ARGENT
ENCYCLOPEDIA

Automated End-to-End Monitoring

Contents

Introduction

Argent has been in the systems management business since 1991 and has over 2,000 customers worldwide such as Walt Disney, Honda, Toyota, IBM, Hewlett Packard, Bayer the aspirin people, Nokia, CBS, the Social Security Administration, Wells Fargo, and Harley Davidson. Argent is over 19 years old and is a private company with no debt and no outside financing.

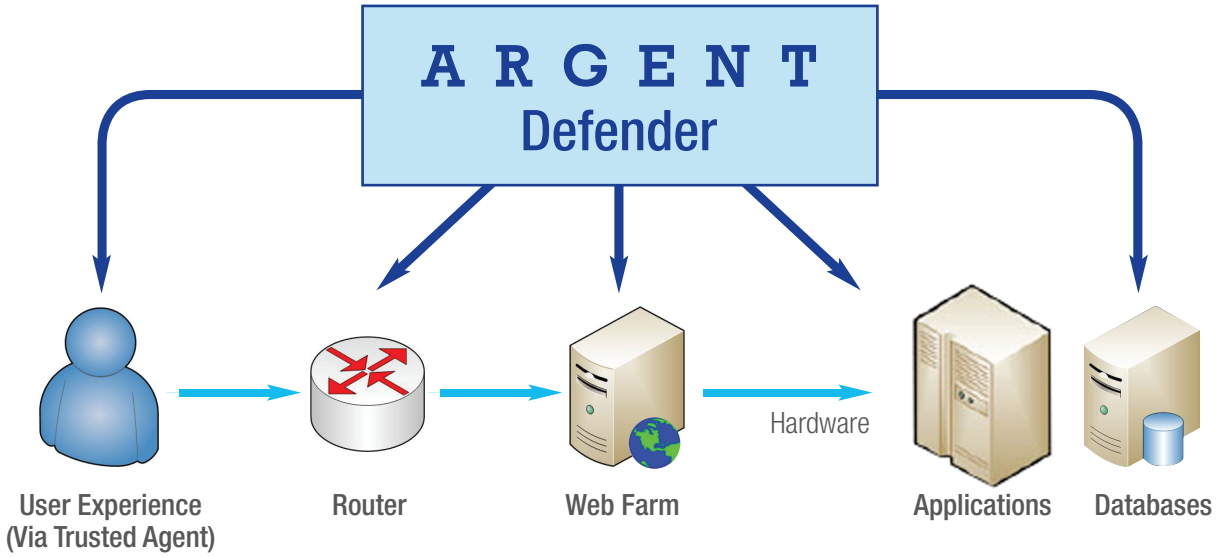
Argent provides automated end-to-end monitoring in two of Argent's flagship products - **Argent Defender** and **Argent Extended Technology**.

Automated End-to-End Monitoring Overview

- Enterprise Monitoring and Alerting
- Intranet and Web Optimization
- Centralized Consoles
- Scalable - Monitor 10 to 10,000 servers
- Agent-Optional Architecture
- Monitor all platforms: Windows, Linux/UNIX, etc.

Argent Defender

The Argent Defender is a complete solution for your Internet web sites or intranet apps.



When your critical online resources slow or crash, your business or department crashes as well.

Your online resources are your business.

Often, “coolness” trumps Total Web Assurance - the screens get all the attention, and the underlying infrastructure is ignored, creating an online resource that does not scale and is unreliable.

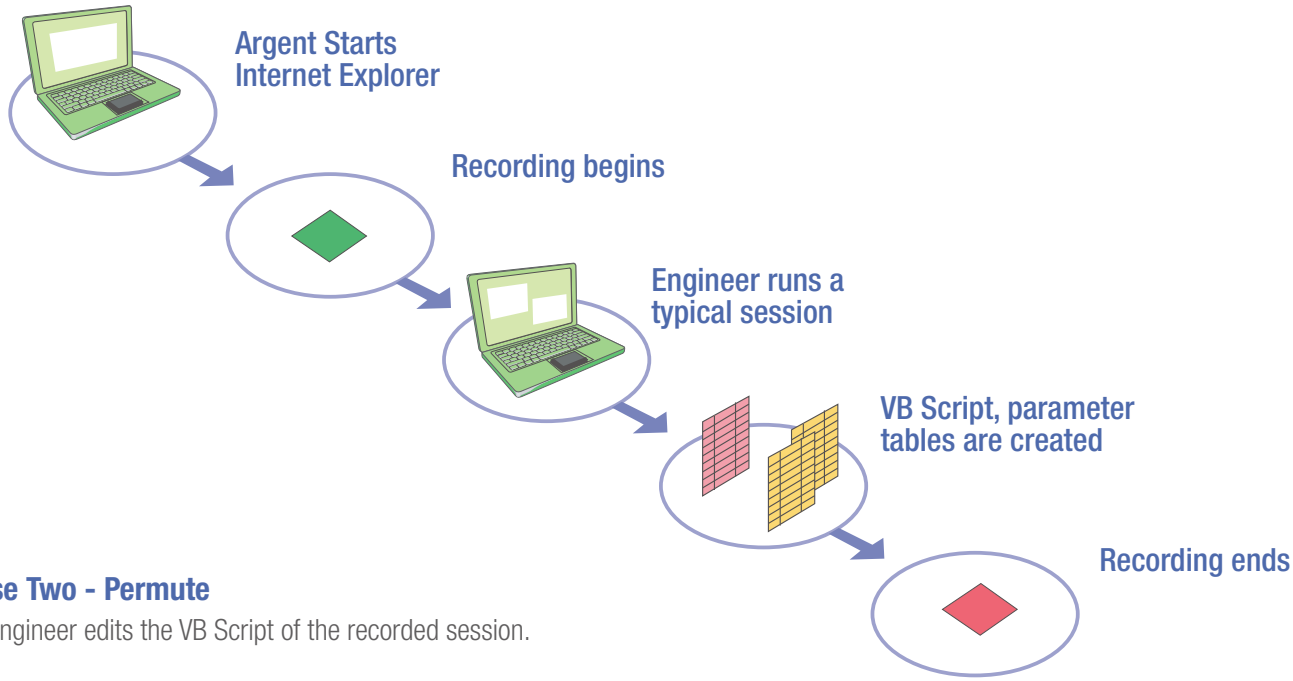
Here's how Argent Defender works:

Phase One - Record

Argent Defender loads Internet Explorer.

Every keystroke, mouse-click, and web page is recorded by Argent as a VB Script.

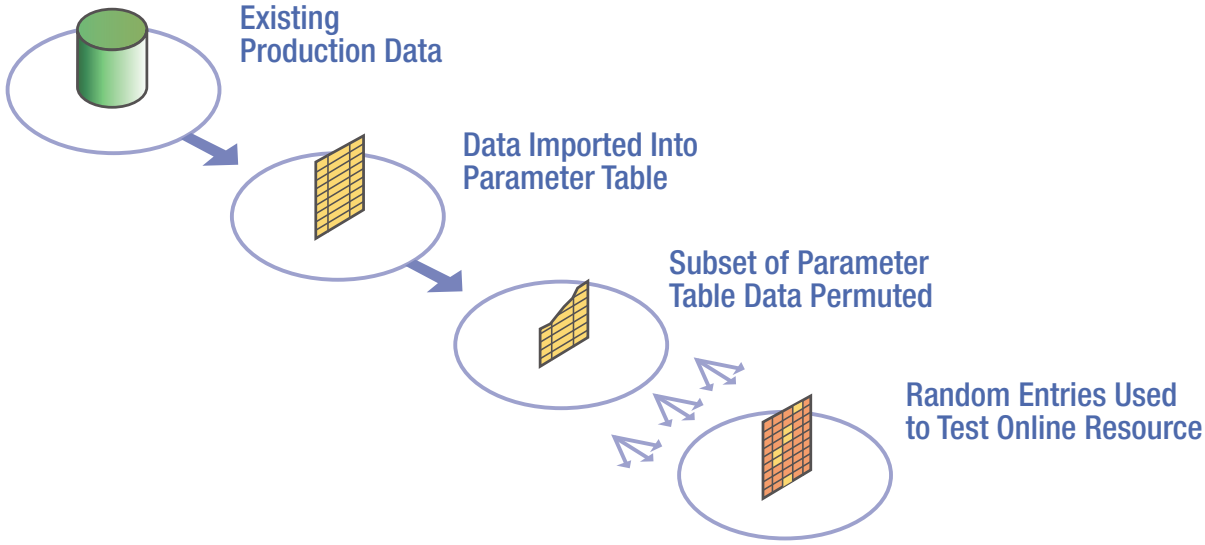
Every time a variable is entered, such as a Customer Id, it is recorded in the Argent parameter table.



Phase Two - Permute

The engineer edits the VB Script of the recorded session.

The Parameter Table is randomized for completely realistic testing - Argent feeds different data to the web site or intranet being tested.



Phase Three - Test and Monitor

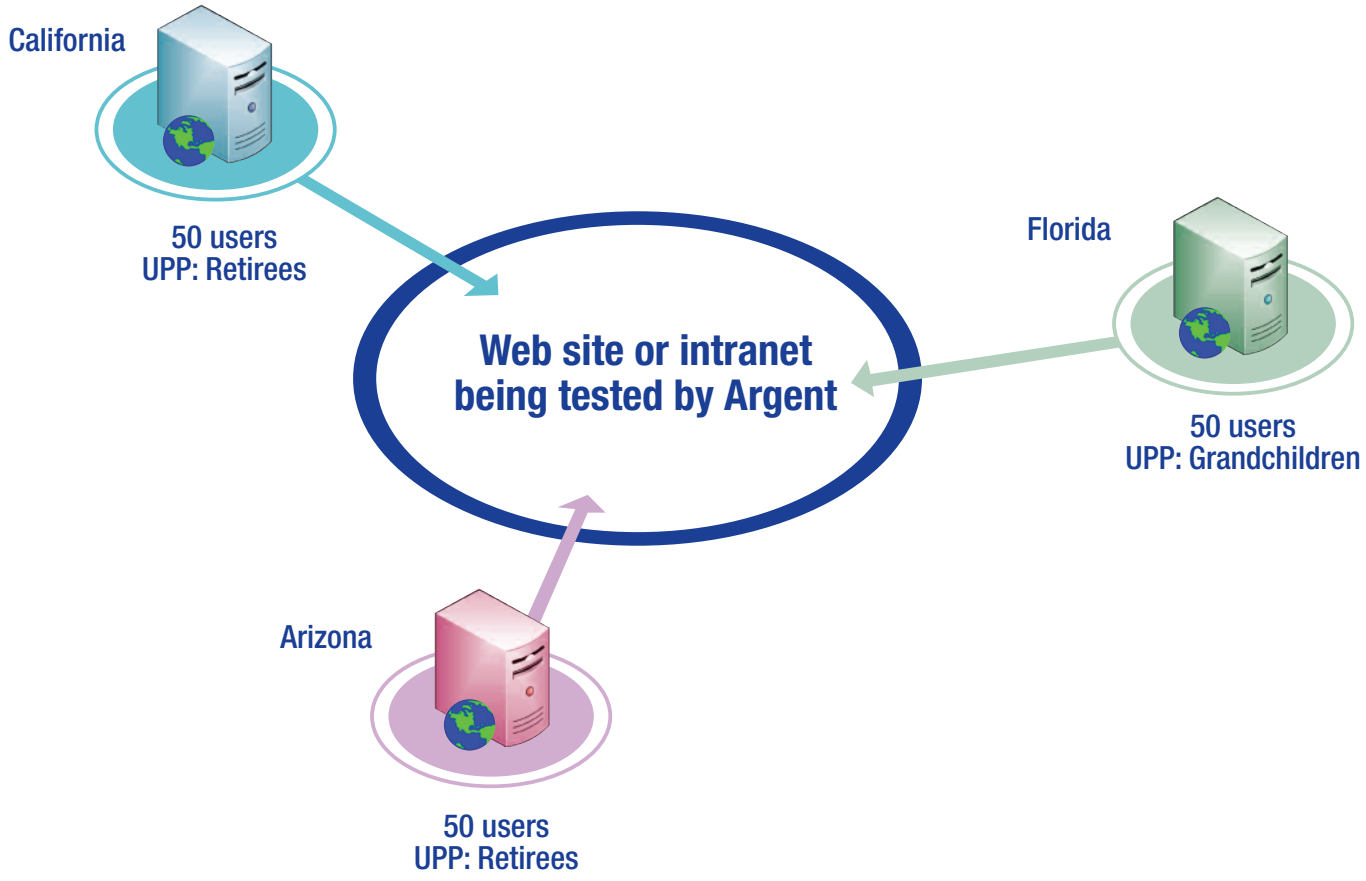
The length and time of the test are defined.

Assume the web site is for retirees in Florida, Arizona, and California and consists of 20 Solaris servers at Two Penn Plaza in Manhattan.

Under your control, Argent replays your scripts in Florida, Arizona, and California (You can replay an unlimited number of different scripts in one test.)

Argent is monitoring everything, from the Solaris machines to the Internet.

Once the test completes, Argent describes the bottlenecks and capacity of the web site or intranet.



Pre-Production

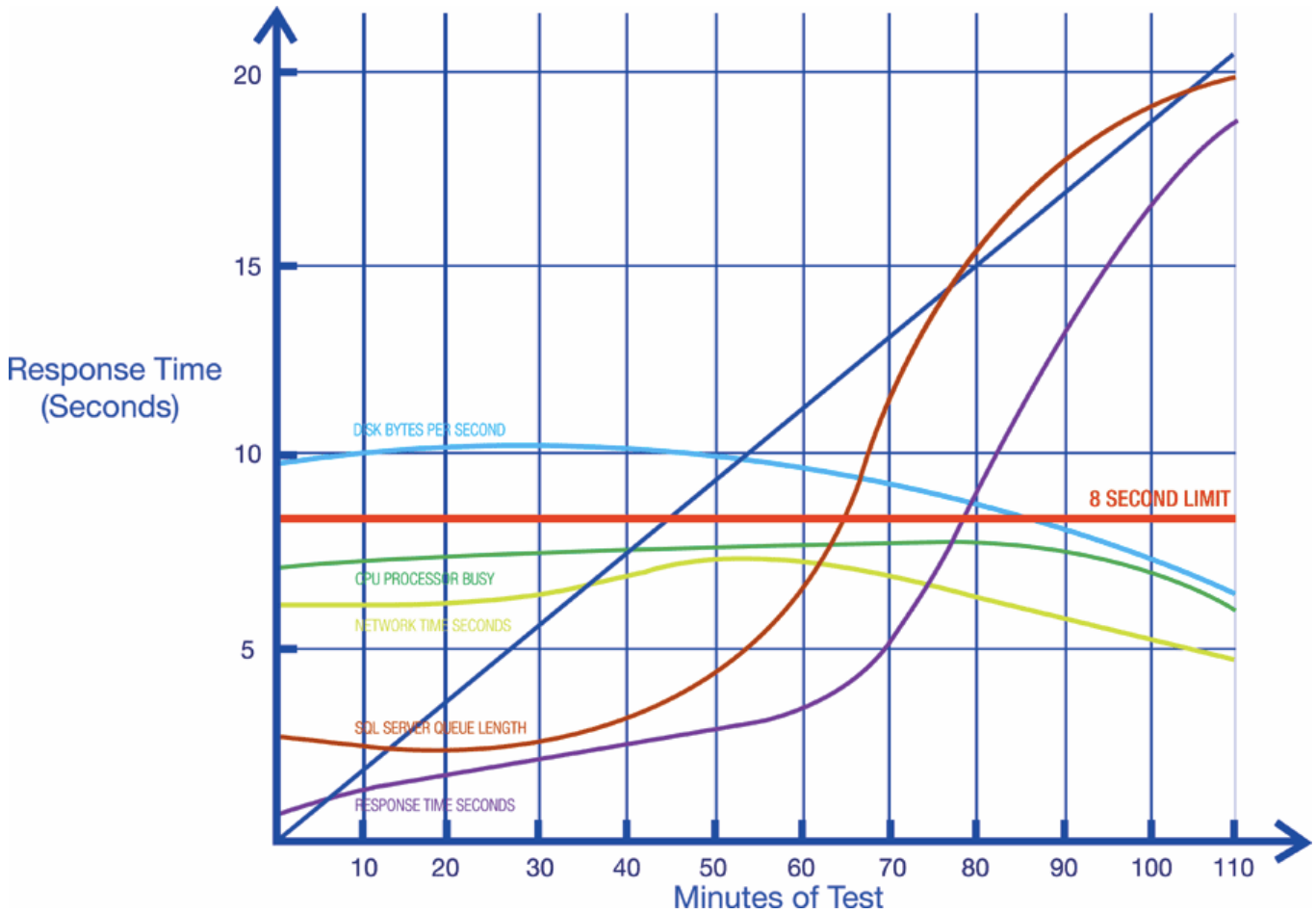
Before you go live, Argent lets you completely test your soon-to-be-live online resource.

Example

Let's assume your test is for two hours. Over those two hours, Argent slowly increases the load - the number of transactions per minute. (That's the straight line in the graph.)

As this load is increased, Argent records all critical metrics and displays them on a single screen in real time. Instead of masses of undigested raw data, **you get a single screen telling you all you need to know.**

By slowly increasing the load over the test period, the traits of the complete environment are shown - how each critical resource changes.



Only Argent has UPPs - Unique Personality Profiles - the ability to perfectly mimic different types of humans. **After all, the goal is to make your testing identical to your actual users.**

So if you're a web site for teenage boys, Argent will go screen-to-screen in milliseconds.

If your web site is for brides-to-be, then it will be at the rate these young ladies read the pages - minutes, not milliseconds. If it's an internal intranet then Argent mimics perfectly these adult users as well.

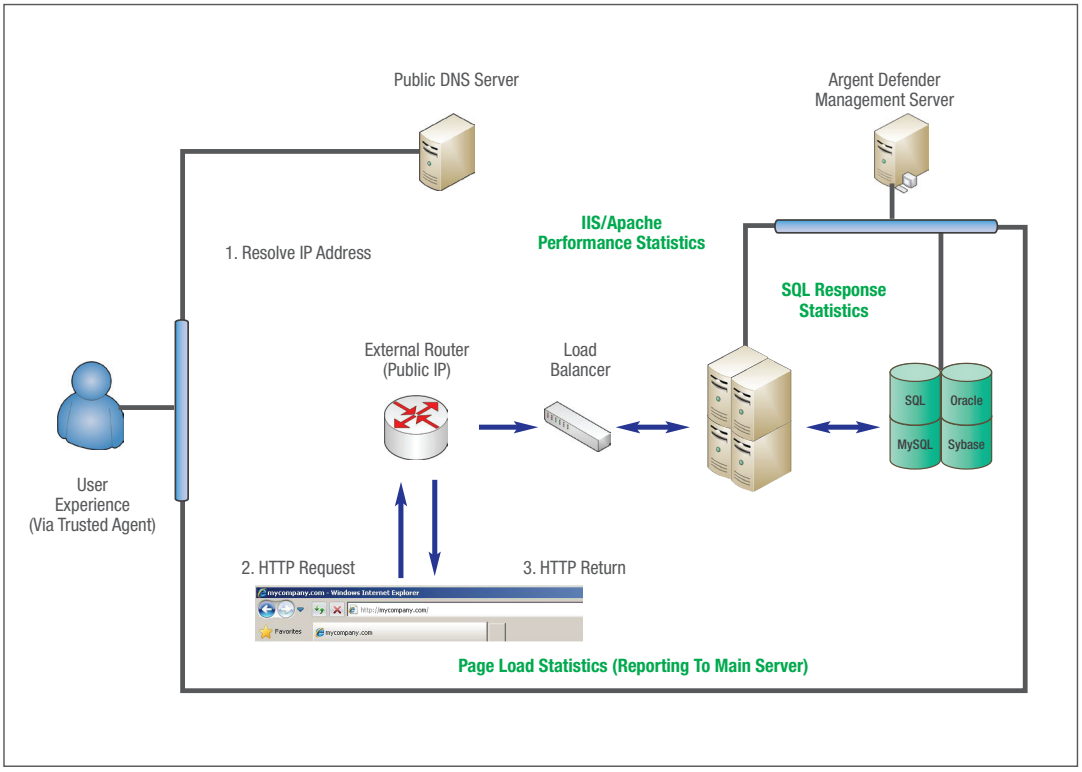
Post-Production

Once in production your needs are precisely the same as in testing, with one critical difference: the load.

In pre-production testing, the load was designed to overwhelm and to deliberately break the nascent online resource. Obviously in production the opposite is true.

