

ELM ENTERPRISE MANAGER™

WHITE PAPER SERIES

REAL-TIME MONITORING
FOR MICROSOFT ISA SERVER

- ELM ENTERPRISE MANAGER™ -
REAL-TIME MONITORING
FOR MICROSOFT ISA SERVER



Software

www.tntsoftware.com

2001 Main Street

Vancouver, WA 98660 USA

Phone 360.546.0878 • Fax 360.546.5017

info@tntsoftware.com

TABLE OF CONTENTS

ABOUT TNT SOFTWARE.....	1
INTRODUCTION	2
How ELM Enterprise Manager Works	3
Summary of Benefits	3
Using this Paper	4
ISA SERVER EVENTS	5
Collecting, Archiving And Monitoring Events.....	5
PREPARING YOUR ISA SERVER.....	7
Installing Agents	7
MONITORING ISA SERVER PERFORMANCE	10
Establishing Performance Baselines	10
Trending	12
Tuning ISA 2000	13
Capacity Planning.....	14
Performance Alarms	14
COLLECTING, ANALYZING AND RESPONDING TO SYSTEM EVENTS	17
The Windows 2000 Event Structure	17
What to look for	18
CONCLUSIONS AND SUMMARY	44
EXPLANATION OF RECOMMENDED PERFORMANCE COUNTER OBJECTS.....	45
ISA Server – Bandwidth Control.....	45
ISA Server – Cache	45
ISA Server – Firewall Service.....	47
ISA Server – H.323 Filter	49
ISA Server – Packet Filter.....	49
ISA Server – Web Proxy Service	49
Logical Disk.....	53
Memory	54
Network Interface	55
Paging File	56
Physical Disk	56
Process.....	56
Processor	57
Redirector	57
Server	58
System	59
ISA SERVER FIREWALL AND WEB PROXY LOG FILE ENTRIES.....	60

FOREWORD

ABOUT TNT SOFTWARE

TNT Software is a Microsoft ISV that develops solutions for Microsoft's Windows operating systems. Our products help automate and simplify the administration of Windows.NET, Windows XP, Windows 2000, Windows NT and TCP/IP devices and services.

We specialize in building administration tools for Microsoft's Windows operating systems. Drawing from years of experience, we have a unique understanding of the importance of having solid tools available to support the administration of today's complex networks.

TNT Software is a private company located in Vancouver, Washington. Our clients include companies of all types, from manufacturing to universities, from news agencies to communications companies, and from aerospace companies to government agencies.

If you would like more information on TNT Software, or any of our products, please visit our web site at <http://www.tntsoftware.com>, or send email to info@tntsoftware.com.

INTRODUCTION

Why ELM Enterprise Manager?

Microsoft's Internet Acceleration and Security (ISA) Server provides secure, fast, and manageable Internet connectivity. ISA Server integrates an extensible, multilayer enterprise firewall and a scalable high-performance Web cache, and it builds on Windows 2000 security and directory services for policy-based security, acceleration, and management of internetworking.

These days, access to the Internet is the norm and not the exception. However, access to this powerful tool and vast web of information does not come without risk. Every single day hackers and crackers try to break into systems and networks, exploit known vulnerabilities for the fun of it, and attempt to steal data. More than ever, administrators need to take a wholistic approach when it comes to maintaining the reliability, availability and security of their networks, servers, applications and data.

Using ELM Enterprise Manager, you can implement proactive management techniques for monitoring your ISA Servers. ELM Enterprise Manager enables you to monitor all aspects of your ISA Server infrastructure, without requiring any add-on modules or the learning of any scripting languages. This type of wholistic management ensures that technical support resources are utilized in the most effective manner possible.

The goal of a responsible ISA Server administrator is to maximize proactive management and minimize reactive management. With proactive management, you are in control; with reactive management you have no control. ELM Enterprise Manager allows you to proactively manage your ISA Servers, permitting you to stay in control.

HOW ELM ENTERPRISE MANAGER WORKS

ELM Enterprise Manager has three main components, the ELM Server, the ELM Console and Agents. Agents are configured, installed and uninstalled directly from the ELM Console, which is the primary user interface for ELM Enterprise Manager. Agents can be physical agents that are installed as a service on the monitored system, or logical (remote) agents where the computer is monitored remotely from the ELM Server without installing any agent software on it.

Monitor Items are assigned to Agents. Monitor Items are the specific items that you want to Monitor. For example, you might assign the following Monitor Items to an Agent that is monitoring an ISA Server:

- **Event Collector.** This Monitor Item collects events and forwards them to the ELM Server for filtering and archiving. Ideally, you will want to monitor the event logs on all ISA Servers, as well as other critical servers in your organization.
- **Service Monitor.** This Monitor Item monitors one or more services/devices. Like many server/network-based applications, ISA Server runs as a set of services on a Windows 2000 Server family product. Service Monitors are used to monitor the state of services (e.g., stopped, started, stopping, starting, paused).
- **Process Monitor.** Each of ISA Server's services represents a specific process. In addition to monitoring these processes for instantiation and termination, you'll want to watch them to make sure they do not monopolize the CPU and cause the system to become unresponsive.
- **File Monitor.** ISA Server can log its activity to file system-based files in W3C and ISA formats. Both of these formats are text-based and can therefore be monitored with a File Monitor.
- **Performance Data Collection Sets.** These Monitor Items are used to collect the values for one or more performance objects, counters and/or instances at scheduled intervals. Regularly collecting performance data is the only way to baseline and trend a server's true performance over time. Without establishing a baseline and then watching performance trends you will not be able to accurately perform capacity planning. In addition to collecting performance data, you'll want to watch various performance counters for thresholds.

SUMMARY OF BENEFITS

ELM Enterprise Manager provides total monitoring for your ISA Servers. By monitoring events, performance data, services and processes, and ISA Server log files, ELM Enterprise Manager enables you to take a proactive approach to server management. With ELM Enterprise Manager you can:

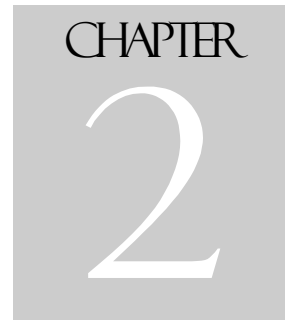
- Monitor your servers' event logs in real-time, and store the events in a database for archiving and auditing;
- Collect and store all published performance counters for baselining, trending and capacity planning;
- Monitor ISA Server log files in the file system;
- Create top-level and drill-down reports of your event data and performance data;

REAL-TIME MONITORING FOR ISA SERVER

- Send and receive alert notifications, including via email and pager, when events occur, services fail or performance exceeds thresholds;
- Automatically restart failed services;
- Stop and start services locally and remotely;
- Kill processes locally and remotely;
- and more...

USING THIS PAPER

This paper is based on ELM Enterprise Manager 3.0, Windows 2000 with Service Pack 2 and ISA Server 2000 with Service Pack 1. We assume that you have already installed and configured ELM Enterprise Manager. For information on installing and configuring ELM Enterprise Manager, review the [Getting Started Guide](#), as well as the product Help file (EEMMMC.CHM) which contains complete product documentation.



ISA SERVER EVENTS

Collecting and Analyzing Events on a Microsoft ISA Server

ISA Server is capable of generating a variety of error and event messages. These messages, which contain important information about the completion of normal tasks, as well as error messages about problems that occur, should be reviewed daily. But you can't research an event or correct any problems until you're aware of them. It's not practical to manually monitor the event logs on a single server, let alone multiple servers.

COLLECTING, ARCHIVING AND MONITORING EVENTS

The ELM Server receives the events from each monitored Agent and displays them in the Events window, which can be sorted a number of ways by clicking the desired column once or twice with the left mouse button.

In addition, you can create customized views for displaying specific events. ELM Enterprise Manager ships with several pre-defined views, including views designated as security views. You can further modify the pre-defined views, or create your own from scratch. This is helpful if you want to isolate events from a specific computer, a specific type of computer, a group of computers, or a specific type of event from one or more computers.

The ELM Server uses the defined Event Filters against events as they arrive. Event Filters are used to process, select, and group events. Event Filters are also used with Rules, which in turn trigger Notification Methods. In addition, Event Filters are processed to create Event Views.

REAL-TIME MONITORING FOR ISA SERVER

Depending upon what components are installed, ISA Server registers some or all of the following event sources:

- ISS Filter
- Microsoft Firewall
- Microsoft Firewall RPC Filter
- Microsoft Firewall Streaming Filter
- Microsoft H.323 Gatekeeper
- Microsoft ISA Firewall H.323 Filter
- Microsoft ISA Report Generator
- Microsoft ISA Server Control
- Microsoft Scheduled Cache Content Download
- Microsoft Web Proxy
- SOCKS Filter

Events from these sources appear in the Application log. ISA Server is capable of logging thousands of different informational, warning and error events. It is critical to find out about some events immediately; however, given the large number of events ISA Server can generate it is impossible to manually wade through them all.

ELM Enterprise Manager automates and simplifies the process of monitoring, collecting and filtering events. Both Views and Notification Methods are based on (and generated by) filters. You can use several levels of filtering so views only show specific events, and so that notification or corrective action only take place for certain events.

PREPARING YOUR ISA SERVER

Installing and Configuring the Agent on a Microsoft ISA Server

The ELM Enterprise Manager Agent is deployed remotely from within the ELM Enterprise Manager Console. You will need administrative privileges on the ISA Server to do this, but you do not need any special privileges within ISA Server itself.

INSTALLING AGENTS

- » To install a Service Agent:
1. Right-click on the Agents container in the ELM Console and select New | Agent. The Agent Installation Wizard will launch. If the Welcome dialog is displayed, click **Next** to continue.
 2. From the dropdown, select **Service Agent** and click **Next** to continue.
 3. Enter the **name** or **IP address** of the system you want to monitor. Click the **Browse** button to browse your network if you are unsure of the computer's name. Click **Next** to continue.
 4. Using the dropdown, select **Service Agent**. Click **Next** to continue.
 5. In the **Listen on TCP Port** field, enter the TCP port on which you want the Agent to listen. Service Agents communicate with the ELM Server over TCP/IP sockets. By default, Service Agents listen on TCP port 1253. You can change the port used by the Agent by selecting an alternative TCP port. Use the **Test** button to verify that the port is available.

 **Note**

Once an Agent has been configured to listen on a specific port, you cannot change the port. If you want the Agent to listen on a different port, you will need to remove and re-add the Agent using the new port.

- Click **Next** to continue. The copy file process will begin. The Agent executable, companion DLL files and configuration data will be copied to the target computer.



Important

In order to install a Service Agent, you must have administrative rights on the monitored system. ELM will attempt to install the Service Agent using your current credentials (e.g., the account you're logged on with); if this account does not have administrative rights on the Service Agent, you will be prompted to specify alternate credentials to perform the installation. Another alternative is to use the setup package you downloaded to [install the Service Agent remotely](#).

- The Agent Categories dialog will appear. Modify the **Categories** field as desired, or leave the default entries. Click **Next** to continue.
- If there are no monitor items configured, click **Finish** to complete the Wizard. If there are monitor items, the **Select Monitors** dialog will appear. In this event, click on each Monitor Item you want applied to this Service Agent. To create a new Monitor Item, right-click in the white space in this dialog and select **New Monitor Item**.
- Click **Next** to continue, then click **Finish**. A service called the TNT Agent will be installed and started, and real-time monitoring of the Service Agent will commence.
- Click **OK** to acknowledge the Agent installation. When prompted to install another Service Agent, click **Yes** or **No**, depending on your needs.

You can also monitor ISA Servers without having to install a Service Agent. This is done by using a Remote Agent. Note that Remote Agents cannot monitor systems in real-time, and they cannot be assigned File Monitors.

➤ To install a Remote Agent:

- Right-click on the Agent container in the ELM Console snap-in and select **New | Agent**. The Agent Installation Wizard will launch. If necessary, click **Next** to continue.
- From the dropdown, select **Remote Agent** and make sure the **IP Agent** checkbox is not checked. Click **Next** to continue.
- Enter the **name** or **IP address** of the system you want to monitor. Click the **Browse** button to browse your network if you are unsure of the computer's name. Click **Next** to continue.
- Modify the **Categories** field as desired, or leave the default entries.
- Click **Next** to continue. If there are no monitor items configured, click **Finish** to complete the Wizard. If there are monitor items, the **Select Monitors** dialog will appear. In this event, click on each Monitor Item

you want applied to this Service Agent. To create a new Monitor Item, right-click in the white space in this dialog and select **New Monitor Item**. Click **Next** to continue. Click **Finish**.

6. Click **OK** to acknowledge the Agent installation. When prompted to install another Remote Agent, click **No**.

The Remote Agent will be added to the list of monitored systems, and the selected Monitor Items for this Remote Agent will be executed according to their settings.

MONITORING ISA SERVER PERFORMANCE

Baseline and Trend your Microsoft ISA Servers

Before you can properly analyze growth – and its effect on performance – you must have a starting point for your analysis. This starting point is known as a **baseline**. A baseline is the initial performance snapshot; performance data that is collected immediately prior to putting the server into production. Without a baseline, it is impossible to determine performance trends over time, or perform any useful capacity planning.

ESTABLISHING PERFORMANCE BASELINES

Baselining a Windows 2000 system is fairly easy, especially with a tool like ELM Enterprise Manager at your disposal. Windows 2000 publishes an extensive list of performance counters; this list is further extended to include ISA-specific performance counters when ISA Server is installed.

Each published object has one or more counters that provide information on the object's utilization. We recommend that you collect data for both Windows 2000 and ISA 2000 objects. In an ISA environment, there are several types of objects that need to be monitored. While the list of available objects is long, you don't need to collect all of them to get an accurate picture of your server's health.

The areas that need to be monitored are CPU, memory, disk, network, ISA Server Cache, ISA Server Firewall Service, ISA Server Packet Filter, and ISA Server Web Proxy Service. Specifically, we recommend monitoring the following objects and counters:

REAL-TIME MONITORING FOR ISA SERVER

Object	Counter	Object	Counter
Processor	Interrupts/sec % Processor Time	Server	Bytes Total/sec Errors Access Permissions Errors Granted Access Errors Logon Errors System Pool Nonpaged Bytes Pool Nonpaged Failures Pool Nonpaged Peak Pool Paged Bytes Pool Paged Failures Pool Paged Peak Server Sessions Sessions Errored Out Sessions Timed Out Work Item Shortages
Process	Handle Count Pages Faults/sec Page File Bytes % Processor Time Private Bytes Thread Count Virtual Bytes Working Set		
Paging File	% Usage % Usage Peak		
System	% Registry Quota in Use Processor Queue Length System Calls/sec System Up Time	Memory	Available MBytes Cache Faults/sec Committed Bytes Commit Limit Page Reads/sec Page Writes/sec Pages/sec Page Faults/sec % Committed Bytes in Use Pool Nonpaged Bytes
LogicalDisk	Avg. Disk Queue Length Avg. Disk Sec/Transfer Current Disk Queue Length Disk Reads/sec Disk Writes/sec Free Megabytes % Free Space	Network Interface	Bytes Total/sec Packets Outbound Errors Packets Received Errors
Redirector	Bytes Total/sec Current Commands Network Errors/sec Reads Denied/sec Writes Denied/sec	PhysicalDisk	Avg. Disk Sec/Read Avg. Disk Sec/Transfer Avg. Disk Sec/Write Current Disk Queue Length
ISA Server Cache	Disk Bytes Retrieved Rate (KB/sec) Disk Cache Allocated Space (KB) Memory Bytes Memory Cache Memory Usage Ratio Percent URLs in Cache	ISA Server Firewall Service	Active Sessions Active TCP Connections Active UDP Connections Available worker threads Bytes read/sec Kernel mode data pumps SecureNat mappings Worker threads

REAL-TIME MONITORING FOR ISA SERVER

Object	Counter	Object	Counter
ISA Server Packet Filter	Cache running hit ratio (%) Client bytes total/sec Current avg ms/request Current users Requests/sec Total Dropped Packets	ISA Server Web Proxy Service	Cache hit ratio (%)

Note: Physical disk counters are only available after **diskperf -y** is run to enable them. This command is run from the command line, and it requires a reboot to take effect. On systems using software RAID, the command used should be **diskperf -ye**. There is a space between **diskperf** and the option specified (-y or -ye). Physical disk counters can be turned off by using **diskperf -n** and rebooting. Collecting physical disk counters does add additional overhead to the system, but this overhead is well worth the benefits of having the physical disk counters available.

