHE_STMT
SNAP_GET_TBSP_V91	MON_FORMAT_LOCK_NAME	MON_FORMAT_LOCK_NAME
SNAP_GET_CONTAINER_V91	WLM_GET_SERVICE_CLASS_AGENTS_V97	WLM_GET_SERVICE_CLASS_AGENTS
SNAP_GET_DYN_SQL_V91	MON_GET_WORKLOAD	MON_GET_WORKLOAD
	MON_GET_TABLESPACE	MON_GET_TABLESPACE
	ENV_GET_DB2_SYSTEM_RESOURCES	ENV_GET_DB2_SYSTEM_RESOURCES
	ON_GET_SERVICE_SUBCLASS_DETAILS	MON_GET_SERVICE_SUBCLASS_DETAILS
	MON_FORMAT_XML_TIMES_BY_ROW	MON_FORMAT_XML_TIMES_BY_ROW
	MON_GET_UNIT_OF_WORK	MON_GET_UNIT_OF_WORK
	MON_GET_BUFFERPOOL	MON_GET_BUFFERPOOL
	MON_GET_TABLE	MON_GET_TABLE
	MON_GET_CONTAINER	MON_GET_CONTAINER
	MON_GET_FCM_CONNECTION_LIST	MON_GET_FCM_CONNECTION_LIST
	MON_GET_CONNECTION	MON_GET_CONNECTION
		MON_GET_MEMORY_POOL
		MON_GET_MEMORY_SET

Table 16. Permissions — Version-specific

9.5	9.7.0.1	10.1
	SNAP_GET_TBSP_V91	SNAP_GET_TBSP
	SNAP_GET_DB_V91	MON_GET_TRANSACTION_LOG
		SNAP_GET_DB
		DB2_GET_INSTANCE_INFO
		ADMIN_GET_STORAGE_PATHS

Table 17. Permissions - 10.5 and later

10.5 and later
ENV_GET_SYSTEM_RESOURCES
MON_GET_INSTANCE
MON_FORMAT_LOCK_NAME
MON_GET_PKG_CACHE_STMT
MON_GET_AGENT
MON_GET_WORKLOAD
ENV_GET_DB2_SYSTEM_RESOURCES
MON_GET_DATABASE
ADMIN_GET_STORAGE_PATHS
DB2_GET_INSTANCE_INFO
MON_GET_TRANSACTION_LOG
MON_GET_CONNECTION
MON_GET_FCM_CONNECTION_LIST
MON_GET_CONTAINER
MON_GET_TABLE
MON_GET_BUFFERPOOL
MON_GET_UNIT_OF_WORK
MON_FORMAT_XML_TIMES_BY_ROW
MON_GET_SERVICE_SUBCLASS_DETAILS
MON_GET_TABLESPACE
MON_GET_MEMORY_POOL
MON_GET_MEMORY_SET

Grant **Select** on these SYSIBMADM administrative views:

- DBPATHS*
- REG_VARIABLES
- BP_HITRATIO
- DBCFG
- ENV_GET_PROD_INFO
- MON_LOCKWAITS*
- SNAPDBM
- SNAPFCM
- SYSIBMADM.ENV_PROD_INFO

* For DB2 version 9.7.0.1 or later

PureScale environments

Grant **Execute on** to these table functions:

- MON_GET_CF
- MON_GET_GROUP_BUFFERPOOL
- BP_HITRATIO

Grant **Select** on these views:

- ENV_CF_SYS_RESOURCES
- SNAPDB
- SYSIBMADM.DB2_MEMBER

Permissions for Azure SQL Database

Foglight for Azure SQL can be used for granting permissions on several levels.

The following sections detail the permissions that can be granted to users of Azure SQL at each level, and instruct how to manually run the grant privileges script.

Granting Permissions to Azure SQL Users

Database-level Permissions

The following permissions are granted at the database level:

- CREATE USER—the lowest permission level, which only allows accessing each database for reading its metadata.