A unique benefit of Argent is all work done in the pre-production phase is re-used in the production phase. The only change is the load - rather than pumping in 10,000 complete transactions a minute, it's two transactions per minute. So all the time and money invested in the pre-production phase is not wasted.

And when the next version or release of the online resource is ready, you already have a complete set of regression tests.



One of the first things to determine is your **requirements**.

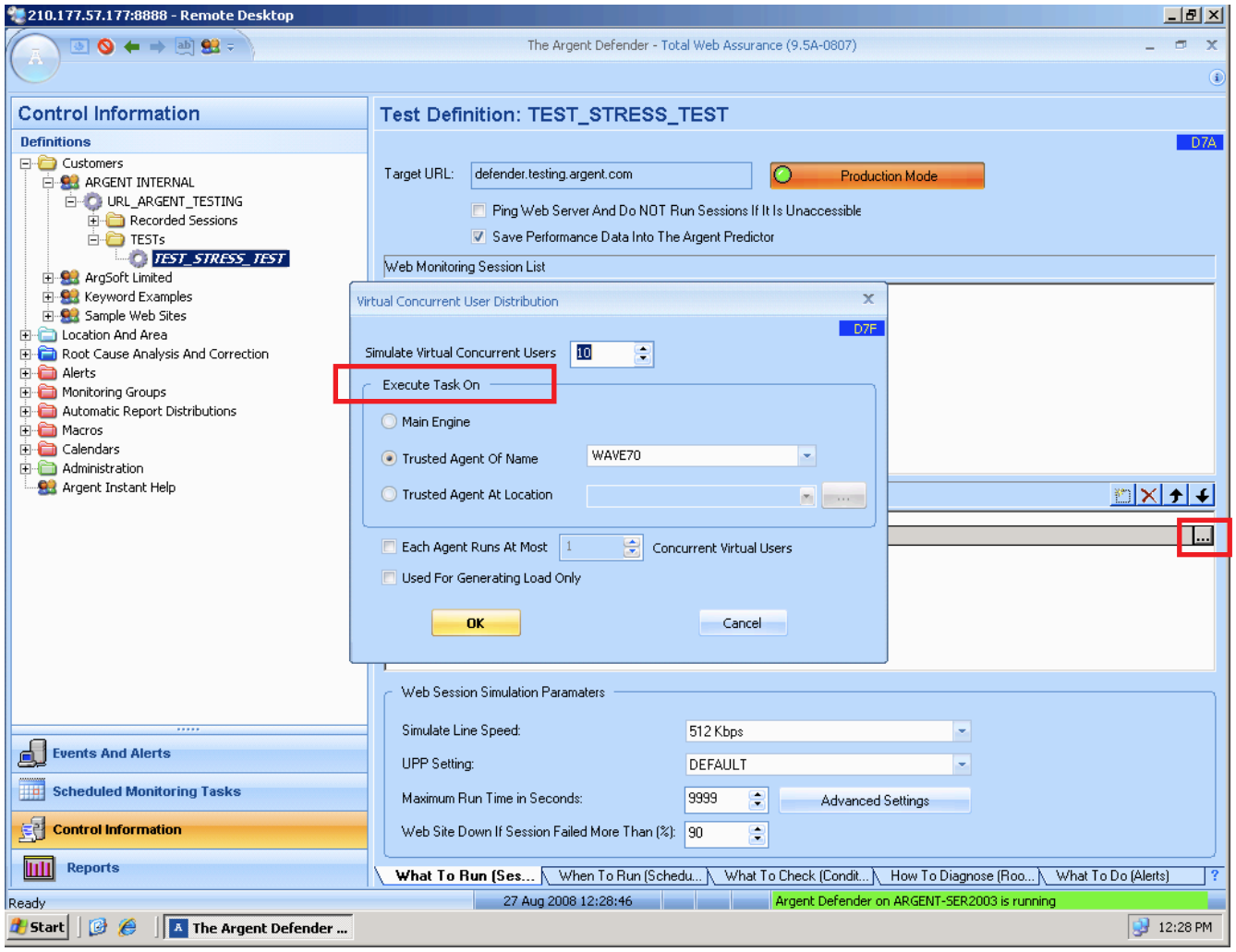
Here are a few things to think about:

1. Is your site a **pre-production** or **production** site?
2. Are you interested in monitoring the logic behind your web pages, or monitoring the user experience and response times?
   Are you interested in testing the performance metrics of the **web server or server farm** itself?
3. What about stress testing? Do you need to simulate personalities to match your audience?
   What about running multiple concurrent users to create a synthetic load on your site?
4. Where is your intended audience? Do you want to drive tests in multiple locations around the world?
5. Think about which features need to be tested. Do you need to test the login (and thus the database), or just your home page response time? What about testing online transactions?
6. How often do you want to perform these tests? Think about the criticality of this feature on your site.
7. If an issue occurs, how would you like to be alerted?
   Would you like the Argent Defender to proactively resolve the issue for you?
   Are you interested in having Argent find the **root cause** of the issue?

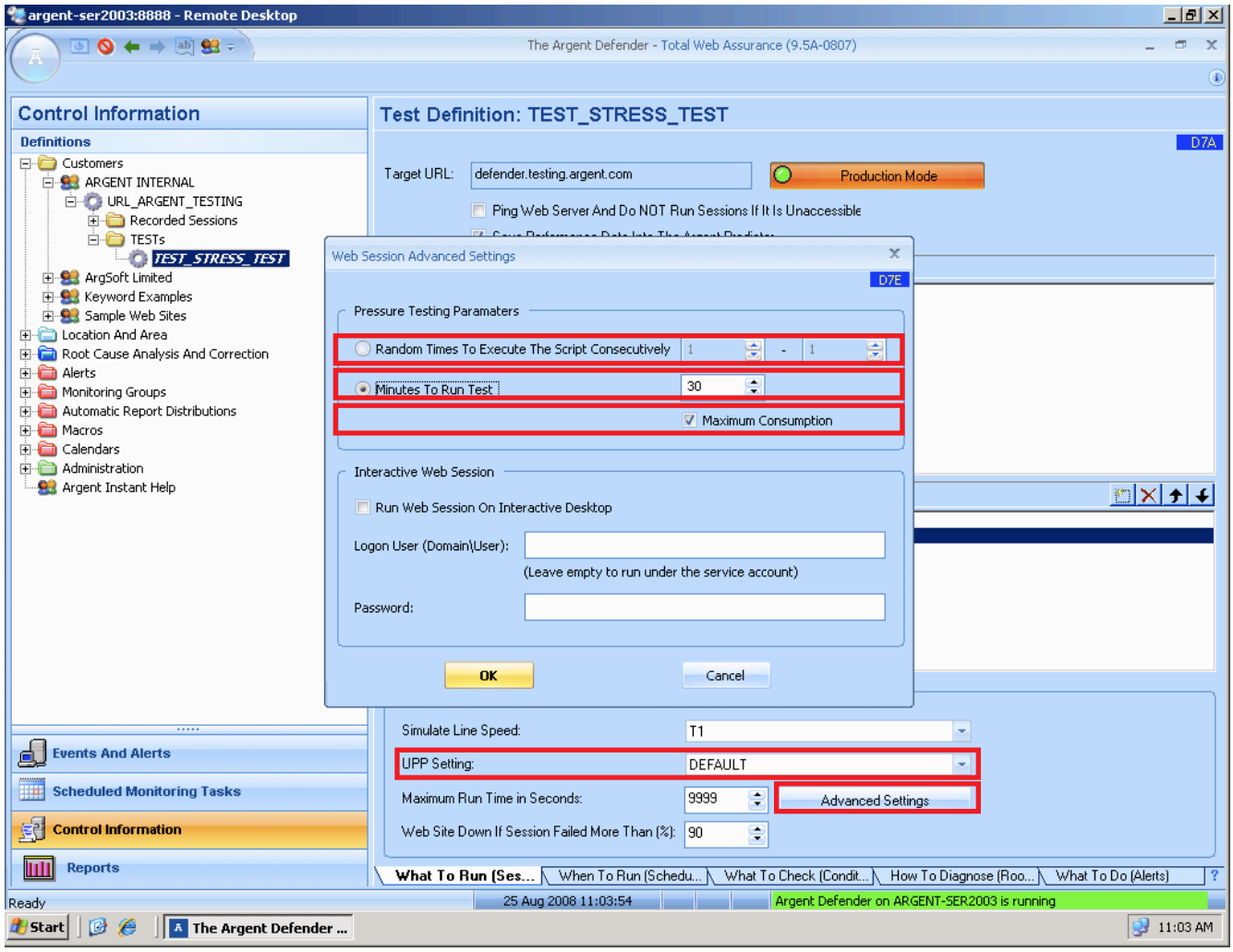
Once you've determined your requirements, the next few pages describe a few of the advanced and useful features of the Argent Defender in more detail.

Argent Defender - Stress Testing

One of the primary functions of the Argent Defender is to perform stress testing. This is done by simulating Virtual Concurrent Users and specifying Pressure Testing Parameters:



Pressure Testing Parameters allow you to customize the load you will be placing on your pre-production site:



Random Times to Execute The Script Consecutively

This field allows you to simulate a random load on your pre-production site. For example, you could have the Argent Defender run the RTP Session 20 to 40 times, which each scheduled test running randomly within this range.

Minutes To Run TEST

This field specifies how long the RTP Session will continuously run for. For example, you could have 50 Virtual Concurrent Users hammering a website for 30 minutes non-stop as one stress test.

Maximum Consumption

If the option is checked, all virtual users start running the RTP Session immediately. If the option is not checked, the virtual users are spread over the run period.

UPP Setting

Unique Personality Profiles (UPP) allow you to simulate your actual user demographic. For example, if your site is targeted at IT professionals, their reaction speeds and navigation speeds may be much faster than a site targeted towards sales or marketing personnel.

Argent Defender - Root Cause Analysis

The first step when using the Argent Defender is to monitor web sites and intranets externally.

Then when issues are detected – such as slowness or unavailability - the second step is to employ Argent's rich array of Root Cause Analysis tools.

Thus, Root Cause Analysis is used to check the internal web servers themselves. Whether a site has one server, or a server farm of 50 - Root Cause Analysis is used for complete testing of a site's frontend and backend .

Argent can successfully run Root Cause Analysis scripts such as CPU Utilization, Memory Usage, IIS Services etc, thereby giving you complete peace of mind that whatever the issue on your Web Portals, Argent will find the root cause.

Being script-based, users have maximum flexibility.

Translated, this means the Argent Defender can proactively take corrective action.

For example, if your IIS service unexpectedly fails - Argent Defender will restart it for you, and send you the logs.

The Argent Defender can be **programmed to correct errors and bottlenecks**, as well as detect them.

All monitoring in the Argent Defender Root Cause Analysis is done with scripts for maximum flexibility and control. The scripts for Windows servers are completely different from the scripts for Linux and UNIX - the Windows scripts are all WMI, while the Linux and UNIX scripts are all Secure Shell.

Scripts come in two types: TEST and GRAPH.

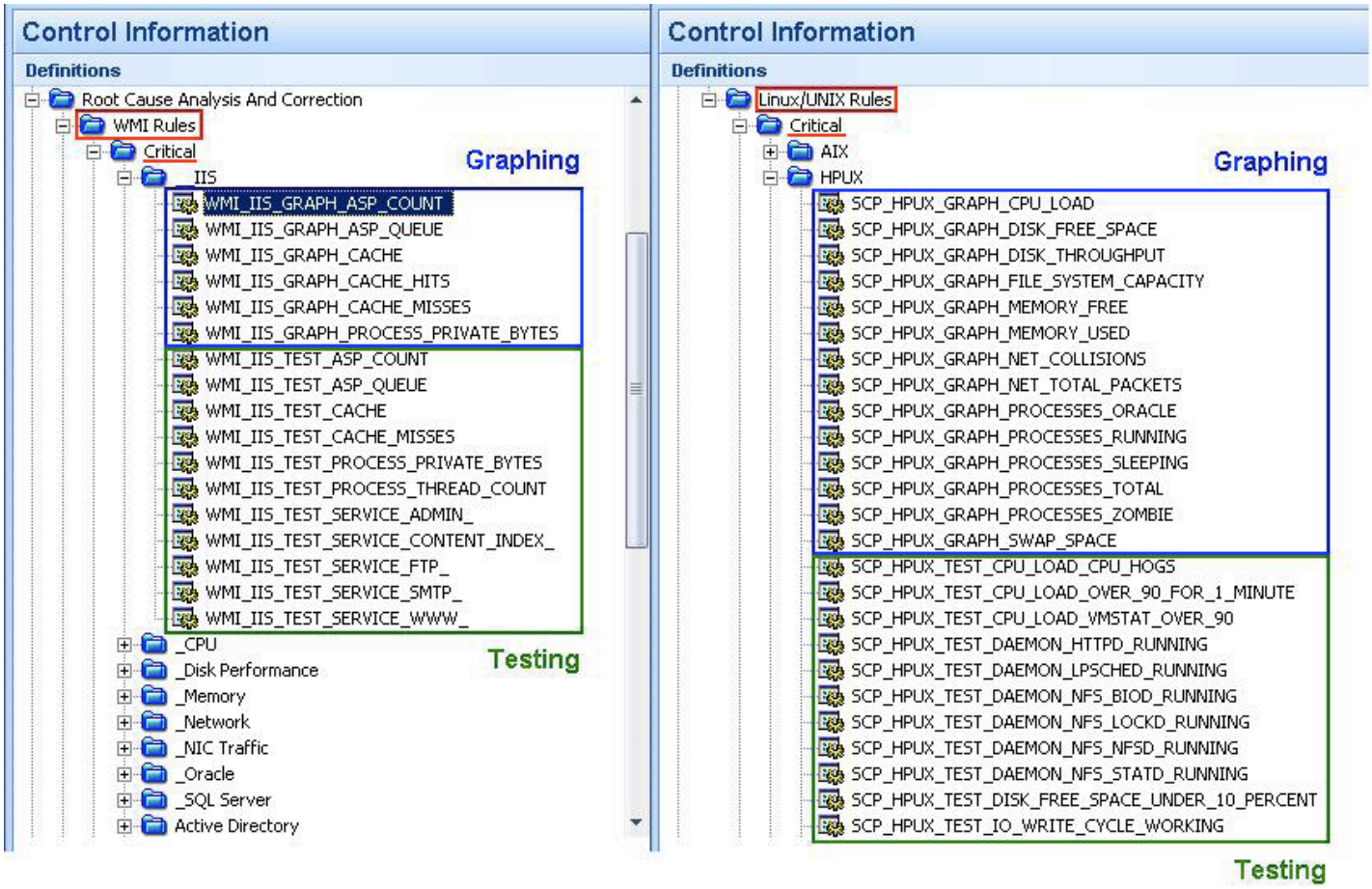
TEST scripts perform the real-time monitoring and alerting:

- If the CPU is too heavily loaded, or
- Checking if free disk space is too small

GRAPH scripts generate the trend analysis and capacity planning data.

There are three classes of Rules: **Critical**, **Important**, **Good To Monitor**

- The Blue box highlights the capacity planning and trend analysis Rules
- Green box highlights the real-time monitoring Rules



Over 300 predefined Root Cause Analysis Scripts are included in the Argent Defender.

Argent Defender - Trusted Agents

In case your websites are servicing other parts of the world, Argent Defender Trusted Agents can be deployed in any part of the world to test and monitor the user experience from that region.

These Trusted Agents act as a remote engine for executing RTP Sessions. All the great features such as UPPs (Unique Personality Profiles) and simulating virtual users are all there.

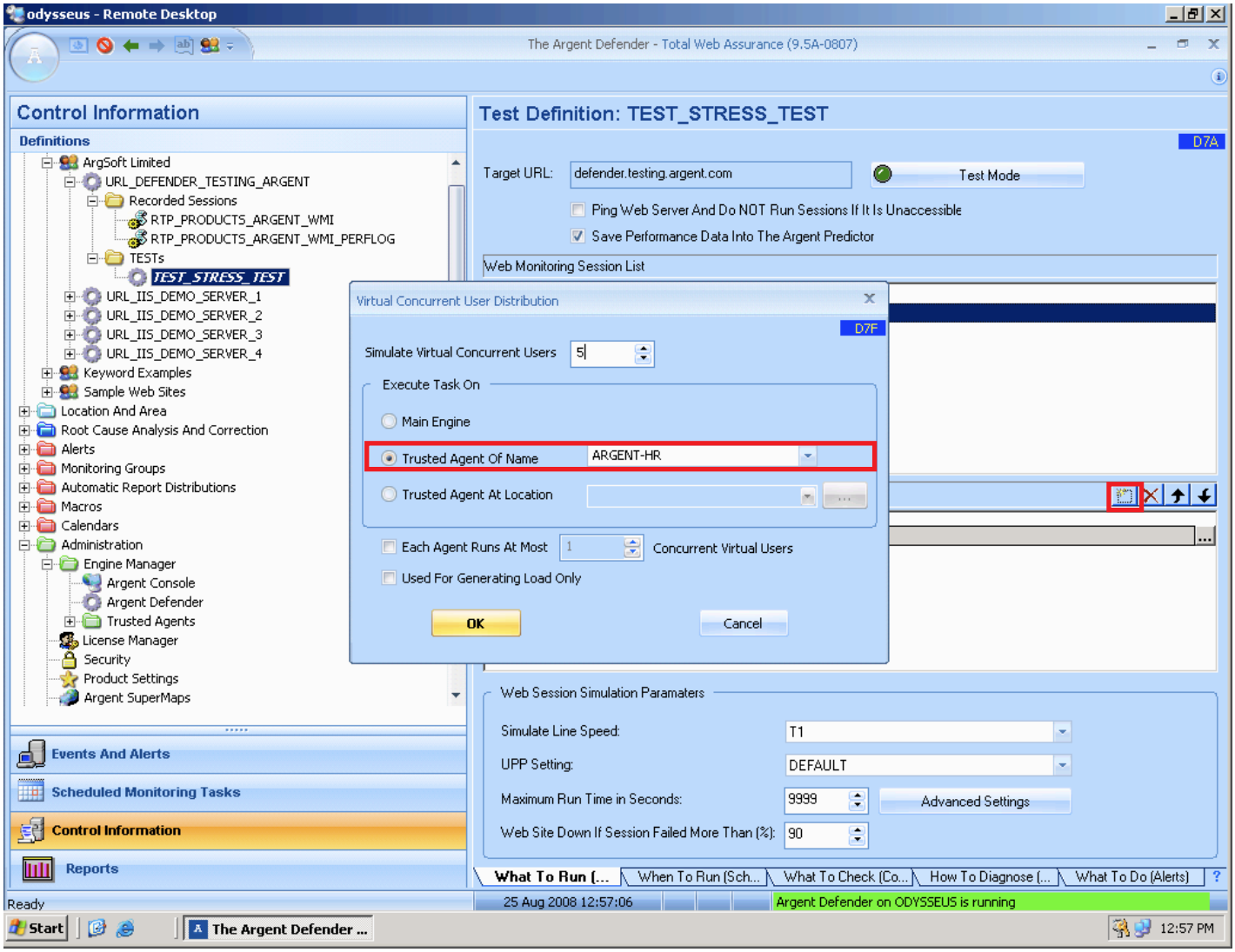
A trusted agent can be pushed out on trusted networks, or installed locally using the Argent Defender setup package.

The connection between the trusted agent and the main engine uses TCP. The main engine is the TCP server listening on **port 3209**. The trusted agent is the TCP client, which initiates the connection. Your firewall needs to be configured properly to handle the communication.

For example, if you have a trusted agent outside the firewall, the firewall needs to be configured to allow incoming connections to TCP port 3209 to travel to the main engine.

When a trusted agent is online, it contacts the main engine and uploads the local hardware and software information. You can modify the default configuration settings. After settings are changed, a trusted agent will download the configuration and use it locally

When assigning a TEST to a trusted agent, you can explicitly specify a particular agent, or allow it to run on any agent.



The Argent Defender can even run RTP Sessions based on geographic location.

For example, 10 Virtual Concurrent Users on Trusted Agents located in Hong Kong, and 5 Virtual Concurrent Users on Trusted Agents located anywhere in the state of New York.

Note: If no agent is available to run the RTP for a specified amount of time, the main engine will take over and run the RTP Session locally.

Argent Extended Technology

The Argent Extended Technology Suite is made up of several products that plug into the Argent Console.

Using the Argent Console, you can consolidate events from any Argent product, as well as third-party products, into a single console.

The Argent Console is both easy to use and reduces the tasks of alerting to a very simple process.