These counters should be collected continuously at regular intervals throughout the life of your ISA servers. Regular analysis of this data allows you to trend the growth of your server and perform capacity planning.

TRENDING

Trending is the analysis of data collected over time. Analyzing trends is important for two reasons. First, it allows an administrator to assess usage patterns. Second, it provides a mechanism for capacity planning. Usage of ISA resources always has highs and lows, especially within 24x7 environments. For this reason, it is important to collect performance data at regular intervals over a 24-hour period. This will provide you with an accurate picture of usage, without adding the overhead associated with continuous real-time monitoring (e.g., collecting every second). We recommend collecting performance data at 5-15 minute intervals; by doing so, you'll learn a great deal about your ISA environment. You'll also start to recognize performance patterns. By understanding these patterns, you'll be able to quickly spot out-of-bounds activity.

As demands for ISA resources increase – due to an increase in the number of users, the addition of ISA-based components, and so on – a historical record of performance data helps to identify bottlenecks. The system component that causes the most delay in the execution of a process or a task is known as a **bottleneck**. The primary goal of system optimization is to eliminate all bottlenecks. The challenge is that, eliminating one bottleneck frequently produces another bottleneck somewhere else. For example, adding a more powerful CPU might result in a memory bottleneck. Adding more memory to compensate might then over-task your disk subsystem, and so on, and so on.

Fortunately, with proper analysis, operating system bottlenecks are generally easy to spot. For example, if the value of Processor - % Processor Time consistently exceeds an average of 80%, Microsoft recommends upgrading your processor. If your paging file is correctly sized and the value for Paging File - % Usage is consistently more than 80%, you should add memory to your system. If the number of disk I/Os per second is greater than the rated value for your disk subsystem, then you need to upgrade your disk subsystem.

TUNING ISA 2000

The greatest variable in tuning ISA Server is environmental variations. Every organization is different in many respects. Companies may have very similar needs but they choose solutions that can differ significantly. Given the number of choices for processors, memory, and disk configurations, you'll definitely want to do some tuning beyond what ISA Server does for itself.

The health and performance of ISA 2000 depends in large part on the choice of server specifications, storage hardware, and topology. These factors should be based on expected levels of usage. Further tuning can be accomplished by modifying the Registry on the ISA server.

ISA Server includes administration COM objects, which are described in the SDK documentation on the ISA Server CD. You can access the ISA Server configuration via a script that includes these COM objects. A few additional configuration options are available only via the Administration COM objects.

You can use the ISA management snap-in to configure ISA Server. Some low-level settings, which can help fine-tune performance, can be set only via the registry. You can modify a few registry entries on your ISA Server to optimize cache performance. After modifying any of the following registry settings, you will need to reboot the computer for your changes to take effect.

The table below lists and describes the registry keys and recommended values. All of the following registry keys are in the specified location under HKLM\System\CurrentControlSet\Services.

Registry Key	Location	Value (DWORD)	Description
TZ Persist Interval Threshold	W3Cache\Parameters	00000001	This key sets the maximum time interval (in minutes) for which recovery data is inconsistent. This value indicates that at most one minute will be lost when cache is recovered if the w3proxy service stops unexpectedly.
Recovery Mru Size Threshold	W3Cache\Parameters	00000005	This key sets the time interval (in minutes) which will be recovered first from the time the w3proxy service stops unexpectedly. This value indicates that content cached in the last five minutes (prior to service shutdown) will be recovered first.
MaxClientSession	W3Proxy\Parameters	00002800	This key sets the size of the pool for the Client Session object. This value means that a client session object is freed and its memory returned to system memory management only if the pool has more than 10240 (2800 Hex) objects. Since freeing an object is time consuming, this key is initially set to a high value.
OutstandAccept	W3Proxy\Parameters	000003e8	This key sets the number of listeners that are waiting for a connection to be established. This value means that there can be 1000 (3e8 Hex) accepts pending for a connection to be established

Registry Key	Location	Value (DWORD)	Description
			before rejecting new connection requests. This value is initially set to a high value to minimize the number of rejected connection requests.
MaxUserPort	Tcpip\Parameters	0000ffff	This key sets the maximum number of TCP/IP ports that can be allocated by a client requesting a connection. This value sets the range for client port numbers to maximum.
TcpTimedWaitDelay	Tcpip\Parameters	3c	This key sets the time interval (in seconds) before a given socket can be reused for a new connection.
StrictTimeWaitSeqCheck	Tcpip\Parameters	1	When set to 1, this key indicates that a socket should not be reused before the time specified by TcpTimedWaitDelay passes.

CAPACITY PLANNING

Capacity planning is a little more difficult than baselining or trending. The answers aren't going to jump out at you like a dramatic change in performance will. Capacity planning is the determination of future server needs to the extent possible. The primary goal of capacity planning is to ensure that you have room for growth, and to let you know when additional resources are needed.

Capacity planning for an ISA infrastructure involves determining current and future needs, and then selecting the hardware resources that meet estimated needs. However, it can also mean upgraded hardware to meet new needs as they arise. Because there are so many variables, and because needs change so rapidly, capacity planning typically requires an iterative approach.

The important thing to remember is that, without a baseline and some trend analysis, capacity planning is impossible. By using ELM Enterprise Manager to collect and store your servers' performance data on a regular basis, you'll be able to baseline and trend your ISA infrastructure, and accurately determine when demand has exceeded available resources.

PERFORMANCE ALARMS

Even if you choose not to collect performance data, you can use **Performance Alarms** to monitor performance and generate alert messages when a performance counter object exceeds the threshold you specify. An Alarm is a condition where a selected performance counter is less than, greater than, or equal to a specific value. Alarms specify what action will be taken when a performance counter is greater than, less than or equal to the specified value for the specified period of time. By configuring Alarms, you'll be able to take action at the first sign of trouble. You can configure Alarms to send email messages and network messages, and even execute commands, batch files and applications.

➤ To create a Performance Alarm:

1. Right-click on the **Monitor Items** container in the ELM Console and select **New | Monitor Item**. The Create Monitor Wizard will appear. Click **Next** to continue.
2. Select **Performance Alarm** and click **Next** to continue.
3. Enter a **Name** and **Description** and click **Next** to continue.
4. The Performance Alarm Watch dialog box will appear.
 - a. In the **Object** drop-down, select the Performance Object you want to monitor. If the object you want to monitor is not listed, you can add additional objects and counters by clicking the **Add** button.
 - b. In the **Counter** drop-down, select the Counter you want to monitor.
 - c. To monitor all instances of a particular counter, leave an asterisk in the Instances field. To monitor a single instance, or a specific set of instances, click the **Add/Remove** button, enter the instance(s) you want to monitor and click **Close**. Alternatively, you can enter multiple instances directly in the **Instances** field; be sure to separate each instance with a semi-colon.
 - d. In the **Condition** field, enter the condition you want to match (e.g., less than, greater than, equal to, and so forth).
 - e. Enter the value you want to match in the **Value** field.
 - f. In the **Occurs** field, enter the number of consecutive times this condition can be met before triggering notification.
5. Click **Next** to continue. The Performance Alarm Action dialog box will appear. Configure the following options for each tab, and click **Next** to continue.
 - **Enable**. When this box is checked, the Action is enabled and will execute as configured. Uncheck this box to disable the Action.
 - **Create New Alert Entry**. Selecting this checkbox to cause an Alert to be generated and posted to the Alerts container within the ELM Console.
 - **Create Application Event Log Entry**. Selecting this enables you to cause a customizable event to be logged to the Application log. Use the **Variables** button to specify any additional variables you want the event to include.
 - **Net Send Message**. Using this option enables you to send a popup message over the network. The target system must have the Messenger Service (Windows NT, Windows 2000 or Windows XP) or WinPopUp (Win9x/WinMe) running in order to receive the Net Send Message. Use the **Browse** button to browse for a target computer, or manually enter the name of the computer to which you want to send messages in the Computer Name field.

- **Run Command.** This option provides a mechanism for executing a batch file, running a command line application or launching a script (CScript or WScript). Use the Edit button to create and edit any scripts or command line parameters you want to execute.
6. The Test Monitor Item dialog box will appear enabling you to test the Performance Alarm before using it. To do this, select an Agent on from the Agent dropdown and click the **Start Test** button.
 7. Click **Next** to continue. The Agents dialog box will appear. Check the checkbox for each Service Agent to which you want to apply the Performance Alarm.
 8. Click **Next** to continue. The Schedule dialog box will appear.
 - On the Scheduled Interval tab, set the frequency at which you want to execute the Alarm. Leaving the interval at the default of 1 second will enable you to monitor the performance counter or object in real-time.
 - On the Scheduled Hours tab, configure the hours and days you want this monitor active.
 9. Click **Finish** to save the Performance Alarm.



COLLECTING, ANALYZING AND RESPONDING TO SYSTEM EVENTS

Capturing and analyzing System, Security and Application events

ISA Server, like many other applications, makes use of the Windows 2000 event subsystem for reporting critical and information messages regarding system events and activities. Careful monitoring of system events can help you identify – and sometimes even predict – system problems. For example, if you see a low disk space event on a heavily used file server, it is likely you're about to run out of disk space. Events can also be used to confirm problems with applications. For example, application events can provide a record of activity leading up to a catastrophic event, such as an application crashing, or the like.

THE WINDOWS 2000 EVENT STRUCTURE

Before you can use event data to diagnose problems, it is essential to have a basic understanding of interpreting the event that is logged. Events are made up of three distinct parts: the Header, the Description, and the Data.

The **Header** contains important information such as the date and time of the event, the event type (e.g., Informational, Warning, Error, Audit Success and Audit Failure), the user and computer name, the event source, the event ID and the category.

The **Description** field contains details on the exact event that occurred. This will vary between event types and, quite frankly, the details aren't always helpful in determining the problem (although they typically will point you in the right direction).

The **Data** field contains binary data for the event. This data is typically used for advance troubleshooting purposes by Microsoft Product Support Services (PSS). Mere mortals generally aren't going to be able to make use of this data. As a result, this data is not collected by ELM Enterprise Manager and can only be viewed using the Windows Event Viewer program.

ISA Server logs four different types of events (Success, Informational, Warning and Error). These events need to be interpreted in a different manner. Success and Informational events typically signify normal system or application operations. Informational events include service initialization or shutdown, background maintenance notification and backup success. Warning events indicate minor problems or inconsistencies that may cause a problem down the road. Error events are more critical and should be investigated upon discovery. They indicate potentially serious problems, such as a service failure or the impending shutdown of a service, the catastrophic failure of an application or hardware component, or some other urgent issue.

WHAT TO LOOK FOR

ISA Server is capable of logging thousands of different events. While some of these events can be safely ignored, others require some sort of administrative attention to either acknowledge them, or address them. The most common events will be service initialization and shutdown messages, background maintenance, and so forth.

The easiest way to track and process events is to set up Rules within ELM Enterprise Manager that process incoming events and trigger the Notification Method(s) you specify.

The table below lists the most common events that are logged on a typical ISA Server. All of the events below have an Event Source of **Microsoft Firewall**.

Event ID	Event Type	Description
1	E	The %1 was unable to load Odbc32.dll for SQL logging due to the following error: %1. The data is the error code. For more information about this event, see ISA Server Help.
1	I	Log
2	E	The %1 was unable to open ODBC Data Source %1, Table: %1, under User Name [%1]. The ODBC Error description is: %1. For more information about this event, see ISA Server Help.
2	I	Packet filter
3	E	The %1 was unable to create the log file directory %1. For more information about this event, see ISA Server Help.
4	E	The %1 failed to log information. The log object was never created possibly due to wrong configuration. For more information about this event, see ISA Server Help.
5	E	The %1 failed to log information to file %1 in path %1. The data is the error code. For more information about this event, see ISA Server Help.
6	E	The %1 failed to log information to ODBC Data Source %1, Table: %1, under User Name [%1]. The ODBC Error description is: %1. For more information about this event, see ISA Server Help.
7	I	The %1 created the log file directory %1 due to logging configuration changes.
10000	W	Name entered is too long. The name entered is either incorrect or has too many characters. Check that the name entered is a valid name. Type the name again and check that no added characters were included.
10000	I	Firewall Service
10001	W	System is not ready.

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
10001	I	Web Proxy Service
10002	W	Current version is not supported. For more information about this event, see ISA Server Help.
10002	I	ISA Server Control Service
10003	W	Service cannot send after socket shutdown. For more information about this event, see ISA Server Help.
10004	W	An interrupted system call was received. For more information about this event, see ISA Server Help.
10005	W	Host was not found. For more information about this event, see ISA Server Help.
10006	W	Try again. For more information about this event, see ISA Server Help.
10007	W	Nonrecoverable error encountered. For more information about this event, see ISA Server Help.
10008	W	No data record is available. For more information about this event, see ISA Server Help.
10009	W	Bad file number encountered. For more information about this event, see ISA Server Help.
10010	W	Operation would block. For more information about this event, see ISA Server Help.
10010	I	Service initialization
10011	W	Operation is in progress. For more information about this event, see ISA Server Help.
10011	I	Alert service initialization
10012	W	Operation is already in progress. For more information about this event, see ISA Server Help.
10012	I	Alert service storage opening
10013	W	Bad network address encountered. For more information about this event, see ISA Server Help.
10013	I	Alert Service storage reading
10014	W	Destination address required. For more information about this event, see ISA Server Help.
10014	I	Local Address Table (LAT) updating
10015	W	Message is too long. For more information about this event, see ISA Server Help.
10015	I	Log files sweeper initialization
10016	W	Protocol family not supported. For more information about this event, see ISA Server Help.
10016	I	Firewall Service remote procedure call (RPC) initialization
10017	W	Directory is not empty. For more information about this event, see ISA Server Help.
10017	I	Bandwidth Control Service remote procedure call (RPC) initialization
10018	W	EPROCLIM returned. A software error occurred. Too many processes are running simultaneously. Quit and restart the current application.
10018	I	Reading cache configuration
10019	W	EUSERS returned. For more information about this event, see ISA Server Help.

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
10019	I	Reading server Internet Protocol (IP) address
10020	W	Disk quota exceeded. The operation required additional disk space that is not authorized by the server. Cancel the current disk operation and change file share permissions to allow more space for the current user.
10020	I	Update of client configuration file
10021	W	ESTALE returned. An unexplained service error occurred in the current environment. Quit the application and restart it.
10021	I	Update of security level
10022	W	Invalid argument. For more information about this event, see ISA Server Help.
10022	I	Reading packet filters
10023	W	Too many open files. For more information about this event, see ISA Server Help.
10023	I	Log files sweeping
10024	W	Too many levels of symbolic links. A software error occurred. Contact the supplier of the current application.
10024	I	Bandwidth Control Service initialization
10025	W	The object is remote
10025	I	Handling Bandwidth Control Service change notification
10026	W	Socket operation was attempted on non-socket. For more information about this event, see ISA Server Help.
10026	I	Reading Bandwidth Control Service configuration
10027	W	Bad or unassigned address. For more information about this event, see ISA Server Help.
10027	I	Initialization of performance counters
10028	W	Address is already in use. For more information about this event, see ISA Server Help.
10028	I	Logging initialization
10029	W	Address family is not supported by protocol family. For more information about this event, see ISA Server Help.
10029	I	Initialization of Domain Name System (DNS) cache
10030	W	Socket type is not supported. For more information about this event, see ISA Server Help.
10030	I	Initialization of data pump
10031	W	Protocol is not supported. For more information about this event, see ISA Server Help.
10031	I	Quota initialization
10032	W	No buffer space is supported. The WinSock implementation was unable to allocate additional memory to accommodate the function request. For more information about this event, see ISA Server Help.
10032	I	Reading access rules
10033	W	Connection timed out. For more information about this event, see ISA Server Help.
10033	I	Initialization of control channel
10034	W	Socket is already connected. For more information about this event, see ISA Server Help.

