Tivoli

IBM

e-business Risk Management

with Tivoli Risk Manager

A comprehensive validation of correlating intrusive events

Integrating a multitude of different sensor technologies

Integration with Tivoli Decision Support

Axel Bücker
Shazli Mohd Ghazali
Vasfi Gucer
Rick Nall
Luis Maria Rodriguez
Sai Sampath
Peter Kai Wimmer

Redbooks

ibm.com/redbooks

SG24-6036-00

International Technical Support Organization

e-business Risk Management with Tivoli Risk Manager

September 2001

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix E, “Special notices” on page 355.

First Edition (September 2001)

This edition applies to Tivoli Risk Manager Version 3.7.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. JN9B Building 003 Internal Zip 2834
11400 Burnet Road
Austin, Texas 78758-3493

Contents

Figures

Tables

Preface

In the emerging world of e-business and worldwide Internet connectivity, organizations have to protect themselves from being attacked by different intruders. They have to protect their online assets, as it might prove disastrous if an attacker succeeds in harming valuable resources. Increasingly, attacks and intrusions target the enterprise as whole, not just a sub-system. Consequently, defending against these attacks requires an enterprise view of security, a coordinated approach that can harness the intelligence across the different security checkpoints within the enterprise.

There are various tools available today that concentrate on observing potential breaches in the networking IT infrastructure. In order to monitor this complete spectrum, an organization would need to deploy a number of different toolsets. Since all tools create individual reports and warnings, including false alarms, a security officer will be prone to errors in managing all the different alarm situations.

Tivoli Risk Manager is the industry's first Enterprise Risk Management product. Risk Manager is an open, cross-platform, standards-based enterprise scale management platform that enables customers to seamlessly manage security intrusions and vulnerabilities across networks, hosts, operating systems, applications, servers, and desktops.

Tivoli Risk Manager will cover the gamut of enterprise security systems, including firewalls, routing infrastructure, network and host-based intrusion-detection systems, host-system security, antivirus systems, and desktop and content security. Using the Tivoli Enterprise Console, customers can centrally monitor, correlate, manage, and respond to firewall alerts, intrusion-detection alerts, virus alerts, unauthorized access, suspicious activities, policy violations, and so on.Tivoli Decision Support enables easy analysis of complex data that has been collected by the Tivoli Enterprise Console Server.

This redbook helps you understand the Risk Manager architecture and implementation process and prerequisites. It will cover the integration of different intrusion detection sensors into the Risk Manager environment and it will talk about the principles of intrusion detection and how Risk Manager can help to handle intrusion detection situations.

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, Austin Center.

Axel Buecker is a Certified Consulting Software I/T Specialist at the International Technical Support Organization, Austin Center. He writes extensively and teaches IBM classes worldwide on areas of Software Security Architecture and Network Computing Technologies. He holds a degree in computer science from the University of Bremen, Germany. He has 15 years of experience in a variety of areas related to Workstation and Systems Management, Network Computing, and e-business solutions. Before joining the ITSO in March 2000, Axel was working for IBM in Germany as a Senior I/T Specialist in Software Security Architecture.

Vasfi Gucer is a Project Leader at the ITSO, Austin Center. He worked with IBM Turkey for 10 years, and has been with the ITSO since January 1999. He has more than eight years of experience in systems management, networking hardware, and distributed platform software. He has worked on various Tivoli customer projects as a systems architect in Turkey and the U.S. Vasfi is also a Certified Tivoli Consultant.

Shazli Mohd Ghazali is an I/T Specialist with IBM Integrated Technology Services, IBM Malaysia Sdn. Bhd. He has three years of experience in AIX Support with a particular focus on TCP/IP application support and various e-Business products running on the RS/6000 platform. He has worked at IBM for three years. His areas of expertise include IBM Firewall and IBM WebSphere products maintenance.

Rick Nall is a Senior Information Security Consultant with Computer Business International, Inc. a training and consulting firm and IBM Business Partner headquartered in Reno, Nevada. He holds certifications in

Information Security, DB2 and AIX, and has 28 years of experience in the IT industry, in both management and technical positions. His areas of expertise include risk analysis, incident response, firewalls, intrusion detection, mainframe and UNIX deployment, disaster recovery, contingency planning, teaching, and course development. For the past six years, he has focused on teaching, designing, and implementing secure architectures for e-commerce, e-finance, and governement agencies.

Luis Maria Rodriguez works as a Tivoli Certified Consultant at BitX SA, a Tivoli Service Business Partner, headquartered at Buenos Aires, Argentina. He has three years of experience in Tivoli Systems Management, and more than six years of experience in networking hardware and distributed platform software. He worked on various IBM customer projects as a Tivoli Consultant in Latin America. He is a Tivoli Certified Consultant (since 1999). He is also Cisco certified (CRLS).

Sai Sampath is a Software Developer with IBM Global Services Ltd. India. He has two and half years experience in developing security tools. He holds a masters degree in computer science. Mr. Sai provides security solutions to customers with IBM Firewall and had two years of experience on software analysis, design, and implementation.

Peter Kai Wimmer is an IT Security Specialist with Haitec AG, an IBM Business Partner in Germany, where he leads a team of security consultants. He holds a degree in computer science from Munich University of Technology. Mr. Wimmer provides costumers with information system security consulting and has three years of experience with firewalls and other security-related technologies.

Thanks to the following people for their invaluable contributions to this project:

International Technical Support Organization, Austin Center
Wade Wallace

IBM/Tivoli Austin, Risk Manager Product and Development Team
Frances Dodson, Ron Edmark, Mike Garrison, William Harrison, Greg Hess, Roy Janik, Luca Loiodice, Rosanne Swart

Comments welcome

Your comments are important to us!

We want our Redbooks to be as helpful as possible. Please send us your comments about this or other Redbooks in one of the following ways:

- Fax the evaluation form found in “IBM Redbooks review” on page 373 to the fax number shown on the form.
- Use the online evaluation form found at **ibm.com**/redbooks
- Send your comments in an Internet note to redbook@us.ibm.com

Part 1. What is e-business Risk Management

Chapter 1. Where do we need to start

This chapter gives an introduction to where today's security risks are coming from and what sort of attacks can occur. The intent is to show that intrusion detection systems need to be applied to all levels within the enterprise and that security point products (such as firewalls) alone are not enough to ensure a secure and safe I/T environment.

1.1 Introduction

In today's complex network environments, a single change can compromise the whole network integrity and can cause financial consequences. This is even more so where the Internet is used to conduct business, such as in the Business to Business (B2B) and Business to Consumers (B2C) models and their derivations. We know that a firewall alone is not enough anymore and that more sophisticated mechanisms on different levels within the company have to be used to detect intrusion.

1.1.1 Reliability of a firewall

The pace of upgrades, patches, and new protocols is staggering, and although it seems positive to have this progress, it actually becomes an advantage for the skilled and experienced hacker. We all know that before installing patches, upgrades or new protocols, they will be thoroughly tested, and it can take weeks if not months to finally introduce a patch into the production environment. Rest assured, that the hacker community is aware of this. They will exploit known bugs and security holes in your firewall software.

Please refer to Section 1.2, "Hacker profiles" on page 6 for a discussion of our understanding of the term 'hacker' throughout this book.

1.1.2 Internal threats

The likelihood of compromising security from within your organization is a lot higher than breaches from outside your organization. Research indicates that 60 percent to 80 percent of all security breaches have been caused by company insiders. The severity of this type of breach is often higher, because people that are familiar with the company's infrastructure are able to do a lot more damage in a short period of time. A firewall is not going to help in this case, but more sophisticated intrusion detection software, in conjunction with state of the art management software and centralized management functions, can help detect malicious attempts from within the organization.

1.1.3 External threats

Although internal threats are more likely, the idea of having people from outside and from all over the world trying to break into your company's infrastructure is a far more frightening thought. Prosecution is in many cases difficult because of the international nature of the hacker community.