  IMPORTANT: The CREATE USER permission does not come as part of the script, as the command is not supported as part of a batch in Azure SQL.

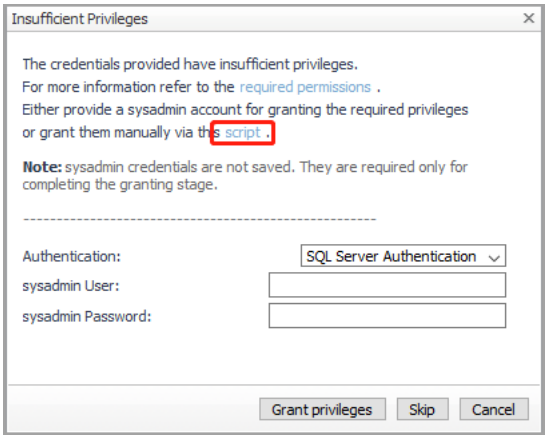
- VIEW DATABASE STATE—required for reading metadata information.
- db_datareader—allows creating user-defined SQL queries for monitoring purposes, via the User-defined Collections global administration screen.

Running the Grant Permissions Script

The file used for granting permissions manually, *SQLAzureGrantPrivilegesScript.sql,* can be downloaded by clicking the link View script under the Instances table, accessible via either of the following methods:

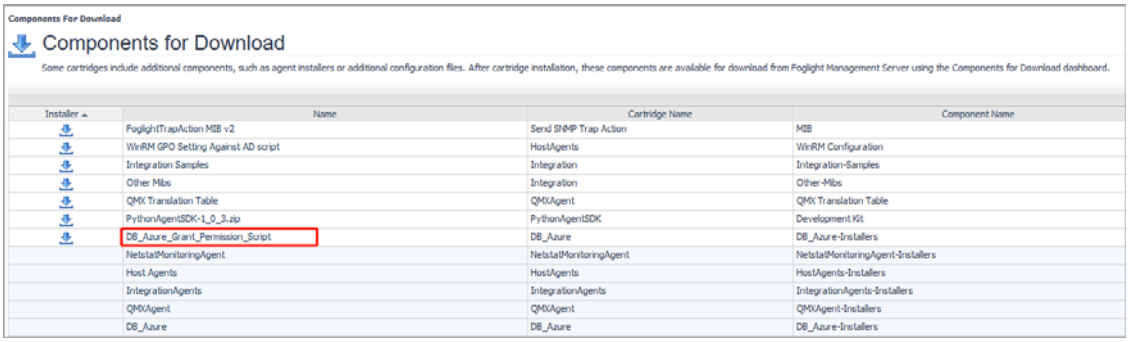
- When running the Monitor Azure SQL Database wizard, the script link is in the *Insufficient Privileges* dialog screen.

Figure 2. Insufficient Privileges dialog



- In the Cartridges - *Components for Download* screen.

Figure 3. Components for Download



> **IMPORTANT:** Running this file requires one of the following server roles:
> - Server admin
> - Active Directory admin
> - Member of the db_owner

To manually run the Grant Permissions script:

1. Run the CREATE USER command on a database to be monitored.

   Upon successful completion of this command, the login becomes a user in the specific database, and therefore able to read the database's metadata.

2. Open the *DBSS_Azure_Permissions_User_Databases.sql* file in SQL Server Management Studio (SSMS).
3. Find the *Select@LoginName = ?* section at the beginning of this file.
4. Replace the question mark with the login name to which the requested permissions are to be assigned.
5. Execute the script.

Permissions for monitored operating systems

For details, see the following topics:

- General Unix requirements
- VMware permissions
- Windows permissions

General Unix requirements

The OS user account for each agent requires:

- Silent log-in — in particular, there must be no user-input required and no special login banners displayed
- For connections using SSH, the sshd daemon must be installed and running.