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
10034	I	Chaining initialization
10035	W	Socket is not connected.
		For more information about this event, see ISA Server Help.
10035	I	Reading Local Domain Table (LDT)
10036	W	Unsupported protocol option used.
		For more information about this event, see ISA Server Help.
10036	I	Reading chaining configuration
10037	W	Connection reset by peer.
		For more information about this event, see ISA Server Help.
10037	I	Initialization of Network Address Translation (NAT)
10038	W	Software caused connection to abort.
		For more information about this event, see ISA Server Help.
10038	I	Initialization of dial-out phone book entry
10039	W	Network is down.
		For more information about this event, see ISA Server Help.
10039	I	Loading application filters
10040	W	Network was reset.
		For more information about this event, see ISA Server Help.
10040	I	Initialization of mapping pool
10041	W	Connection refused
10041	I	Initialization of reverse Network Address Translation (NAT).
10042	W	Host is down.
		For more information about this event, see ISA Server Help.
10042	I	Reading protocols
10043	W	Host is unreachable.
		For more information about this event, see ISA Server Help.
10043	I	Reading protocol rules
10044	W	Protocol is the wrong type for socket.
		For more information about this event, see ISA Server Help.
10044	I	Reading access rules
10045	W	Operation is not supported on socket. For more information about this event, see ISA Server Help.
10045	I	Reading bandwidth rules
10046	W	Internet Control Message Protocol (ICMP) network is unreachable. For more information about this event, see ISA Server Help.
10046	I	Reading proxy configuration
10047	W	Too many references used. The requested operation contained additional information that cannot be processed correctly through the remote connection. Retry the request, or contact the supplier for the current application.
10047	I	Reading logging configuration
10048	W	Not owner. You do not have permission or ownership rights to access this remote shared resource. Ask the network administrator to check permissions.
10048	I	Creation of logging module
10049	W	No such file or directory exists. The requested file operation cannot be completed because the file or directory does not exist on the remote server. Check file or

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
		directory settings.
10049	I	Reading publishing rules
10050	W	No such process exists. The requested operation is not recognized by the remote server. The operation might be the result of errors in data or invalid user input. Try the operation again.
10050	I	Reading client configuration
10051	W	System call interrupted. For more information about this event, see ISA Server Help.
10051	I	Creation of bandwidth flow
10052	W	Input/Output (I/O) Error encountered. The problem might be caused by instability in the local system environment. Quit the application and restart the computer. Try the operation again.
10052	I	Unavailable context
10053	W	No such device or address exists. For more information about this event, see ISA Server Help.
10053	I	Checking site of server
10054	W	Argument list too long. The requested operation contained additional information or parameters that cannot be processed correctly through the current connection. Retry the request.
10054	I	Storage notification handling
10055	W	Executed format error. A software error has occurred. Retry the operation.
10055	I	Setting ISA Server components
10056	W	Bad file number encountered. For more information about this event, see ISA Server Help.
10056	I	Execution of alert actions
10057	W	No children exist for parent object
10057	I	Setting load size
10058	W	Operation would block one in progress. For more information about this event, see ISA Server Help.
10058	I	Handling request to add bandwidth flow
10059	W	Not enough memory is available.
		For more information about this event, see ISA Server Help.
10059	I	Handling request to remove bandwidth flow
10060	W	Permission denied.
		The remote server refused access to the requested resource. Contact the administrator for the remote server and report the problem.
10060	I	Handling of cache dirs change
10061	W	Bad address encountered.
		For more information about this event, see ISA Server Help.
10061	I	The error description is: %1
10062	W	Mount device or directory is busy.
		The remote server drive is unavailable or is out of space. Wait and retry the requested operation.
10062	I	Handling of network configuration changes
10063	W	File already exists.
		The attempt to create or save a file on the remote server cannot be completed because a file of the same name already exists. Save the new file under a different name, or rename the old file.
10064	W	A cross-device link exists.
		A device on the remote server system that is required for this operation cannot be

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
		accessed for the current connection. Confirm that the device is available and is not already in use by other connected sessions.
10065	W	No such device exists.
		The device or address entered cannot be located on the network. Make sure that the device name or address has been entered correctly and that the device is operational and configured properly on the client computer.
10066	W	Is not a directory.
		A file object has been selected for the current operation where a directory was expected. Select a directory to complete this operation, or cancel the operation.
10067	W	Is a directory.
		A directory object has been selected for the current operation where a file was expected. Select a file to complete this operation, or cancel the operation.
10068	W	Invalid argument used.
		For more information about this event, see ISA Server Help.
10069	W	File table has overflowed.
		For more information about this event, see ISA Server Help.
10070	W	Too many files are open.
		For more information about this event, see ISA Server Help.
10071	W	Is not a typewriter.
		The current configuration does not support the attempted method of input. Check application instructions or contact the supplier of the application and report the problem.
10072	W	File is too large.
		A disk restriction did not permit the file operation to be completed. A disk quota might be set for the destination folder, or there is a lack of available space on the targeted drive. Verify that sufficient space is available on the drive and that the folder does not have disk space restrictions.
10073	W	No space is left on device. There is a lack of available space on the destination drive. The file copy operation cannot be completed, possibly because a disk quota has been set for the destination folder path. Make sure that the amount of disk space is sufficient on the destination drive and the folder does not have disk-space restrictions.
10074	W	Illegal seek performed. There is an error in shared file permissions or possible errors in the file table. Verify that permissions are set. If the problem continues, verify the integrity of the disk by using appropriate utilities for the disk operating system that is in use.
10075	W	Read-only file system in use.
		For more information about this event, see ISA Server Help.
10076	W	Too many links used. You have reached the maximum number of links that can be opened. Close other connections or applications and retry the operation. If the problem continues, report it to the application supplier.
10077	W	Pipe has broken. The current operation was suspended because the data or connection is experiencing a failing network connection or errors on the network.
		Reconnect to the remote source. If the problem continues, check for further errors on the network or excessive traffic on the network segment.
10078	W	Math argument used. The input for the current operation was of an invalid type or unexpected for the current application, possibly because of an error in the data or software-based restrictions. Enter the data again. If the problem continues, report

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
		the problem to the application supplier.
10079	W	Result is too large. The output for the current operation was invalid for the system or application, possibly because of an error in the data or because of software-based restrictions. Enter the data again. If the problem continues, report the problem to the application supplier.
10080	W	A resource deadlock would occur. The requested operation cannot be completed because sufficient resources do not exist or are not available on the local system. Close other applications to free resources or restart the system. If the problem continues, check your computer configuration.
10081	W	No message of desired type exists. A message cannot be located, or the current application does not support messages of this type. Verify that the message exists at the expected source location. If a message exists, report the problem to the application supplier or see the applications documentation.
10082	W	Identifier removed.
		For more information about this event, see ISA Server Help .
10083	W	Channel number is out of range. A port or protocol error has occurred in the application or network environment.
		Check that all service ports are defined correctly for the application and the Firewall service. If the problem continues, contact the application supplier to report the problem and obtain an updated file or workaround.
10084	W	Level 2 is not synchronized. There is a data line problem for the currently connected operation, possibly because of noise or interference on the line. Check for performance problems or further errors on the line. For further assistance in resolving the problem, report the line problem to your appropriate service provider.
10085	W	Level 3 halted. The network has been stopped. The current connection probably failed. Check the client network connection or have the client reconnect to the network. If the message is repeated for other clients, check for problems in network cabling or termination. Or, check that network hardware or software has not been stopped.
10086	W	Level 3 reset. The network has been reset, probably because an intermediate network host servicing the current connection (for example, a router) was reset. The current connection has failed. Reestablish the remote connection. If the problem continues, check for errors or excess traffic on the network.
10087	W	Link number is out of range. The number specified for linking is invalid. The link is broken.
		Attempt to re-create the link by using the options within the application. If the problem continues, contact the application supplier to report the problem and obtain an updated file or workaround.
10088	W	Protocol driver is not attached. There is no driver for a supported protocol bound to the network adapter on the local computer. Check the network configuration for the local computer. Verify that a supported network protocol for the Firewall service is bound to the network adapter.
10089	W	No CSI structure is available. A required, specialized component is missing. The operation cannot be completed within the active application. For further assistance in resolving the problem, contact the application supplier to report the problem and obtain an updated file or workaround.
10090	W	Level 2 halted. A problem has occurred at the data-link level, or the link connection has been cleared. Check for errors logged for data link or data communications hardware devices. For further assistance in resolving the problem, report the line to the appropriate service provider.
10091	W	An invalid exchange was made. There is an error in the data, or an exchange between the remote server and the client has been attempted that is not allowed within the software. Reenter the data and retry the operation. If the problem continues, contact the supplier of the current application to report the problem and obtain a fix or workaround.

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
10092	W	Invalid request descriptor used. There is an error in the data, or an exchange between the remote server and the client has been attempted that is not allowed within the software. Reenter the data and retry the operation. If the problem continues, contact the supplier of the current application to report the problem and obtain a fix or workaround for the problem.
10093	W	Exchange is full. There is an error in the data, or an exchange between the remote server and the client has been attempted that cannot be completed. The system might be too busy to process the request at this time. Retry the operation later. If the problem continues, contact the application supplier to report the problem and obtain an updated file or workaround.
10094	W	No anode exists. There is an error in the data or an exchange between the remote server and the client has been attempted that is not allowed within the software. Reenter the data and retry the operation. If the problem continues, contact the application supplier to report the problem and obtain an updated file or workaround.
10095	W	Invalid request code used. For more information about this event, see ISA Server Help .
10096	W	Invalid slot used. A configuration error in hardware settings has been applied by the current operation. Review the settings used for hardware device access or communication within the application to ensure that the settings are correct.
10097	W	Bad font file format used. A font file is of incorrect format or is outdated. To report the problem and obtain an updated file or workaround, contact the application supplier to report the problem and obtain an updated file or workaround.
10098	W	Device is not a stream. There is an error in the data, or an exchange between the remote server and the client has been attempted that is not allowed within the software. Reenter the data and try the operation again. If the problem continues, contact the application supplier to report the problem and obtain an updated file or workaround.
10099	W	No data was found. No data was received to complete the current operation. Enter the data again and retry the operation. If the problem continues, verify that the connection to the network is still active.
10100	W	Timer has expired
10101	W	System is out of streams resources. Insufficient streams buffers are available, or a buffer overrun has occurred. Increase the buffer count for streaming protocol (that is, Transmission Control Protocol (TCP)) or modify the connection rate.
10102	W	Machine is not on network. The local computer is not connected to the network. Connection to the network must be made before the request can be processed.
10103	W	Package is not installed. The requested application feature is not currently installed. Reinstall the application or upgrade to install the missing application feature. For more information, see the application documentation.
10104	W	The object is remote. For more information about this event, see ISA Server Help .
10105	W	The link has been severed. The current connection has been broken. Quit the application and check for other related communications hardware and software failures on the local computer. Restart the application and try to connect again. If the problem continues, check for other failures on the network or verify that the remote server has not been shut down or removed from the network.
10106	W	Advertise error occurred. For more information about this event, see ISA Server Help .
10107	W	Server mount error occurred. The server is advertising on the network, but a resource on the server is not mounted or is otherwise unavailable. Check for hardware failure on the remote server or to verify that the requested server resource is mounted.
10108	W	Communication error in sending. An error occurred in sending information between the remote server and the local client. Retry the requested communication. If the problem continues, check for network errors. If there are no significant errors on the network, contact the application supplier to report the problem.

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
10109	W	Protocol error encountered. A protocol error has occurred in the application or network environment. Check that all service ports are defined correctly for the application and the Firewall service. If the problem continues, contact the application supplier.
10110	W	Multihop attempted. For more information about this event, see ISA Server Help.
10111	W	Inode is remote. Input for the current operation cannot be obtained from a remote source. Contact the supplier of the current application to obtain and report the problem.
10112	W	Cross mount point achieved
10113	W	Trying to read unreadable message. The message input has errors or is of an incorrect type to be processed by this operation. Check the message data for errors or report the problem to the supplier of the current application.
10114	W	Log name used is not unique. For more information about this event, see ISA Server Help.
10115	W	Remote address changed. The network address for the remote server has been changed to a different address. Reconnect to the remote server, or contact the administrator for the remote server to obtain more information about this problem.
10116	W	Can't access a needed shared library. Software components installed or called by the current application are missing or corrupted. Or, there might be disk errors. Reinstall the current application and retry the current operation. If the problem continues, contact the application supplier to obtain an update, fix, or workaround.
10117	W	Accessing a corrupted shared. There might be disk errors on the remote drive. In some cases, the file system might be of an unrecognized or unsupported type for the current application or platform. Check that the remote disk drive is not corrupted, and review the installation requirements for the current application.
10118	W	Library section in code file corrupted. Software components installed or called by the current application are missing or corrupted, or there might be disk errors. Reinstall the current application and check the system for disk errors by using disk utilities appropriate for the current disk operating system. If the problem continues, contact the application supplier to obtain an update, fix, or workaround.
10119	W	Attempting to link in too many libraries. For more information about this event, see ISA Server Help.
10120	W	Attempting to execute a shared library. An incorrect file type was specified for execution on the system, possibly because a required shared library is missing. Reinstall the current application to restore missing libraries or components. If the problem continues, contact the application supplier to obtain an update, fix, or workaround.
10121	W	Socket operation attempted on non-socket
10122	W	Cannot assign requested address. For more information about this event, see ISA Server Help.
10123	W	Address is already in use. For more information about this event, see ISA Server Help.
10124	W	Address family is not supported by protocol family. For more information about this event, see ISA Server Help.
10125	W	Socket type is not supported. For more information about this event, see ISA Server Help.
10126	W	Protocol is not supported. For more information about this event, see ISA Server Help.
10127	W	No buffer space is available. There is no buffer space available to maintain the current streamed connection. Allocate space for streams buffers on the server. For

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
		more information about setting Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) buffer size for clients by using the registry on the server, see Windows 2000 Help.
10128	W	Connection timed out. For more information about this event, see ISA Server Help.
10129	W	Socket is already connected. For more information about this event, see ISA Server Help.
10130	W	Socket is not connected. For more information about this event, see ISA Server Help.
10131	W	Bad protocol option used. For more information about this event, see ISA Server Help.
10132	W	Connection reset by peer. For more information about this event, see ISA Server Help.
10133	W	Software caused connection to abort. For more information about this event, see ISA Server Help.
10134	W	Network is down. For more information about this event, see ISA Server Help.
10135	W	Connection refused. For more information about this event, see ISA Server Help.
10136	W	Host is unreachable. For more information about this event, see ISA Server Help.
10137	W	Protocol is wrong type for socket. For more information about this event, see ISA Server Help.
10138	W	Operation not supported on socket. For more information about this event, see ISA Server Help.
10139	W	IP Subnet table is full. The address table for routing hosts on the network indicates that all addresses on this subnetwork are in use. Rebuild routing tables for affected hosts, or assign the host to a new subnetwork with available address space.
10140	W	Subnet module not linked. A required software component is missing or is not configured. Check network configuration settings for the client and try to reinstall the application. If the problem continues, report the problem to the application supplier.
10141	W	Unknown input/output (I/O) control call used. A software error occurred. Report the problem to the application supplier.
10142	W	Failure in streams buffer allocation. There is insufficient buffer space available to maintain the currently streamed connection. Increase the allocated space for streams buffers on the server. For more information about setting Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) buffer size for clients by using the registry on the server, see Windows 2000 Help.
10143	W	Internet Control Message Protocol (ICMP) protocol is unreachable. The remote server is not responding. You might be unable to reach the remote server because hardware has failed or because a nonexistent address was specified. Verify that the address entered for the connection is correct and retry the operation. If the problem reoccurs, contact the network administrator for the remote server.
10144	W	Internet Control Message Protocol (ICMP) port is unreachable. The remote server port is not responding. You might be unable to reach the remote server because hardware has failed or because a nonexistent address was specified. Verify that the address entered for the connection is correct and retry the operation. If the problem reoccurs, contact the network administrator for the remote server.
10145	W	Internet Control Message Protocol (ICMP) network is unreachable. A routing failure has occurred. The local network system might generate this error if there is no default route configured. Typically, WinSock generates this error when it receives a host unreachable Internet Control Message Protocol (ICMP) message from a router. Investigate routers on local or remote networks to see that they are active and properly configured. Contact your network administrator to confirm the status of the remote host.
10146	W	Invalid Ethernet packet in use. For more information about this event, see ISA Server Help.
10147	W	An error in type registration occurred. A software error occurred. Report the problem

