ARGENT
ENCYCLOPEDIA

Best Practices with Argent

Contents

System Requirements

To install Argent Extended Technology, the following minimum system requirements need be met.

- Windows 200x (2003 with latest service pack strongly recommended)
- Internet Explorer 6.0 or higher (7.0 is recommended)
- ADO 2.6 or higher
- 2 GB RAM (4GB recommended)
- 1 GB of disk space MINIMUM
- P4 Processor Equivalent or higher (SMP Supported)

Optional requirements for SQL database used by the products:

- SQL 7.0 or Higher
- Minimum 512 MB Database
- Minimum 512 MB Transaction Log

Optional Requirements for Oracle database used by the products:

- Oracle Server 8.0 or Higher
- Minimum 256 MB RAM

Optional requirements for the web products of Argent Business Manager/Argent Ninja

- IIS 4.0 or higher
- ASP.NET

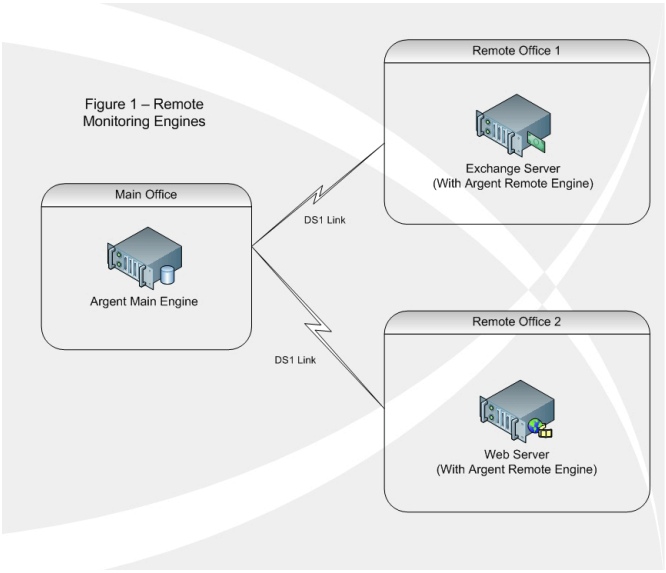
Virtualizing the main Argent Server or Argent Motors is not recommended

Remote Monitoring Engines

Deciding if and when remote Monitoring Engines should be deployed is an important consideration. Most of the time when servers are all located on the same physical network there is no need at all to deploy any remote Monitoring Engines. Argent's products are streamlined to provide maximum levels of monitoring with the least possible network bandwidth. However, there are some situations where a remote Monitoring Engine should be considered: The same rules apply when considering a remote Transfer Engine (the Argent Data Consolidator) or an Argent Exchange Monitor remote Monitoring Engine.

- Customer needs to monitor a group of devices on the other side of ANY network link less than 1.544MB (T-1) speed. Remote Monitoring Engines will help to minimize the traffic across these links.
- Customer needs to monitor devices where there is no TRUST RELATIONSHIP present between the devices.
- Customer needs to monitor devices on the DMZ or otherwise behind a firewall of any kind.

For more information on whether customers need to deploy any type of remote engine, please contact Argent Technical Service at at **http://help.Argent.com.**



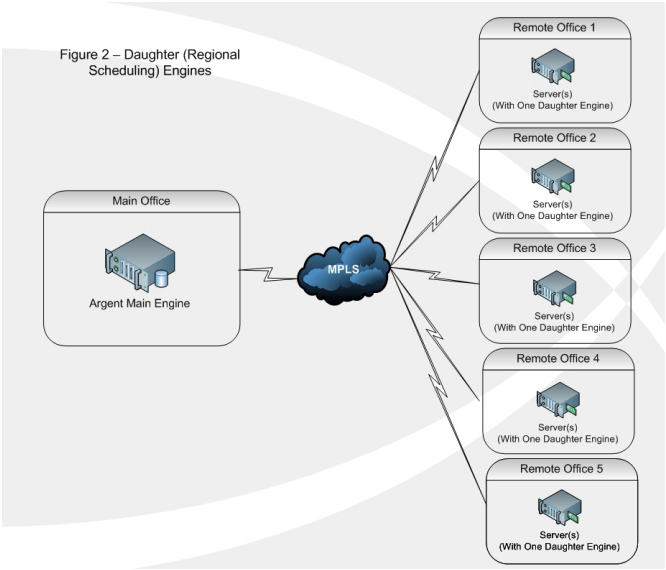
Daughter Engines

Daughter Engines (also known as Regional Supervising Engines) are nothing more than a remote monitoring engine with a companion Scheduling Engine installed. The goal with Daughter Engines is to minimize the SCHEDULING traffic between the main Argent server and remote locations. This also provides for a more robust system in situations where links between WAN sites fail.