1.1.4 Common forms of attacks

Although the attacks and techniques are changing daily, there are a few common forms of attacks that we would like to touch on briefly.

1.1.4.1 Internal intruders

Internal intruders take advantage of sloppy administrators, non existent or poorly designed business processes, and the lack of security management.

Some common breaches are:

- Searching for shared drives in the Windows Network Neighborhood that are not password protected.
- Downloading scripts from the Internet to crack passwords or identify weak passwords.
- Installing of trojan horse programs (also referred to as backdoor programs) to enable future access to files and systems.
- Looking for offices with Post-It notes that have passwords and login IDs written on them.
- Using social engineering, which is the use of people skills to obtain passwords and other information with the intent to gain access to the infrastructure.
- After leaving the company, the employee still has a dialup account due to sloppy procedures. How often do we escort a departing employee out of the building but we do not make sure that all his accounts are disabled prior to leaving the building?
- Attaching a sniffer device to the local area network.

1.1.4.2 External attacks

Some common techniques are used to obtain access to infrastructures:

- Social engineering
- Hackers normally scan a large number of devices connected to the Internet and try to obtain as much information on the systems as possible by using different techniques. Home users are vulnerable by default, and hackers like to place keystroke monitoring trojan horse programs on these

home computers to obtain passwords, VPN secret keys, and other relevant information.

> **Note**
>
> Think of this scenario: you use your desktop computer at home to browse the Internet and also log in to the corporate VPN to check e-mail and other business related activities. If a malicious hacker placed a trojan horse program on your desktop, he is able to obtain the information he needs to access your corporate network.

- Spoofing of a DNS connection to redirect the information to a server controlled by the hacker.
- Using operating system information to determine version and release in order to use the known bugs and security holes. This is done by looking at the header information when doing an FTP or login attempt to a targeted server.
- Script kids using publicly available hack scripts to change Web pages and crack passwords.

> **Note**
>
> Malicious hackers normally do not advertise that they have intruded on your network.

1.1.4.3 Access points

Access points are obviously a target for external hackers and, in most cases, access points are managed on a case by case basis without centralized management. In most cases, the security policies are weak or non-existent. The phrase “We are secure, we have a firewall” or even “We are very secure, we have multiple firewalls” is still common, but, unfortunately, this does not prevent hackers from entering your enterprise’s I/T infrastructure.

> **Note**
>
> A false sense of security is more dangerous than no security at all.

Access points are either created on purpose, such as dial-up connections, or accidently, such as, a development server with Internet connectivity. Networks that have been linked due to consolidation or merger activities could be left with no one in control of the entire I/T infrastructure for a transitional period.

1.2 Hacker profiles

The term hacker in this redbook is used to describe a person or groups of people that are trying to gain unauthorized access to computer systems and infrastructures without the proper permission. They use the information, that can be found on the targeted infrastructure, for criminal or improper use.

There are three types of hackers, and they all need to be treated with care and diligence:

- Script kids: Youngsters that look for existing scripts that enable them to gain access through the firewall, attempt to break passwords, and modify Web pages. These script kids do not realize the legal implications of their actions and their attempt is more based on curiosity than to create damage. Not only do they run scripts without understanding what these are doing, but they also jeopardize their own security by installing malicious code that could have been hidden in the script file. Malicious hackers are now able to launch attacks from these compromised systems to large corporations and the script kid might not be aware of this!

  An interesting statistic shows that 90 percent of all hackers are script kids.

  Script kids are not considered the most dangerous hackers, but they are responsible for a large number of attacks and traffic that could cause serious problems, such as Denial of Service (DOS) attacks and an enormous creation of events.

  Script kids' ability in general does not exceed the “Scan & Attack” step, with the exceptions that reach the “Island” step (see Figure 2 on page 9 for more details).

- Experienced Programmers: By definition, these people have broad experience in debugging code, finding bugs, and creating workarounds for problems. They are typically skilled in a variety of programming languages, including (mainly) C and C++. They use bug lists of applications to determine known vulnerabilities and their own creativity to obtain ways of accessing protected information by exploiting these bugs.

  The majority of scripts that are available on the Internet hack sites are created, modified, and enhanced by this group.

  Less than 9 percent of all hackers fit in this category. Although their skill level is high it is not their main goal to abuse falsely gained information maliciously but more to boost their reputation and the “I have done it” feeling.

These experienced programmers usually get to the “Continue Dig” step (see Figure 2 on page 9 for more details), but usually are not able to cover their tracks completely, which is caused in part by their lack of expertise in Protocol and Intrusion Detection technology.

- Protocol experts that are highly skilled programmers: This group of people is able to break into a secure I/T infrastructure, change code, obtain sensitive information (such as credit card data), and leave the wire without being traced. Their excellent understanding of protocols, such as TCP/IP, UDP, IPsec, L2TP, VPN, encryption methodologies, Intrusion Detection techniques, firewalls, packet wrappers, and a multitude of low level programming languages make them a hot asset and a dangerous opponent (in case they decide to use their capabilities for illegal purposes).

  This group is also responsible for some of the best hacker tools and concepts, yet their intelligence prohibits them from posting these programs (nor do they brag about them).

  Less than 1 percent of all people classified as hackers belong to this group.

  This group is able to go all the way to the “Takeover” step (see Figure 2 on page 9) and attempt a takeover of the compromised equipment; therefore, there are potentially the most dangerous type of hacker.

  The actual severity of these hacks is relative to the threat they represent (see Figure 1 on page 8). Note, however, that there have been cases where script kids have caused serious damage through the use of tools created and provided by experts.

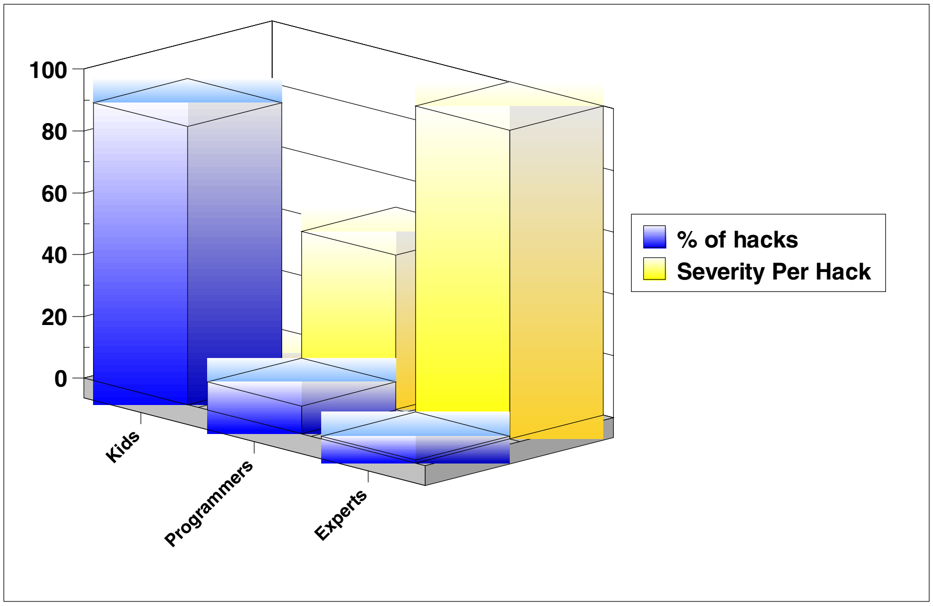


Figure 1. Percentage of hacks relative to severity

1.2.1 Hacker methods

The following chart is a high level overview of the steps taken by hackers with the goal to take over your network.

