



# Active Directory Monitoring for Foglight

## I. Monitoring Active Directory for Foglight

Monitoring Active Directory can be broken down to four sections: Monitoring the domain controller, monitoring the performance counters, monitoring the database counters, and monitoring the FRS counters. Those four sections are described below along with complete lists of their collectables. All of this data can be retrieved using a combination of standard Foglight agents and Performance Counter retrieval functionality. Note that all data is automatically published to the system performance counter manager except the database objects below, which require a specialized installation.

### I. Monitoring the Domain Controller.

Domain Controllers should always be generally monitored (processor utilization/disk/network load, etc). This can be done with standard Foglight Agents. If the domain controller is overloaded, then service levels will degrade. The domain controller houses the active directory database files, log files, and other related information.

## II. Active Directory Performance Counters

DRA Inbound Bytes Total/sec	Indicates the total number of bytes (per second) received through replication. It is the sum of the number of bytes of uncompressed data and compressed data.
DRA Inbound Object Updates Remaining in Packet	Indicates the number of object updates received in the current directory replication update packet that have not yet been applied to the local server. This counter indicates that the monitored server is receiving changes, but is taking a long time applying them to the database.
DRA Outbound Bytes Total/sec	Indicates the total number of bytes sent per second. This is the sum of the number

	of bytes of uncompressed data and compressed data.
DRA Pending Replication Synchronizations	Indicates the number of directory synchronizations that are queued for this server that are not yet processed. This counter helps determine the replication backlogthe higher the counter, the larger the backlog.
DS Threads in Use	Indicates the current number of threads in use by the directory service.
Kerberos Authentications/sec	Indicates the number of Kerberos authentications (per second) serviced by the domain controller.
LDAP Bind Time	Indicates the time (in milliseconds) required for the completion of the last successful LDAP binding.
LDAP Client Sessions	Indicates the number of sessions of connected LDAP clients.
LDAP Searches/sec	Indicates the number of search operations (per second) performed by LDAP clients.
LDAP Successful Binds/sec	Indicates the number of LDAP bindings (per second) that occurred successfully.
NTLM Authentications	Indicates the number of NTLM authentications (per second) serviced by the domain controller.

### III. Active Directory Database Performance Counters

Database performance object counters enable you to monitor the Active Directory database at an advanced level. These counters provide information regarding the performance of the database cache, database files, and database tables. You can use some of these counters to determine whether you need more hard disks to store additional Active Directory data.

The database performance counters for active directory must be explicitly installed by copying two DLLs and making some modifications in the registry. It is a simple 15 minute process.

Counter	Description
Cache % Hit	Indicates the percentage of page requests for the database file that were fulfilled by the database cache without causing a file operation.
Cache Page Fault Stalls/sec	Indicates the number of page faults (per second) that cannot be serviced because there are no pages available

Counter	Description
	for allocation from the database cache.
Cache Page Faults/sec	Indicates the number of page requests (per second) for the database file that require the database cache manager to allocate a new page from the database cache.
File Operations Pending	Indicates the number of reads and writes issued by the database cache manager to the database file or files that the operating system is currently processing.
File Operations/sec	Indicates the number of reads and writes (per second) issued by the database cache manager to the database file or files.
Log Record Stalls/sec	Indicates the number of instances (per second) that a log record cannot be added to the log buffers because the buffers are full.
Log Threads Waiting	Indicates the number of threads waiting for data to be written to the log so that an update of the database can be completed.
Table Open Cache Hits/sec	Indicates the number of database tables opened (per second) by using cached schema information.

#### IV. File Replica Set (change notification) Performance Counters

Counter	Description
Change Orders Received	Indicates the number of change notifications received from inbound partners.
Change Orders Sent	Indicates the number of change notifications sent out to outbound partners.
File Installed	Indicates the number of replicated files installed locally.
Packets Received	Indicates the amount of data received locally. These packets can be change notifications, file data, or other command packets.
Packets Sent	Indicates the amount of data sent. These packets can be change notifications, file data, or other command packets.
USN Records Accepted	Indicates the number of records that are accepted for replication. Replication is triggered by entries

## Counter

### Description

written to the NTFS change journal. FRS reads each file close record from the journal and determines whether to replicate the file.

An accepted record generates a change order, which is then sent out. A high value on this counter (about one every five seconds) indicates a lot of replication traffic, which can cause replication latency.