A few situations where Daughter Engines should be considered

- Extremely poor or high-latency WAN links
- Scheduling load on the main Argent server needs to be minimized
- Widely distributed network (i.e. 20 or more WAN locations)

For more information on whether customers need to deploy any type of remote engine, please contact Argent Technical Service at at **http://help.Argent.com.**



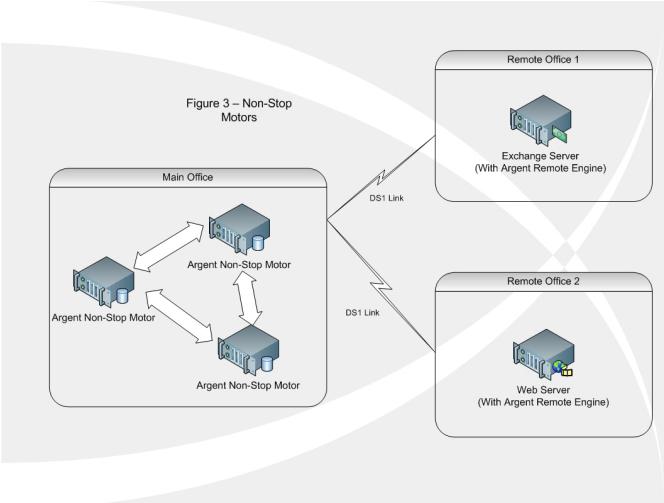
Non-Stop Monitoring

Non-Stop Monitoring is now available for the Argent Console and the Argent Guardian.

The processing for all Monitoring tasks can be shared among a pool of load-balanced Mother Engine servers, all sharing the same backend ODBC database, increasing load-balancing, expanding scalability, and improving reliability.

For clarity, the term “Argent Motor” is used to describe a monitoring server that processes work from the common pool.

The system requirements for each Argent Motor are identical to those for ANY main engine.



For more information on whether customers need to deploy Non-Stop Monitoring for their environment, please contact Argent Technical Service at **http://help.Argent.com.**

What to Monitor On All Servers

Daughter Engines (also known as Regional Supervising Engines) are With well over 3,000 Rules present in the current release of the Argent Guardian, deciding what to monitor on all of the servers must be well planned.

Of Course, the specific variables to monitor will vary from user to user. Customers must decide whether to alert when a CPU is hung at 100% or when it is hung at 90%. Argent Technical Services will be glad to assist customers with making these decisions.

There are several things that customers should monitor on ALL of their servers, regardless of their applications or purpose.

It is VERY IMPORTANT to note that Argent has the capability to monitor, alert, and trend on ANY performance counter on ANY server if that counter is available through Windows Performance Monitor or WMI.

Windows provides over 6,500 unique counters as of the release of Windows 2008. Choosing which ones to use takes a little thought.

Some very important metrics and performance counters include the following:

- SLA availability (Using the TOD API call if Windows)
- SERVICES deemed critical to your environment
- CPU Utilization
- Memory Utilization (% Committed Bytes In Use + Pages Per Second)
- Disk Space consumption.
- Disk Performance (Average Disk Queue Length – Physical Disk)
- Network Performance (Current Commands of Redirector)
- Cache Hit Ratios
- Errors and Warnings in Event Logs
- Security Audit Failures in the Event Logs

For additional information on building baseline rules, please check **http://help.Argent.com.**

What to Monitor On Domain Controllers

Windows 200x domain controllers have some specific metrics that should be watched closely, and Argent has all of these covered for customers.