The Argent Console provides the following facilities:

- Unlimited Alerting and Alert Escalation
- Automatic Report Distribution Facility
- Complete SDK

The Argent Console includes a comprehensive set of Alerting functions to notify or provide corrective actions.

The Argent Console includes an Automatic Report Distribution facility that allows you to generate and distribute the reports that are important to you on your own schedule.

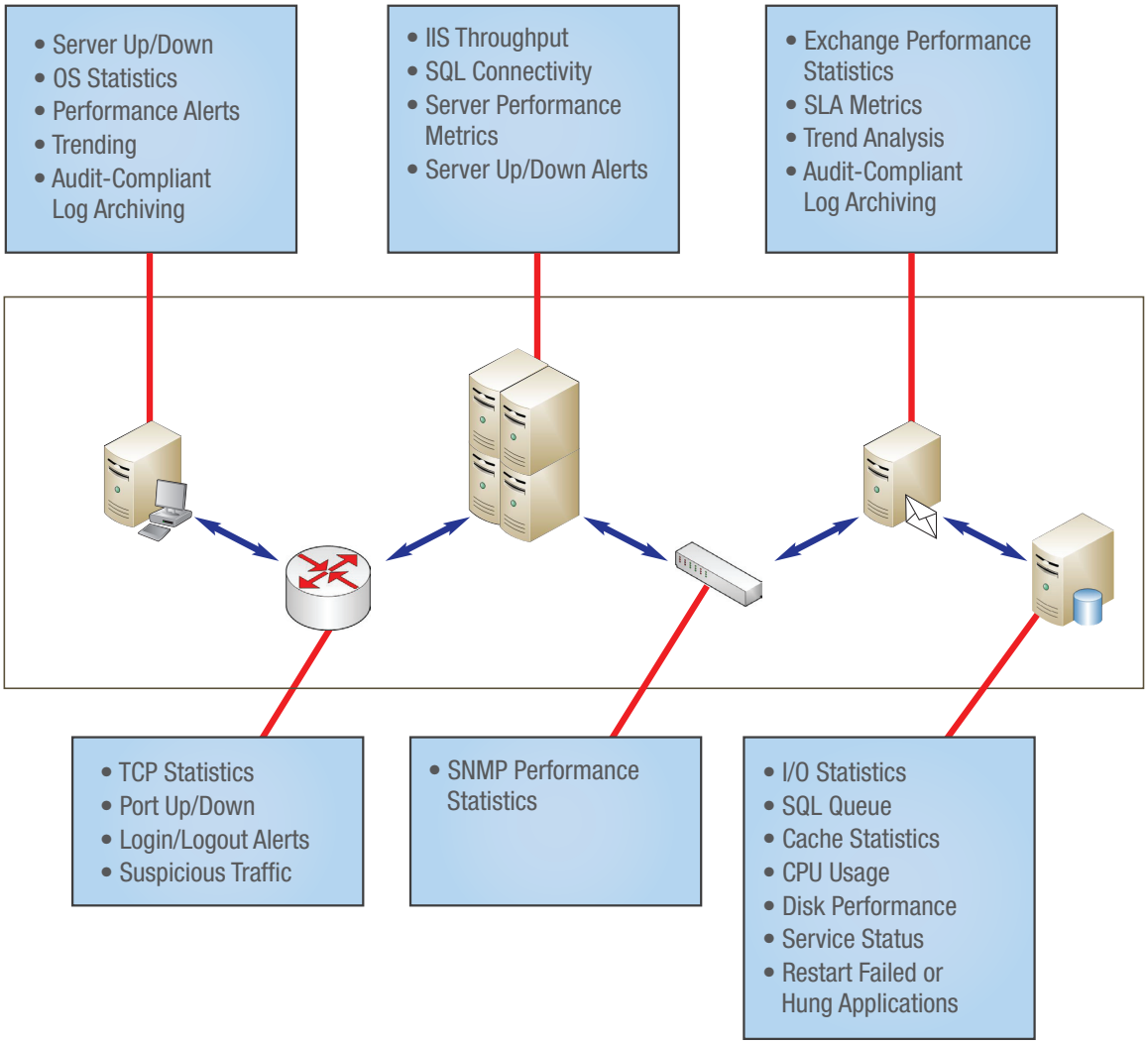
The Argent Console allows third-party products to send alerts directly to Argent so you can track all events as they occur on your network on the central Argent Console screen. With the Argent SDK, you can use Argent alerts with your own applications – simply send the event to the Argent Console, specify the alert to be fired, and Argent does the rest.

The Argent Console is available both as a GUI and as a web-based interface, giving you unlimited mobility and the convenience of managing your entire network from anywhere in the world.

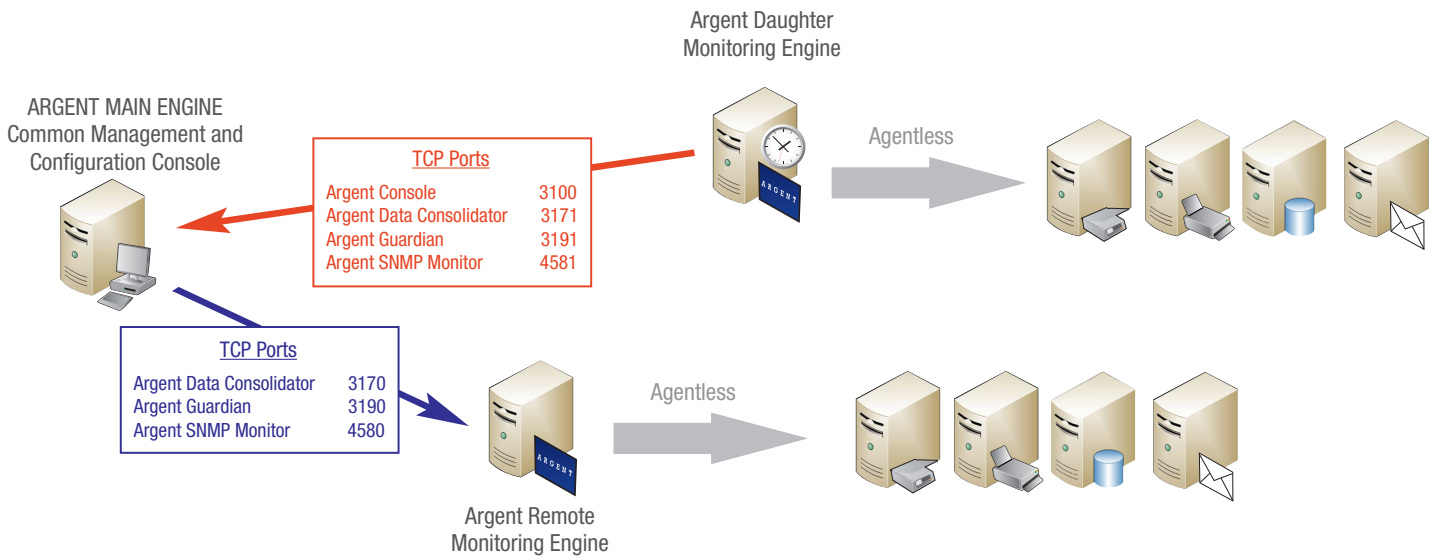
Argent Extended Technology Products that integrate into the Argent Console are:

Argent Guardian	Linux/UNIX and Windows OS Level Monitoring
Argent Data Consolidator	Linux/UNIX and Windows Data Consolidation
Argent SNMP Monitor	SNMP based device monitoring
Argent WMI Monitor	Windows WMI Specific scripting
Argent SQL Monitor	SQL Server Monitoring
Argent Monitor for Oracle	Monitoring Oracle
Argent Exchange Monitor	Exchange 5.5 to Exchange 2007 Monitoring
Argent SAP Monitor	SAP Instance Monitoring
Argent Monitor for VMware	ESX/VMware Guest monitoring
Argent Sentry	URL Monitoring

With Argent Extended Technology's extensive suite of products ranging from Windows, Linux/UNIX, iSeries, SNMP, VMware ESX servers, and all applications – virtually anything can be monitored.



Architecture Overview



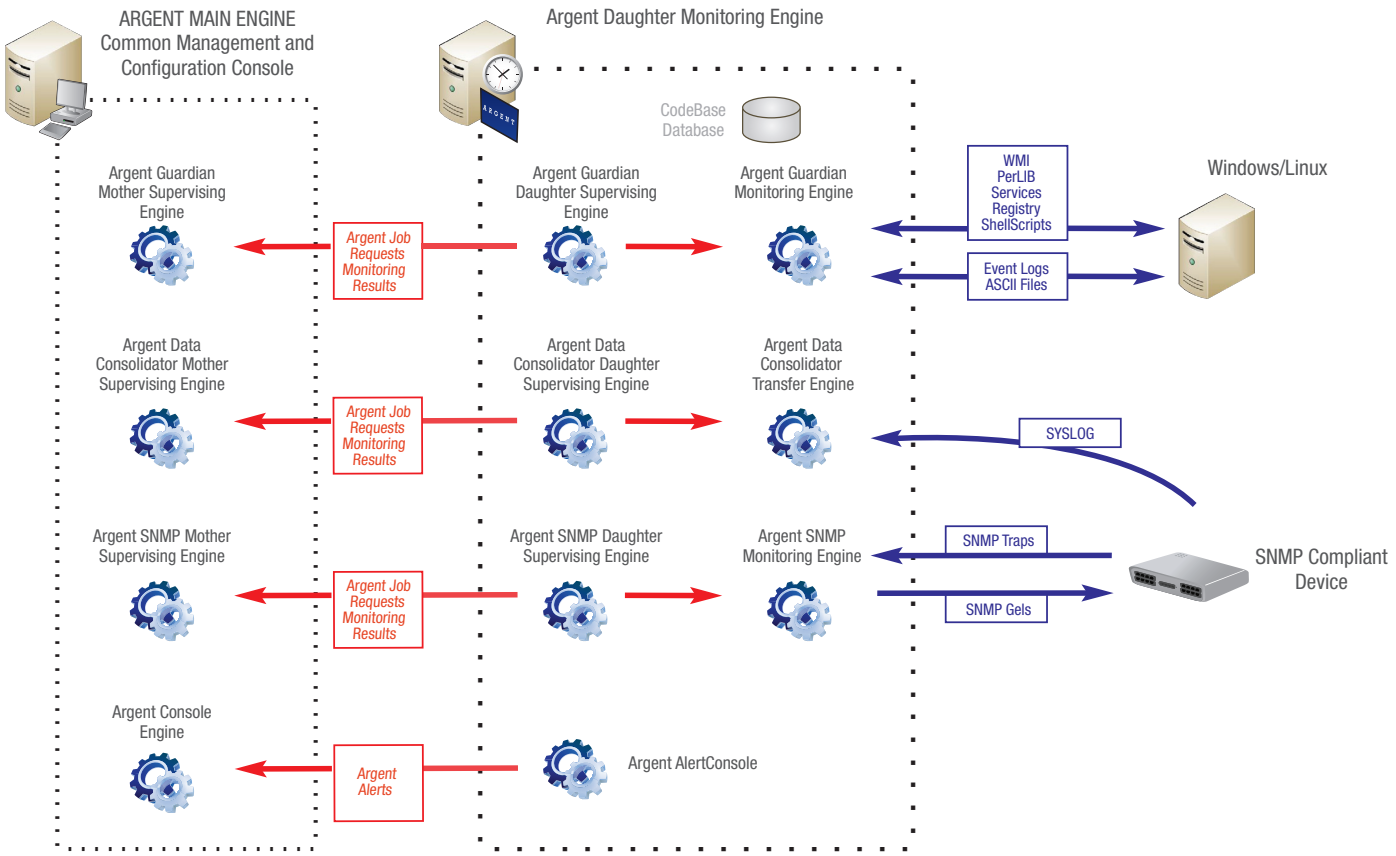
A Remote Monitoring Engine can be used to communicate with servers in untrusted domains, for load-balancing, or failover. The installation needs to be driven by the Supervising Engine (either Mother or Daughter).

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.

No Agents are required on any servers in a trusted domain. All communication is done using native product interfaces - this assumes that there are no port restrictions on communications between the Argent Monitoring Engines and monitored devices.

The Mother/Daughter architecture is the optimal solution for geographically distributed networks, slow links, firewalls, or other complicating factors in their enterprise layout. Each network location, or subnet, contains a Daughter Engine pointing back to a central Mother Engine.

A Daughter Engine is more than just a monitoring engine - it contains its own local scheduling engine as well. This local scheduling facility in the Daughter Engine enables monitoring to continue uninterrupted when the link to the Mother Engine fails, and thus provides complete redundancy.



The Mother stores the entire Argent configuration in the main database. When changes affecting the Daughters are made, the Master Control Information is exported to a file. The Daughter regularly checks the timestamp of this file on the Mother.

If the timestamp changes, the file is downloaded and the Daughter database is updated. The Daughter then executes the instructions contained in its own local (codebase) database, and sends the results back to the Mother.

Argent Guardian

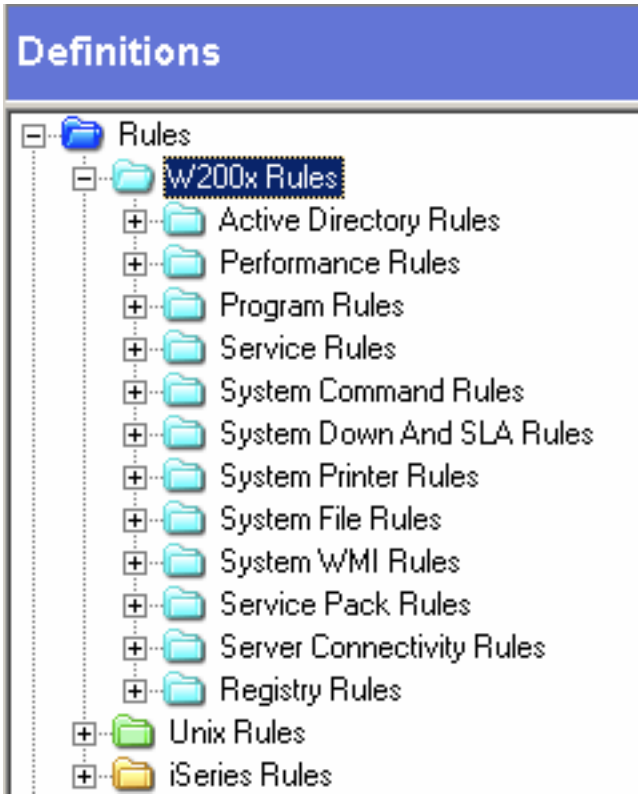
The Argent Guardian is the world's most scalable monitoring solution for all Windows, Linux/UNIX, and iSeries applications, monitoring the health and performance of all critical business applications through a unique architecture - Argent provides the same level of monitoring with or without agents, and there is no cost difference. When issues arise, actions are taken by the Argent Console to correct the issue and to alert the appropriate people.

Because Argent is completely cross-platform, it monitors multiple aspects of your critical applications to help pinpoint key areas of failure.

Argent goes far beyond just checking CPU busy. Argent provides Application Assurance.

Here are just a few of the areas you can monitor with Argent:

- Monitor the health of Active Directory
- Check the availability of your Blackberry environment
- Logon to a Citrix farm
- Verify BIND DNS zone transfers are working
- Ensure the DHCP address pool is sufficient
- Availability - Ping, Open File, NetAPI or TCP Port Scan
- CPU Queue Overload
- Memory overload conditions (Page Faults / Second)
- Free Disk Space on all logical drives (% Free Space or MB Free)
- Physical Disk Q (Average Disk Queue Length)
- Network Overload Conditions (Current Commands of REDIRECTOR)
- Specific Errors or Warnings in the Event Logs (Using the Argent Data Consolidator) - Typically start with any Errors in the Application or Sys Event Log
- Anti Virus Status - via Vendor Logs (Using the Argent Data Consolidator) specific Virus found messages.



This screenshot show the categories of Rule types within the Argent Guardian

Performance Rules - allow access to any Windows Performance API Counters

Program Rules - allow tracking of Windows Processes

Argent Guardian for UNIX/Linux Overview

The following provides an overview of the key features provided in the Argent Guardian for UNIX/Linux – support for following flavors - Solaris, HP-UX, AIX, SCO & Linux.

Connectivity Rules (SLA UP-Down)

The Rules provide the following options for checking connectivity:

- Ping
- TCP/IP port scan (SSH Listener Port 22 for example)
- SSH Logon/Logoff test
- File Open (check the existence of a file)

The following shows an example of some of the typical most often used rules for Monitoring Linux / Unix Platforms – this is just a sample of the rules available:

CPU

- CPU Utilization
- CPU trend analysis
- 1-minute load average
- Excessive CPU by process

Disk

- Free disk space
- Used disk space
- Swap space used
- Available swap space

Memory

- Free Memory
- Excessive memory usage by process

Network

- Network bandwith
- Network traffic
- Network issues
- Network performance
- Network connections

Processes

- Oracle user processes
- Running processes
- Sleeping processes
- Zombie processes

Databases

- Oracle
- MySQL
- Sybase

System

- TCP/IP Ping
- DB2 port check
- Oracle listener port check
- SMTP port check
- POP3 protocol verification
- SMTP protocol verification
- Server response time
- Connected user
- OS level

Daemons

- lpsched
- NFS blod
- NFS lockd
- NFS mountd
- NFS nfsd
- NFS statd

Miscellaneous

- Web server response
- System log
- Bot log
- Cron log
- FTP log
- Sendmail log
- Postfix log
- NTP log

Argent Guardian for Windows Overview

The following provides an overview of the key features provided in the Argent Guardian for Windows

Connectivity Rules (SLA Up-Down)

The Rules provide the following options for checking connectivity:

- Ping
- TCP/IP port scan (WWW Listener Port 80 for example)
- Win32 API call response
- File Open (check the existence of a file)
- Checking the availability of a Cluster node object (Microsoft cluster resource)

The following shows an example of some of the typical most often used rules for Monitoring Windows Platforms – this is just a sample of the Rules available:

CPU
CPU Utilization
Processor bottleneck
Excessive CPU Utilization by process
Processor errors

Disk
Free disk space
Used space
Disk Queue length
Dick I/O by processes

Memory
Available Memory
Excessive memory usage by process
Memory shortage

Network
Network bottleneck
Network availability
Inbound traffic
Outbound traffic
Network errors
Cluster network availability
Cluster network interface availability

Processes
Hung Processes
Key application processes

Active Directory
Bad logons
Replication traffic

Databases
SQL Server
Oracle
DB2

Services
Active Directory (DNS Server, File Replication, Kerberos KDC)
ArcServe
Backup Exec
DB2
DHCP Client / DHCP Server
Lotus Domino
IBM Websphere HTTP
IIS
Oracle
Routing And Remote Access
Print Spooler
SQL Server
ICA Browser
Terminal Services

System
Availability
Response time
TCP/IP port checks
File accessibility
Protocol verification
System uptime
Event Logs (System, Security, Applicatiopn, all others)
ASCII text logs (IIS logs, ISA logs, etc.)
DNS resolutions (any DNS record type)
Service Pack level
WMI connectivity

Argent Data Consolidator

The following provides an overview of the key features provided in the Argent Data Consolidator.

The Argent Data Consolidator provides you with all the archiving and compliance facilities you need, in a single product, regardless of platform - Windows, Linux/UNIX, IBM mainframe, Cisco device or any network device.

Argent can even consolidate logs and files from air conditioning units and UPS power supplies - if the hardware has a log or file Argent can consolidate it.

Argent consolidates your logs and files to one or more central ODBC databases for reporting or analysis. During consolidation you have the option of analyzing each record, and are alerted when anomalies are detected.