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
		to the application supplier.
10148	W	Sockets library is not initialized. For more information about this event, see ISA Server Help.
10149	W	Unknown error number encountered. A software error occurred. Report the problem to the application supplier.
11000	E	%1 failed to start. The failure occurred during %1 because the configuration property %1 of the key %1 could not be accessed. Use the source location %1 to report the failure. The error code in the Data area of the event properties indicates the cause of the failure. For more information about this event, see ISA Server Help.
11001	E	%1 failed. The failure occurred during %1 because the configuration property %1 of the key %1 could not be accessed. Use the source location %1 to report the failure. The error code in the Data area of the event properties indicates the cause of the failure. For more information about this event, see ISA Server Help.
11002	E	%1 failed to start. The failure occurred during %1 because the configuration property %1 of key %1 is not valid. Use the source location %1 to report the failure. The error code in the Data area of the event properties indicates the cause of the failure. For more information about this event, see ISA Server Help.
11003	E	%1 failed. The failure occurred during %1 because the configuration property %1 of key %1 is not valid. Use the source location %1 to report the failure. For more information about this event, see ISA Server Help. The error code in the Data area of the event properties indicates the cause of the failure. For more information about this event, see ISA Server Help.
11004	E	%1 failed to start. The failure occurred during %1 because the system call %1 failed. Use the source location %1 to report the failure. The error code in the Data area of the event properties indicates the cause of the failure. For more information about this event, see ISA Server Help.
11005	E	%1 failed. The failure occurred during %1 because the system call %1 failed. Use the source location %1 to report the failure. The error code in the Data area of the event properties indicates the cause of the failure. For more information about this event, see ISA Server Help.
11006	E	%1 failed to start. A shortage of available memory caused the service to fail during %1. Use the source location %1 to report the failure. For more information about this event, see ISA Server Help.
11007	E	A shortage of available memory caused the %1 to fail during %1. Use the source location %1 to report the failure. For more information about this event, see ISA Server Help.
11008	E	%1 failed to start. The service failed to register for storage notification on key %1 during %1. Use the source location %1 to report the failure. The error code in the Data area of the event properties indicates the cause of the failure. For more information about this event, see ISA Server Help.
11009	E	%1 failed to start. The storage of the current array %1 (or server %1) could not be accessed during %1. The error code in the event viewer indicates the source of the failure. Use the source location %1 to report the failure. If your server is a stand-alone ISA Server, try to restore the ISA Server configuration, otherwise, check the connectivity to domain controller (DC), and the

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
		DNS configuration.
11010	E	%1 failed. The storage of the current array %1 (or server %1) could not be accessed during %1. The error code in the event viewer indicates the source of the failure. Use the source location %1 to report the failure. If your server is a stand-alone ISA Server, try to restore the ISA Server configuration, otherwise, check the connectivity to domain controller (DC), and the DNS configuration.
12001	W	No more Internet handles can be allocated. The Web server does not have enough available resources to support the request for service at this time. Try again later.
12002	W	The operation timed out. The remote server did not respond within the set time allowed. The server might be unavailable at this time. Try again later or contact the server administrator.
12003	W	The server returned extended information. This is typically a string or buffer containing a verbose error message. For more information, review the request output.
12004	W	A software error occurred for a Windows Internet extension application that is required for the current operation.
12005	W	The Uniform Resource Locator (URL) is invalid. The request was not entered correctly. Enter the correct URL and try again.
12006	W	The Uniform Resource Locator (URL) does not use a recognized protocol. Either the protocol is not supported or the request was not typed correctly. Confirm that a valid protocol is in use (for example, HTTP for a Web request).
12007	W	The server name or address could not be resolved. This message might indicate an error in client or server configuration settings for DNS, WINS, or DHCP services that are actively in use. Review the TCP/IP properties for these services.
12008	W	A protocol with the required capabilities was not found. ISA Server does not support the request protocol. Enter the request again. Verify that the protocol is a supported type (for example, HTTP, FTP, or Gopher).
12009	W	The option is invalid. The requested option is not available with your current configuration. Clear the message and select a different option, or check configuration.
12010	W	The length is incorrect for the option type. Reselect the current option and type the data again. Verify that you did not type extra characters and that the value you typed in is within the permitted length.
12011	W	The option value cannot be set. The server does not support this value, or the value was typed incorrectly. Retry the operation. If you still get this message, ask your network administrator to check the status of the remote computer.
12012	W	Windows Internet Extension support has been shut down. Open the required Internet Extension application and reselect the command option.
12013	W	The user name was not allowed. Try a different name, or retry the same name after verifying that it is typed correctly.
12014	W	The password was not allowed. The password might have been changed or typed incorrectly. Try typing the password again. If the problem continues, contact the administrator for the remote server and report the problem.
12015	W	The login request was denied. The logon account might have been disabled or logon information might have changed. Log on again to verify that the information was typed correctly. If the problem continues, report the problem to the administrator of the Internet server you are requesting.
12016	W	The requested operation is invalid. The operation entered in the Uniform Resource Locator (URL) is not allowed or is not recognized by the remote Internet server. Type the URL again or select a different operation.
12017	W	The operation has been cancelled. Try the operation again.
12018	W	The supplied handle is the wrong type for the requested operation.
12019	W	The handle is in the wrong state for the requested operation.
12020	W	The request cannot be made on an ISA Server session.

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
12021	W	The registry value could not be found.
12022	W	The registry parameter is incorrect
12023	W	Direct Internet access is not available
12024	W	No context value was supplied. An asynchronous request could not be made because a zero context value was supplied.
12025	W	No status callback was supplied.
12026	W	There are outstanding requests. The required operation could not be completed because one or more requests are pending.
12027	W	The information format is incorrect.
12028	W	The requested item could not be located.
12029	W	A connection with the server cannot be established.
12030	W	The connection with the server was terminated abnormally.
12031	W	The connection with the server was reset.
12110	W	There is already an File Transfer Protocol (FTP) request in progress during this session. For more information about this event, see ISA Server Help.
12111	W	The File Transfer Protocol (FTP) session was terminated. The connection was closed because of either a possible attempted security violation or a time out on the remote server. Reconnect to the server or check for server availability. No further action is required.
12130	W	A Gopher protocol error occurred. In some cases, protocol errors can occur between a server that supports only standard Gopher and a client that uses Gopher Plus. Verify that the server supports the same version of Gopher protocol used by the client.
12131	W	The Uniform Resource Locator (URL) must be for a file. The URL that was entered describes a directory location and not a file. Type a Gopher URL that contains a file name. Browse through the directory listing to locate the file.
12132	W	An error was detected while parsing the data. There may be a problem with the Gopher server that you are trying to connect to. In some cases, protocol errors can occur between a server that supports only standard Gopher and a client that uses Gopher Plus. Try again later and in addition, verify that the server supports the same version of Gopher protocol that is used by the client.
12133	W	There is no more data. No more data exists beyond the last block of data returned from the server. Stop the request for additional data by canceling the operation in progress.
12134	W	The Uniform Resource Locator (URL) is not valid for the remote Gopher server. Browse through the directory to verify that you used the correct path to locate the requested file.
12135	W	The Uniform Resource Locator (URL) type is incorrect for this operation. A file name or directory name might be applied incorrectly. Verify that the name that specifies the location is a file or directory name and matches the operation.
12136	W	The request must be for a Gopher Plus item. The server and client do not support the same version of Gopher protocols. Modify or upgrade the client to use Gopher Plus.
12137	W	The requested attribute is supported for Gopher Plus servers and was not found on the server. Reconfigure the client to use standard Gopher protocol and resend the request.
12138	W	The Uniform Resource Locator (URL) type is not recognized. An incorrect Gopher type was used, or the Gopher type is not supported. Verify that the name that specifies the location is a file or directory name and is correctly matched for the operation.
12150	W	The requested header was not found. Reload the document using the Refresh function of your Web browser.
12151	W	The server does not support the requested protocol level. Verify that the protocol you typed is a supported protocol (such as FTP, Gopher, HTTP) for the Web Proxy service.
12152	W	The server returned an invalid or unrecognized response. The HTTP request cannot be fully or correctly interpreted by the server. The request might have been

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
		corrupted by transmission errors. Try reloading the document in your Web browser to correct the problem.
12153	W	The supplied HTTP header is invalid and not recognized by the remote server. Check that your browser is supported.
12154	W	The request for a HTTP header is invalid. A header contained within the Uniform Resource Locator (URL) request is not recognized by the remote server. Check that your browser is supported.
12155	W	The HTTP header already exists. Contact your ISA Server administrator.
12156	W	The HTTP request includes a non-supported header. Contact the Server administrator.
12201	W	A chained proxy server or array member requires proxy-to-proxy authentication. Please contact your server administrator.
12202	W	The ISA Server denies the specified Uniform Resource Locator (URL).
12203	W	The ISA Server has detected the server software expired.
12204	W	The specified Secure Sockets Layer (SSL) port is not allowed. ISA Server is not configured to allow SSL requests from this port. Most Web browsers use port 443 for SSL requests.
12205	W	The ISA Server evaluation version expired. For more information, contact Microsoft.
12206	W	The ISA Server detected a proxy chain loop. There is a problem with the configuration of the ISA Server routing policy. Please contact your server administrator.
12209	W	The ISA Server requires authorization to fulfill the request. Access to the Web Proxy service is denied.
12210	E	An Internet Server API (ISAPI) filter caused an error or terminated with an error.
12210	W	An Internet Server API (ISAPI) filter has finished handling the request. Contact your system administrator.
12211	W	The ISA Server requires a secure channel connection to fulfill the request. ISA Server is configured to respond to outgoing secure (that is, Secure Sockets Layer (SSL)) channel requests.
12212	W	The ISA Server requires a high-security connection to fulfill the request. A Secure Sockets Layer (SSL) Web server requires 128-bit encryption, an enhanced security mechanism, for access to published sites. Use a browser that supports this enhanced encryption.
12213	W	The ISA Server requires a client certificate to fulfill the request. A Secure Sockets Layer (SSL) Web server, during the authentication process, requires a client certificate.
12214	W	An Internet Server API (ISAPI) filter caused an error or terminated with an error.
12215	W	The size of the request header is too large. Contact your ISA server administrator.
12216	W	The size of the response header is too large. Contact your ISA server administrator.
12221	W	A chained server requires authentication. Contact the server administrator.
12222	W	The server denies the specified Uniform Resource Locator (URL). Contact the server administrator.
12223	W	The server has detected the server software expired. Contact the server administrator.
12225	W	The server evaluation version expired.
12226	W	The server detected a chain loop. There is a problem with the configuration of the server routing policy. Contact the server administrator.
12227	E	The dial-out connection failed. The dial-out connection failed with the specified phonebook entry. The administrator should manually dial the specified phonebook entry to confirm that the problem is not the Windows 2000 auto-dial facility.
12228	E	The server is too busy to handle this request. Reenter request or try again later.
12229	E	The server requires authorization to fulfill the request. Access to the Web server is denied. Contact the server administrator.
12230	E	An Internet Server API (ISAPI) filter has finished handling the request. Contact the server administrator.
12231	E	The page must be viewed over a secure (that is, Secure Sockets Layer (SSL))

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
		channel. Contact the server administrator.
12232	E	The page requires 128-bit encryption, an enhanced security mechanism. To view the page contents, use a browser that supports this enhanced encryption.
12233	E	The page requires a client certificate as part of the authentication process. Contact the server administrator.
12235	E	The size of the request header is too large. Contact the server administrator.
12236	E	The size of the response header is too large. Contact the server administrator.
12260	E	Fatal error occurred when attempting to access %1 certificate private key. For more information about this event, see ISA Server Help. The error code in the Data area of the event properties indicates the cause of the failure.
13000	I	BWCNTRL_EVENT_E_SUCCESS
13002	I	Bandwidth control completed successfully.
13103	E	Initialization of bandwidth control failed. The ISA Server that uses the bandwidth controller failed to initialize the client dynamic-link library (DLL). Look at previous event entries to find the reason for the failure.
13104	E	The call to %1 failed. The failure is probably due to insufficient memory. Close some applications and try again. If that does not work, verify that Active Directory is working. For more information about managing memory resources, see Windows 2000 Help.
13105	E	Insufficient memory for %1. The bandwidth control did not have sufficient memory resources. Close some applications and try again. For more information about managing memory resources, see Windows 2000 Help.
13106	E	Cannot match IP to an interface. Flow control for the specified IP address did not take effect. If message was reported during network configuration changes it can be ignored. If you continue to receive this message, you may need to restart ISA services.
13107	W	The Scheduled Content Download Service has stopped the job %1. %1 pages visited.
13108	W	The Scheduled Content Download Service found an unauthorized URL and called unauthorized page %1 while executing the job %1.
13109	E	The Scheduled Content Download Service was unable to connect to the Web Proxy Service while executing the job %1. Check that the Web Proxy Service is running using ISA Management. If not, start the service.
13110	W	ISA Server snapin failed to retrieve the arrays list since connection to Global Catalog could not be established. It will next try to retrieve the arrays information from current domain. Check your Active Directory configuration, DNS settings and ensure that the Net Logon service is started.
13111	W	The url, %1, cannot be retrieved from %1, during the scheduled content download job, %1. The http status code, %1, was returned. The failure was encountered on the first url specified in the job. Normally, a successful http request returns HTTP code 200. For specific details of this failure, check the standard http status code, %1. Check the configuration of this schedule content download job.
13112	E	The service failed to start. The failure occurred during initialization because the version of the array configuration is not supported.
14000	E	ISA Server cannot connect to %1 proxy server, because the server requires authentication, either when chaining or for intra-array communication. However authentication failed because the specified credentials were incorrect. Check authentication credentials and try again.
14001	E	Firewall Service failed to initialize. The internal error code in the Data area of the event properties indicates the cause of the failure. Previous event log entries might help determine the proper action.
14002	E	The Firewall service cannot initialize WinSock. The error code in the Data area of the event properties indicates the cause of the failure.

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
		For more information about this event, see ISA Server Help.
14003	I	Firewall service started.
14004	E	The Firewall service cannot start due to a shortage of available memory. The error code in the Data area of the event properties indicates the cause of the failure. For more information about this event, see ISA Server Help.
14006	W	The Firewall service cannot start the performance counters. Restart the Firewall service. The error code in the Data area of the event properties indicates the cause of the failure.
14007	E	A shortage of available memory caused the Firewall service to fail. The Event Viewer Data window displays the number of active connections. For more information about this event, see ISA Server Help.
14008	I	1%
14010	E	The Firewall service did not start due to corrupt data in the registry or Active Directory, depending on the ISA Server configuration. The error code in the Data area of the event properties indicates the cause of the failure. For more information about this event, see ISA Server Help.
14011	W	The Firewall service failed to bind its socket to %1, port %1. This could be caused by another service that is already using the same port or by the network interface that is not functional. The error code in the Data area of the event properties indicates the cause of the failure. For more information about this event, see ISA Server Help.
14012	I	Client from %1 attempted to access ISA Server using control protocol version %1. The server supports version %1. The version of the client software is incompatible with the server version. If the client software is older than the server software, upgrade the client software. If the server software is older, either upgrade the server or direct the client to a different server that uses the newer software.
14013	E	The Firewall service requires Windows 2000 Server with Service Pack 1 or later.
14014	E	The Firewall service requires Windows 2000 Server with Service Pack 1 or later.
14015	E	The Firewall service failed to load a security dynamic-link library (DLL). The required DLL is missing or cannot be found. Make sure that the Security.dll is located in the Windows 2000 system directory (typically, systemroot\System32 directory), and then restart the Firewall service.
14016	E	The Firewall service failed to determine the network addresses because either there are improper network connections or there is insufficient memory. Check network connections and restart the service. If this problem occurs again, close some applications, stop the service, and then restart the service.
14017	E	Incorrect network configuration. The server address is not internal and is not in the Local Address Table (LAT). For more information about this event, see ISA Server Help.
14021	E	The Firewall service failed to initialize because the system call %1 failed. If an error code appears in the Data area of the event properties, it indicates the cause of the failure. For more information about this event, see ISA Server Help.
14022	E	Microsoft ISA Server Control Service failed to initialize because the system call %1 failed. The error occurred during %1. Use the source location %1 to report the failure. If an error code appears in the Data area of the event properties, it indicates the cause of the failure. For more information about this event, see ISA Server Help.