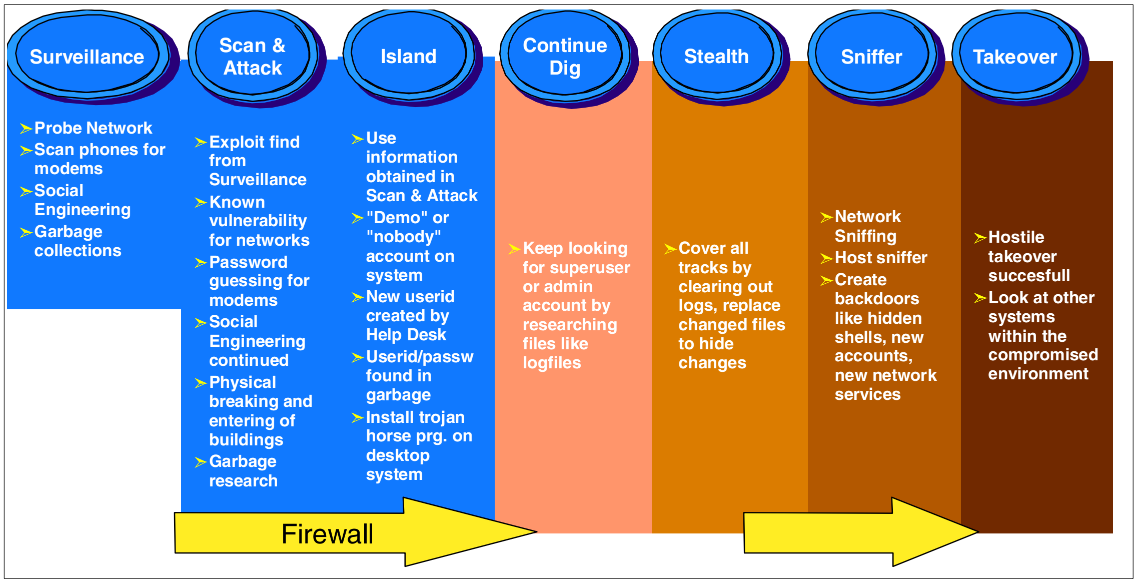

Surveillance
Scan & Attack
Island
Continue Dig
Stealth
Sniffer
Takeover
➢Probe Network
➢Scan phones for modems
➢Social Engineering
➢Garbage collections
➢Exploit find from Surveillance
➢Known vulnerability for networks
➢Password guessing for modems
➢Social Engineering continued
➢Physical breaking and entering of buildings
➢Garbage research
➢Use information obtained in Scan & Attack
➢"Demo" or "nobody" account on system
➢New userid created by Help Desk
➢Userid/passw found in garbage
➢Install trojan horse prg. on desktop system
➢Keep looking for superuser or admin account by researching files like logfiles
➢Cover all tracks by clearing out logs, replace changed files to hide changes
➢Network Sniffing
➢Host sniffer
➢Create backdoors like hidden shells, new accounts, new network services
➢Hostile takeover succesfull
➢Look at other systems within the compromised environment
Firewall

Figure 2. Hacker steps

This introduction shows, that in order to successfully detect intrusions, we have to be able to monitor all the different components within the corporate infrastructure, and not just equip the firewall with intrusion detection software. After the firewall is breached, an intruder is able to “play” around and will try to gain access to even more resources.

Note

To centrally and effectively manage the different sorts of breaches and attacks (in order to reconcile the necessary countermeasures), a holistic IT security infrastructure is the only acceptable solution.

Having said that, a holistic security infrastructure approach should follow the characteristics outlined in the next section.

1.2.1.1 Holistic security infrastructure characteristics

A firewall is good initial protection, and it stops most hackers. But once the intruder passes the firewall, he is virtually free to do as he pleases. A good intrusion detection approach has the following characteristics:

- All network devices report to a central repository about possible breaches. This includes but is not limited to firewalls, Web servers, DNS servers, application servers, remote workstations (home office users), and so on.

- The central repository is managed 24 hours a day and suspicious events are reacted on immediately.
- Enterprise Risk Management processes and procedures are defined, constantly updated, and adhered to by all involved employees.
- Event flooding[1] and false positives[2] can deter support staff away from actual breaches. Therefore, a *correlation engine* (see Section 3.4.4, “Correlation for enterprise risk management” on page 36 and Chapter 2, “The importance of correlation” in the redbook *Tivoli SecureWay Risk Manager: Correlating Enterprise Risk Management*, SG24-6021) is an absolute must.
- Pervasive intrusion detection, which is implemented by installing a sensor or agent on every device, which constantly monitors for suspicious signatures or patterns, just like antivirus software vendors have been doing. This allows for constant updates to the signature database and provides a flexible and easy to manage intrusion detection system. More details on the different supported adapters and sensors can be found in Chapter 5, “Deploying Tivoli Risk Manager” on page 67.
- A holistic security infrastructure approach is necessary to make intrusion detection and management of breaches an integral part of the network topology and business practice.
- A consistent enterprise security policy is in place. All components are set up and configured in compliance with this policy.
- Conduct regular vulnerability assessment by utilizing scanners to detect and report on weaknesses, like weak or blank passwords, unused open TCP ports, and so on. This includes testing for compliance with the security policy.
- Implement centralized reporting and analysis of breaches. This should be handled by highly skilled security specialists who are physically separated from the operation and traditional network management areas.

[1] Events are stored in a repository, but the amount of events is causing the information to become cluttered and unusable.

[2] An event indicating that a breach occurred but is a false alarm instead.

Chapter 2. Business benefits

Implementing a centralized risk management console with different sensors deployed throughout the I/T is the only way for an administrator to appropriately react to specific threats and attacks. With an overwhelming amount of network activities and a multitude of intrusion detection point products installed, he has to become aware of the real threats, and not be distracted by false positives. Only by using different sources of information will he be able to act to eliminate a threat.

Since almost every enterprise is exposed to the Internet community or to business partners, it is very important to retain all business operations on a 24 x 7 schedule. Being able to react to hacker attacks and prevent severe loss of data, fraud, loss of online access, or even corporate image demonstrates the direct business benefits for a central risk management approach.

2.1 Today’s situation

Businesses are facing increasing risks from a multitude of fronts (virus threats, unauthorized access, denial of service attacks, and other forms of intrusions) that target networks, servers, and desktops. The risks increase as more enterprise systems and applications become accessible on the Internet. In the highly competitive world of e-business, customers are demanding and expecting the highest quality of service, trust, and security from corporations.

e-business implementations must be secure, protect the privacy of business transactions, ensure the integrity of business operations, protect customer data, and provide round-the-clock access. Businesses who have carefully built their brand equity understand that brand equity in the Internet world could be quickly eroded or destroyed by an attack, and availability of business-critical systems could be compromised by an Internet virus. Virus threats, unauthorized access to company resources, and hacking attempts, such as denial of service attacks, are some of the most serious threats faced by businesses today.

Virus threats, such as the Melissa virus and the ILOVEYOU virus, and other attacks create havoc by forcing businesses to shut down critical applications. Corporations need to be careful to avoid becoming victims of viruses.

The well-publicized denial of service attacks launched in early 2000[1] on the Internet portal sites Yahoo, eBay, Amazon, and Buy.com brought down

[1] IDG News Service, February 9, 2000: www.idg.net/idgns/2000/02/09/UPDATEEBayAmazonBuy.comHitBy.shtml

several Web servers for several hours, resulting in significant revenue losses for those companies, not to mention negative publicity.

2.2 Introducing Tivoli Risk Manager

Tivoli Risk Manager is the industry's first enterprise risk management product that enables system administrators to take control of their enterprise intrusions. Today, corporations are deploying a number of security solutions, such as firewalls, intrusion detection systems, and access control mechanisms, as part of their overall security strategy to achieve the simple objective of "Let the good guys in; keep the bad guys out." Security policies implemented at the network level, host level, and application level allow access to only authorized users' applications and systems.