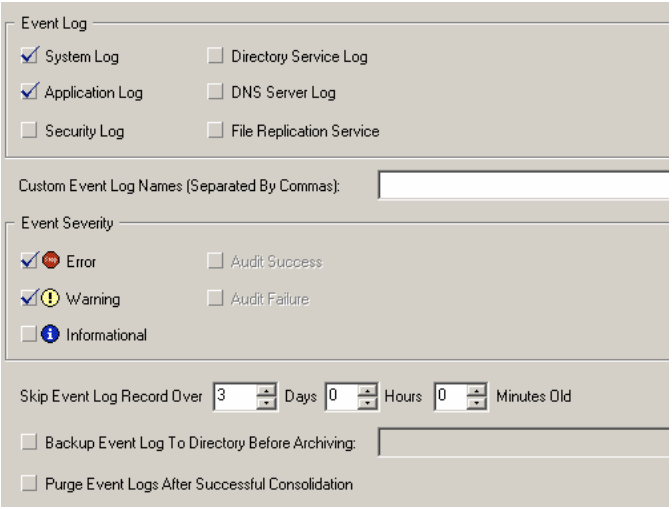
Because Argent supports any ODBC backend, you might use Argent to do this:

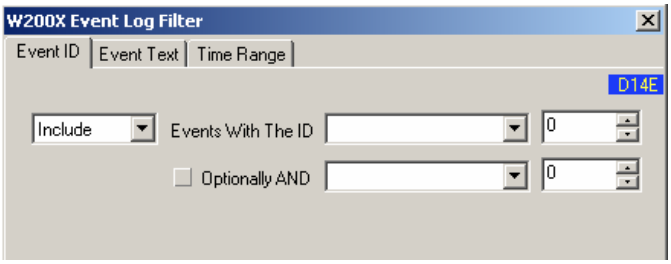
- Windows System and Application Event logs to central DB
- Alert if System Event Log contains SQL Server Error events
- Alert if Application Log contains ORACLE error events
- Unix SYSLOG
- Custom Application Logs (Alert when certain keywords are found)

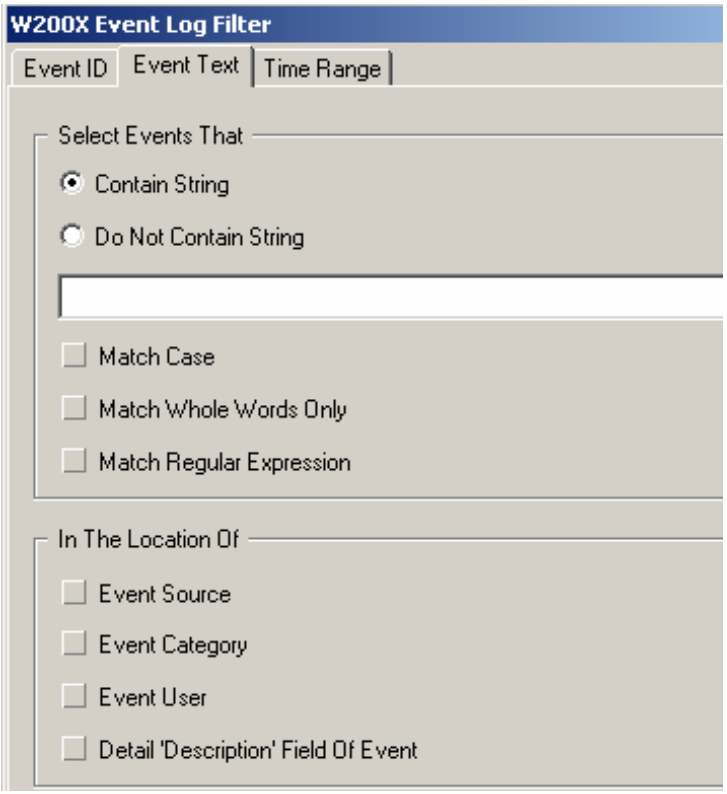
In addition to checking for anomalies, you can also optionally limit the records to be consolidated - you can consolidate all the records from a Data Source, or you can selectively consolidate.

ASCII File - This Rule checks any type of ASCII log file from any platform. If it's ASCII this Rule can be quickly and easily used to check for anomalies. Does not matter the hardware, if it's ASCII and has an IP address, Argent can handle it for you. The Argent Data Consolidator's built-in parser supports the delimited ASCII-based log files.

Windows Event Logs - This Rule is specific to Windows Event Logs. It very effectively handles all the common Event Log anomalies and automatically alerts you of issues.

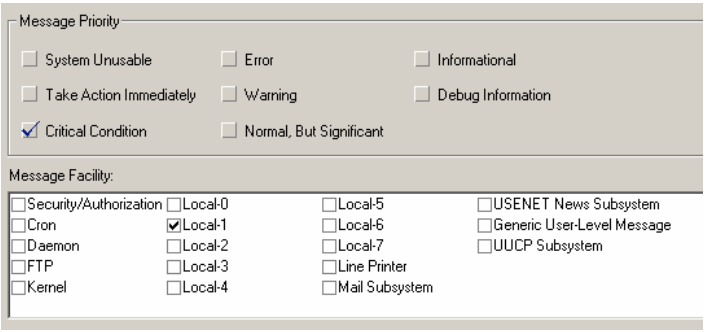






SNMP Traps - This Rule alerts you on anomalies and errors detected by Argent in the unsolicited SNMP traps sent from any SNMP-compliant device.

SYSLOG Messages - The SYSLOG Rule checks any Unix SYSLOG. As is seen in the detailed Argent Instant Help article, all formats of Unix SYSLOG from any Unix platform are supported by Argent.



iSeries Logs - This Rule lets you check iSeries log files.

Custom - The above Rules are nice, they're useful. But they all suffer the same limitation - they are all based on the assumption the format of the data is open and not proprietary to an application. So to address this limitation, Argent provides you with the option to add Custom Filters. You can add Custom Filters using VB or ActiveX.

Compliance

Government regulations are changing the ways all companies and government agencies and departments run. Argent's compliance solution, the Argent Data Consolidator collects, scans, and consolidates all critical data from across the worldwide enterprise into centralized ODBC databases. Argent processes data from any data source – Windows, Solaris, HP-UX, AIX, SCO, Linux, Novell, iSeries, even legacy mainframes.

Argent scales for the real world - Argent can collect, scan and archive data at over 600 gigabytes per hour. Because Argent uses ODBC back end databases, you can use your current database - Oracle, SQL Server, MySQL, DB2, Sybase - any ODBC database.

And you can mix and match databases - your IIS logs can be consolidated to SQL Server, your Email files in Oracle, and so on. Argent does not limit you to one database.

Argent is designed for the real world, where unreliable networks are far more common that T3 lines - Argent has full failover and redundancy built into the product. Argent uses Two Phase Commit - data is never lost with Argent.

Argent has a built-in scheduling so customers can schedule data consolidation in real-time or only during the evenings, on the weekends, or at night, when network load is minimal.

Out-of-the-box Monitoring for Sarbox, HIPAA, PCI, and GLBA

With Argent there is no learning curve, and no need for expensive consultants. In the same day, you can show your auditors automatically generated Crystal Reports about all your compliance requirements.

Argent SNMP Monitor

The Argent SNMP Monitor is a comprehensive SNMP monitoring and alerting solution operating on both sides of SNMP by proactively checking SNMP statistics while also listening for SNMP Traps. The following provides an overview of the key features provided in the Argent SNMP Monitor.

Connectivity Rules (SLA Up-Down)

The Rules provide the following options for checking connectivity:

- Ping
- TCP/IP port scan (WWW Listener Port 80 for example)
- SNMP Service

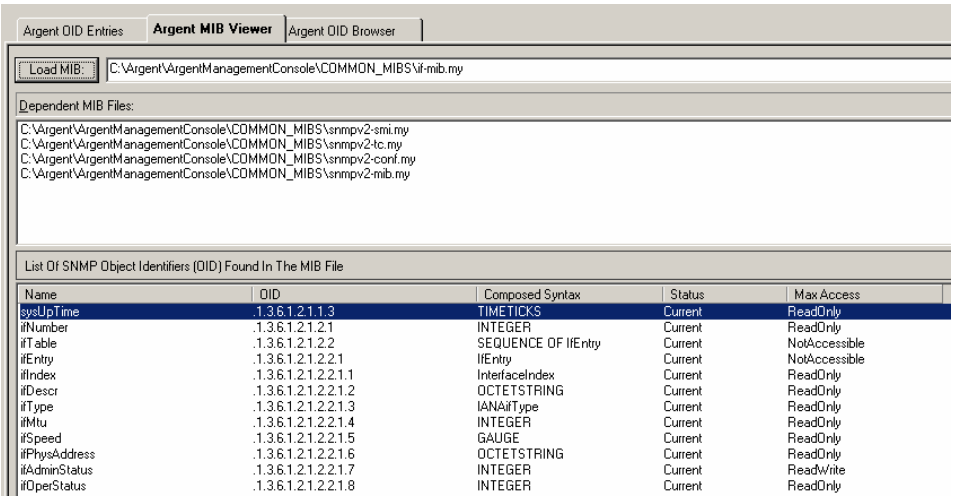
The SNMP Service option verifies the device is online, and also verifies the SNMP community string is accurate.

An SNMP community string is a text string that acts much like a password. It is used to authenticate messages sent between the management station (the SNMP manager – Argent SNMP Monitor, in this case) and the device (the SNMP agent). The community string is included in every packet between Argent and the device.

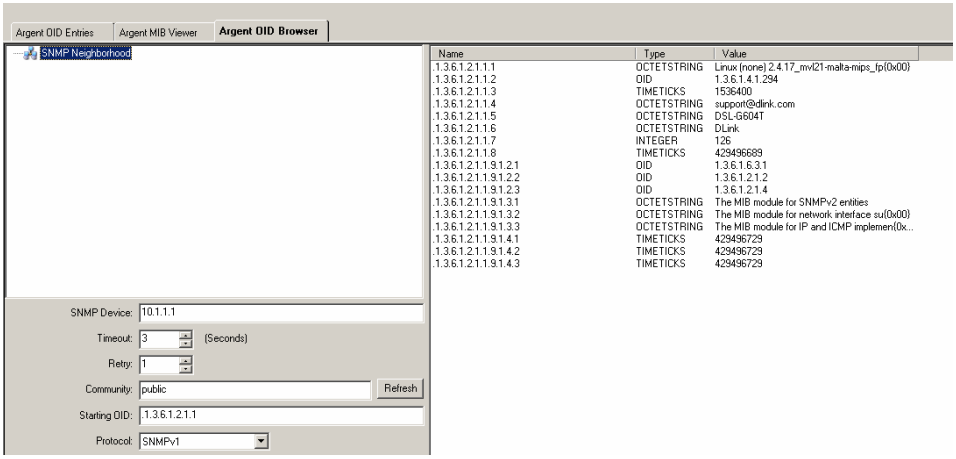
The following sections cover main Argent SNMP Monitor features:

Argent OID Entries - The Argent OID Entries allows you to select commonly used Object Identifiers in your SNMP Rules. For example, “sysUpTime” is a lot easier for most of us to remember than “.1.3.6.1.2.1.1.3”.

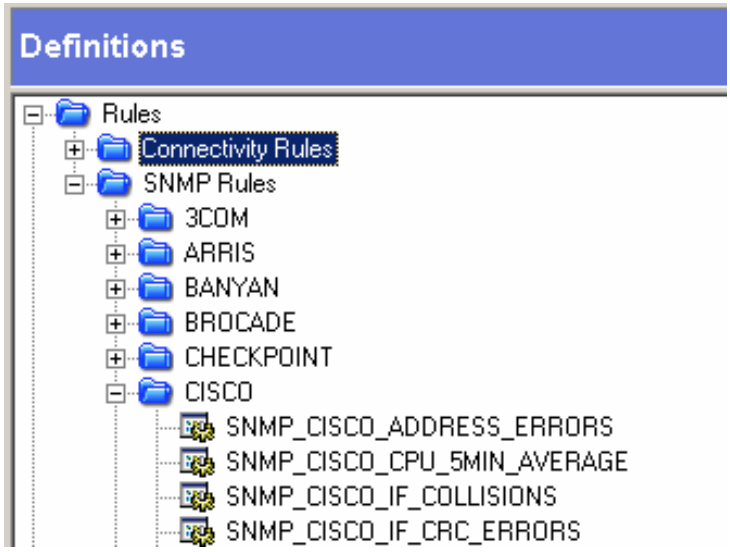
Argent MIB Viewer - The Argent MIB Viewer allows you to create SNMP Rules from any manufacturer's MIB files. The MIB files govern what's possible to do or see via SNMP for a particular device. MIBs usually reference other manufacturer or RFC MIBs to reduce duplication of effort (at least on the part of the device manufacturer). If necessary, Dependent MIB Files are inserted (usually automatically, because Argent includes a host of standard MIB files, but manually if necessary) into the Dependent MIB Files section. Once the MIB file loads, the OIDs are displayed in the lower section of the window. If you select any item, the human-readable description appears at the bottom of the window.



Argent OID Browser - The Argent OID Browser scans for all SNMP-compliant devices in your SNMP neighbourhood, and lets you retrieve all available OID entries from that device. The Argent OID Browser is especially useful for troubleshooting. If you find that you're unable to get any metrics from a device. Browse the SNMP device directly by typing the IP into the SNMP Device field - this will retrieve ALL available SNMP metrics from that device. If nothing shows up, you know the device isn't responding to SNMP requests, and chances are - SNMP hasn't been enabled in its configuration settings.

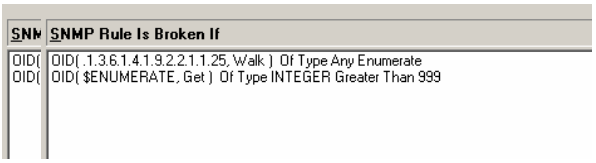


SNMP Rules - Any SNMP-compliant device can be monitored using the Argent SNMP Monitor. You can create your own custom SNMP rules based on any manufacturer's SNMP information. There are a set of predefined rules for most manufactures as an example – these can be used as templates to create your own.

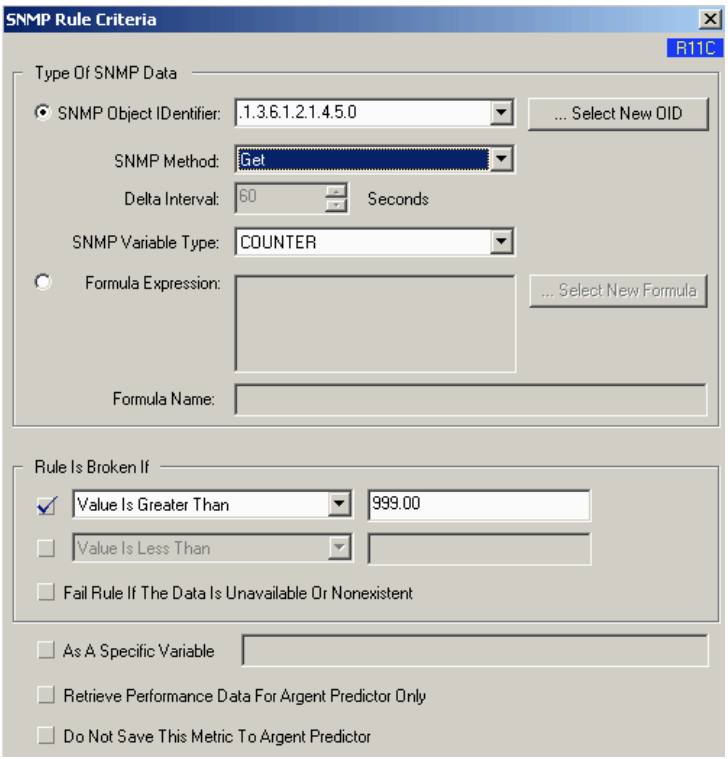


This shows an example screenshot of Some SNMP Rules

Below shows the SNMP Rule Logic



Below shows the Rule criteria



SNMP Object Identifier - Enter the name of the Object ID manually or by using the drop-down, or click the Select New OID button.

SNMP Method - *(Get, Get Next, Walk Within Branch, Long Walk)*

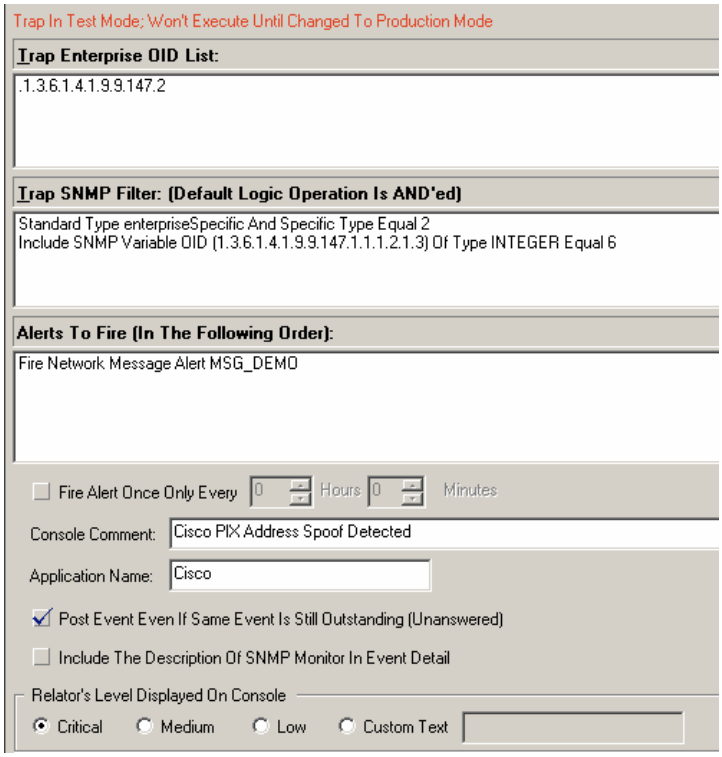
Variable Type - *(INTEGER, OCTETSTRING, OID, IPADDRESS, COUNTER, GAUGE, TIMETICKS, OPAQUE, SENTENCE, ANY).*

SNMP Trap Monitors - SNMP Traps are unsolicited SNMP information packets sent from any SNMP-compliant device to SNMP manager such as Argent. Traps can be sent for many reasons, such as hard drive failures, cooling fans that aren't spinning at the right speed (or spinning at all), network interfaces suddenly dropping, or even for simple informational reasons like the SNMP service starting.

SNMP Rules run in Relators at scheduled intervals, so something like a fan problem that comes and goes quickly might not be noticed. On the other hand, if the device sends an SNMP Trap that the fan isn't running right, Argent can notify you immediately.

The Argent's SNMP Trap Monitor definitions are sort of like Relators. You configure Argent to listen for specific traps, even for specific information within a trap, and which alerts to fire if that trap arrives. If a trap that arrives matches the SNMP Trap Monitor definition that's in Production Mode, the selected alerts are fired.

The Argent SNMP Monitor comes equipped with a large number of pre-defined SNMP Trap Monitor definitions for a wide variety of devices.



Trap Enterprise OID List - Whenever an SNMP Trap is sent, it includes an Enterprise OID. This includes the manufacturer ID, and maybe even a particular class or section of traps related to the sending application.

Trap SNMP Filter - In order to differentiate between, say, a trap indicating a power supply failure and a trap showing that a fan was inserted, we need to get a little more specific. Otherwise, any trap with a specified Enterprise OID would create the same alert.

To define the filer, click the Insert button and select or enter the appropriate information. Traps can be filtered by specific trap types (such as trap number 1354), the contents of the trap message body (such as "fan failed"), or by a Variable OID appearing in the trap message body.