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
14023	I	1%
14024	E	Microsoft ISA Server Control Service requires Windows 2000 Server with Service Pack 1 or later.
14025	E	Microsoft ISA Server Control Service requires Windows 2000 Server with Service Pack 1 or later.
14026	E	The Microsoft ISA Server Control Service failed to initialize. The internal error code in the Data area of the event properties indicates the cause of the failure. Restart the service.
14027	I	The Microsoft ISA Server Control Service started.
14028	E	The Firewall service did not initialize the network dial-up entry. Try an alternative manual dial-up entry. If successful, retry the dial-up entry. If the problem still exists, restart the Firewall service. If this does not solve the problem, restart Windows 2000.
14029	W	The Firewall service failed to create a socket. If an error code appears in the Data area of the event properties, it indicates the source of the failure.
14030	W	The Firewall service failed to associate a control socket with a completion port.
14031	E	The Firewall service failed to initialize control or refresh sockets.
14032	E	The Firewall service was stopped. The evaluation period has expired.
14033	W	Alert service did not start. Alerts are limited to event reporting. There might be a problem in the Microsoft ISA Server Control Service. Restart the service. The Firewall and Web Proxy services are dependent on this service, so you also need to restart them.
14034	E	The Firewall service did not listen on all Transmission Control Protocol (TCP) sockets. The reason for the failure of the service can be determined by examining previous event log entries.
14035	W	The Firewall service failed to listen on the Transmission Control Protocol (TCP) socket bound to %1. The error code in the Data area of the event properties indicates the cause of the failure.
14036	W	The IP address (or DNS name) %1, from configuration file %1, cannot be used to connect to the ISA server, or it could not be found. Use ISA Management to configure the IP address or DNS name to which Firewall clients should connect.
14038	E	ISA Server packet filter log service cannot allocate memory. The packet filter log component of ISA Server logs this event when it fails to allocate memory where memory resources are low. The packet filter log component cannot operate until the low memory situation is resolved. The ISA Server administrator can stop and restart the ISA Server services to resolve the low memory situation if logging of packet filter data is mandatory.
14039	E	ISA Server packet filter logging component cannot obtain the log contents. Restarting the service might solve the problem.
14040	E	Mail Alert service stopped responding because Mapi.dll cannot be located.
14043	E	The system-wide packet filter log event cannot be created.
14044	W	The packet filter is dropping Internet Protocol (IP) packets. For more information about this event, see ISA Server Help.
14045	E	Mail alert for %1 failed
14046	E	Packet filter protocol violation. For more information about this event, see ISA Server Help.
14047	E	Failed to write to %1 log file in directory %1. There is no space on the disk drive. Delete unnecessary files.
14048	E	Failed to stop the %1 during %1. Use the source location %1 to report the failure. The error code in the Data area of the event properties indicates the cause of the failure. The computer should be restarted.

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
14049	E	%1 was stopped because of a logging failure. For more information about this event, see ISA Server Help.
14050	W	Mail alert %1 stopped because of a configuration error (%1).
14051	W	Mail alert %1 (%1) stopped because it could not log on or connect to the server. The server may be down or incorrectly specified.
14052	W	Mail alert %1 stopped because the mail server refused to accept the message.
14053	W	Mail alert %1 stopped because the sender name is not valid.
14054	W	Mail alert %1 stopped because the recipient name is not valid.
14055	E	The Firewall service encountered an illegal operation (runtime error R6025), in a pure virtual function. To resolve this error, remove recently installed application filters and restart the service.
14056	E	The application filter (%1, CLSID=%1) performed an illegal operation inside the Firewall service process at method %1. The Firewall service terminated. To resolve this error, remove recently installed application filters and restart the service. If this does not resolve the problem, contact the component vendor.
14057	E	The Firewall service stopped because an application filter module %1 generated an exception code %1 in address %1 when function %1 was called. To resolve this error, remove recently installed application filters and restart the service.
14058	E	The Firewall service cannot connect to another proxy server. Authentication was rejected. Check the credentials for the account that is used for proxy-to-proxy authentication.
14059	E	The Firewall service cannot connect to another proxy server. Authentication failed. A chained proxy server or array member requires proxy-to-proxy authentication. Authentication failed because the credentials that were supplied were incorrect. Check authentication credentials and try again.
14060	W	Cannot load an application filter %1 (%1). %1 failed with code 0x%1. To attempt to activate this application filter again, stop and restart the Firewall service.
14061	W	The Firewall service detected that the upstream proxy server %1 is not available. If the upstream proxy server %1 becomes available, you may proceed as usual. If it does not become available, check the status of the upstream proxy server.
14062	I	The Firewall service detected that the upstream proxy %1 is now available.
14063	E	The Firewall service failed to initialize because of a corrupted registry. Error Code %1, Key=%1 Value=%1. For more information about this event, see ISA Server Help.
14064	E	Unknown event %1 signaled the alert service. The reported event does not appear in storage. If you recently installed an application filter, it is probably the source of the error. Remove any application filters that have been installed recently. If this does not solve the problem, reinstall ISA Server.
14065	E	Alert Service: One or more of the actions associated with alert %1 has failed. Failure are linked to configuration settings. The mail server may be down, or the specified command may not exist. Check the Event Viewer for related errors and fix them accordingly.
14066	E	Failed to read the dial-up entry configuration. The error code in the Data area of the event properties indicates the cause of the failure. For more information about this event, see ISA Server Help.
14067	E	Failed to load Rasapi32.dll. The system configuration is incorrect. Check the system configuration for errors. Manually dial an entry to verify that the dial-out works and then restart the failed service. The error code in the Data area of the event properties indicates the cause of the failure.
14068	E	A network dial-up connection was assigned an incorrect IP address %1. The IP address must not be defined in the local address table (LAT). All traffic passing through this interface will be blocked. Check the LAT configuration, or contact your

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
		ISP to check the IP address pool.
14069	W	The alert service found more than one alert with the same event condition, server name, and additional key. The duplicated alert %1 is ignored. For more information about this event, see ISA Server Help.
14070	E	The service could not start because it failed to connect to ISA Server Control service. The error code in the Data area of the event properties indicates the cause of the failure. Check the Event Viewer for related error messages.
14071	E	The Firewall service did not start because the application filter component %1 did not start on time. Reinstall the application filter. Contact the application filter vendor.
14072	E	The alert service failed to logon as user %1 to run the command %1 specified for the alert %1. The error code in the Data area of the event properties indicates the cause of the failure. For more information about this event, see ISA Server Help.
14073	I	Microsoft ISA Server Control Service successfully executed the security editing application. The computer must be restarted for the new security settings to take effect.
14076	E	Microsoft ISA Server Control Service failed to execute the security editing application. For more information about this event, see ISA Server Help. Error code: %1.
14077	W	Failed to start the %1 during %1. Use the source location %1 to report the failure. The error code in the Data area of the event properties indicates the cause of the failure. For more information about this event, see ISA Server Help.
14078	W	Microsoft ISA Server Control Service failed to delete Web Proxy cache file %1 during %1. Use the source location %1 to report the failure. Try to delete the folder manually.
14079	E	Due to an unexpected error, the service %1 stopped responding to all requests. This occurred %1 time(s) in the past %1 hours. Try to stop the service or kill the corresponding process if it does not respond, and start it again. Check the Event Viewer for related error messages.
14080	E	Microsoft ISA Server Control Service failed because an application filter component (%1) performed an illegal operation at method %1 GUID=%1. Try removing recently installed application filters and restart the service. Otherwise, contact the component vendor.
14081	E	ISA Server Control Service discovered a missing application filter component (%1) GUID %1. The application filter cannot be found on this server. Check that the specified filter was installed. The error code in the Data area of the event properties indicates the cause of the failure.
14082	E	ISA Server Control Service cannot load the application filter component (%1) GUID %1, because it does not support necessary interfaces. This indicates a version mismatch, and the filter can no longer be used. Check the filter was installed correctly, or contact the component vendor. The error code in the Data area of the event properties indicates the cause of the failure.
14083	E	ISA Server Control Service cannot load the application filter component (%1) GUID %1. Check that the application filter is installed properly. The error code in the Data area of the event properties indicates the cause of the failure.
14084	E	ISA Server Control Service failed to start. All array members must be in the same site (%1). However, this server is in site %1. The server may have been moved to a different site than its containing array. Move the server to an array in its new site.

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
14085	E	ISA Server Control Service failed to start. All array members must be in the same domain (%1). However, this server is in domain %1. The server was apparently moved to a different domain than its containing array. The server should be added to an array in its new domain.
14086	E	Insecure configuration detected. Internet Protocol (IP) routing is enabled while packet filtering is disabled. All packets will be routed, regardless of access policy. It is recommended that you enable IP routing only when you also enable packet filtering.
14087	E	Insecure configuration detected. ISA Server uses its own Network Address Translation (NAT) editor to fully secure your system. However, ISA Server found one or more different NAT editors, which might have been installed by the following drivers: %1. It is recommended that you uninstall the drivers listed. For more information about this event, see ISA Server Help.
14088	W	Server publishing rule [%1] that maps %1 %1 to %1 for protocol [%1] violates %1 rule [%1]. For more information about this event, see ISA Server Help.
14089	E	Server publishing rule [%1] failed. Cannot create session for the server %1. Location %1. For more information about this event, see ISA Server Help.
14090	W	Server publishing rule [%1] that maps %1 %1 to %1 for protocol [%1] failed to bind to external interface. The server publishing rule cannot be applied. The Firewall service failed to bind a socket for the server. The error code in the Data area of the event properties indicates the cause of the failure.
14091	W	Server publishing rule [%1] failed. The protocol specified cannot be used for publishing. Location %1. The server publishing rule cannot be applied. The protocol must be inbound. Check with the application filter vendor.
14092	E	Server publishing rule [%1] failed. The protocol specified cannot be used for publishing. Location %1. For more information about this event, see ISA Server Help.
14093	W	The Microsoft Firewall Service cannot start because the ISA Server was installed in Cache mode. Usually the Firewall service is disabled if ISA Server is not installed in Integrated or Firewall mode. It is possible that during the first boot after the Firewall component was uninstalled, the service was started, and shortly after stopped. To use the service, reinstall ISA Server in Integrated or Firewall mode.
14094	W	The Microsoft Scheduled Cache Content Download service cannot start because the ISA Server was installed in Firewall mode. Usually the Scheduled cache content download service is disabled if ISA Server is not installed in Cache or Integrated mode. It is possible that during the first boot after the Cache component was uninstalled, the service was started, and shortly after stopped. To use the service, reinstall ISA Server in Integrated or Cache mode.
14095	E	Failed to initialize server publishing. Location %1. Internal error. Storage might be corrupted.
14096	E	Failed to read server publishing rules. Location %1. Internal error. Storage might be corrupted.
14097	E	Failed to read one or more server publishing rules. Location %1. Internal error. Storage might be corrupted.
14098	E	Failed to read parameters of the publishing rule [%1]. The rule is discarded. Location %1.

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
		The storage might be corrupted. Delete this rule and create a new one.
14099	W	Publishing rule [%1] could not be applied to this array member because IP %1 is not available. A server publishing rule can only be applied to one server from the array. All other servers will report this event. Note that an Internet Protocol (IP) address might be temporarily unavailable (for example, dial-up connection is disconnected).
14109	E	The ISA Server Standard edition cannot run. Either the server is using more than 4 processors, or it is configured to use the Active Directory Service. The error code in the Data area indicates the cause of the failure. Use the source location %1 to report the failure. Contact Microsoft for more information.
14110	W	Publishing rule [%1] should not be applied because IP address %1 is not external to the local address table (LAT).
14111	E	ISA Server Cache could not start because it was configured incorrectly. Use ISA Management or manually edit the registry to correct the error, and then restart the service. For more information about this event, see ISA Server Help.
14118	E	The Web Proxy Service was stopped. The evaluation period has expired.
14119	E	An external interface could not be found for packet filtering. For more information about this event, see ISA Server Help.
14120	E	The ISA Server services cannot create a packet filter %1. This event occurs when there is a conflict between the Local Address Table (LAT) configuration and the Windows 2000 routing table. Check the routing table and the LAT to find the source of the conflict.
14121	E	The packet filter dial-out interface cannot be rebound. For more information about this event, see ISA Server Help.
14122	E	A packet filter interface could not be bound. For more information about this event, see ISA Server Help.
14123	E	Failed to create the Internet Protocol (IP) packet filter. For more information about this event, see ISA Server Help.
14124	E	Filtering disabled as requested.
14125	I	The Web Proxy service received %1 requests from the Internet port during the past %1 seconds while Web publishing was disabled. When ISA Server publishing is disabled, this event message displays the number of requests from the Internet during the specified time, in seconds.
14126	I	The Web Proxy service configuration has been modified %1 times during the past %1 seconds.
14127	E	The Web Proxy service could not initialize (error code %1). The internal error code in the Data area of the event properties indicates the cause of the failure.
14128	I	The Web Proxy service is paused.
14129	I	The Web Proxy service was resumed. No further action necessary.
14130	W	The Web Proxy service detected that the upstream proxy %1 is not available. For more information about this event, see ISA Server Help.
14131	I	The Web Proxy service detected that the upstream proxy %1 is now available. If you were able to work around the upstream proxy server, no further action is necessary.

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
		If you changed the configuration of the primary route to the upstream ISA Server, you might want to change it back.
14132	W	The Web Proxy service detected that the array member %1 is down. Check the array member intra-array address or the network to find out why this array member is not available.
14133	I	The Web Proxy service detected that the array member %1 is available.
14136	E	ISA Server dial-out connection failed. The administrator should manually dial the specified phonebook entry to determine if the number can be reached.
14137	W	Some of this information may be out of date because of network problems. An attempt to respond to this request from a remote location was unsuccessful. The response is an expired version of the object found in the cache.
14138	W	Some of this information has not been updated in the past 24 hours.
14140	W	Some of this information may be out of date.
14141	W	ISA Server detected a proxy chain loop. There is a problem with the configuration of the ISA Server routing policy.
14142	W	The dial-up network connection %1 failed. The error description is: %1. The error code shown in the Data area of the event properties is specific to the Routing and Remote Access service (RRAS).
		For more information about this event, see ISA Server Help.
14143	W	ISA Server is too busy to handle this request. Reenter the request or renew the connection to the server (now or at a later time).
14144	W	The alert service failed to initialize because system call %1 failed. Some information in the response may have already expired in the cache. If an error code is shown in the Data area of the event properties, it indicates the cause of the failure.
14145	E	ISA Server failed to initialize due to a corrupted registry. Restart the service. If this does not resolve the problem, reinstall the server to replace any missing files. If the condition persists, restore the registry.
		Error Code %1, Key=%1, Value=%1.
14146	E	ISA Server failed to load Web Filter DLL %1. The error code shown in the Data area of the event properties indicates the cause of the failure.
14148	W	Web Proxy service failed to bind its socket to %1 port %1. This could be caused by another service that is already using the same port or by a network interface card that is not functional. The error code specified in the Data area of the event properties indicates the cause of the failure.
		For more information about this event, see ISA Server Help.
14149	W	Web Proxy service failed to listen to %1 port %1. The network interface card might not be functional. The error code specified in the Data area of the event properties indicates the cause of the failure.
		For more information about this event, see ISA Server Help.
14150	E	The ISA Server cache could not initialize the URL cache on disk. The ISA Server cache files are corrupted.
14151	E	The ISA Server cache could not initialize the URL cache on disk. The ISA Server cache disk is full.
14152	W	A User Datagram Protocol (UDP) packet was dropped because it was larger than the maximum UDP packet allowed by the Firewall service.
14153	E	The Web Proxy service is not listening on the defined intra-array address on port %1, although resolving requests within an array is enabled. For more information about this event, see ISA Server Help.
14154	I	The Scheduled Content Download Service started the job %1.
14155	I	The Scheduled Content Download Service finished the job %1. %1 pages visited.
14156	I	The Web Proxy Service switched from primary route %1 to backup route %1.
		The Web Proxy Service is configured to switch to the backup route if there is some

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
		problem with the primary route.
14157	I	The Web Proxy Service switched from backup route %1 to primary route %1. Following a problem with the primary route, the Web Proxy service switches to the configured backup route. While using the backup route, the service moves back to the primary route when it is available.
14158	E	The <I>IntraArrayAddress</I> defined on this server is not in the Local Address Table (LAT). For more information about this event, see ISA Server Help.
14159	E	Failed to read reference to the protocol from the server publishing rule [%1]. Location %1. Storage may be corrupted. Delete this rule and create a new rule.
14160	W	Server publishing rule [%1] that maps %1 %1 to %1 for protocol [%1] is not applied since enterprise policy does not allow publishing. The enterprise policy can be changed to allow publishing.
14161	I	Server publishing rule [%1] that maps %1 %1 to %1 for protocol [%1] was applied successfully. This rule previously failed, but now completed successfully.
14162	W	Server publishing rule [%1] will not be applied since the filter that supports the protocol is not enabled. Enable the filter and then apply the rule.
14163	W	Server publishing rule [%1] that maps %1 %1 to %1 for protocol [%1] failed because the port on the external interface is being used by another application. The Firewall service failed to bind socket for the server on the firewall since another process is using the same port. Check for any other process using the same port and terminate if necessary.
14164	W	All cache drives failed to initialize properly.
14165	W	There is inconsistency in some cache files. While initializing cache, some cache files were detected as being from previous cache configurations. For more information about this event, see ISA Server Help.
14166	W	Cache is intentionally disconnected from the rest of the network. Information is now being served from the cache and there is no connection to the Internet at the present time.
14167	I	Recovery of data cache file %1 was completed. If the operation did not complete successfully you may use the error code in the Data area indicates the cause of the failure.Recovery operation result is: %1
14168	I	Some errors were encountered when ISA Server restored specific data cache files. ISA Server will now attempt to recover these files. These errors may have occurred because there was not enough time to complete all necessary shutdown operations, when ISA Server was previously shut down. To avoid this in future, you can increase the value of the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\WaitToKillServiceTimeout registry key.
14169	W	While restoring cache data, %1 objects with conflicting information were detected. These objects were ignored, and were not restored. This may occur when there is conflict between cache data from previous and present cache configurations. You may consider deleting the cache files that were added to the current configuration, in order to avoid inconsistent data retrieval.
14170	I	Restoration of cache data completed. %1 Cache performance will now be at optimal level.
14171	I	Cache data was restored successfully from all data cache files.