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

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

Linux/UNIX permissions

Table 18. Linux/UNIX Permissions

Permission	Linux®	Solaris®	AIX®	HP-UX
Execute	awk	awk	awk	awk
	df	db2ptree	df	bdf
	free	df	head	bindprocessor
	getconf	head	hostname	getconf
	head	hostname	iostat	head
	hostname	iostat	lsattr	hostname
	iostat	lsnrctl	lsdev	ioscan
	lsnrctl	mpstat	lsnrctl	iostat
	netstat	uptime	netstat	lsattr
	ps	netstat	oslevel	lsdev
	sed	pagesize	pagesize	lsnrctl
	tail	ps	ps	netstat
	sysstat	psrinfo	tail	oslevel
	uname	tail	uname	pagesize
	uptime	uname	uptime	ps
	vmstat	vmstat	vmstat	sar
	/proc/	/usr/sbin/prtconf		tail
				uname
				uptime
				vmstat
				/usr/sbin/

Table 18. Linux/UNIX Permissions

Permission	Linux®	Solaris®	AIX®	HP-UX
Read	cpuinfo free* getconf sysstat package* /proc /proc/cpuinfo* /proc/net/dev /proc/stat /proc/vmstat on Linux >= 2.6			/var/adm/syslog/syslog.log

VMware permissions

To monitor VMware®, users must have **read only** access to the virtual center.

Windows permissions

Foglight support monitoring Windows® operating system in one of two ways: WinRM and WMI. The preferred method is WinRM when no WinRM connection WMI connection is used.

WinRM (default) - Based on Kerberos authentication or Basic authentication uses standard HTTP headers. For more information, see http://support.quest.com/technical-documents/foglight-agent-manager/5.9.5/foglight-agent-manager-guide/advanced-system-configuration-and-troubleshooting/configuring-windows-remote-management-winrm.

WMI (fallback) — Permission to access both DCOM and WMI. For more information, see

http://support.quest.com/technical-documents/foglight-agent-manager/5.9.5/foglight-agent-manager-guide/advanced-system-configuration-and-troubleshooting/configuring-windows-management-instrumentation-wmi.

2

Install the DB cartridge and DB agent

This section includes details about the following topics:

- Install the DB cartridge
- Install a single DB agent

Install the DB cartridge

Foglight for database cartridges run on the Foglight Management Server, which is the operation framework. Therefore, Foglight Management Server must be installed before installing a database cartridge.

To install the Foglight for <database> cartridge:

1. Copy the cartridge car file included in the installation media to your local computer. This file is named as follows:
   - For Foglight for DB2 LUW: DB_DB2-5_9_5_10.car
   - For Foglight for Oracle: DB_Oracle-5_9_5_10.car
   - For Foglight for SQL Server: DB_SQL_Server-5_9_5_10.car
   - For Foglight for Azure SQL Database: DB_Azure-5_9_5_10.car
2. Log in to the Foglight browser interface.
3. On the navigation panel, click **Dashboards > Administration > Cartridges > Cartridge Inventory**.
4. On the Cartridge Inventory dashboard, click **Install Cartridge** to find the CAR file on your local computer.
5. Click **Install Cartridge**.

Install a single DB agent

For details, see the following topics:

- Install a single SQL Server or Oracle agent
- Install a single DB2 agent
- Install a single Sybase agent
- Install an Azure SQL DB agent

Install a single SQL Server or Oracle agent

To install a single SQL Server or Oracle agent:

1. On the Foglight navigation panel, click **Homes > Databases**.
2. Click **Monitor > <DB type>** in the lower left corner of the Databases View.

   The Monitor Instance dialog box appears.
3. Choose the agent manager on which the agent is running. The default is the agent manager with the least agents installed.
4. On the Monitor Instance pane, provide connection details.
5. Select an Alarm Sensitivity Level to determine what level of alarms the system stores and displays for this instance.
6. Optional SQL PI- In the Monitoring Extensions pane, click the SQL PI monitoring extension. You are prompted to choose the Agent Manager on which the SQL PI repository is installed.
7. **Optional OS**. In the Monitoring Extensions pane, click the **Operating System** link. To configure the extension, choose the connection details of the host on which the SQL Server instance is running.
8. **Optional VM**. In the Monitoring Extensions pane, click **Collect VM** statistics. To configure the extension, select the connection details of the vCenter® or ESX® on which the SQL Server instance is running.
9. Click **Monitor**.