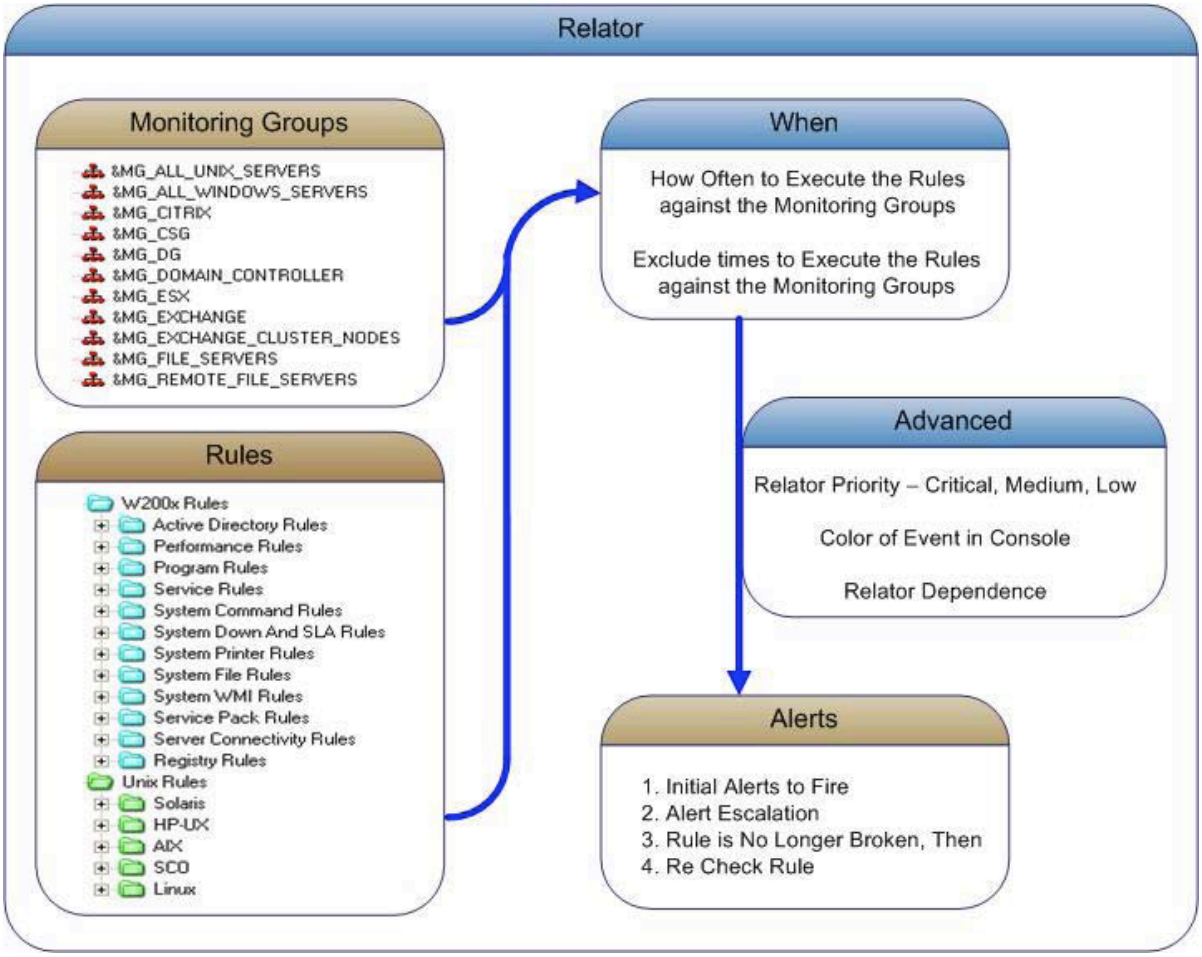
Proactive Monitoring

Monitoring with the Argent Extended Technology Suite is performed by using 4 Building Blocks.

Rules	Tests for conditions. A Rule is broken if the threshold is exceeded.
Monitoring Groups	Lists of one or more servers or IP addresses.
Alerts	Used to either notify you or others of issues, or **take corrective actions.**
Relators	Tie together - or *relate* - the three components of Rules, Alerts, and Monitoring Groups.

Relators

In a Relator the Rule to be executed against the servers and devices in the Monitoring Groups are specified.



Also specified are the Alerts fired when an issue is detected.

When

Each Relator has its own monitoring Schedule which has four options:

- Daily
- Weekly
- Monthly
- Use Calendar

The relator can be excluded from executing during a specific time window.

Advanced

Advanced Features provide a number of different types of customization in the following areas:

- Relator Priority - Appearance of Alerts on the main Argent Console screen (Critical, low etc)
- Relator Dependency - Option for bypassing nodes that are not accessible
- Additional Rules used as prerequisites before the Relator is executed
- Ability to set the server state if additional Rules fail

Alerts

This allows you to customise the sequence of events to be taken when a rule is broken:

- Create a series of alerts for different people
- Take corrective action to correct the problem causing the alert
- Reset and turn off the alert sequence when the problem has been corrected
- Trigger an escalation if event has not been responded to
- Set different alerts based on different time periods in your day – Email while you're in the office, and SMS outside of work hours.
- Notify all support lines automatically when an issue has been ad dressed.

Each server and device is checked independently of the others – the results of checking one server or device in the Monitoring Group in no way affects the results of checking other servers or devices.

Monitoring Groups

For all Argent products, Monitoring Groups define the servers and devices to be processed - Monitoring Groups are shared by all Argent products. The same Monitoring Group can be used by any number of Relators in any number of Argent products.

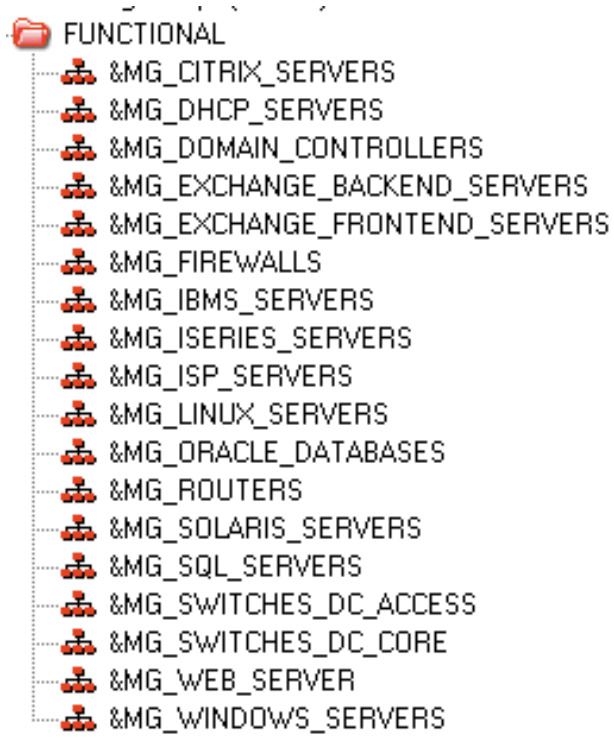
By not having to specify servers and devices in the actual Relators, and by sharing Monitoring Groups, only the Monitoring Groups need change when a new production server comes online (or an existing server is replaced), rather than having to change hundreds of occurrences of the same server name or device address.

There is no limit to the ways Monitoring Groups can be created. You can have a Monitoring Group consisting of the servers and devices in the Accounting Department, and another Monitoring Group of those in the Engineering Department.

These same servers and devices can be in different Monitoring Groups, may list servers by application - all production Exchange servers in one Monitoring Group, all production Oracle servers in another Monitoring Group, all test Linux machines in another Monitoring Group, and all network printers in another Monitoring Group.

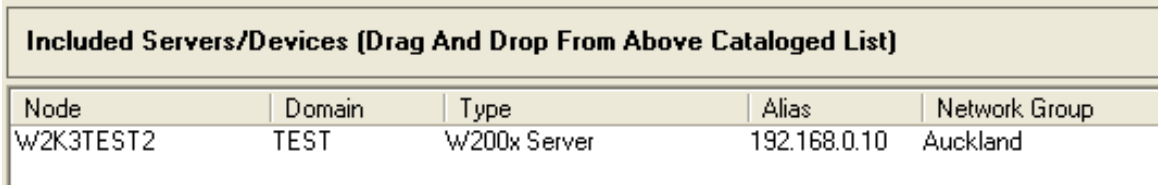
Functional Grouping (SuperConsoles)

There are many different ways of configuring devices into monitoring groups but the most used and best method is to group devices by there Function (FUNCTIONAL SuperConsole). Below shows an example of how this may be used:

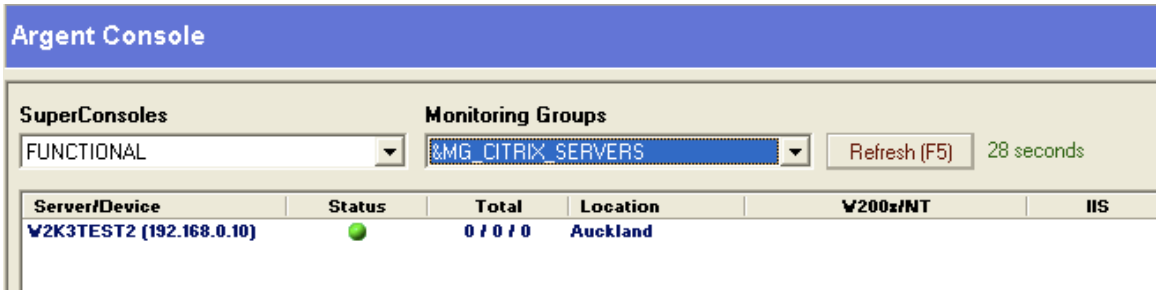


Each functional unit has a monitoring group ie CITRIX_SERVERS this contains all of the citrix servers.

Eg. CITRIX_SERVERS (Monitoring Group) could contain

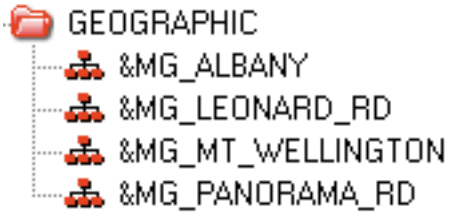


These groups would be used within Relators

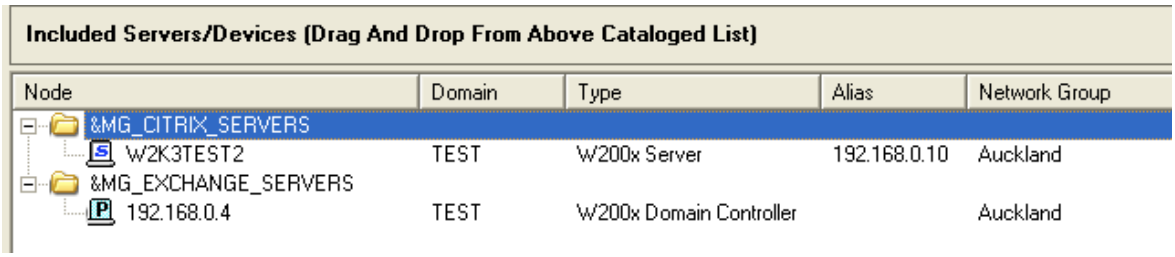


Geographical Groupings (SuperConsoles)

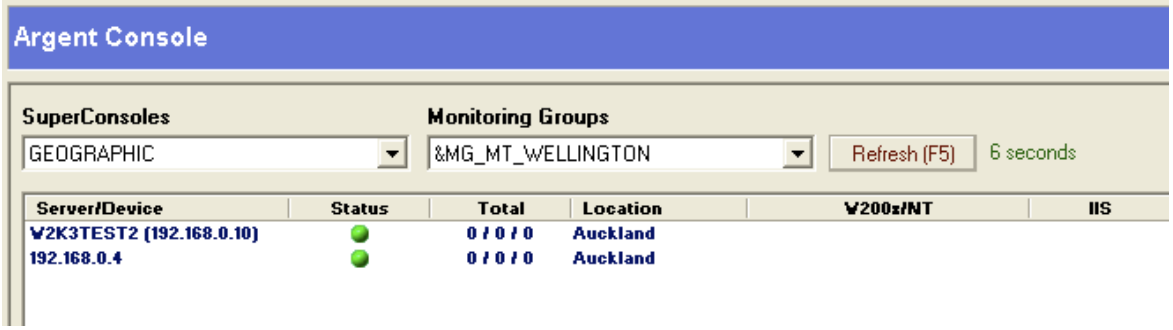
A Geographic (SuperConsole) can also be used to provide a method of grouping servers by location – within this, there would be a set of Monitoring Groups for each location, each of these groups would contain the appropriate functional Groups.



Eg. MT_WELLINGTON (Monitoring Group) could contain



These groups may not be used for monitoring (not assigned to relators) but would provide a way of filtering based on location.

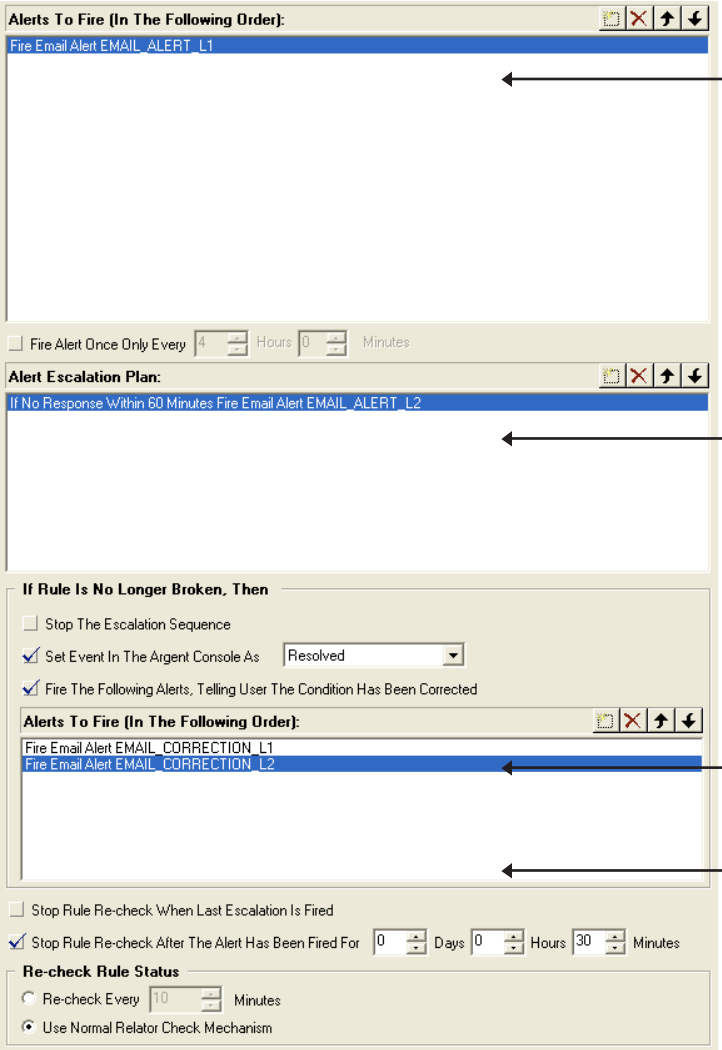


From the Argent Console views can be created based on SuperConsoles and then further filtered by Monitoring Groups.

This provides a mechanism to allow customers to see their servers only by securing the Monitoring Groups to a particular Security context – this is achieved by utilising the Argent Ninja Security Node Manager.

Alerting Structure Overview (Relator)

The Alert structure is used to perform a task or notify when a particular event has happened. The following is an example of an Alert sequence.



An email is fired when an event is generated also an event is generated in the Argent Console with a status of answered =

NO

A Script here can perform automation

If the event in the console is not set to answered or resolved within 60 minutes another email address

If the event is fixed the status is set to Resolved

Emails are sent to notify that the issue is now resolved

Building An Alert Structure

To achieve a reliable robust alerting structure several things need to be investigated.

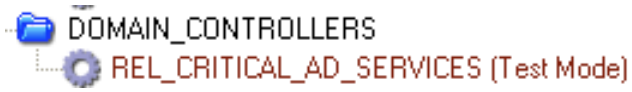
- Categorising monitoring tasks (Relators) into levels (Severity).
  Eg. Critical - Windows services that will stop users from working
  - Server Down
  Medium- Disk Space 5% may eventually affect applications
  - Windows service that will not directly affect users
  Low - Disk Space 10% pre-warning
  - Backup Failed
- Defining who will be alerted about different Severity issues
- How long can an issue be outstanding before being fixed/ Investigated?
- Who needs to be notified if the issue is not fixed within initial time windows?
- Who needs to be notified when an issue is resolved?

How Do We Achieve The Above In Argent?

By creating Relator templates we can easily apply this process to any new monitoring required.

We would create a template for each of the Severity levels as above.

Within each template we define the procedure for each Severity, this allows us to then copy any of the above relator templates eg Copy *Rel_Template_Critical* with a new name for checking AD Services.



We would then change the Rule and Monitoring group to achieve the appropriate check.

Producing a table similar to below of each Rule and its process will help simplify building the relators.

Rule	Server	Severity	Initial Alert	Escalation	Escalation Alert
Exchange Services	Exchange	Critical	Helpdesk (8am to 5pm) On call (5pm to 8am)	30mins	Infrastructure Email, SMS
AV Service	All	Medium	Helpdesk (8am to 5pm) Restart Script	120mins	Infrastructure Email, SMS
Disk Space 10%	SQL	Low	Helpdesk (8am to 5pm)	240mins	DBA Email, SMS
Disk Space 5%	SQL	Critical	Helpdesk (8am to 5pm) On call (5pm to 8am)	30mins	DBA Email, Infrastructure Email

Critical Severity Relator Example

Let's look at the details of a Critical Template Example.

The Basic TAB

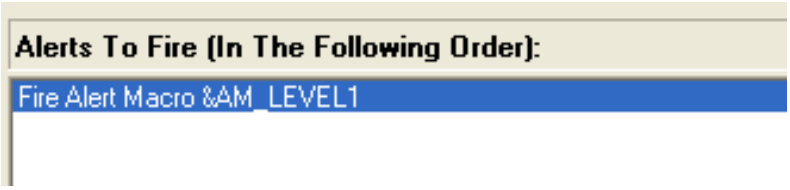
- The rule will be whatever metric you are testing
- The monitoring group will be the servers to apply the rule against

The When TAB

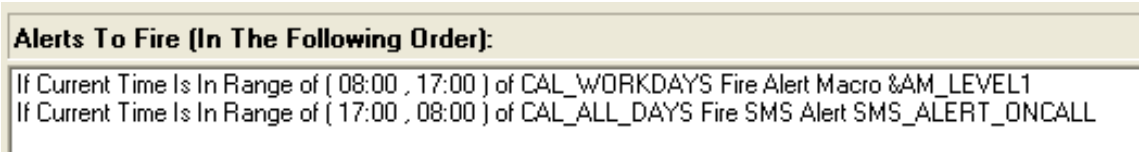
- When to Execute the Relator – as this is a critical Relator it may be executed every 1-5mins

The Alert TAB

- First an email is sent to the Level 1 Email address – this is typically the Help Desk

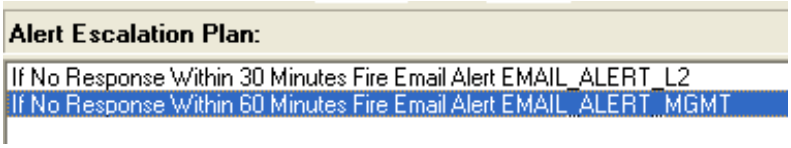


A more complete Initial Alert may be of the following configuration



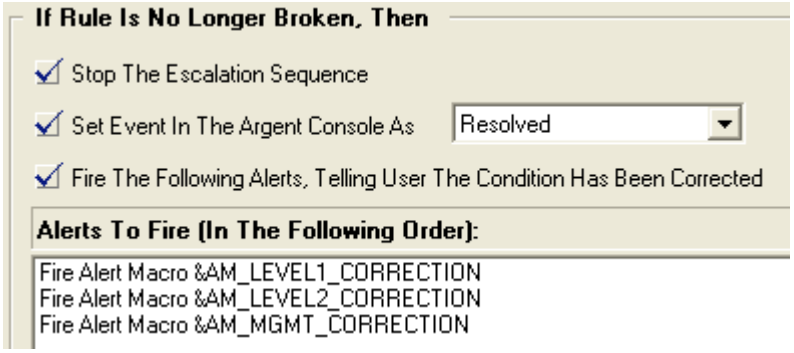
An email sent to Level 1 during weekday work hours, outside this an SMS is sent to ON Call person.

- If the issue is not resolved in 30mins then Level 2 Email is sent, if it is then not resolved in 30mins MGMT Email is sent



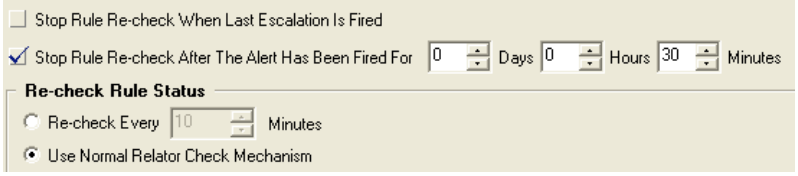
This would typically send an email to the second line engineers to resolve and then notify management if it is not fixed within 60 minutes of initial event.

- Once the issue is resolved the event is set to resolved and Escalation is Stopped



An email is sent to Level 1, Level 2 and MGMT notifying that the issue is resolved

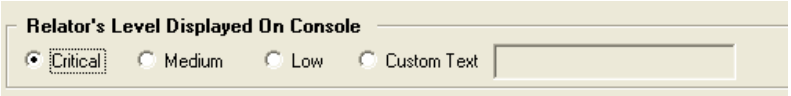
- This specifies the re-check process; the first check box stops the re-check after the last escalation in the sequence has been fired. The following check box sets the maximum time to re-check the condition after this time the relator is not run.



The Re-Check Rule Status sets the 'When' after the relator has fired an event.