Yet businesses still face increasing risks from virus threats, unauthorized access, and denial of service attacks that target the enterprise. Threats can originate internally from within the enterprise or externally from the Internet. Informal surveys suggest that almost half of the internal threats are malicious, and the other half are accidental and arise from misconfigured systems or weak security policies. Effectively guarding against these different threats requires an enterprise view of security. This coordinated approach can harness the intelligence across the different security checkpoints within the enterprise. Enterprise risk management seeks to accomplish the following broad objectives:

- Provide a simple, easy-to-use enterprise security console to monitor, view, and manage alert events across the enterprise. This approach enables companies to identify and manage threats and vulnerabilities throughout the enterprise and ensures that access to networks, systems, applications, and desktops is consistent with enterprise security policies.
- Enable system administrators to precisely identify different types of threats and attacks using advanced correlation techniques, so corporations can identify patterns of intrusions, eliminate clutter, reduce false-positive alerts, and quickly identify real security threats to speed response time.
- Provide decision support through an analytical and Web-based historical reporting decision support guide that enables organizations to comprehend their business risks proactively and take immediate action. With decision support, security administrators can pinpoint vulnerable hot spots and take corrective action by upgrading their security policies.
- Provide a variety of predefined reaction tasks to quickly resolve urgent security issues, such as denial of service attacks, viruses, or unauthorized

accesses. Predefined tasks include reconfiguring a firewall, revoking user accounts on servers, and deleting viruses from a desktop.

- Integrate with multivendor security technology products to provide comprehensive security management.
- Leverage integration with the full range of Tivoli network, system, and security management products to take long-term corrective actions and constantly improve enterprise security policies.

Tivoli Risk Manager is an open, cross-platform, standards-based enterprise management platform that enables customers to seamlessly manage security intrusions and vulnerabilities across networks, hosts, operating systems, applications, servers, and desktops. Increasingly, attacks and intrusions target the enterprise as a whole, not just as a subsystem. Consequently, defending against these threats requires an enterprise view of security: a coordinated approach that can harness the intelligence across different security checkpoints within the enterprise.

Tivoli customers can leverage their existing investments in Tivoli Enterprise Console and the Tivoli Framework to seamlessly implement enterprise risk management as a subset of traditional enterprise management. Tivoli Risk Manager can manage a broad range of security technologies and products that are widely deployed within the enterprise: events and alerts from firewalls, routers, network and host-based intrusion detection systems, host system security, antivirus systems, and desktop security systems. Using advanced knowledge-based correlation techniques, Tivoli Risk Manager significantly reduces clutter and repetition by aggregating and summarizing thousands of alerts, reducing false positives, and enabling system administrators to identify threats through correlation, alert aggregation, and summarization. Severe alerts (attacks, unauthorized access, suspicious activities, and policy violations) can be responded to with automatic tasks, such as updating firewall policies, disabling a user account, resetting hostile TCP connections, or updating router Access Control Lists.

In order to position Risk Manager within a typical e-business environment and understand the necessary infrastructure, refer to Chapter 3, “Risk Manager topology and infrastructure” on page 19.

Table 1 summarizes the business benefits of Risk Manager.

Table 1. Risk Manager benefits

Management service	**What it does**	**What it means to you**
Enterprise risk management	Leverages security intelligence across different security products, such as firewalls, intrusion detection systems, networks, applications, and desktops, to identify intrusions and threats.	Enables customers to understand the overall risk to the enterprise and allows them to upgrade their policies and mitigate the risk.
Centralized correlation	Collects input from multiple sensors and intelligently correlates the outputs and alerts to determine whether an attack has really occurred.	Eliminates the *noise* for security analysts and allows them to focus on the underlying cause. Eliminates the nightmare of false positives and simplifies administration for non-security experts.
Centralized console management	Manages security events from a standalone console or integrates them with the Tivoli Enterprise Console.	Simplifies security management and allows non-expert administrators to confidently monitor and assess risks across multiple checkpoints.
Hierarchical and scalable architecture	Allows various layers to perform data reduction and correlation functions, so only significant incidents are reported up the hierarchy for further analysis.	Improves scalability by monitoring attacks and intrusions across a number of network intrusion sensors and Web server sensors.
Management of intrusions on the e-business security infrastructure	Provides a complete solution set for managing intrusions across the DMZ (networks, hosts, and applications).	Quickly deploys an out-of-the-box solution to manage intrusions in the DMZ and protect your e-business infrastructure from unauthorized access and intrusions.

Management service	What it does	What it means to you
Persistent storage of alerts and intrusions	Enables you to store alert intrusions in a relational database, such as Oracle, SQL server, and DB2.	Provides organizations with historical records of their attacks and intrusions that can be used for incident management, law enforcement, and decision support.

Part 2. Integrating business line operation with Risk Manager

Chapter 3. Risk Manager topology and infrastructure

This chapter focuses on a general example layout of an enterprise e-business IT infrastructure. Some people might find a lot of similarities with their own setup but others can have a completely different organizational IT installation. Since a lot of the components mentioned in this overview will be found in almost every installment, the integration of these components into a centralized enterprise risk management implementation will be very much like ours.

Since the Tivoli Risk Manager builds upon the Tivoli Framework infrastructure we will line out the general aspects of integration. A more detailed Tivoli Framework overview with the necessary components can be found in Section 3.3, “Tivoli Framework architecture” on page 24. Based on the Tivoli Framework foundation, we will briefly describe all the available Tivoli Risk Manager elements and how they fit together. Detailed information on each of these can be found in the product documentation.

3.1 From the front door to the backyard

The recently reported increase of cyberattacks against e-businesses highlight the need for an integrated, multivendor approach to security management. New forms of cyberattacks constantly emerge and security administrators must address the business risks arising from different increasing risks, such as:

- Virus threats
- Unauthorized access to Web servers
- Denial of service threats
- Network intrusion attacks

There are a number of ways to configure the IT infrastructure for an enterprise, depending on the size of the organization and on what you are trying to achieve. Basically it is divided into three sections, as depicted in Figure 3 on page 20:

1. Nonsecure network

   A public network that uses the Internet protocol and the public telecommunication system to securely share part of a business information or operation with suppliers, vendors, partners, customers, or other businesses.

2. DMZ

   The demilitarized zone (DMZ) is a computer host or small network that detects as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. It is an optional and more secure approach to a firewall and effectively acts as a proxy server as well. Users of the public network outside the company can access only resources in the DMZ.

3. Secure network

   The secure network is a private network within an enterprise (also known as an intranet). Typically, an intranet includes connections through one or more gateway computers to the outside Internet.

4. Extranet

   This term is only a "state of mind," in which the Internet is perceived as a way to do business and connect with other companies, like subcontractors or business partners. The intention is to establish secure connections from one company to the other by using the Internet as the network provider.

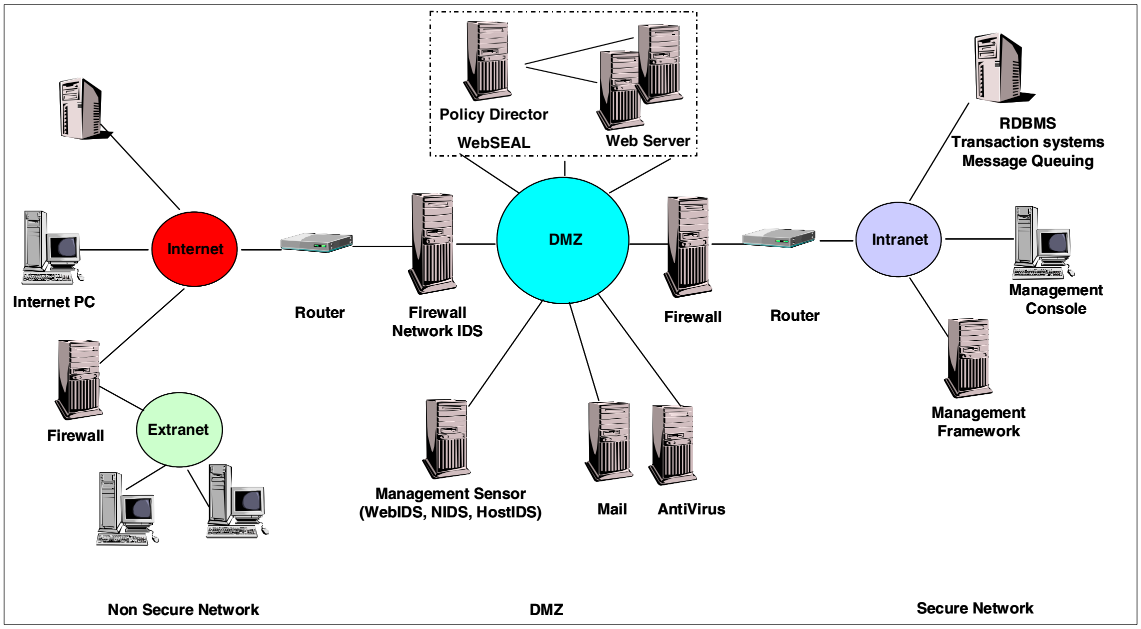


Figure 3. e-business topology

3.2 Overview of components

In Figure 3 on page 20, we show a complex e-business scenario that might be found in today's enterprise environments. This section will briefly discuss all the components involved in this infrastructure.