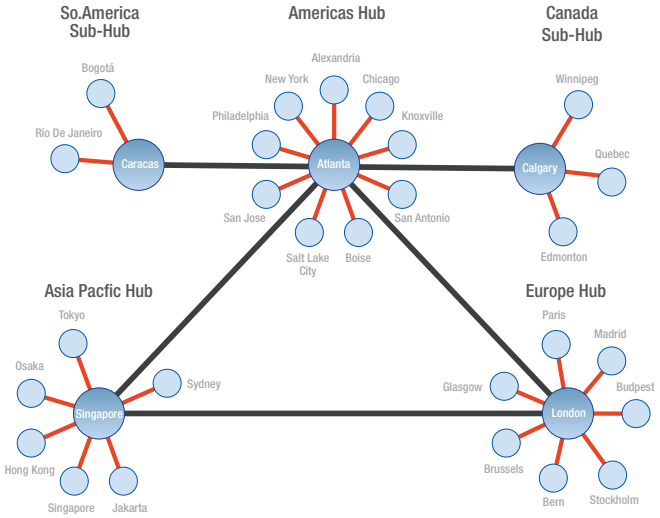
Some specific things customers should consider while monitoring their domain controllers:

Active Directory Rules present in the Argent Guardian:

Pending Active Directory Synchronizations (Found in PERFORMANCE Rules under the PRF_AD group.

DNS / WINS / DHCP services (where applicable).

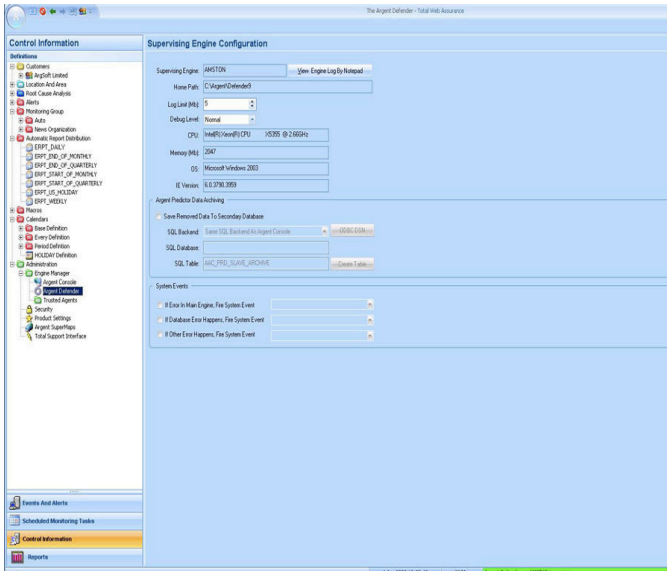
More extensive auditing of the SECURITY logs on a regular basis (using the Argent Data Consolidator



What to Monitor On IIS Servers

When deciding what to monitor on the IIS servers, customer choices may depend on variables such as whether the device is an internal or an external web-server and on the exact purpose of the sites located on the devices. Following are some general guidelines with regard to items customer should always keep track of on the IIS servers:

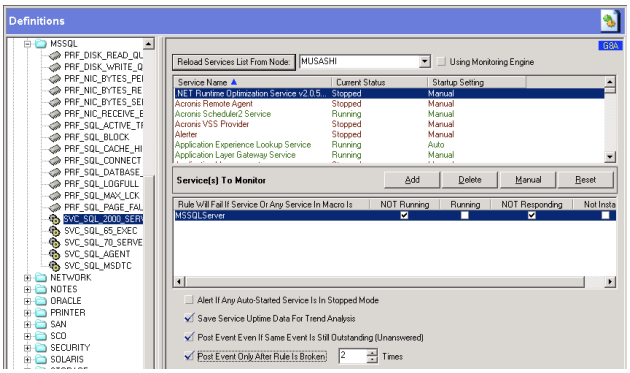
- IIS Services (using Service Rules)
- IIS Performance Statistics (using the Performance Rules PRF_IIS)
- Monitoring of the IIS logs on the IIS servers to watch for failed logons
- Use of a System Down / SLA Rule to scan port 80 (or other HTTP port)
- **Use of the Argent Defender to monitor the web applications themselves.**



The screenshot below shows the Argent Defender GUI.

For more information on the Argent Defender, please visit Argent website, **www.Argent.com.**

What to Monitor on SQL Server



Microsoft SQL Server can present some unique challenges to monitoring, as the size, use,and database specifications on these servers can vary widely from company to company.

Following are some items that customers should always monitor on their SQL servers.

Consult with the DBA for additional requirements.

- SQL Services (using Service Rules).
- SQL Performance Statistics (using Performance Rules).