The Advanced Features TAB

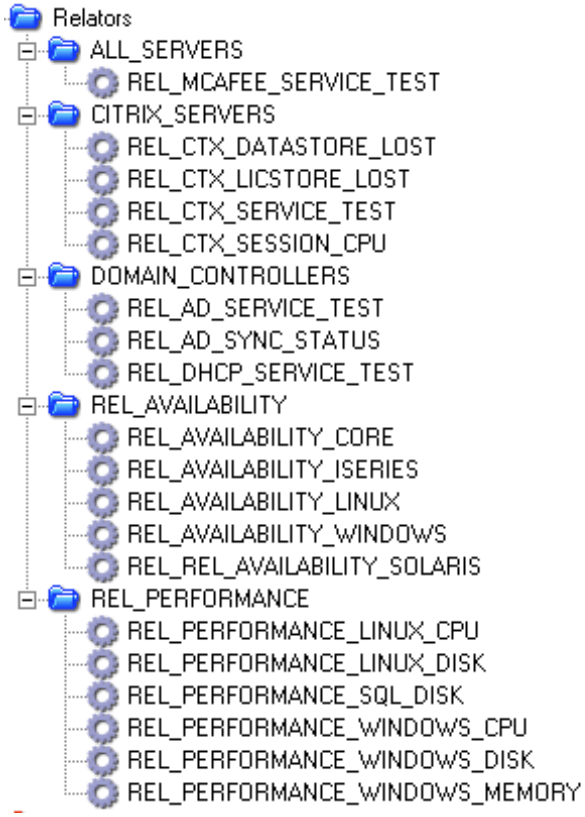
- The Level of Severity for an Event as seen in the Argent Console is set within the Advanced Features TAB of the Relator – see below



This now defines the appropriate alerting process required for any check that is deemed as critical.

Once the Monitoring groups and Alert structures have been configured and the relator templates have been built - these templates can be copied to create the functional tests.

The best approach is to group Relators by the Function they perform, below is an example of a typical setup - each of these Relators would be copied from one of the templates described above.



Proactive Alerting

An Alert is used to either notify you and others of issues, or to take corrective actions.

For example, an Email Alert can send details of why a Rule was broken, the value causing the Rule to be broken, as well as the server with the issue. An example of a corrective Alert is when a SQL Alert runs a SQL Query to correct an issue on a SQL database.

If a SQL Transaction Log becomes too large for example, then an Email Alert can be fired, but also a SQL Alert can be executed to run a SQL Query to reduce the size of the SQL Transaction log. In this way, Argent first alerts you of the presence of the issue and then corrects it.

Argent has 16 different types of Alerts as described below.

Notification Alerts	Corrective Action Alerts
Alphanumeric Pager	Alphanumeric Pager
Email	Email
Network Message	Network Message
SMS	SMS
SNMP	SNMP
System Alarm	System Alarm
Unix Action Script	Unix Action Script
W200x Event Log	W200x Event Log

Alphanumeric Pager Alerts

Send either an alphanumeric message with details of a broken Rule to alphanumeric pagers, or can page a simple beeper.

Email Alerts

Send an email message to any MAPI or SMTP email system. The level of detail in the email message can be selected, from a simple generic message to an email containing all the details of the broken Rule.

iSeries Command Alerts

Execute commands on iSeries machines with the option of including one or more system parameters. Thus actions to correct the cause of the issue can be taken.

Network Message Alerts

Network Message Alerts send a message to one or more accounts in the enterprise. Like Email Alerts, the level of detail in the message can be selected, from a simple generic message, to a message containing all the details of the broken Rule.

SMS Alerts

SMS stands for Short Message Service. Argent SMS Alerts send messages to cellular or mobile GSM phones. Like Email and Network Message Alerts, the level of detail in the message can be selected, from a simple generic message, to a message containing all the details of the broken Rule.

SMS also guarantees delivery of the short message by the network. Temporary failures due to unavailable receiving stations are identified, and the SMS message is stored in the SMSC until the destination device becomes available again. SMS provides a mechanism for transmitting messages to and from wireless devices.

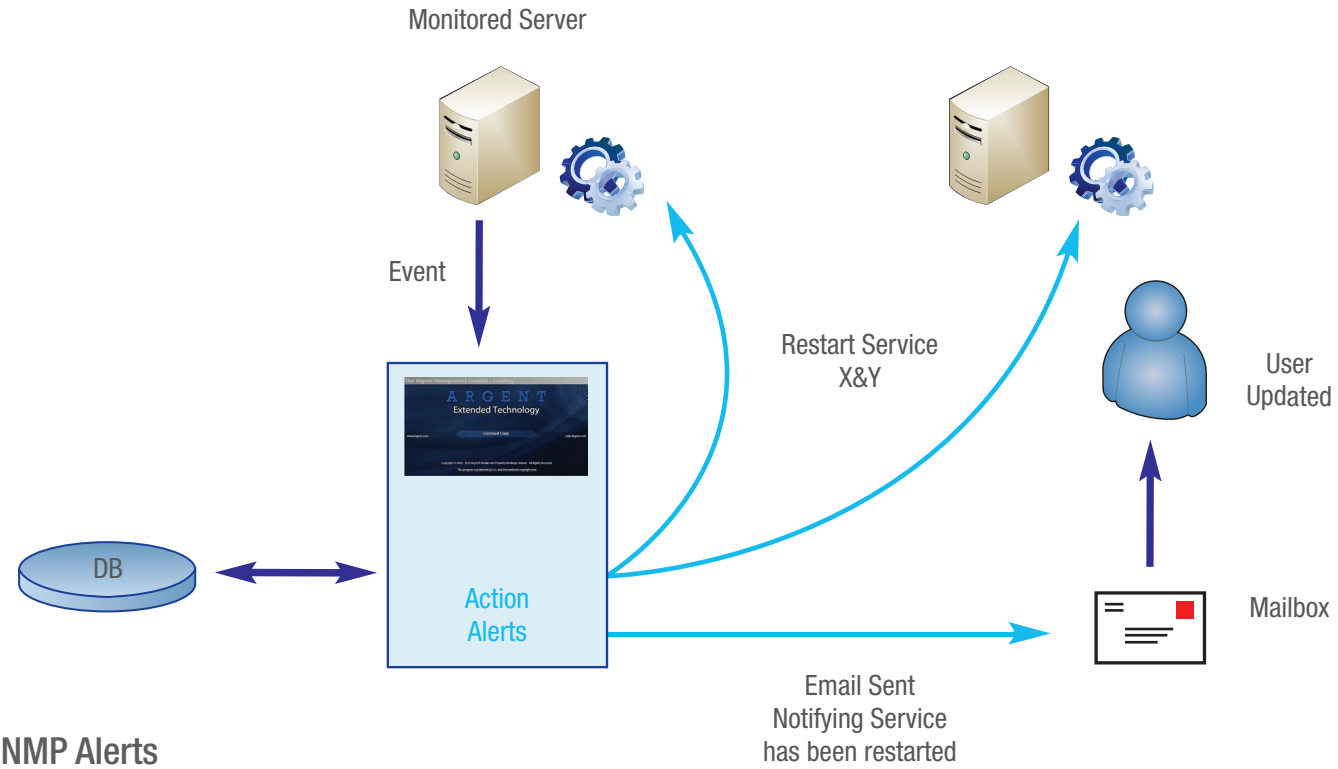
What you need to send SMS Alerts is a GSM modem attached to the Argent Server, SIM card and Service Provider Account.

Service Alerts

Service Alerts are used to start, stop, or pause any service. Argent Service Alerts have the intelligence to start a related series of services in the correct sequence.

The ability to detect a Hung service, restart that service and any others.

The ability to stop a service can be useful when an unauthorized service is detected on a production server.



SNMP Alerts

SNMP Alerts send a message to an SNMP trap or write data directly to an OID address. For example, you can issue SNMP SET commands to perform actions (e.g. disable a port) on a SNMP-compliant device.

SQL Alerts

SQL Alerts enable a SQL Query to be executed. Thus actions can be taken to correct issues.

If a SQL Transaction Log becomes too large for example, then an Alphanumeric Pager Alert and an Email Alert can be fired, but also a SQL Alert can be executed to run a SQL Query to reduce the size of the SQL Transaction log. In this way, Argent first alerts you of the presence of the issue and then corrects it.

System Alarm Alerts

System Alarm Alerts sound the system bell on the central server.

System Command Alerts

System Command Alerts execute a Windows 200x command file - a cmd or bat file or even an exe file. The submitted command file can take corrective action.

For example, if a Rule tests for dangerously low disk space on a production Exchange server, then an Email Alert can be fired also a System Command Alert can be executed to delete the unnecessary temporary files on the Exchange server. In this way, Argent first alerts you of the presence of the issue and then corrects it.

System Help Desk Alerts

System Help Desk Alerts forward any Argent Alerts to any help desk. Argent can detect issues and alert you, as well as take corrective actions. And all these actions can also be sent to the help desk using the System Help Desk Alert.

System Reboot Alerts (Restricted)

System Reboot Alerts enables a server to be rebooted to address a severe issue. Some issues are so severe – such as critical heap shortages – that the only alternative is to reboot the server.

UNIX Action Script Alerts

Unix Action Script Alerts enable any UNIX script to be run on all common flavors of UNIX. These scripts can use Telnet, or SSH/SCP, the Argent Script Agent, or the Secure Argent Script Agent.

Unix Action Scripts enable corrective actions to be taken automatically.

W200x Event Log Alerts

W200x Event Log Alerts generate and write an Event Log entry containing details of the broken Rule to the Windows Event Log. These Event Log Alerts have a large array of optional variables, such as the name of the person to contact, the server name, etc.

WMI Action Script Alerts

WMI Action Script Alerts enable any WMI script to be run to enable a WMI script to take corrective actions.

Monitoring And Alerting Using Custom Scripts

Argent Extended Technology has two primary methods of achieving monitoring using custom built scripts and providing custom alerting or actions.

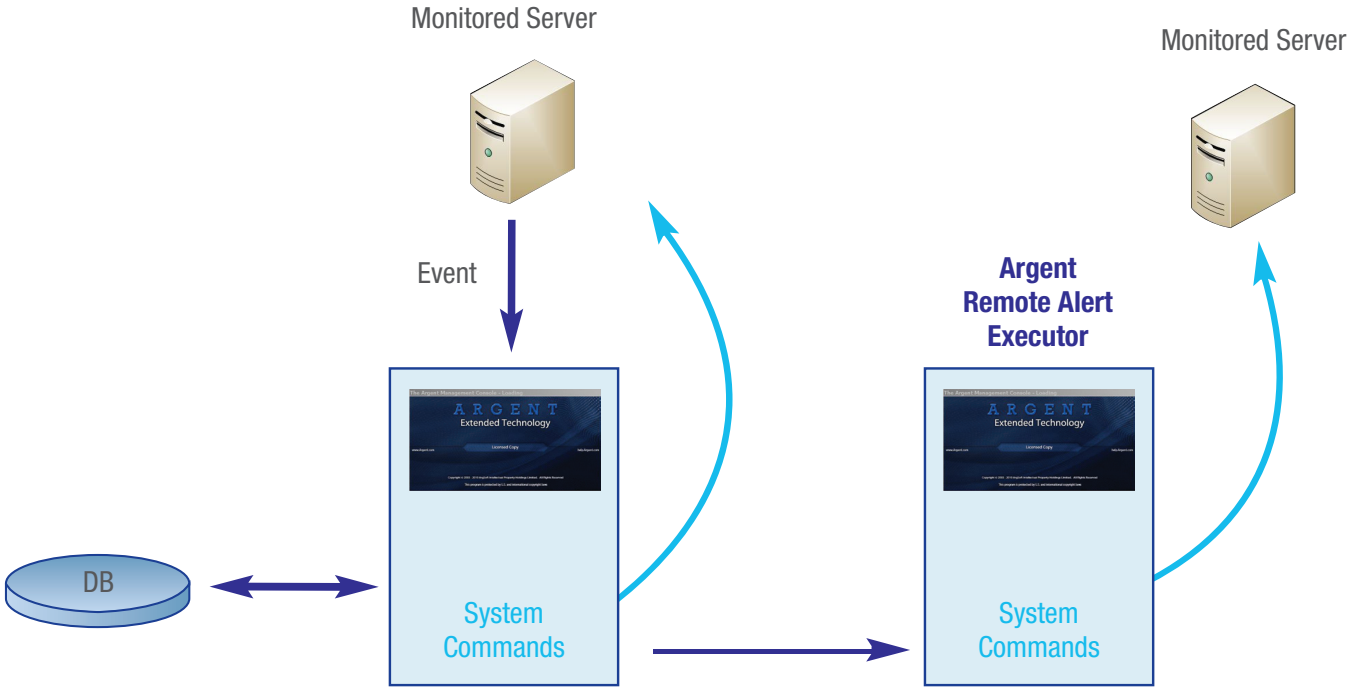
Windows Systems

By using System Command Rules and System Command Alerts you could conceivably monitor much of your windows enterprise. It would be very labour intensive and time consuming, but it does illustrate the power of the System Command feature.

What makes System Command Rules so powerful and useful is their ability to execute any program or command file you have, and then to examine the results.

- Pass Argent variables to the system command
- Check the Exit code of the system command
- Check the system command line output (string checks)

The System Command Alerts allow you to configure any program or command file to be executed against the monitored server as an automated action.



For example, if a Rule tests for dangerously low disk space on a production server, then an SMS Alert can be fired also a System Command Alert can be executed to delete the unnecessary temporary files on the server. In this way, Argent first alerts you of the presence of the issue and then corrects it. The System command can also be executed from another server if it is configured to be an Argent Remote Alert Executor – this can be useful if system commands need to be executed in a DMZ or secure environment.

Unix/Linux Systems

By using Unix Rules and Unix Action Script Alerts you could conceivably monitor much of your UNIX enterprise. It would be very labour intensive and time consuming, but it does illustrate the power of the UNIX script feature.

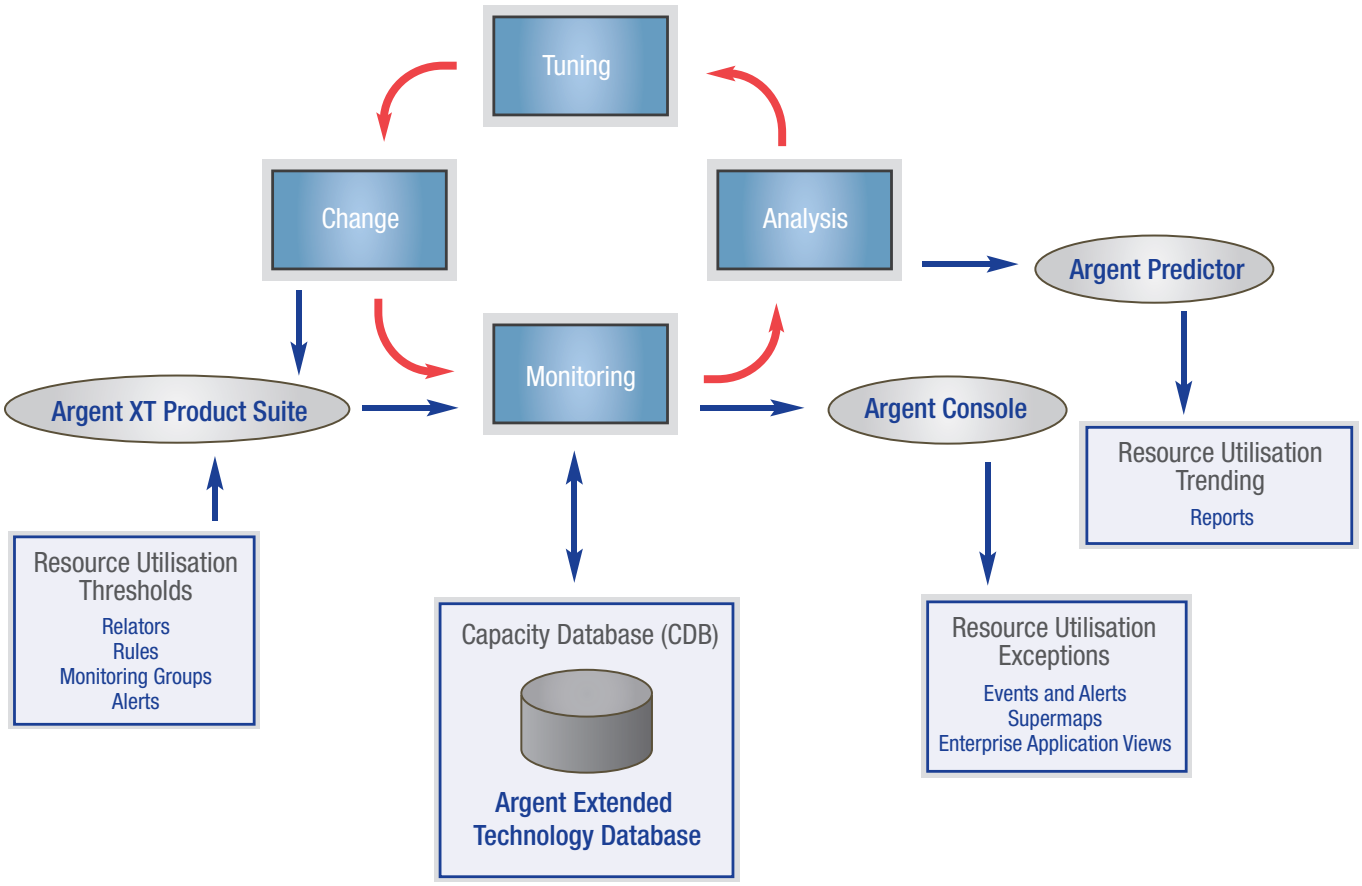
What makes Unix Rules so powerful and useful is their ability to execute any shell script you have, and then to examine the results.

The Unix Action Script Alerts allow you to configure any shell script to be executed against any server using telnet, SSH or Argent Agents.

Collection Of Performance And Capacity Data

The Argent Extended Technology suite provides important functionality in aligning with ITIL based Service Capacity Management, by providing the ability to capture monitored metrics as well as alert on them and store these into a relational database for future reporting and capacity trending.

The diagram below shows a simplified view of where Argent Extended Technology products provide functionality to achieve Performance and Capacity management.



The Argent Extended Technology suite provides a mechanism called the Argent Predictor which allows performance data metrics to be captured and stored into a database. This feature can be enabled, on a rule by rule basis.

Any Argent Extended Technology Product's Rules can be configured to store data using the Argent Predictor for later reporting. Here are some examples of common metrics that are stored:

- CPU Utilisation
- Disk Space Free
- Disk Queue – Read & Write
- Memory – Committed, Paged and Pooled
- Server Availability
- Network Availability
- Disk Space Trending
- Issue Count

Custom Crystal Reports can be configured to provide resource usage reports.

Reporting

The Argent Extended Technology suite provides a mechanism to generate reports of any data that has been captured by the Argent Predictor.

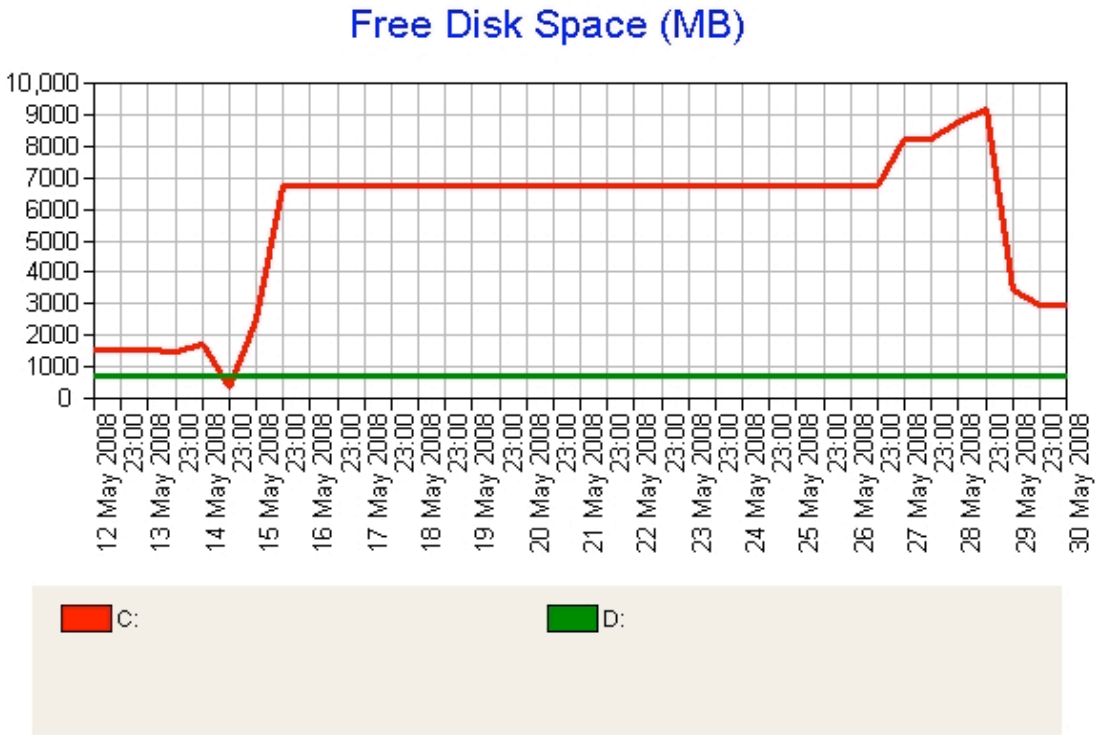
Reporting is an essential part of monitoring. Ordinarily, you'll know when things go wrong because Argent alerts you. But a server could be running just below your thresholds and you might never know it unless you run a report.