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
14172	E	Cache failed to initialize properly. %1 Caching will be disabled. The error code in the Data area of the event properties indicates the cause of the failure. (internal code %1). Identify the specific reason for failure from previous relevant event logs. Fix the problem and restart the Web Proxy service to enable caching.
14173	E	Path name too long. Specify a shorter path name.
14174	E	Invalid size specified. Specify a valid disk cache size and restart the Web Proxy service.
14175	E	Invalid volume specified. The volume must be a NTFS volume with supported sector sizes. Specify a valid volume as a cache drive. You may need to change your hardware if the required sector size is not supported. Restart the Web Proxy service.
14176	E	Disk cache %1 failed to initialize. %1 Identify the reason for cache failure by examining previous recorded events, or the error code. The error code in the Data area of the event properties indicates the cause of the failure (internal code: %1).
14177	E	Some certificates cannot be initialized (error code %1). The Web Proxy service could not initialize. Check that all certificates used by the Web Proxy service are valid. The internal error code in the Data area of the event properties indicates the cause of the failure.
14178	I	The Web Proxy service identified that the address %1 was removed from the interface table and stopped listening on port %1.
14179	I	The Web Proxy Service identified that the address %1 was added to the interface table and start listening on port %1.
14180	E	Alert Service: failed to log event to system log. The following message %1 could not be logged.
14181	I	The ISA Server Control Service was stopped gracefully.
14182	I	The Firewall Service was stopped gracefully.
14183	I	The Web Proxy Service was stopped gracefully.
14184	I	The Scheduled Cache Content Download Service was stopped gracefully.
14185	I	The Scheduled Cache Content Download Service was started successfully.
14186	I	The Web Proxy Service was started successfully.
14187	I	ISA Server detected a change in the IP addresses of the computer.
14188	I	ISA Server detected a change in the IP routing table of the computer.
14189	I	ISA Server detected that a change was made to the local address table (LAT).
14190	I	ISA Server detected that network interface card (NIC) %1, with IP address %1, was enabled.
14191	I	ISA Server detected that network interface card (NIC) %1, with IP address %1, was disabled.
14192	E	Microsoft ISA Server Control Service failed to start because the operating system service %1 is already running. To fix this problem use ISA Server setup to reinstall ISA.
14192	I	Recovery of data cache was completed.
14193	W	Cache was initialized with less memory cache than configured. This is because there is not enough free memory available for ISA Server caching.
14194	W	The value specified for the maximal URL size for memory cache is too big. ISA Server reconfigured it to %1 bytes.
14195	W	ISA Server will not be able save all the run-time configuration information of disk cache %1 when you shut down ISA Server. For this reason, ISA Server may start relatively more slowly and some cache data may be lost the next time you shut down and then restart ISA Server. To prevent this problem, free up some disk cache space. The error code in the Data area of the event properties indicates the cause of the failure (internal code: %1).
14196	E	ISA Server failed to reduce the size of %1 cache file. The error code in the Data area of the event properties indicates the cause of the failure.
14197	E	ISA Server failed to write content to cache file. The error code in the Data area of

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
		the event properties indicates the cause of the failure.
14198	E	The Web Proxy service failed to create a network socket because there are no available ports on this computer. ISA server already reset the maximal port number to 65535. Make sure this is the value at HKLM\System\CurrentControlSet\Service\TcpIp\Parameters\MaxUsePort and restart the computer to apply this change
14199	W	The dial-up network multi-link connection %1 was established. However, some links failed with error: %1. The error code shown in the Data area of the event properties is specific to the Routing and Remote Access service (RRAS). For more information about this event, see ISA Server Help.
14200	E	ISA Server failed to establish an SSL connection with %1. %1
14201	E	HTTP proxy report message
14202	E	HTTP proxy reports
14203	E	The ISA Server encountered an error.
14204	E	Server error message
14205	E	ISA Server: extended error message
14206	E	Directory is empty.
14207	E	Root directory
14208	E	Gopher root at %s.
14209	E	FTP root at %s.
14210	E	Gopher directory at %s.
14211	E	FTP directory %s at %s.
14212	E	Web Proxy Cache initialization failed due to thread initialization failure.
14213	W	400 Bad Request
14214	W	401 Unauthorized
14215	W	403 Forbidden
14216	W	404 Not Found
14217	W	407 Proxy Authentication Required
14218	W	414 Request-URI Too Large
14219	W	502 Proxy Error
14220	W	500 Internal Server Error
14221	W	503 Proxy is busy
14222	W	504 Proxy Timeout
14300	W	No
14301	W	Yes
15001	W	ISA Server detected a Windows out-of-band attack. For more information about this event, see ISA Server Help.
15002	W	ISA Server detected an Internet Protocol (IP) half scan attack. For more information about this event, see ISA Server Help. For more information about this event, see ISA Server Help.
15003	W	ISA Server detected a land attack. For more information about this event, see ISA Server Help.
15004	W	ISA Server detected a well-known port scan attack. A well-known port is any port in the range of 1-2048. For more information about this event, see ISA Server Help.
15005	W	ISA Server detected an all port scan attack. For more information about this event, see ISA Server Help.
15006	W	ISA Server detected a User Datagram Protocol (UDP) bomb attack. For more information about this event, see ISA Server Help.

REAL-TIME MONITORING FOR ISA SERVER

Event ID	Event Type	Description
15007	W	ISA Server detected a ping of death attack. For more information about this event, see ISA Server Help.
15008	W	ISA Server detected a spoof attack. A spoof attack occurs when an IP address that is not reachable via the interface on which the packet was received. If logging for dropped packets is set, you can view details in the packet filter log.
15101	W	ISA Server detected a windows out-of-band attack from Internet Protocol (IP) address %1. For more information about this event, see ISA Server Help.
15102	W	ISA Server detected an Internet Protocol (IP) half-scan attack from IP address %1. For more information about this event, see ISA Server Help.
15103	W	ISA Server detected a land attack on Internet Protocol (IP) address %1. For more information about this event, see ISA Server Help.
15104	W	ISA Server detected a well-known port scan attack from Internet Protocol (IP) address %1. A well-known port is any port in the range of 1-2048. For more information about this event, see ISA Server Help.
15105	W	ISA Server detected an all port scan attack from Internet Protocol (IP) address %1. For more information about this event, see ISA Server Help.
15106	W	ISA Server detected a User Datagram Protocol (UDP) bomb attack from Internet Protocol (IP) address %1. For more information about this event, see ISA Server Help.
15107	W	ISA Server detected a ping-of-death attack from Internet Protocol (IP) address %1. For more information about this event, see ISA Server Help.
15108	W	ISA Server detected a spoof attack from Internet Protocol (IP) address %1. A spoof attack occurs when an IP address that is not reachable via the interface on which the packet was received. If logging for dropped packets is set, you can view details in the packet filter log.



CONCLUSIONS AND SUMMARY

ELM Enterprise Manager is the Best Solution for Total Management of your ISA Servers

No matter how good your management processes are, there will be problems with your systems. Problem management can be divided into three separate areas - problem detection, problem notification and problem resolution. All problem identification in an ISA environment is ultimately based on the continuous monitoring of two data sources - the Windows 2000 event subsystem and the Windows/ISA performance counters. Once a problem is detected, ELM Enterprise Manager provides a wide range of notification mechanisms to ensure that support personnel are appropriately alerted.

ISA servers are expected to deliver a wide variety of functionality: firewall and security, content download and caching, and proxy services. No matter how big or small your ISA infrastructure is, or how you use it, it requires careful and proactive monitoring.

ELM Enterprise Manager is the best solution for proactively monitoring all aspects of your ISA infrastructure in real-time.



EXPLANATION OF RECOMMENDED PERFORMANCE COUNTER OBJECTS

ISA SERVER - BANDWIDTH CONTROL

Actual Inbound Bandwidth is the actual inbound bandwidth in bytes/sec.

Actual Outbound Bandwidth is the actual outbound bandwidth in bytes/sec.

Assigned Connections tracks the number of connections with an assigned bandwidth priority. Connections with assigned bandwidth priorities have higher precedence than those without assigned priorities.

Assigned Inbound Bandwidth tracks the assigned inbound bandwidth in bytes/sec.

Assigned Outbound Bandwidth tracks the assigned outbound bandwidth in bytes/sec.

ISA SERVER - CACHE

Active Refresh Bytes Rate (KB/Sec) measures the rate at which bytes of data are retrieved from the Internet to actively refresh popular URLs in the cache. This will relate to the configuration set for active caching.

Active URL Refresh Rate (URL/Sec) measures the rate at which popular cached URLs are actively refreshed from the Internet. This will relate to the configuration set for active caching.

Disk Bytes Retrieve Rate (KB/sec) measures that rate at which "bytes of data" are retrieved from the disk cache. This counter is similar to Disk URL Retrieve Rate, but monitors bytes, rather than URLs.

Disk Cache Allocated Space (KB) measures how much space is being used by the disk cache. It will be equal to or less than the amount configured for the disk cache.

Disk Content Write Rate (Writes/Sec) measures the number of writes per second to the disk cache for the purpose of writing URL content to the cache disk.

Disk Failure Rate (Fail/Sec) measures the number of input/output (I/O) failures per second. An I/O failure occurs when ISA Server fails to read from or write to the disk cache. This counter, together with **Total Disk Failures**, will give a clear indication of disk cache problems.

Disk URL Retrieve Rate (URL/Sec) measures how many URLs are sent to clients from the disk cache in one second. This is a useful counter to measure at peak and off-peak times to check how the disk cache is performing. It can be compared with **Memory URL Retrieve Rate** to see how cache disk and memory are being utilized.

Max URLs Cached measures the maximum number of URLs that have been stored in the cache.

Memory Bytes Retrieved Rate (KB/Sec) measures the rate at which bytes of data are retrieved from the memory cache. This counter is similar to Memory URL Retrieve Rate, but monitors bytes, rather than URLs.

Memory Cache Allocated Space (KB) measures how much space is being used by the memory cache. It should be equal to or less than the amount configured for the memory cache.

Memory URL Retrieve Rate (URL/Sec) measures how many URLs are sent to clients from the memory cache in one second. This is a useful counter to measure at peak and off-peak times, to check how the memory cache is performing and whether available memory allocated for caching purposes is being used efficiently.

Memory Usage Ratio Percent (%) shows the ratio between the amount of cache fetches from the memory cache in a percentage and the amount of cache fetches in total. A high percentage may indicate that it is worthwhile allocating more available memory resources to the cache. A low counter may indicate that memory resources may be better used elsewhere.

Total Actively Refreshed URLs displays the cumulative number of popular URLs in the cache that have been actively refreshed from the Internet. This counter will give an indication of active caching performance.

Total Bytes Actively Refreshed (KB) displays the total number of bytes that have been retrieved from the Internet to actively refresh popular URLs in the cache. This counter will give an indication of active caching performance.

Total Disk Bytes Retrieved (KB) measures the cumulative number of disk bytes that have been retrieved from the disk cache. This counter, added to **Total Memory Bytes Retrieved (KB)**, will indicate the total number of bytes retrieved from the cache.

Total Disk Failures measures the number of times that the Web Proxy service failed to read from or write to the disk cache due to an input/output (I/O) failure. A low counter will indicate that a disk is performing properly. A high counter will indicate a cache disk that is too small, too slow, or corrupted.

Total Disk URLs Retrieved measures the cumulative number of URLs that have been retrieved from the disk cache. This counter, added to **Total Memory URLs Retrieved**, will indicate the total number of URLs retrieved from the cache.

Total Memory Bytes Retrieved (KB) measures the cumulative number of memory bytes that have been retrieved from the memory cache in response to client requests to the cache. A low number might indicate that memory resources dedicated to the cache are not being used efficiently. A high number might indicate that more memory resources should be allocated to the cache.

Total Memory URLs Retrieved measures the cumulative number of URLs that have been retrieved from the memory cache in response to client requests to the cache. A low number might indicate that memory resources dedicated to the cache are not being used efficiently. A high number might indicate that more memory resources should be allocated to the cache.

Total URLs Cached measures the cumulative number of URLs that have been stored in the cache. If this counter and URLs in Cache is low, it may indicate a problem with the cache. The cache may not be configured for optimal use or the cache size may be too small.

URL Commit Rate (URL/Sec) indicates the speed at which URLs are being written to the cache. If rate of this counter is comparable to the rate of **Disk Failure Rate(Fail/Sec)**, it indicates that a high proportion of attempts to write to the cache are failing. This could indicate a problem with cache configuration, a cache disk that is too slow, or a cache size that is too small.

URLs in Cache measures the current number of URLs in the cache.

ISA SERVER - FIREWALL SERVICE

Accepting TCP Connections is the number of connection objects that wait for a Transmission Control Protocol (TCP) connection from Firewall clients.

Active Sessions is the number of active sessions for the Firewall service.

Active TCP Connections is the total number of active TCP connections currently passing data. Connections pending or not yet established are counted elsewhere.

Active UDP Connections is the total number of active User Datagram Protocol (UDP) connections.

Available Worker Threads is the number of Firewall worker threads that are available or waiting in the completion port queue.

Back-connecting TCP Connections is the total number of TCP connections awaiting an inbound connect call to complete. These are connections placed by the Firewall service to a client after the Firewall service accepts a connection from the Internet on a listening socket.

Bytes Read/sec is the number of bytes read by the data-pump per second.

Bytes Written/sec is the number of bytes written by the data-pump per second.

Connecting TCP Connections is the total number of TCP connections pending. These are connections awaiting completion between the Firewall service and remote computers.

DNS Cache Entries is the current number of DNS domain name entries cached as a result of Firewall service activity.

DNS Cache Flushes is the total number of times that the DNS domain name cache has been flushed or cleared by the Firewall service.

DNS Cache Hits is the total number of times a DNS domain name was found within the DNS cache by the Firewall service.

DNS Cache Hits % is the percentage of DNS domain names serviced by the DNS cache, from the total of all DNS entries that have been retrieved by the Firewall service.

DNS Retrievals is the total number of DNS domain names that have been retrieved by the Firewall service.

Failed DNS Resolutions is the number of *gethostbyname* and *gethostbyaddr* API calls that have failed. These are calls used to resolve host DNS domain names and IP addresses for Firewall service connections.

Kernel Mode Data Pumps is the number of kernel mode data pumps created by the Firewall service.