3.2.1 Web server environment

The Web server environment includes different kinds of Web servers, Web application servers, and corresponding management and security technologies for these servers.

3.2.1.1 Web servers

A Web server provides informational content in the form of Web pages to Web browsers. Web servers may contain pages about a company, product offerings, technical information, or other static content. Web servers also offer some ways of providing dynamic content and scripting capabilities. Due to security and management reasons, these areas are more and more delegated to specialized Web application servers.

3.2.1.2 Web application servers

Web application servers provide the business logic for an application program in a distributed network environment. These applications are mainly based on Java servlet or Enterprise Java Beans (EJB) technology nowadays. Web application servers can be found in any size of company in order to provide access to valuable business data through Internet type browser based access models. They can be placed in the DMZ as well as in the intranet part of the IT infrastructure.

3.2.1.3 Policy Director WebSEAL integration

Policy Director is a robust policy management tool for e-business and distributed applications for taking care of authentication and authorization for accessing enterprise data. It includes:

- Access control for Web applications
- Authorization service and API for legacy and distributed application integration based on C++ and Java2
- Access control for MQSeries based applications
- Highly-available and high-performing Management Server infrastructure

More information on Policy Director can be found via the Tivoli Web site at:

`http://www.tivoli.com/products/index/secureway_policy_dir/`

3.2.2 Back-end data

The back-end data reflects the most valuable assets a company owns, not only in IT means.

3.2.2.1 Database systems

A database holds information that is organized, so that its contents can easily be accessed, managed, and updated. Databases contain aggregations of data records or files, such as sales transactions, product catalogs and inventories, and customer profiles. Typically, a database manager provides users the capabilities of controlling read/write access, specifying report generation, and analyzing usage. Databases and database managers are prevalent in large mainframe systems, but are also present in smaller distributed workstation and mid-range systems. Controlling access to these systems and protecting them against fraudulent action is most important.

3.2.2.2 Transaction systems

A transaction usually means a sequence of information exchange and related work (such as database updating) that is treated as a unit for the purposes of satisfying a request and for ensuring database integrity. For a transaction to be completed and database changes to made permanent, a transaction has to be completed in its entirety.

3.2.2.3 Message queueing

Message queueing is a method by which processes can asynchronously exchange or pass data using an interface to a system-managed queue of messages. This queue is created by one process and used by multiple other processes that read and write messages to the queue.

This system connects many commercial systems in business today and it works independently of network disruptions, meaning that important data is always delivered.

3.2.3 Firewall

A firewall is a program, located at a network gateway, that protects the resources of a private network from users from other networks. Security policies implemented at the network level, host level, and application level allow access to only authorized users, applications and systems.

An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to.

Basically, a firewall examines each network packet to determine whether to forward it toward its destination. A firewall also includes or works with a proxy server that makes network requests on behalf of workstation users.

A firewall is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources.

Any abnormal attempt to access network resources through firewall devices has to be monitored actively and carefully.

3.2.4 Router

A router is a device that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to. A router is located at any gateway (where one network meets another), and it is often included as part of a network switch.

A router may create or maintain a table of the available routes and their conditions and use this information, along with distance and cost algorithms, to determine the best route for a given packet. Typically, a packet may travel through a number of network points with routers before arriving at its destination.

3.2.5 Intrusion Detection System

An Intrusion Detection System (IDS) is a type of security management system for computers (Host IDS), Web servers (Web IDS) and networks (Network IDS). An IDS gathers and analyzes information from various areas within a computer or a network in order to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). An IDS uses vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network.

Intrusion detection functions include:

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns

- Tracking user policy violations

IDS is being developed in response to the increasing number of attacks on major sites and networks, including those of the Pentagon, the White House, NATO, and the U.S. Department of Defense. The safeguarding of security is becoming increasingly difficult, because the possible technologies of attack are becoming ever more sophisticated; at the same time, less technical ability is required for the novice attacker, because proven past methods are easily accessed through the Web.

3.2.5.1 Web IDS

Web Server Intrusion Detection has been introduced with Tivoli Risk Manager. It uses the actual access log files generated by a Web server to perform the analysis that detects the Web server attacks. Web IDS, which is deployed on each Web server, will monitor the log in real time, using a knowledge based approach to detect malicious access attempts.

Most companies use a multitude of Intrusion Detection Systems on a variety of systems in order to gain as much information as possible about malicious access attempts. It is very challenging to stay focused with the amount of alerts and false positives coming in from all the IDS.

3.2.6 Antivirus

Antivirus features are integrated with operating system management. This software is a class of program that searches hard drive and floppy disks for any known or potential viruses.

3.2.7 Mail infrastructure

Electronic mail is the exchange of computer-stored messages by telecommunication. It is one of the protocols included with the Transport Control Protocol/ Internet Protocol (TCP/IP). The most popular protocol for sending e-mail is Simple Mail Transfer Protocol (SMTP); for receiving, it is POP3.

3.3 Tivoli Framework architecture

Tivoli Risk Manager adds enterprise risk management to the comprehensive list of enterprise management solutions and third-party applications based on the Tivoli Management Framework. The Tivoli management architecture manages thousands of machines from a single server. Servers can interconnect to manage large multiple-domain networks.

The Tivoli management architecture is based on a three-tier structure (see Figure 4) with four basic components: server, desktop, agent, and gateway.

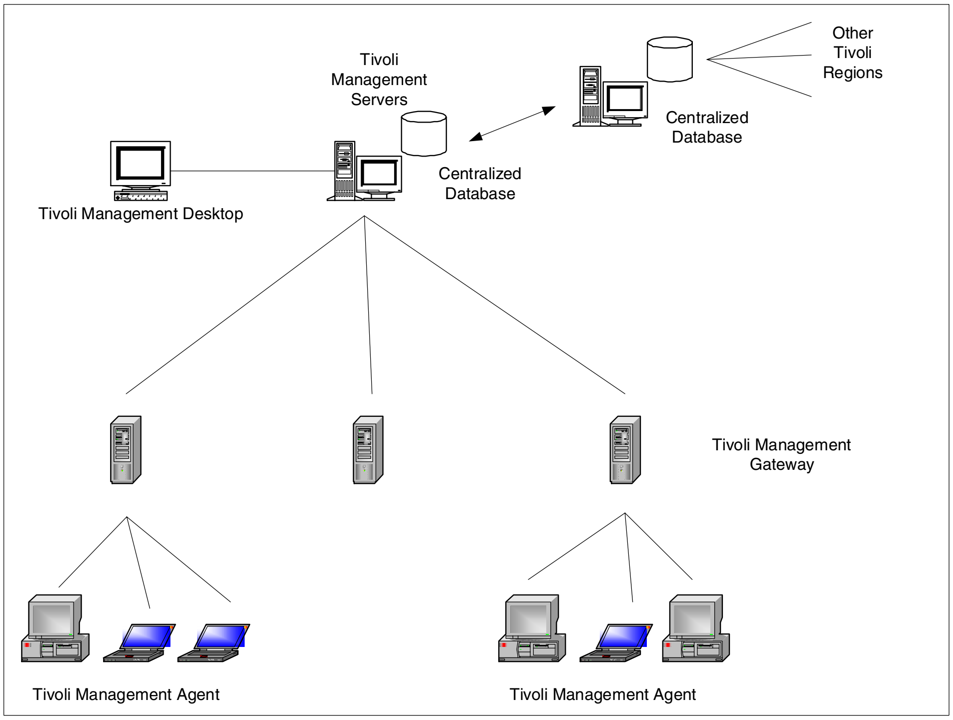


Figure 4. Tivoli management architecture

The Tivoli Management Framework provides a set of common services or features that are used by other Tivoli applications installed on top of the Tivoli Management Framework. These services include, but are not limited to, the following set:

- A task library through which you can create tasks and execute them on multiple Tivoli resources.
- A scheduler that enables you to schedule all Tivoli operations, including the execution of tasks created in the Tivoli task library.
- An RDBMS Interface Module (RIM) that enables some Tivoli applications to write application-specific information to relational databases.
- A query facility that enables you to search and retrieve information from a relational database.