Reports are also a great way to determine how your enterprise normally looks. Based on what you see in the reports, you can adjust your monitoring thresholds accordingly. After all, rules of thumb are good, but really knowing your environment is much better.

In the Argent products, there are generally two types of reports:

- Argent Graphs
- Argent Reports

The Argent Graphs are, as the name implies, graphical reports. Graphical reports are great for displaying performance metrics such as CPU, disk space, and memory. You choose the type of graph (including area, bar, line, log/lin, or tape), the time frame, and the servers/devices to display, and Argent does the rest.



The Argent Reports are Crystal Reports-based reports. While some of the Crystal templates included with Argent do contain graphs, there are mainly text-oriented reports. Crystal Reports templates can be easily customized. If you have Crystal Reports 9 or higher, you can create or edit the templates yourself. If not, Argent's engineers can do it for you.

The Argent Reports are textual reports. These reports are great for displaying SLA metrics and summary performance metrics such as CPU, disk space, and memory.

SLA Reporting

UPTIME BY DEVICE					
Device	Detected Down	Detected Up	Total Outage Time (hh:mm:ss)	Total Up Time	Total Down Time
	Wed, 15 Oct 2008 10:26:44 AM	Wed, 22 Oct 2008 06:52:06 PM	56:25:22		
	Wed, 29 Oct 2008 03:40:41 PM	Thu, 30 Oct 2008 01:02:45 PM	21:22:04		
192.168.0.66				**86.16%**	**17:47:26**

SLA reporting can be achieved by monitoring using the following rules and saving the result to the Argent Predictor.

- Ping
- TCP/IP port scan (Port 1433 for example)
- Win32 API call response
- Checking the availability of a Cluster node object (an MSCS cluster resource)
- File Open
- SSH Logon Test
- Windows Service Availability
- Custom System Command

Crystal Reports is the industry standard for report generation and this comes built into Argent. Not only can you generate Crystal Reports, but Argent can automatically distribute the reports with the Automatic Report Distribution feature. These reports can be automatically published to any of the following:

- Network Share (UNC)
- Email Address
- FTP Server

Reports can be generated in the following formats – PDF, Excel, Word, RTF, XML, HTML, and PowerPoint.

Argent Visualisation

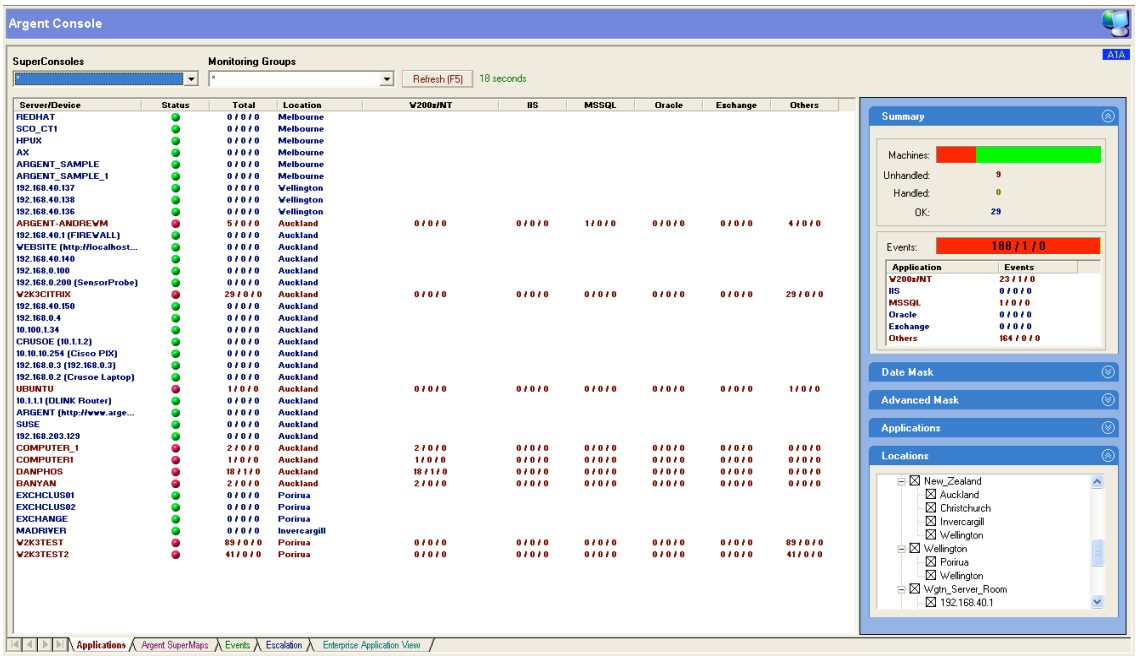
Argent Extended Technology provides a number of different graphical views to enhance the visibility of events and the status of the System Infrastructure. These include the following

- **Argent Applications -**
  displays status details of the servers and devices
- **Argent SuperMaps -**
  displays the status of the entire enterprise in a graphical fashion (device centric)
- **Argent Events -**
  displays details of various Events associated with the applications, servers, or devices.
- **Argent Escalation -**
  displays critical events that have not been answered.
- **Argent Enterprise Application View -**
  displays the status of Critical Applications (service type view)
- **Argent Ninja -**
  web based views for Help Desk personnel who need to be able to see the status of servers or devices, but don't allow changes to be made in how they are monitored – can restrict what users can view.
- **Argent Business Manager -**
  you can create web-based business views of your entire enterprise that allow changes to how devices are monitored

Argent Applications View

The following view represents the Application View or a list of all monitored devices in the infrastructure.

The list can be sorted by Monitoring Groups or SuperConsole (grouping of Monitoring Groups).



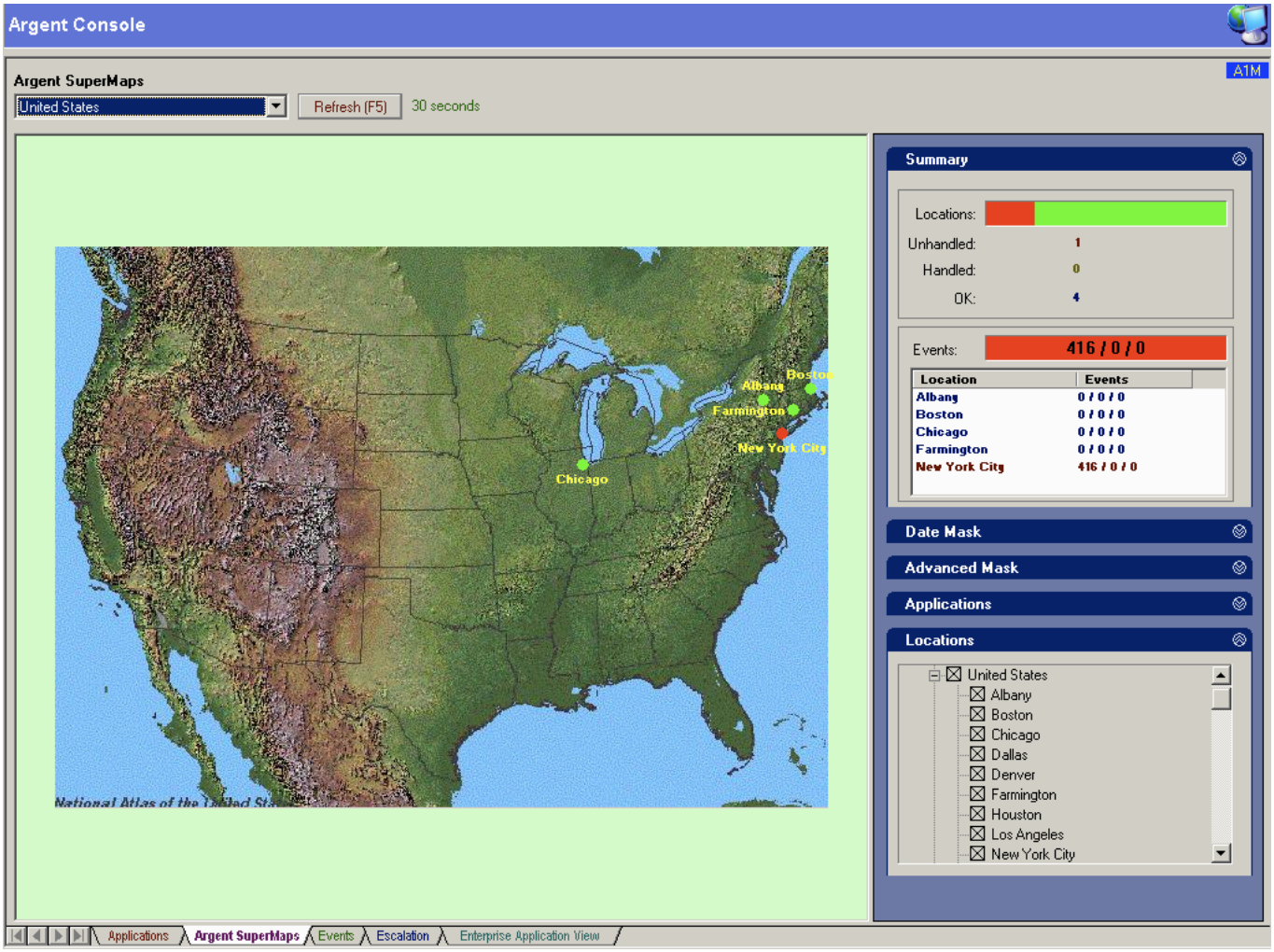
The view can also be filtered by Date, Device Type, Application and Location.

The view shows the number of events for each device.

Argent SuperMaps View

The following view represents the SuperMaps View a graphical representation of all monitored devices in the infrastructure.

You can add and customize maps or corporate schematics to the Argent SuperMaps by using the option adding Your Own Map (Any JPEG, BMP, or DIB format can be used) from the combo box or selecting Argent SuperMaps from the Administration module.



Each dot on the Argent SuperMap represents a geographical location, a Monitoring Group, or an individual server or device.

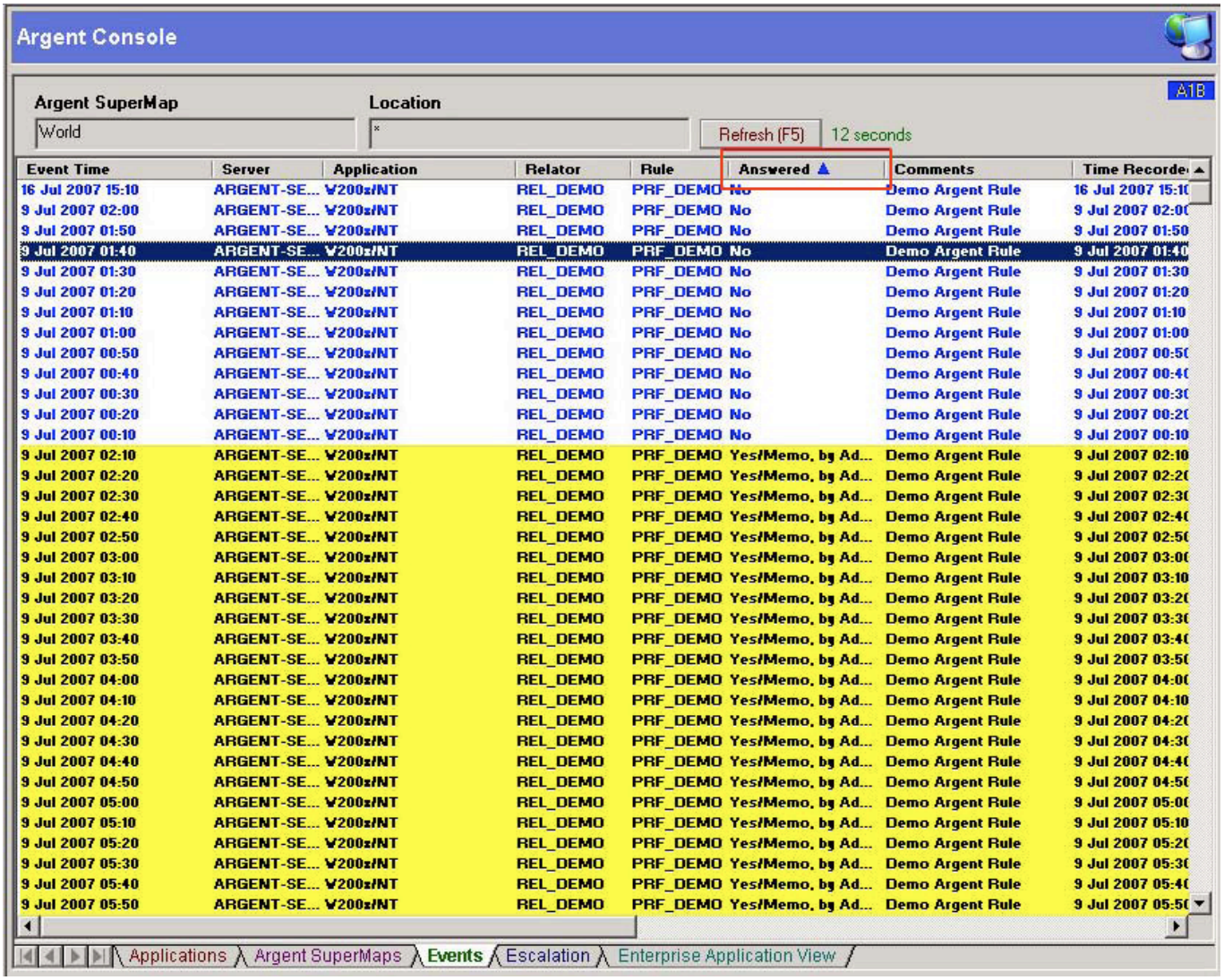
The status of the represented item is displayed as **red**, **orange**, **yellow**, or **green** dots, depending on the status of the server or device.

By default, a blinking **red** dot represents a critical event. A blinking **orange** dot represents a medium-priority event. And a blinking **yellow** dot represents a low-priority event. A solid **yellow** dot represents an event that's been answered or resolved. And a solid **green** dot represents an item with no registered events.

Individual Argent SuperMaps can be hot-linked together, allowing you to effectively zoom in and see more details graphically. Hot links are made to other Argent SuperMaps, or even to a URL. Left-clicking on a hot link takes you down a level, while left double-clicking brings you back up a level. You have full control over text alignment and colour.

Argent Events View

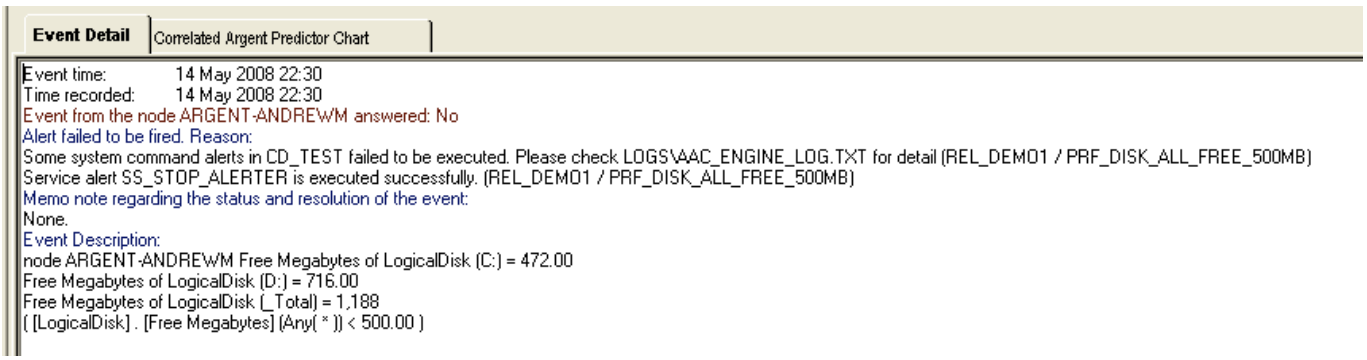
The following view represents the Events View a list of events associated devices in the infrastructure.



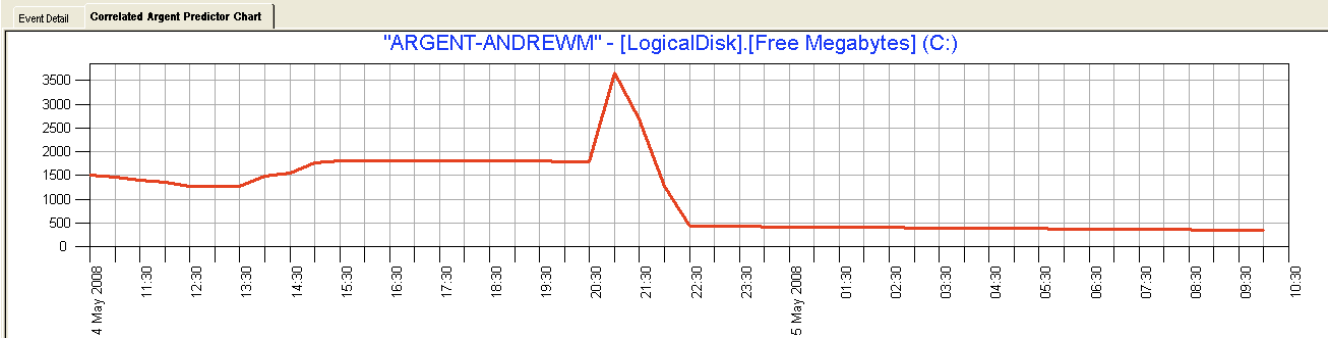
Event Time	Server	Application	Relator	Rule	Answered	Comments	Time Recorde
16 Jul 2007 15:10	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	No	Demo Argent Rule	16 Jul 2007 15:1
9 Jul 2007 02:00	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	No	Demo Argent Rule	9 Jul 2007 02:0
9 Jul 2007 01:50	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	No	Demo Argent Rule	9 Jul 2007 01:50
9 Jul 2007 01:40	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	No	Demo Argent Rule	9 Jul 2007 01:4
9 Jul 2007 01:30	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	No	Demo Argent Rule	9 Jul 2007 01:30
9 Jul 2007 01:20	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	No	Demo Argent Rule	9 Jul 2007 01:20
9 Jul 2007 01:10	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	No	Demo Argent Rule	9 Jul 2007 01:10
9 Jul 2007 01:00	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	No	Demo Argent Rule	9 Jul 2007 01:00
9 Jul 2007 00:50	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	No	Demo Argent Rule	9 Jul 2007 00:5
9 Jul 2007 00:40	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	No	Demo Argent Rule	9 Jul 2007 00:4
9 Jul 2007 00:30	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	No	Demo Argent Rule	9 Jul 2007 00:3
9 Jul 2007 00:20	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	No	Demo Argent Rule	9 Jul 2007 00:2
9 Jul 2007 00:10	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	No	Demo Argent Rule	9 Jul 2007 00:10
9 Jul 2007 02:10	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 02:10
9 Jul 2007 02:20	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 02:2
9 Jul 2007 02:30	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 02:3
9 Jul 2007 02:40	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 02:4
9 Jul 2007 02:50	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 02:5
9 Jul 2007 03:00	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 03:0
9 Jul 2007 03:10	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 03:10
9 Jul 2007 03:20	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 03:2
9 Jul 2007 03:30	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 03:3
9 Jul 2007 03:40	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 03:4
9 Jul 2007 03:50	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 03:5
9 Jul 2007 04:00	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 04:0
9 Jul 2007 04:10	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 04:10
9 Jul 2007 04:20	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 04:2
9 Jul 2007 04:30	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 04:3
9 Jul 2007 04:40	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 04:4
9 Jul 2007 04:50	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 04:5
9 Jul 2007 05:00	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 05:0
9 Jul 2007 05:10	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 05:10
9 Jul 2007 05:20	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 05:2
9 Jul 2007 05:30	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 05:3
9 Jul 2007 05:40	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 05:4
9 Jul 2007 05:50	ARGENT-SE...	¥200z/NT	REL_DEMO	PRF_DEMO	Yes/Memo, by Ad...	Demo Argent Rule	9 Jul 2007 05:5

The event view can be sorted by a column.