  Specifically, watch items such as TOTAL SQL SERVER MEMORY, LOCKS, and BLOCKS. With SQL 2000, monitoring of database sizes has become less important (due to the auto-grow feature).
- SQL Server Errors logged to the Event Logs. Use the Argent Data Consolidator.
- Information logged to the TEXT based SQL logs (such as job completions, DTS Packages, etc). Use the Argent Data Consolidator.

What to Monitor on Microsoft Exchange

Argent monitors and corrects all of the common Microsoft Exchange issues with the introduction of the Argent ExchangeMonitor.

And Argent handles all versions of Exchange from 5.5 to the 64-bit Exchange Server 2007.

Using this product, customers can monitor, report, and alert on literally hundreds of specific metrics. Some things that all Exchange Administrators should keep track of are shown below.

Some very important metrics and performance counters include the following:

- Server up and down status for the Exchange Server (using PING, API and MAPI logon).
- Exchange services (using Service Rules).
- Exchange protocol handshaking (using customized port scanning).
- Total Information Store Size.
- Size of the PRIVATE information Store(s).
- Size of the PUBLIC information Store(s).
- SMTP Queue Lengths
- Total IMAP connections (if applicable)
- Size and last access time for every or some mailboxes.
- Message Traffic levels between Sites / Domains at LEAST every 24 hours.
- Top 25 Senders / Receivers (locating abusers).
- Average Disk Queue Length (Especially on LARGE Exchange environments).
- Round-Trip Test Rules (to show when Email delivery is taking too long).

Remember that with Exchange 2007, you will be dealing with 64-bit only performance counters. You may need to modify some of your Exchange monitoring rules once you migrate to this new Exchange architecture.

UNIX Servers

Argent Engineers have decades of experience managing, maintaining, and tuning UNIX servers of numerous different types including Linux, Solaris, AIX, HPUX, SCO, SUSE, and others.

The TOP counters you should monitor on all your UNIX servers are as follows:

- Disk Space
- Swap Space
- CPU Utilization
- Network Bandwidth
- Failed Logon Attempts
- SUID Scripts owned by ROOT
- Password Aging
- Trusted Host Settings
- NFS Mount Settings
- System Load

Argent can customize UNIX shell scripts for you at no additional charge. Visit **http://help.Argent.com** for more details.

Other Servers and Devices

Argent will always attempt to provide customers with the Rules they need. If customers have a specific platform or hardware device that needs to be monitored, but do not see the Rules, contact Argent Technical Services for assistance at **Support@Argent.com** or online at **http://help.Argent.com.**

There are thousands of different platforms and hardware devices that could be monitored with Argent products.

When requesting a new set of custom rules, it may be faster to try building the rule yourself.

Almost all modern applications and services such as Symantec, BackupExec, Acronis, Cisco Call Manager, and many others ALL have their own specific performance counters when they are deployed to a Windows server.

Due to recent advances in the Argent Extended Technology Products GUI, creating these custom rules has never been easier. It takes less than 30 seconds to create a new rule from scratch.

The "How Often" Question

One of the questions Argent Engineers hear on a regular basis is "How often do I monitor XXXX?"

This is a tough question to answer, because every environment is different, but there are a few things to keep in mind when setting schedules for your monitoring policy.

- SLA metrics usually introduce a negligible amount of traffic on the LAN / WAN. There is nothing wrong with pinging devices every single minute. The more frequently polling is done, the more data is logged in the database.

- Performance variables will vary widely in their frequency… Monitoring CPU utilization should be done more frequently (say every 5-15 minutes), while a counter that does not change too frequently (% disk space) may be monitored every 4 hours.

  Keep this in mind when saving performance counters to the Argent Predictor database…

  Imagine 100 servers all have 5 logical disks. Relators are trending % Free Space and % Disk Time on all 5 logical disks every 5 minutes. That's 2 counters with 5 instances on 100 servers every 5 minutes. How many lines of data are being logged per hour?

  100 Servers X
  2 Counters X
  5 Instances
  = 1,000 data points every 5 minutes.
  That's 12,000 per hour. 288,000 per day.

  Always take database space into consideration, and implement a GOOD database maintenance plan.

- Consolidating event logs can be bandwidth intensive and use a lot of disk space if not done properly. It is ALWAYS best to consult **http://help.Argent.com** if there are any questions.

  Typically event log entries on a Windows server average 300 bytes each. If you consolidate 10,000 events per hour, that equals 2.86 Megabytes per hour. Add it all up and you get 66.86 Megabytes per day, or 195.80 GIGABYTES per year.