3.3.1 Tivoli Management Server

The Tivoli Management Region server (TMR server) includes the libraries, binaries, data files, and graphical user interface (GUI) needed to install and manage your Tivoli environment. The TMR server maintains an internal database that includes information about the managed objects, such as workstations, databases, and applications, and it coordinates all communication with Tivoli managed nodes. In addition, the endpoint manager is part of the TMR server and is responsible for endpoints. The server also performs all authentication and verification necessary to ensure the security of Tivoli data.

3.3.2 Tivoli management desktop

The management desktop enables the administrator to access the Tivoli management applications from any location in the network.

When you install the TMR server on a UNIX system, the Tivoli management desktop is automatically installed. When you install the server on a Windows NT system, you must install it separately.

The Tivoli management desktop, shown in Figure 5 on page 27, is a graphical user interface (GUI). It presents an administrator's view of the Tivoli environment. From the Tivoli management desktop, resources and perform tasks can be easily accessed across the enterprise.

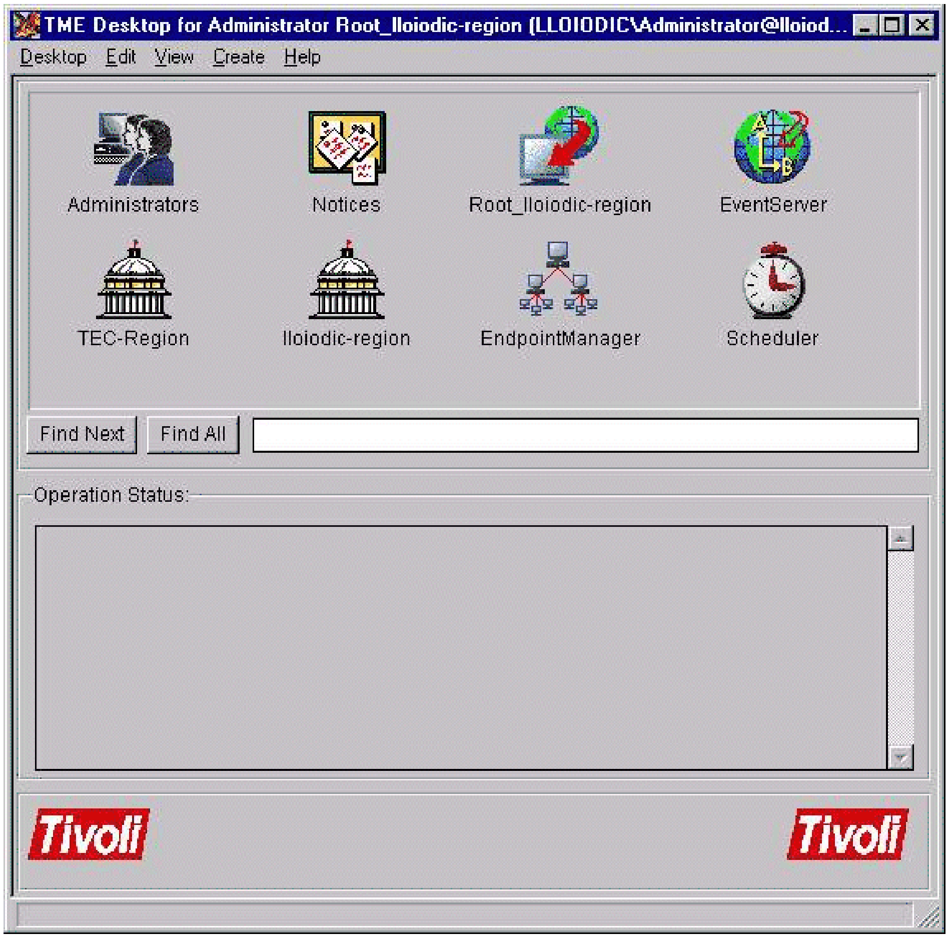


Figure 5. Tivoli management desktop

The Tivoli management desktop can display a variety of resources:

- Administrators
- Bulletin boards
- Policy regions
- Schedulers
- Generic collections
- Application-specific resources

3.3.3 Managed node

A Tivoli *managed node* runs the same software that runs on a TMR server. Managed nodes maintain their own databases that can be accessed by the TMR server. When managed nodes communicate directly with other managed nodes, they perform the same communication or security operations performed by the TMR server.

The difference between the TMR server and the managed node is that the TMR server database is global to the entire TMR (including all managed nodes). In contrast, the managed node database is local to the particular managed node. For management of the computer system that hosts the managed node, install an endpoint on that managed node.

3.3.4 Tivoli endpoint

An endpoint is a PC or UNIX workstation running the Tivoli Management Agent. It enables one-touch management by quickly detecting changes within the environment and bringing them under Tivoli management. Each event source integrated into the management framework needs to be configured as an endpoint. Endpoints provide the framework services to Tivoli applications that run on the workstation or desktop. Adapters, which are described in Section 3.4.1, “Adapters” on page 34, use the endpoint to communicate alerts to the Tivoli event management platform.

3.3.5 Gateway

A gateway controls all communication with and operations on Tivoli endpoints. A single gateway can support communication with thousands of endpoints. A gateway can launch methods on an endpoint or run methods on the endpoint’s behalf.

A gateway is created on an existing managed node. This managed node provides access to the endpoint methods and provides the communication with the TMR server that the endpoints occasionally require.

3.3.6 Policies and policy regions

Policies and policy regions play a fundamental role in the Tivoli architecture. In the Tivoli environment, a policy is a set of rules applied to managed resources. A policy enables the administrator to control the default values of newly created resources (default policy) and maintain the guidelines when administrators modify or operate on resources (validation policy).

A specific rule in a policy is a policy method. A default policy method can supply a constant value or run a shell script or a program that generates a value, whereas a validation policy method typically runs a program or shell script to verify values supplied by the administrator. Administrators can define and maintain policies.

Policy regions are containers for managed resources that use the same set of policies (for example, a collection of desktops within a given administrative domain). Collectively, these desktops can be administered using permissions or roles that are assigned to administrators on the basis of policy regions. Policy regions can help organize the managed resources in the desktop and define and limit administrator access to these resources.

3.3.7 Centrally managed policies

Tivoli Risk Manager leverages policy regions, which enable security management staff to centrally manage policies and determine who is allowed to support which targets and in what manner. This can be done on the basis of skills (for example, antivirus administrators) or on the basis of geographical location (for example, New York branch analysts).

Tivoli Risk Manager offers policy-based delegation of authority, and IT management groups target into policy regions. If a simple marketing department policy region contains four PCs, the antivirus administrator supporting the marketing department has authorization to access this policy region. A senior administrator can set up the policy region and delegate the support of the marketing department to a junior administrator. In this case, the defined policy may require antivirus signatures to be updated to all the desktops every week. The administrator uses a virus signature profile to implement the organization’s antivirus update policy.