Event Detail can be seen by zooming in on the event.



The Argent Predictor Chart shows the trend for the event.

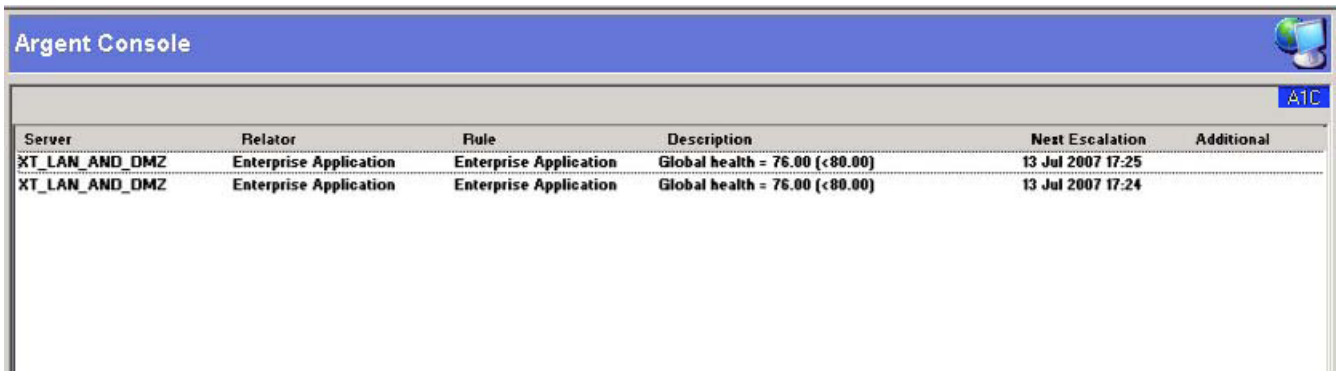


Events View can also perform the following functions;

- Purging of single or selected events from the Event View into the Event Archive
- Answering of Events – adding comments to Event
- Run Report Wizard against device that generated the Event
- Display Run Book for Rule that generated the Event (A Run book is the optional text file to explain to the reader what to do when the Rule is broken. It's a simple text file created by the person who creates or updates the Rule.)
- Display SuperLinks – hyperlink to a web page

Argent Escalation View

The Escalation View allows you to see the escalation status of unanswered Events:



Server	Relator	Rule	Description	Next Escalation	Additional
XT_LAN_AND_DMZ	Enterprise Application	Enterprise Application	Global health = 76.00 (<80.00)	13 Jul 2007 17:25	
XT_LAN_AND_DMZ	Enterprise Application	Enterprise Application	Global health = 76.00 (<80.00)	13 Jul 2007 17:24	

A powerful and popular feature of the Argent is Alert Escalation. Alert Escalation enables you to define a series of alerts.

An unlimited number of additional Alerts can be sent, until the issue is corrected. This means no critical issue is ever missed.

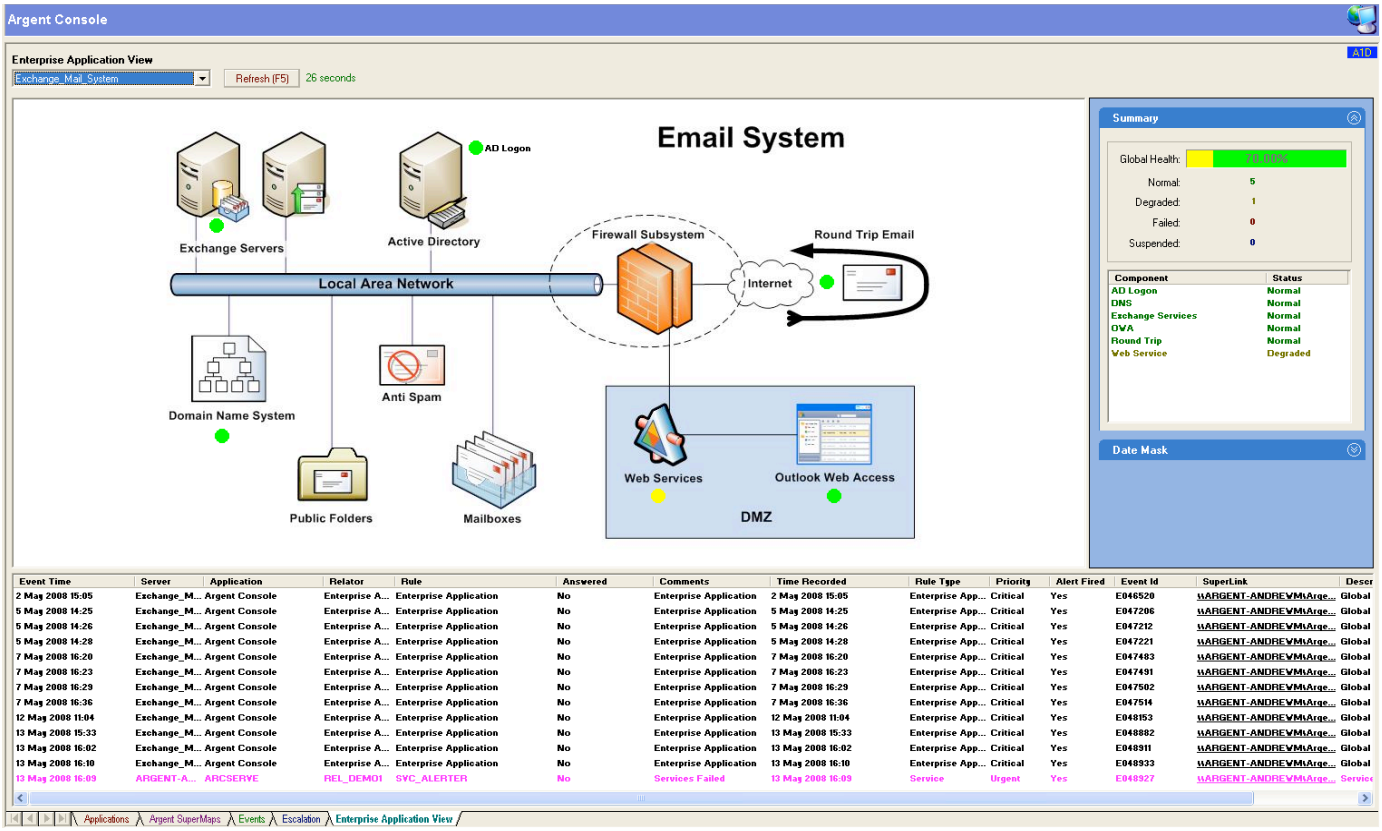
For example, if the first Alert is not answered within a certain time, say 10 minutes, a second Alert is then sent.

In addition, once the broken Rule is back within bounds additional Alerts can be fired to cancel the original Alphanumeric Pager Alert and Email Alert.

Argent Enterprise Application View

The Enterprise Application View allows you to view Events as you apply to various Applications running in the environment or as ITIL Service type Views. Instead of looking at the status of individual servers or devices, you can look at the big picture.

For example, you could create an Email Application View (below).



This would combine the following type of metrics as an example;

- Round Trip Email test
- Outlook Web Access site responding
- Exchange specific DNS
- AD Authentication checks
- Exchange Services
- Firewall Availability
- Exchange Mail Queues

These metrics would also be given a weighting to represent there importance in the application.

Typically the metrics in these views would represent components that affect the users' experience of the application.

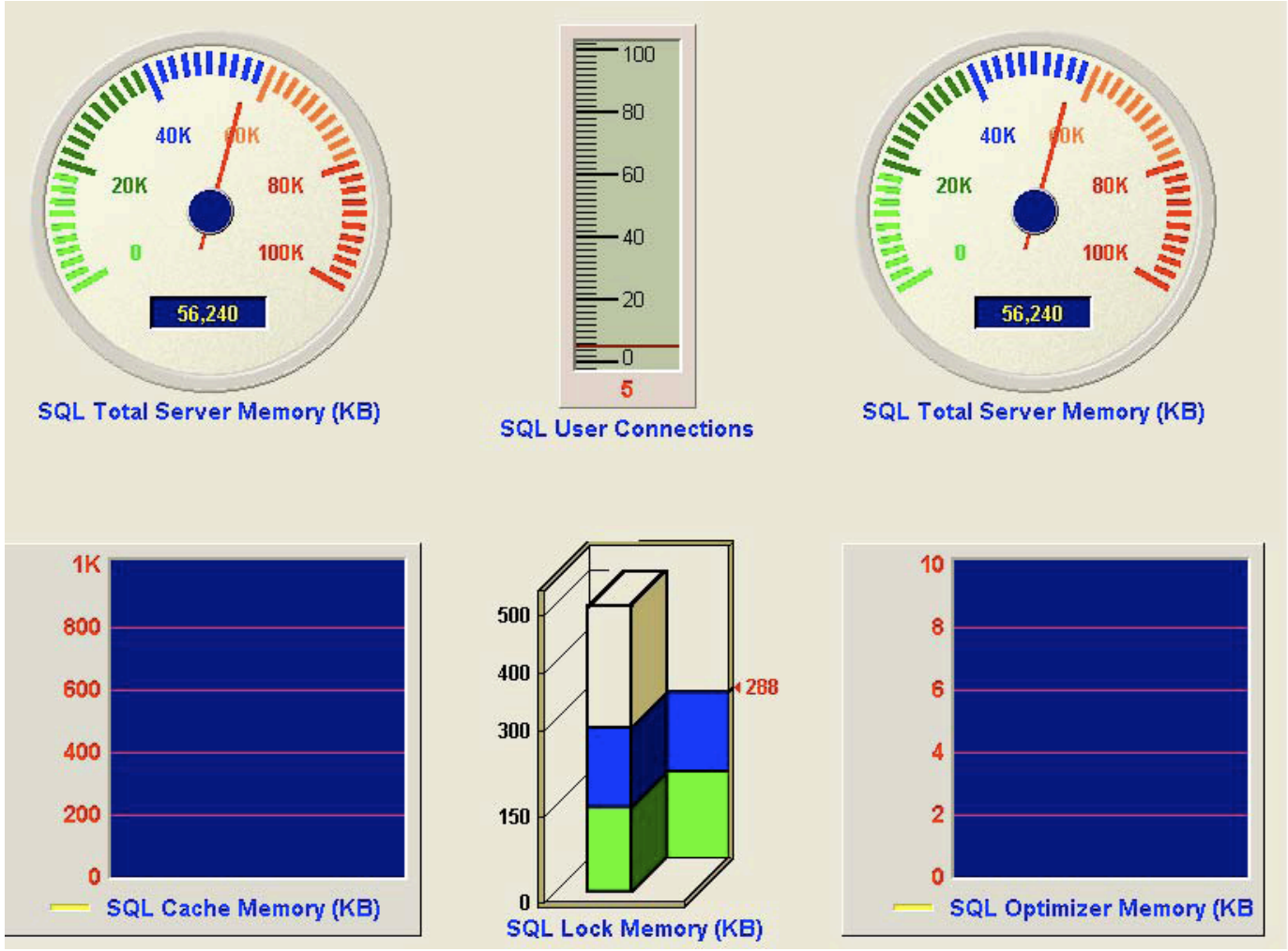
Some work will need to be done on specifying what each Service View is made of and what are the critical components. These views would typically be set up once the base metrics are in place and the alerting system is working to process.

The Enterprise application views are also able to generate separate events that can be used to alert the business (service delivery manager) with its own alerts separate from the engineering team.

Argent Dashboards

You can leverage Argent's powerful visual display technology by using the rich array of real-time Argent Controls in your own existing applications. All your existing applications running on any platform can use the Argent Dashboard. For example a web or intranet application can dynamically display logon counts and error rates.

The screen below shows an example Dashboard View – each of the controls can be customised.



Any application capable of creating an 8-byte ASCII text file can display any Argent Control in your Argent Dashboard.

In other words, any application able to periodically update the ASCII text file in a W200x directory can use the Argent Dashboard in real time. (Just use a shared directory or gateway for other server platforms, such as UNIX, Linux, or iSeries to write the 8-byte ASCII file.)

Also any Windows Performance counter, SNMP metric or Shell Script results can be used to display a control in real-time.

Threshold can be set for these controls and alerts triggered also.

Security

The Argent Security Manager lets you control how your users work with the Argent Products by letting you assign various level of permission granted to the users. You can select any or all of the following and limit users:

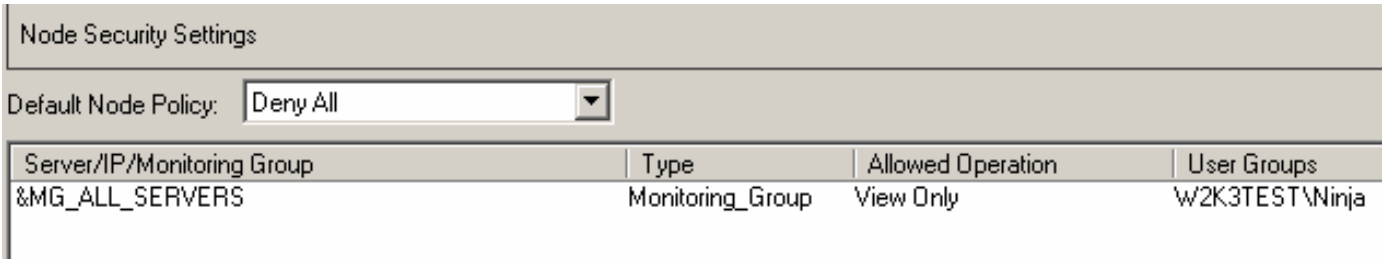
- Start/Stop Service
- Backup/Restore Database
- Apply License
- View Console And Change Console Settings
- Answer Pending Events And Purge Events Manually
- View/Modify Engine Settings
- Fire Event Through Total Support Interface
- Maintain/Modify Master Catalog
- Install/Modify Argent SuperMaps
- View/Modify General Database Information
- Put Relator To Production Mode Or Test Mode
- Server-Level Security Controlling Events Viewed/Answered By Console Operators
- Modify/View Definitions

The security settings are specific for each product (Argent Console, Argent Guardian etc), so the Argent Console can have a system administrator different from the Argent Guardian.

The Argent Security Manager also allows control of the Views in the Argent Ninja and Business Manager, by providing security that restricts some users to viewing:-

- Individual Devices
- Monitoring Groups
- SuperMaps
- Enterprise Application Views

Argent Security Manager can authenticate users against Local Computer accounts or Domain Based Accounts.



Service Desk Integration

Argent Extended Technology supports native integration with the following Service desk packages:-

- Tivoli
- Remedy
- Max/E

Other Methods for Integration include

Append To ASCII File - This option allows the Argent Console to append Alert details to a specified ASCII file that can be passed over or passed to a Third Party Help Desk. This System Help Desk Alert allows the Argent Console to interface with Third Party Applications and Help Desks. This allows the Argent Console to raise calls or register incidents with the designated help desk system, automating the monitoring procedure.

Utilising and customising any of the Argent Alerts such as-

SNMP Traps - Forward Argent information as an SNMP trap to any system that supports receiving and configuration of Trapping Information. The Argent SNMP Alerts causes Argent Console to send an SNMP trap containing the details of the broken Rule.

Email Alerts - sending formatted emails to a mailbox read by the Service Desk product.

SQL Alert - Execute a SQL statement on the Service desk Database.

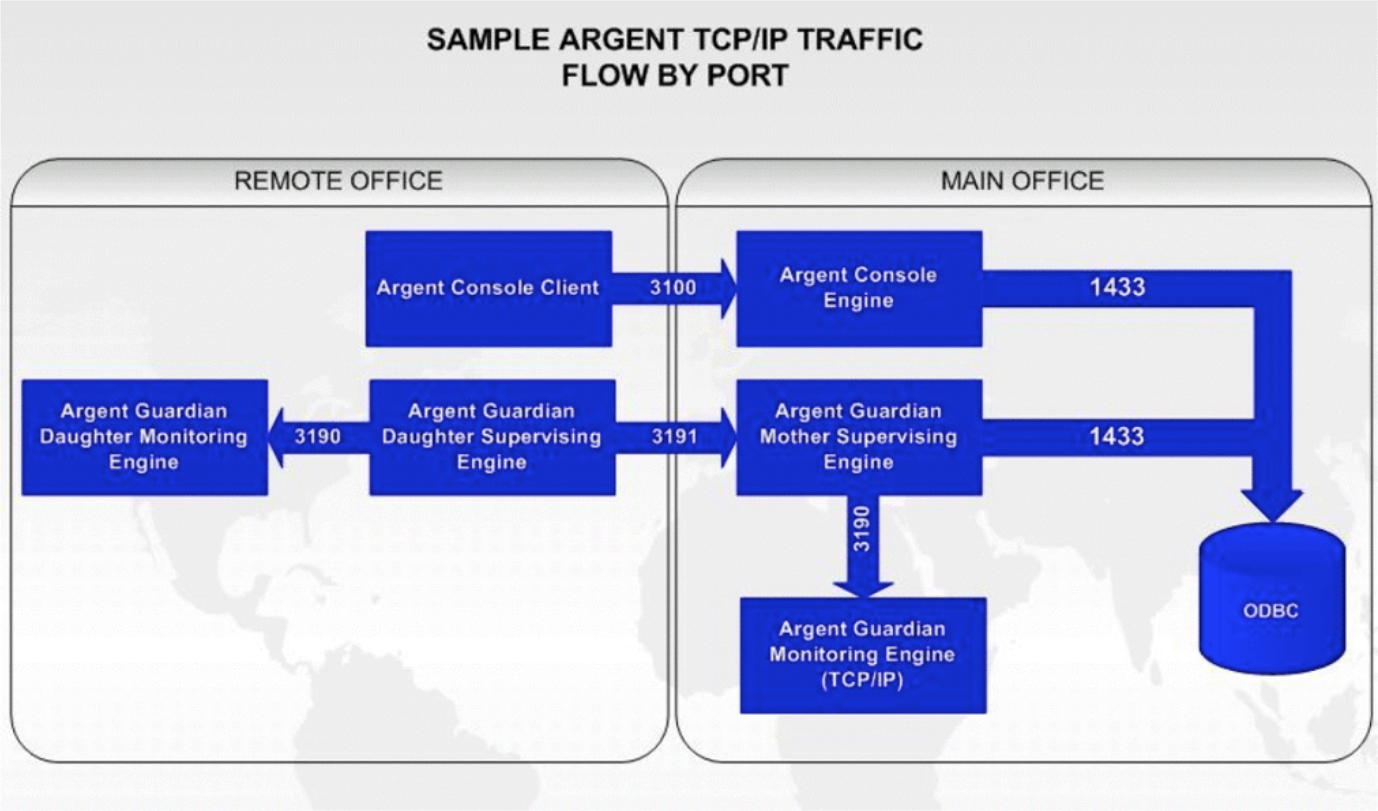
System Command - execute an external script with variables against the Service Desk product.

WMI Alerts - execute VBscripts directly against Service Desk API.

Integration with the Service desk is a Professional Service that Argent can provide as part of the Implementation of the Argent Extended Technology Suite; it will involve input from the Service desk vendor and the customer to achieve the best-fitting integration solution.

Appendix A - TCP Ports Used By Argent XT

3100	Argent Console
3171	Argent Data Consolidator Supervising Engine
3170	Argent Data Consolidator Transfer Engine
3160	Argent Data Consolidator Database Engine
4780	Argent Global Directory Central Location
3191	Argent Guardian Supervising Engine
3190	Argent Guardian Monitoring Engine
4381	Argent Monitor for Oracle Supervising Engine
4380	Argent Monitor for Oracle Monitoring Engine
5881	Argent SAP Monitor Supervising Engine
5880	Argent SAP Monitor Monitoring Engine
4481	Argent Sentry Supervising Engine
4480	Argent Sentry Monitoring Engine
4281	Argent SQL Server Monitor Supervising Engine
4280	Argent SQL Server Monitor Monitoring Engine
4581	Argent SNMP Monitor Supervising Engine
4580	Argent SNMP Monitor Monitoring Engine
4881	Argent WMI Monitor Supervising Engine
4880	Argent WMI Monitor Monitoring Engine



Appendix B - TCP Ports Used By Argent Defender

3209	Argent Defender Trusted Agents
3229	Argent Defender Root Cause Analysis Script Executors