Listening TCP Connections is the number of connection objects that wait for TCP connections from remote Internet computers.

Memory Allocation Failures is the number of memory allocation errors.

Non-connected UDP mappings is the number of mappings available for UDP connections.

Pending DNS Resolutions is the number of *gethostbyname* and *gethostbyaddr* API calls pending resolution. These are calls used to resolve host DNS domain names and IP addresses for Firewall service connections.

SecureNAT Mappings is the number of mappings created by secure network address translation.

Successful DNS Resolutions is the number of *gethostbyname* and *gethostbyaddr* API calls successfully returned. These are calls used to resolve host DNS domain names and IP addresses for Firewall service connections.

TCP Bytes Transferred/sec by Kernel Mode Data Pump is the number of TCP bytes transferred by the kernel mode data-pump per second.

UDP Bytes Transferred/sec by Kernel mode Data Pump is the number of UDP bytes transferred by the kernel mode data-pump per second.

Worker Threads is the number of Firewall worker threads that are currently active.

ISA SERVER - H.323 FILTER

Active H.323 Calls is the number of H.323 calls that are currently active.

Total H.323 Calls is the total number of H.323 calls handled by the H.323 filter since the ISA Server computer was started.

ISA SERVER - PACKET FILTER

Packets Dropped Due to Filter Denial is the total number of packets dropped because dynamic packet filtering rejected the data. Dropped packets counted here are any packets which are not covered by Packets Dropped Due to Protocol Violations. In other words, this counter represents packets dropped because of the default "deny-all" policy in ISA Server. The only exception will be where exception filters have been set, explicitly allowing these packets through.

Packets Dropped Due to Protocol Violations represents the total number of packets dropped as a result of a protocol anomaly. These are packets dropped due to reasons other than the default filtering rules. For example, if you have chosen to implement packet filtering of IP fragments, or you have enabled intrusion detection, packets dropped because of these configuration choices will increment this counter.

Total Dropped Packets represents the total number of dropped or filtered packets, regardless of why they have been dropped or filtered.

Total Lost Logging Packets is the total number of dropped packets that cannot be logged.

ISA SERVER - WEB PROXY SERVICE

Array Bytes Received/Sec tracks the rate at which data bytes are received from other ISA Server computers within the same array.

Array Bytes Sent/Sec tracks the rate at which data bytes are sent to other ISA Server computers within the same array.

Array Bytes Total/Sec represents the sum of **Array Bytes Sent/Sec** and **Array Bytes Received/Sec**. This is the total rate for all data bytes transferred between the ISA Server computer and other members of the same array.

Cache Hit Ratio % determines how many Web Proxy client requests have been served using cached data (**Total Cache Fetches**), as a percentage of the total number of successful Web Proxy client requests to the ISA Server computer (**Total Successful Requests**). Its value gives a good indication of the effectiveness of the cache. A high counter will indicate that a high level of requests are being serviced from the cache, meaning faster response times. A zero counter indicates that caching is not enabled. A low counter may indicate a configuration problem. The cache size may be too small, or requests may not be cacheable.

Cache Running Hit Ratio (%) measures the amount of requests served from the cache as a percentage of total successful requests serviced. This ratio is the same as that measured by **Cache**

Hit Ratio(%). The difference between these two counters is that Cache Running Hit Ratio measures this ratio for the last 10,000 requests serviced, and Cache Hit Ratio measures this ratio since the last time that the Web Proxy service was started. This means that Cache Running Hit Ratio gives a more dynamic evaluation of cache effectiveness.

Client Bytes Received/sec indicates the rate at which data bytes are received from Web Proxy clients. The value will change according to the volume of Web Proxy client requests, but a consistently slow rate may indicate a delay in servicing requests.

Client Bytes Sent/Sec measures the rate at which data bytes are sent to Web Proxy clients. The value will change according to the volume of Web Proxy client requests, but a consistently slow rate may indicate a delay in servicing requests.

Client Bytes Total/Sec represents the sum of **Client Bytes Sent/Sec** and **Client Bytes Received/Sec**. This is the total rate for all bytes transferred between the ISA Server computer and Web Proxy clients.

Current Array Fetches Average (Milliseconds/Request) gives the mean number of milliseconds required to service a Web Proxy client request that is fetched through another array member. This does not include requests for services by the SSL tunnel.

Current Average Milliseconds/Request represents the mean number of milliseconds required to service a Web Proxy client request, not including requests serviced by the SSL tunnel. This counter can be monitored at peak and off-peak times to get a comprehensive picture of how fast client requests are being serviced. A counter that is too high might indicate that the ISA Server is having difficulty in handling all requests and that requests are being delayed.

Current Cache Fetches Average (Milliseconds/Request) is the mean number of milliseconds required to service a Web Proxy client request from cache. This does not include requests for services by the SSL tunnel.

Current Direct Fetches Average (Milliseconds/Request) is the mean number of milliseconds required to service a Web Proxy client request directly to the Web server or upstream proxy. This does not include requests for services by the SSL tunnel.

Current Users indicates how many clients are currently running the Web Proxy service. Monitoring this counter at both peak and off-peak times will give a good indication of server usage. The configuration setting for maximum Web request connections will influence this value. This counter may also be useful if you need to temporarily stop ISA Server services.

DNS Cache Entries details the current number of DNS domain name entries cached by the Web Proxy service. A high counter suggests a beneficial impact on performance, since a DNS cache entry eliminates the need for a DNS lookup, saving system resources.

DNS Cache Flushes details the total number of times that the DNS domain name cache has been flushed or cleared by the Web Proxy service. When there is no room left for more data in the DNS cache, the DNS cache is flushed to allow new entries to be made.

DNS Cache Hits tracks the total number of times a DNS domain name was found within the DNS cache by the Web Proxy service. This counter can be compared with previous DNS counters to find out if DNS caching is working efficiently. A low number of DNS cache hits will impact performance, as every DNS lookup will slow performance down, particularly if a problem arises in the lookup process.

DNS Cache Hits % determines how many DNS entries have been resolved using cached data (**DNS cache hits**), as a percentage of the total number of DNS domain names retrieved by the Web Proxy service (**DNS retrievals**). A high counter means better performance as the DNS data is served from the cache, rather than incurring the overhead of resolving DNS lookups.

DNS Retrievals is the total number of DNS domain names that have been retrieved by the Web Proxy service.

Failing Requests/Sec is the rate per second that Web Proxy client requests that have completed with some type of error. This counter can be compared with Requests/Sec to give an indication of how well ISA Server is servicing incoming Web requests. A high failure rate, in comparison to the rate of incoming requests, will suggest that ISA Server is having difficulty in coping with all incoming requests. Connection settings for incoming Web requests may be incorrectly configured, or connection bandwidth may be insufficient.

FTP Requests is the number of FTP requests that have been made to the Web Proxy service. A consistently low counter may influence the caching policy for FTP objects.

Gopher Requests is the number of Gopher requests that have been made to the Web Proxy service.

HTTP Requests is the number of HTTP requests that have been made to the Web Proxy service.

HTTPS Sessions is the total number of HTTPS sessions serviced by the SSL tunnel.

Maximum Users is the maximum number of users that have connected to the Web Proxy service simultaneously. This counter can be useful for determining load usage and license requirements.

Requests/Sec is the rate of incoming requests that have been made to the Web Proxy service. A higher value means that more ISA Server resources will be required to service incoming requests.

Reverse Bytes Received/sec is the rate at which data bytes are received by the Web Proxy service from Web publishing servers in response to incoming requests. This rate can be monitored at peak and off-peak times as an indication of how ISA Server is performing in servicing incoming Web requests.

Reverse Bytes Sent/sec is the rate at which data bytes are sent by the Web Proxy service to Web publishing servers in response to incoming requests. This rate can be monitored at peak and off-peak times as an indication of how ISA Server is performing in servicing incoming Web requests.

Reverse Bytes Total/sec is the total sum of **Reverse Bytes Sent/Sec** and **Reverse Bytes Received/Sec**. This is the total rate for all bytes transferred between the Web Proxy service and Web publishing servers in response to incoming requests.

Site Access Denied is the total number of Internet sites to which the Web Proxy service has denied access. An excessively high number might indicate that your access policy is too restrictive.

Site Access Granted is the total number of Internet sites to which the Web Proxy service has granted access. This can be compared with Site Access Denied to give a numeric summary of the results of access policy configuration.

SNEWS Sessions is the total number of SNEWS sessions serviced by the SSL tunnel.

SSL Client Bytes Received/Sec is the rate at which SSL data bytes are received by the Web Proxy service from secured Web Proxy clients. This is similar to **Client Bytes Received/Sec**, but counts only SSL requests.

SSL Client Bytes Sent/Sec is the rate at which SSL data bytes are sent by the Web Proxy service to secured Web Proxy clients. This is similar to **Client Bytes Sent/Sec**, but counts only SSL requests.

SSL Client Bytes Total/Sec is the sum of **SSL Client Bytes Sent/Sec** and **SSL Client Bytes Received/Sec**. This is the total rate for all bytes transferred between the Web Proxy service and SSL clients.

Thread Pool Active Sessions is the number of sessions being actively serviced by thread pool threads.

Thread Pool Failures is the number of requests rejected because the thread pool was full.

Thread Pool Size is the number of threads in the thread pool. This thread pool represents the resources available to service client requests.

Total Array Fetches is the total number of Web Proxy client requests that have been served by requesting the data from another ISA Server within this array. These requests are the result of the Cache Array Routing Protocol (CARP) algorithm, which randomly stores objects in any one of the member servers cache. This counter is influenced by the cache size for each ISA Server in the array, since a server with a larger cache will hold more cache items. The load factor for each server can also be configured, to determine how workload is divided amongst array members.

Total Cache Fetches is the total number of Web Proxy client requests that have been served by using cached data. A high number will indicate a cache being fully exploited.

Total Failed Requests is the total number of requests that have failed to be processed by the Web Proxy service due to errors. Errors can be the result of the Web Proxy service failing to locate a requested server URL on the Internet or because the client did not have authorized access to the requested URL. This counter should be far lower than **Total Successful Requests**. If it is not, it is an indication that ISA Server is failing to service requests effectively. This could be a configuration problem, or a connection that is too slow. It could also indicate an access policy that is too restrictive.

Total Pending Connects is the total number of pending connections to the Web Proxy service.

Total Requests is the total number of requests that have been made to the Web Proxy service. It is the total of two other counters, Total Successful Requests and Total Failed Requests.

Total Reverse Fetches is the total number of incoming requests that have been served by requesting the data from Web publishing servers.

Total SSL Sessions is the total number of SSL sessions serviced by the SSL tunnel.

Total Successful Requests is the total number of requests that have been successfully processed by the Web Proxy service. This counter can be compared with **Total Requests** and **Total Failed Requests** to indicate the effectiveness of ISA Server in servicing requests.

Total Upstream Fetches is the total number of requests that have been served by using data from the Internet or from a chained proxy computer. This counter can be compared to Total Cache Fetches to see what proportion of requests are being serviced from remote servers on the Internet or upstream proxies, compared with those being serviced from the cache.

Total Users is the total number of users that have ever connected to the Web Proxy service. It represents a history of past server usage.

Unknown SSL Sessions is the total number of unknown SSL sessions serviced by the SSL tunnel.

Upstream Bytes Received/Sec is the rate at which data bytes are received by the Web Proxy service from remote servers on the Internet or from a chained proxy computer in response to requests from the Web Proxy service. The value of this counter will depend to some extent on the connection bandwidth. If the counter value is consistently low, it may indicate a bottleneck caused by a slow connection. Changing the bandwidth priority configuration may help in this situation, or a faster connection may be required.

Upstream Bytes Sent/Sec is the rate at which data bytes are sent by the Web Proxy service to remote servers on the Internet or to a chained proxy computer. The value of this counter will depend to some extent on the connection bandwidth. If the counter value is consistently low, it may indicate a bottleneck caused by a slow connection. Changing the bandwidth priority configuration may help in this situation, or a faster connection may be required.

Upstream Bytes Total/Sec is the sum of **Upstream Bytes Sent/Sec** and **Upstream Bytes Received/Sec**. It represents the total rate for all bytes transferred between the Web Proxy service and remote servers on the Internet or a chained proxy server.

LOGICAL DISK

Avg. Disk Queue Length is the average number of both read and write requests that were queued for the selected disk during the sample interval. Increases over the initial baseline typically indicate a disk bottleneck.

Avg. Disk Sec/Transfer is the time, in seconds, of the average disk transfer. Increases over the initial baseline typically indicate a disk bottleneck.

Current Disk Queue Length is the number of requests outstanding on the disk (including requests in service) at the time the performance data is collected. This is an instantaneous length, not an average over the time interval. Multi-spindle disk devices can have multiple requests active at one time, but other concurrent requests are awaiting service. This counter may reflect a transitory high or low queue length, but if there is a sustained load on the disk drive, it is likely that this will be consistently high. Requests are experiencing delays proportional to the length of this queue minus the number of spindles on the disks. The queue length should always be less than half of the number of disks in a volume. So, if you have 8 disks in a volume, the queue length should always be less than 4.

Disk Reads/Sec is the rate of read operations on the disk. Most disk and disk controller manufacturers have formulas for measuring total disk I/O, which use this counter as part of that formula.

Disk Writes/Sec is the rate of write operations on the disk. Most disk and disk controller manufacturers have formulas for measuring total disk I/O, which also use this counter as part of that formula.

Free Megabytes is the amount of unallocated space on the disk in megabytes. This is a very important counter to monitor. Alarms should be configured so that alerts will be generated as the disks or disk volumes approach capacity. When using this counter, one megabyte equals 1,048,576 bytes.

% Free Space is the ratio of the free space available on the logical disk to the total usable space on selected logical disk.

MEMORY

Available Mbytes is the amount of physical memory available (in megabytes) to running processes. It is calculated by summing space on the Zeroed, Free, and Standby memory lists. Zeroed memory refers to pages of memory filled with zeros to prevent later processes from seeing data used by a previous process. Free memory is ready for use. Standby memory is memory removed from a process' working set on route to disk, but is still available to be recalled. This counter displays the last observed value only; it is not an average.

Cache Faults/sec is the number of faults that occur when a page sought in the file system cache is not found there and must be retrieved from elsewhere, either in memory (a soft fault) or from disk (a hard fault). The file system cache is an area of physical memory that stores recently used pages of data for applications. Cache activity is generally a reliable indicator of most application I/O operations. This counter represents the number of faults, without regard for the number of pages faulted in each operation.

Commit Limit is the size (in bytes) of virtual memory that can be committed without having to increase the size of the paging file. If Committed Bytes approaches the Commit Limit, and the paging file cannot be extended, there are simply no more available pages in main memory or in the paging file. If this occurs you may see three errors in the System Log from source: SRV:

2001: The server was unable to perform an operation due to a shortage of available resources.

2016: The server was unable to allocate virtual memory.

2020: The server was unable to allocate from the system paged pool because the pool was empty.

This is generally related to a memory leak in another process. To determine the process at fault you can monitor each process's Page File bytes or Working Set.

Committed Bytes is the amount of committed virtual memory, measured in bytes. Committed memory is physical memory for which space has been reserved on the paging file in case it needs to be written back to disk. This counter must not exceed the overall size of the paging file, as this would indicate that too much application data has been committed to virtual space.

Pages/sec is the number of pages written to or read from disk to resolve hard page faults. This counter is meant to be the primary indicator of the kinds of faults that cause system-wide delays.

It is counted in numbers of pages, so it can be compared to other counts of pages, such as Memory – Page Faults/sec, without requiring any conversion.

Page faults/sec is the overall rate that faulted pages are handled by the CPU. It is measured in numbers of pages faulted per second. A page fault occurs when a process requires code or data that is not in its space in physical memory. This counter includes both hard faults and soft faults. Most CPUs can handle large numbers of soft faults without consequence. Hard faults, however, can cause significant system delays.

Page Reads/sec is the number of times the disk was read to resolve hard page faults. A hard page fault occurs when a process requires code or data that is not in its working set or elsewhere in physical memory, and must be retrieved from disk. This counter is a primary indicator of the kinds of faults that cause system-wide delays. It includes reads to satisfy faults in the file system cache (usually requested by applications) and in non-cached mapped memory files. This counter counts numbers of read operations, without regard to the numbers of pages retrieved by each operation.