The policy regions in Tivoli Risk Manager provide granular access control and implement enterprise risk management in large organizations. Centrally managing policy makes the product scalable, because the complexity of management does not increase exponentially as the size of the network increases. Administrators are assigned roles on a region-by-region basis. Roles can help restrict the level of operations that an administrator can perform.

3.3.8 Tivoli Enterprise Console

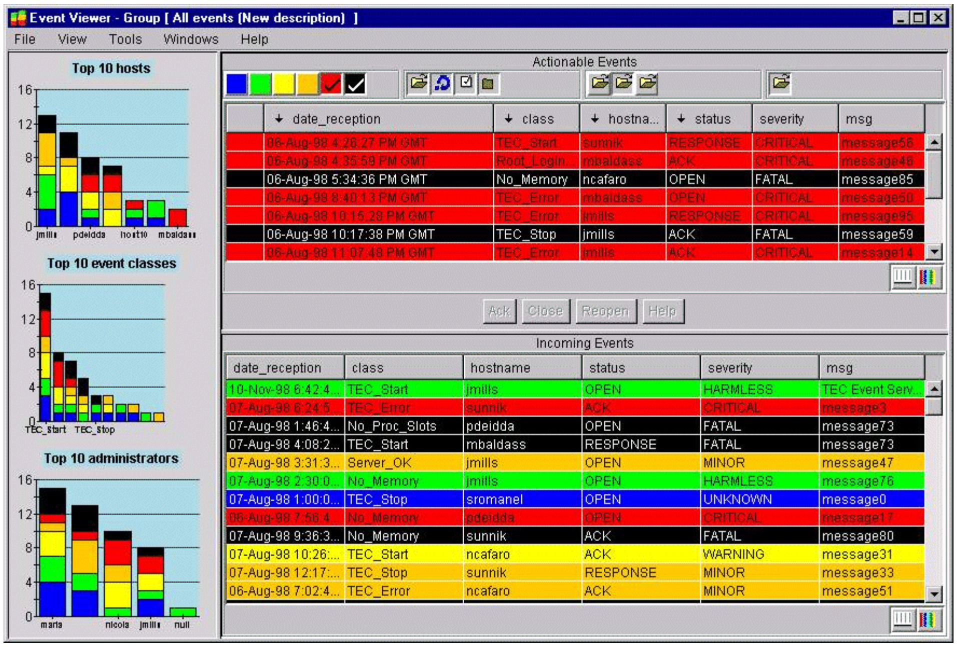
Tivoli Enterprise Console (TEC) is a robust platform for centralized event management across the enterprise. Events generated from distributed event sources are stored in a relational database and managed by the Tivoli desktop console. System administrators use the Tivoli desktop console to manage events from applications, such as Tivoli Distributed Monitoring and

Tivoli Security Manager, and manage events generated from third-party applications.

Tivoli Enterprise Console collects and integrates disparate management information into a common model for event processing and provides a central operations view. Types of event processing include event correlation, filtering, dropping duplicates, prioritizing, consolidating, closing self-correcting events, escalating events, and forwarding events. Tivoli Enterprise Console handles events from applications, databases, and systems and network devices.

When events are defined, Tivoli Enterprise Console rules can correlate events and define automated actions. Correlation automatically closes events related to resolved problems. An automated response capability enables problem resolution with no user intervention.

Security analysts can use Tivoli Risk Manager to quickly troubleshoot problems logged in to Tivoli Enterprise Console, such as monitoring open events, generating trouble tickets for problem resolution, or responding to serious events with actions. The new Tivoli Enterprise Console Java console panel in Figure 6 shows a view of the list of open events.



Actionable Events

	↓ date_reception	↓ class	↓ hostna...	↓ status	severity	msg
	06-Aug-98 4:26:27 PM GMT	TEC_Start	sunnik	RESPONSE	CRITICAL	message58
	06-Aug-98 4:35:59 PM GMT	Root_Login...	mbaldass	ACK	CRITICAL	message48
	06-Aug-98 5:34:36 PM GMT	No_Memory	ncafaro	OPEN	FATAL	message85
	06-Aug-98 8:40:13 PM GMT	TEC_Error	mbaldass	OPEN	CRITICAL	message50
	06-Aug-98 10:15:28 PM GMT	TEC_Error	jmills	RESPONSE	CRITICAL	message95
	06-Aug-98 10:17:38 PM GMT	TEC_Stop	jmills	ACK	FATAL	message59
	06-Aug-98 11:07:48 PM GMT	TEC_Error	jmills	ACK	CRITICAL	message14

Incoming Events

date_reception	class	hostname	status	severity	msg
10-Nov-98 6:42:4...	TEC_Start	jmills	OPEN	HARMLESS	TEC Event Serv...
07-Aug-98 6:24:5...	TEC_Error	sunnik	ACK	CRITICAL	message3
07-Aug-98 1:46:4...	No_Proc_Slots	pdeidda	OPEN	FATAL	message73
07-Aug-98 4:08:2...	TEC_Start	mbaldass	RESPONSE	FATAL	message73
07-Aug-98 3:31:3...	Server_OK	jmills	OPEN	MINOR	message47
07-Aug-98 2:30:0...	No_Memory	jmills	OPEN	HARMLESS	message76
07-Aug-98 1:00:0...	TEC_Stop	sromanel	OPEN	UNKNOWN	message0
06-Aug-98 7:56:4...	No_Memory	pdeidda	OPEN	CRITICAL	message17
07-Aug-98 9:36:3...	No_Memory	sunnik	ACK	FATAL	message80
07-Aug-98 10:26:...	TEC_Start	ncafaro	ACK	WARNING	message31
07-Aug-98 12:17:...	TEC_Stop	sunnik	RESPONSE	MINOR	message33
06-Aug-98 7:02:4...	TEC_Error	ncafaro	ACK	MINOR	message51

Figure 6. TEC Java console

The newest release of Tivoli Enterprise Console adds significant performance enhancements with hundreds of events per second throughput and high-capacity event throttling. It enables extensive flexibility and scalability in large environments. No other event management system offers high-speed, logic-based reasoning and can centrally control and manage the intelligence with drag-and-drop interfaces.

Tivoli Risk Manager leverages Tivoli Enterprise Console capabilities to centrally manage enterprise intrusions. Alerts from a variety of sources, such as firewalls, routers, intrusion detection systems, antivirus, servers, desktops, and applications, are grouped centrally and managed from the Tivoli desktop console. Alerts from distinct event sources are aggregated and stored in Tivoli Enterprise Console event groups.

There are three main components in the Tivoli Enterprise Console:

- Event Sources

  These are applications that gather information about resources throughout the IT environment. These applications typically run on any machine where availability is of concern. Once the information has been gathered, it is converted into an event and forwarded to the event server.

- Event Server

  The event server is a group of cooperating processes that run on a single managed node within a TMR.

  These processes cooperate with each other to receive events from various sources, perform various levels of processing on received events, and forward the events to the corresponding event consoles. The event server is the heart of TEC; it provides the Prolog engine for applying rules to received events.

- Event Consoles

  This is the user interface that an administrator uses to interact with the Enterprise Console. Each instance of an event console is configured to display logical groupings of events.

  The administrator can perform actions to events displayed on the console, such as viewing the detail. Any changes made to an event from other consoles or the event server will be reflected on each console that has the event in its view.

3.3.9 Availability Intermediate Manager (AIM)

Tivoli Enterprise Console includes the new AIM, a mid-level management server for Tivoli Enterprise Console events, to better control the environment and event management process. With the multitiered (n-tiered) capabilities of AIM, tremendous flexibility and scalability for the event stream result in better bandwidth utilization and more control over event flow, event storm protection, aggregation capabilities, and redundancy. The architectural scalability enables sophisticated filtering, routing, correlation, and automation to be performed anywhere in the event stream, as shown in Figure 7.