Install a single DB2 agent

To install a DB2 agent:

1. On the Foglight navigation panel, click **Homes > Databases**.
2. Click **Monitor > DB2** in the lower left corner of the Databases View.

   The Monitor Instance dialog box appears.
3. Follow the prompts to configure an agent to monitor the DB2 host, instance, and databases. For help with options, click the **'i'** icon.

IMPORTANT:
1. When DB2 authentication type is CLIENT, the login credentials provided during installing for the database agent are overwritten with the fglAM user. Ensure that the fglAM user can connect to the DB2 instance and has all the relevant permissions as described in the Permissions section.
2. When trying to connect to DB2 instance with SSL, import SSL certificate into FglAM first. Go to directory `<FglAM_HOME>/agents/DB_DB2/<DB2_version>-<DB2_version>-<BUILD_ID>/lib/`, run command `certificate-<DB2_version>-ksh.ksh(certificate-<DB2_version>-bat.bat)`

Install a single Sybase agent

To install a Sybase agent:

1. On the Foglight navigation panel, click **Homes > Databases**.
2. Click **Monitor > Sybase** in the lower left corner of the Databases View.

   The Monitor Instance dialog box appears.
3. Follow the prompts to configure an agent to monitor the Sybase host, instance, and databases. For help with options, click the **'i'** icon.

Install an Azure SQL DB agent

To install an Azure SQL DB agent:

1. On the Foglight navigation panel, click **Homes > Databases**.
2. Click **Monitor > Azure SQL** in the lower left corner of the Databases View.

   The *Monitor Azure SQL Database* dialog box appears.
3. Follow the prompts to configure an agent to monitor the Azure SQL host, instance, and databases. For help with options, click the **'i'** icon.

3

Special configurations

This section documents the product settings required for special configurations:

- Foglight Upgrades
- High Availability
- Federation
- Concentrator (Proxy)

Foglight Upgrades

If your environment has either of the following deployments, contact your Account Manager or Quest Support prior to performing the Foglight Management Server upgrade:

- More than 50 monitored instances
- Federation
- High Availability (HA)

High Availability

The *Foglight High Availability Field Guide* is available online at:

http://support.quest.com/technical-documents/foglight/5.9.5/high-availability-field-guide/

NOTE: HA is not supported for:

- Sybase Agents
- SQL PI repositories

Federation

The Foglight Federation Field Guide is available online at:

http://support.quest.com/technical-documents/foglight/5.9.5/federation-field-guide/

Concentrator (Proxy)

Information is available online:

- **Agent Manager —** http://support.quest.com/technical-documents/foglight-agent-manager/5.9.5/foglight-agent-manager-guide/configuring-the-agent-manager/configuring-an-agent-manager-instance-as-a-concentrator
- **DB agent —** Step by step configuration is provided in the “Configuring the On Demand Port on the Agent Manager Concentrator” section in the *Foglight for Oracle User and Reference Guide* and in the *Foglight for SQL Server User and Reference Guide*.

NOTE: Not supported for Sybase agents.

Table 1. Concentrator Agent Manager

Number of Agents	<100	<200
JVM Settings**	2048MB	4096MB
CPUs (2.4GHz)*	2 cores	4 cores
RAM*	4GB	6GB

CPUs (2.4GHz)* — for a virtual machine the CPU allocation must be reserved. The reservation is expressed in MHz

RAM*- for a virtual machine the memory allocation must be reserved.

*** —** After locating your hardware requirements in the tables, ensure that you complete the manual JVM Setting configuration as described in Manual configuration required by all users.

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit https://www.quest.com/company/contact-us.aspx.

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