Page Writes/sec is the number of times pages were written to disk to free up space in physical memory. Pages are written to disk only if they are changed while in physical memory, so they are likely to hold data, not code. This counter counts write operations, without regard to the number of pages written in each operation.

% Committed Bytes in Use is the ratio of the Committed Bytes to the Commit Limit. This is an instantaneous value, not an average, which represents the amount of available virtual memory in use. Note that the Commit Limit may change if the paging file is extended.

Pool Nonpaged Bytes is the number of bytes in the Nonpaged Pool, a system memory area where space is acquired by operating system components as they accomplish their appointed tasks. Nonpaged Pool pages cannot be paged out to the paging file, but instead remain in main memory as long as they are allocated. A slow rise in the value for this counter could indicate a memory leak.

NETWORK INTERFACE

Bytes Total/sec is the rate that bytes are sent and received on the interface, including framing characters. You can use this counter to monitor the overall network traffic to that server and compare it to the maximum available bandwidth for that segment. If the sum is close to the maximum available bandwidth, you will know that segment is reaching maximum capacity. In this event, you should add a new segment to the network.

Packets Outbound Errors is the number of outbound packets that could not be transmitted because of errors. Some errors are to be expected, but if you see a large number of errors over your baseline, you probably need to replace your network cable or network adapter.

Packets Received Errors is the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. Some errors are to be expected, but if you see a large number of errors over your baseline, you probably need to replace your network cable or network adapter.

PAGING FILE

% Usage is the amount of the paging file instance in use. This indicates how much of the page file is in use, which is in turn used to determine if a memory bottleneck exists.

% Usage Peak is the peak usage of the selected paging file instance given as a percentage.

PHYSICAL DISK

Avg. Disk sec/Read is the average time in seconds of a read of data from the disk.

Avg. Disk sec/Write is the average time in seconds of a write of data to the disk.

Avg. Disk sec/Transfer is the time in seconds of the average disk transfer.

Current Disk Queue Length is the number of requests outstanding on the disk at the time the performance data is collected. It includes requests in service at the time of the snapshot. This is an instantaneous length, not an average over the time interval. Multi-spindle disk devices can have multiple requests active at one time, but other concurrent requests are awaiting service. This counter might reflect a transitory high or low queue length, but if there is a sustained load on the disk drive, it is likely that this will be consistently high. Requests are experiencing delays proportional to the length of this queue minus the number of spindles on the disks. This value for this counter should generally be less than 2. If it is higher than 2 for a sustained period of time, your disks or disk subsystem may be a bottleneck.

PROCESS

Handle Count is the total number of handles that are currently open by the process. This number is the sum of the handles currently open by each thread in this process.

Page faults/sec is the rate at which page faults occur in the threads executing in this process. A page fault occurs when a thread refers to a virtual memory page that is not in its working set. This will not cause the page to be fetched from disk if it is on the standby list and hence already in main memory, or if it is in use by another process with which the page is shared.

Page File Bytes is the current number of bytes this process has used in the paging file(s). Because paging files are shared by all processes, the lack of available space within the paging file can prevent other processes from allocating memory. This counter can be used to isolate memory leak in a process.

% Processor Time is the percentage of elapsed processor time used by all threads of the selected process. An instruction is the basic unit of execution in a computer, a thread is the object that executes instructions, and a process is the object created when a program is run. Code executed to handle some hardware interrupts and trap conditions are included in this count. On SMP machines, the maximum value of the counter is 100% times the number of processors.

Private Bytes is the current number of bytes this process has allocated that cannot be shared with other processes.

Thread Count is the number of threads that are currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.

Virtual Bytes is the current size of the virtual address space (in bytes) that the process is using. This counter is critical in determining if the store cache size is large enough.

Working Set is the current amount of RAM used by this process and its data. The Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed, they will then be soft-faulted back into the Working Set before they leave main memory. See Microsoft Knowledge Base article [Q184699](https://support.microsoft.com/kb/q184699) for more information on this counter.

PROCESSOR

Interrupts/sec is the number of device interrupts the processor experiences. A device interrupts the processor when it has completed a task or when it otherwise requires attention. Normal thread execution is suspended during interrupts. An interrupt may cause the processor to switch to another, higher priority thread. Clock interrupts are frequent and periodic and create a background of interrupt activity. This counter needs to be compared with baselines taken during normal operations to determine if the present value indicates a problem of some sort.

% Processor Time is the percentage of time the processor is executing a non-idle thread. This counter is the primary indicator of processor activity. It is calculated by measuring the time the processor spends executing the thread of the Idle process in each sample interval, and subtracting that value from 100%. Each processor has an Idle thread which consumes cycles when no other threads are ready to run. If this counter is consistently above 75%, you have a CPU bottleneck.

REDIRECTOR

Bytes Total/sec is the rate at which the Redirector processes data bytes. This includes all application and file data, and protocol information such as packet headers.

Current Commands is the number of requests to the Redirector that are currently queued for service. If this number is much larger than the number of network adapter cards installed in the server, then the network and/or the server are seriously bottlenecked.

Network Errors/sec is the count of network errors encountered by the Redirector. A few errors are to be expected, so this counter should be continuously monitored and compared to baselines recorded during normal operating conditions. Higher than normal values generally mean that the Redirector is having serious communication problems. Some of these errors will result in events being generated, which provides additional troubleshooting information.

Reads Denied/sec is the rate at which the server is unable to accommodate requests for Raw Reads. When a read is much larger than the server's negotiated buffer size, the Redirector requests a Raw Read which, if granted, permits the transfer of the data without lots of protocol overhead on each packet. To accomplish this the server must lock out other requests, so the request is denied if the server is really busy.

Writes Denied/sec is the rate at which the server is unable to accommodate requests for Raw Writes. When a write is much larger than the server's negotiated buffer size, the Redirector requests a Raw Write which, if granted, permits the transfer of the data without lots of protocol overhead on each packet. To accomplish this, the server must lock out other requests, so the request is denied if the server is really busy.

S E R V E R

Bytes Total/sec is the number of bytes the server has sent to and received from the network. This value provides an overall indication of how busy the server is. If this counter is close to the maximum transfer rate of your network, you may need to segment your network.

Errors Access Permissions is the number of times opens on behalf of clients have failed with Access Denied. A high number could indicate that somebody is randomly attempting to access files in hopes of getting at something that was not properly protected. If you have auditing enabled, each failed attempt will generate a Failure Audit event. A network sniffer, such as Network Monitor, can be used to identify the source of these attempts.

Errors Granted Access is the number of times accesses to files opened successfully were denied. This could also indicate attempts to access files without proper access authorization. If you have auditing enabled, each failed attempt will generate a Failure Audit event. A network sniffer would help here, too.

Errors Logon is the number of failed logon attempts to the server. This could indicate that a password cracking program is being used to hack into the server. If you have auditing enabled, each failed attempt will generate a Failure Audit event. A network sniffer would help here, too.

Errors System is the number of times an internal Server Error was detected. Unexpected errors usually indicate a problem with the server. Check to see whether the server is running out of memory and check the collected system events to see if you have a hardware problem. If neither is indicated, you might consider contacting Microsoft Product Support Services.

Pool Nonpaged Bytes is the number of bytes of non-pageable memory the server is currently using. A slow rise in the value of Pool Nonpaged Bytes could indicate a memory leak. You should also make sure the Server service is set to "Maximize Throughput for Network Applications."

Pool Nonpaged Failures is the number of times allocations from nonpaged pool have failed. Any value above zero could indicate that more memory is needed.

Pool Nonpaged Peak is the maximum number of bytes of nonpaged pool the server has had in use at any one point. This counter provides a good indication of how much physical memory the server should have.

Pool Paged Bytes is the number of bytes of pageable memory the server is currently using.

Pool Paged Failures is the number of times allocations from paged pool have failed. This could indicate that the server doesn't have enough physical memory or that the paging file is too small.

Pool Paged Peak is the maximum number of bytes of paged pool the server has had allocated. This counter can be used to determine the proper sizes of the paging file and proper amounts of physical memory.

Server Sessions is the number of sessions currently active in the server.

Sessions Errored Out is the number of sessions that have been closed due to unexpected error conditions. This counter indicates how frequently network problems are causing dropped sessions on the server.

Sessions Timed Out is the number of sessions that have been closed due to their idle time exceeding the autodisconnect parameter for the server. This counter will indicate whether or not the autodisconnect setting is helping to conserve resources.

Work Item Shortages is the number of times STATUS_DATA_NOT_ACCEPTED was returned at receive indication time. This occurs when no work item is available or can be allocated to service the incoming request. This indicates whether the InitWorkItems or MaxWorkItems parameters need to be adjusted.

S Y S T E M

% Registry Quota in Use indicates the percentage of the Total Registry Quota Allowed currently in use by the system. This is especially important to monitor if your ISA server is also a domain controller, because user accounts, system policies, and related information can cause a registry quota to become exhausted, especially on large networks. If this value begins to approach 100%, you should increase the total registry size. If this happens and your ISA Server is not a domain controller, then you should examine the Registry to determine why it has grown so large.

Processor Queue Length is the instantaneous length of the processor queue in units of threads. This counter is always 0 unless you are also monitoring a thread counter. All processors use a single queue in which threads wait for processor cycles. This length does not include the threads that are currently executing. If this counter is greater than two, something is causing congestion. This could also indicate a processor bottleneck.

System Calls/Sec is the frequency of calls to system service routines. These routines perform all of the basic scheduling and synchronization of activities on the computer, and provide access to non-graphical devices, memory management, and name space management. If there are many more processor interrupts per second than system calls, it could indicate that a hardware device is generating an excessive number of interrupts.

System Up Time is the elapsed time (in seconds) that the computer has been running since it was last started. This counter displays the difference between the start time and the current time.



ISA SERVER FIREWALL AND WEB PROXY LOG FILE ENTRIES

You can use a File Monitor (with a Service Agent only) to parse the ISA Server logs and analyze the status of the Firewall and Web Proxy services. ISA Server can log using the World Wide Web Consortium (W3C) extended log format, and an ISA Server log format.

The table below lists the fields that you can include in each of the ISA Server log files. The field name in parentheses is only relevant for the World Wide Web Consortium (W3C) extended log file format. Some fields are relevant for either Web Proxy Service or Firewall Service, but not both. In this case, the table indicates to which service the field applies.

When using the ISA Server log format, the field will appear in the log with a hyphen (-). When using the W3C format, the field will not appear if it is not applicable to the service.

Field position	Descriptive name (field name)	Description
1	Client IP (c-ip)	The Internet Protocol (IP) address of the requesting client.
2	Client user name (cs-username)	Account of the user making the request. If ISA Server Access Control is not being used, ISA Server uses <i>anonymous</i> .
3	Client agent (c-agent)	The client application type sent by the client in the Hypertext Transfer Protocol (HTTP) header. When ISA Server is actively caching, the client agent is <i>ISA Server</i> .
4	Authentication status (sc-authenticated)	Indicates whether or not client has been authenticated with ISA Server. Possible values are <i>Y</i> and <i>N</i> .
5	Date (date)	The date that the logged event occurred.

Field position	Descriptive name (field name)	Description
6	Time (time)	The time that the logged event occurred. In W3C format, this is in Greenwich mean time.
7	Service name (s-svcname)	The name of the service that is logged. <ul style="list-style-type: none"> • w3proxy indicates outgoing Web requests to the Web Proxy service. • fwsrv indicates Firewall service. • w3reverseproxy indicates incoming Web requests to the Web Proxy service.
8	Proxy name (s-computername)	The name of the computer running ISA Server. This is the computer name that is assigned in Windows 2000.
9	Referring server name (cs-referred)	If ISA Server is used upstream in a chained configuration, this indicates the server name of the downstream server that sent the request.
10	Destination name (r-host)	The domain name for the remote computer that provides service to the current connection. For the Web Proxy service, a hyphen (-) in this field may indicate that an object was retrieved from the Web Proxy server cache and not from the destination.
11	Destination IP (r-ip)	The network IP address for the remote computer that provides service to the current connection. For the Web Proxy service, a hyphen (-) in this field may indicate that an object was sourced from the Web Proxy server cache and not from the destination. One exception is negative caching. In that case, this field indicates a destination IP address for which a negative-cached object was returned.
12	Destination port (r-port)	The reserved port number on the remote computer that provides service to the current connection. This is used by the client application initiating the request.
13	Processing time (time-taken)	This indicates the total time, in milliseconds, that is needed by ISA Server to process the current connection. It measures elapsed server time from the time that the server first received the request to the time when final processing occurred on the server—when results were returned to the client and the connection was closed. For cache requests that were processed through the Web Proxy service, <i>processing time</i> measures the elapsed server time needed to fully process a client request and return an object from the server cache to the client.
14	Bytes sent (cs-bytes)	The number of bytes sent from the internal client to the external server during the current connection. ^

REAL-TIME MONITORING FOR ISA SERVER

Field position	Descriptive name (field name)	Description
		hyphen (-), a zero (0), or a negative number in this field indicates that this information was not provided by the remote computer or that no bytes were sent to the remote computer.
15	Bytes received (sc-bytes)	The number of bytes sent from the external computer and received by the client during the current connection. A hyphen (-), a zero (0), or a negative number in this field indicates that this information was not provided by the remote computer or that no bytes were received from the external computer.
16	Protocol name (cs-protocol)	Specifies the application protocol used for the connection. Common values are HTTP, File Transfer Protocol (FTP), Gopher, and Secure Hypertext Transfer Protocol (HTTPS). For Firewall service, the port number is also logged.
17	Transport (cs-transport)	Specifies the transport protocol used for the connection. Common values are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
18	Operation (s-operation)	Specifies the application method used. For Web Proxy, common values are GET, PUT, POST, and HEAD. For Firewall service, common values are CONNECT, BIND, SEND, RECEIVE, GHBN (GetHostByName), and GHBA (GetHostByAddress).
19	Object name (cs-uri)	For the Web Proxy service, this field shows the contents of the URL request. This field applies only to the Web Proxy service log.
20	Object MIME (cs-mime-type)	The Multipurpose Internet Mail Extensions (MIME) type for the current object. This field may also contain a hyphen (-) to indicate that this field is not used or that a valid MIME type was not defined or supported by the remote computer. This field applies only to the Web Proxy service log.
21	Object source (s-object-source)	Indicates the source that was used to retrieve the current object. This field applies only to the Web Proxy service log.
22	Result code (sc-status)	This field can be used to indicate: <ul style="list-style-type: none"> • For values less than 100, a Windows (Win32) error code • For values between 100 and 1,000, an HTTP status code • For values between 10,000 and 11,004, a Winsock error code

Field position	Descriptive name (field name)	Description
23	Cache info (s-cache-info)	This number reflects the cache status of the object, which indicates why the object was or was not cached. This field applies only to the Web Proxy service log.
24	Rule #1 (rule#1)	This reflects the rule that either allowed or denied access to the request, as follows: <ul style="list-style-type: none"> • If an outgoing request is allowed, this field reflects the protocol rule that allowed the request. • If an outgoing request is denied by a protocol rule, this field reflects the protocol rule. • If an outgoing request is denied by a site and content rule, this field reflects the protocol rule that would have allowed the request. • If an incoming request was denied, this field reflects the Web publishing or server publishing rule that denied the request. • If no rule specifically allowed the outgoing or incoming request, the request is denied. In this case, the field is empty.
25	Rule #2 (rule#2)	This reflects the second rule that either allowed or denied access to the request. <ul style="list-style-type: none"> • If an outgoing request is allowed, this field reflects the site and content rule that allowed the request. • If an outgoing request is denied by a site and content rule, this field reflects the site and content rule that denied the request. • If no rule specifically allowed the outgoing or incoming request, the request is denied. In this case, the field is empty.
26	Session ID (sessionid)	This identifies a session's connections. For Firewall clients, each process that connects through the Firewall service initiates a session. For secure network address translation (SecureNAT) clients, a single session is opened for all the connections that originate from the same IP address. This field is not included in the Web Proxy service log. This field applies only to the Firewall service log.
27	Connection ID (connectionid)	This identifies entries that belong to the same socket. Outbound TCP usually has two entries for each connection: when the connection is established and when the connection is terminated. UDP usually has

REAL-TIME MONITORING FOR ISA SERVER

Field position	Descriptive name (field name)	Description
		two entries for each remote address. This field is not included in the Web Proxy service log. This field applies only to the Firewall service log.