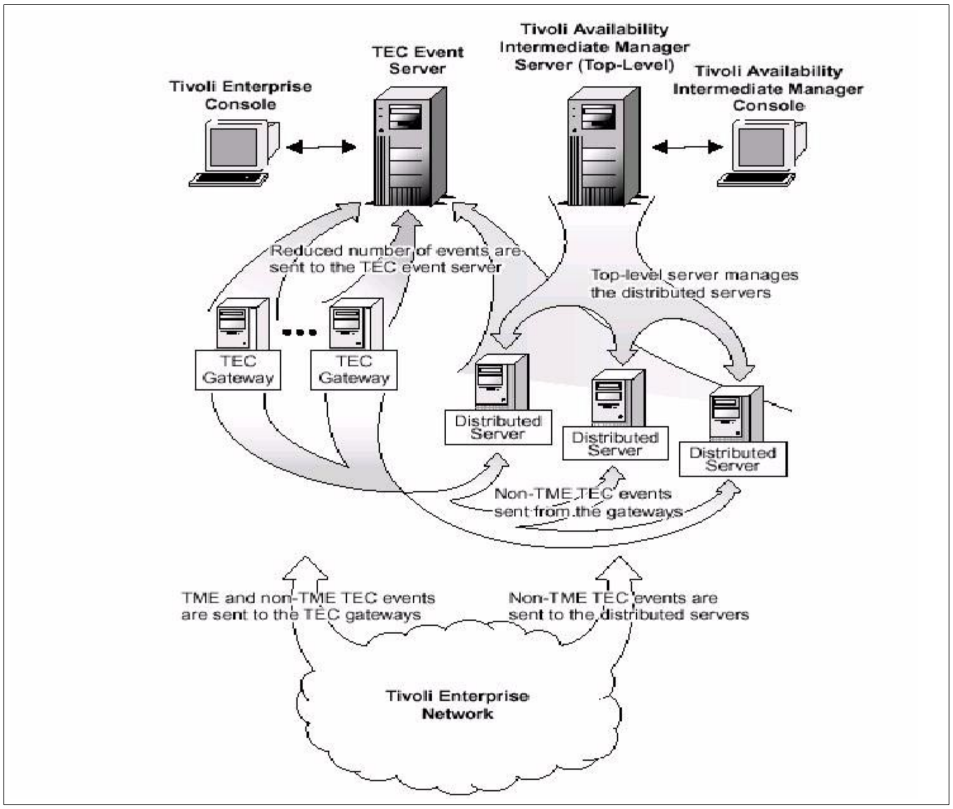
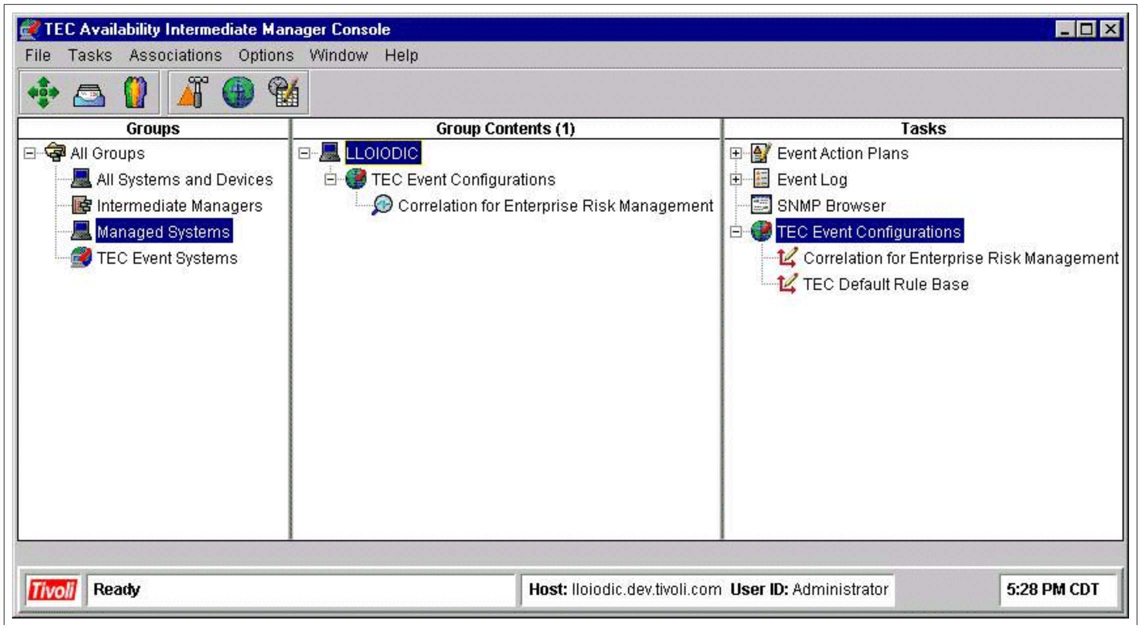

Tivoli Enterprise Console
TEC Event Server
Tivoli Availability Intermediate Manager Server (Top-Level)
Tivoli Availability Intermediate Manager Console
Reduced number of events are sent to the TEC event server
Top-level server manages the distributed servers
TEC Gateway
TEC Gateway
Distributed Server
Distributed Server
Distributed Server
Non-TME TEC events sent from the gateways
TME and non-TME TEC events are sent to the TEC gateways
Non-TME TEC events are sent to the distributed servers
Tivoli Enterprise Network

Figure 7. AIM topology

Additionally, AIM has an easy-to-use drag-and-drop GUI to create simple filters without any scripting and also has a critical management console to maintain and control a distributed intelligence environment. Figure 8 on page 33 shows the AIM console.



Ready

Host: lloiodic.dev.tivoli.com **User ID:** Administrator

5:28 PM CDT

Figure 8. Tivoli Enterprise Console AIM

3.4 Risk Manager architecture

Tivoli Risk Manager is an add-on classic Tivoli Enterprise Console application that leverages the Tivoli Enterprise Console event management system to manage enterprise security threats. Figure 9 on page 34 describes the architecture that follows the Tivoli Enterprise Console guidelines for building Tivoli Enterprise Console adapters, Tivoli Enterprise Console rules, and Tivoli Enterprise Console tasks.

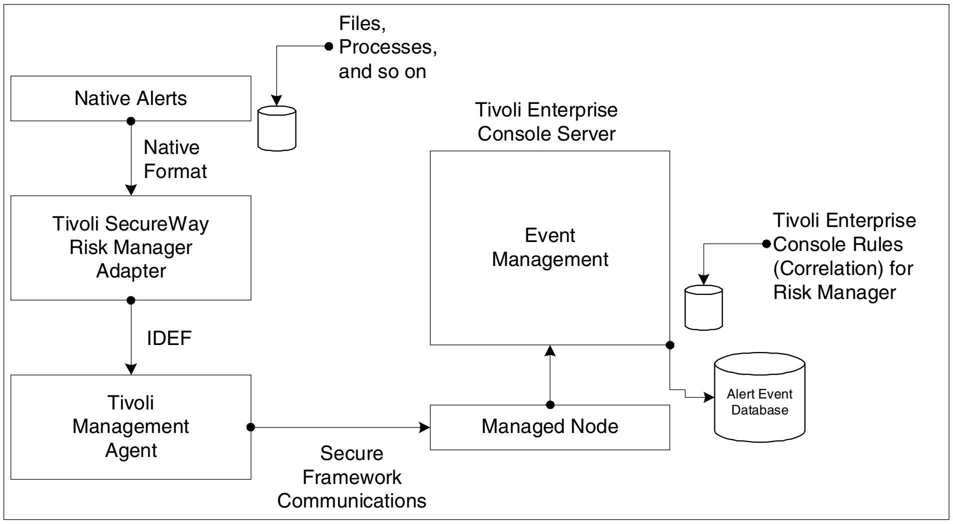


Figure 9. Risk Manager architecture

If you are familiar with the Tivoli Enterprise Console architecture, you will notice that Tivoli Risk Manager is a logically layered architecture that leverages Tivoli Enterprise Console components to implement enterprise risk management. Each of the managed technologies, such as firewalls, intrusion detection systems, routers, and hosts, has Tivoli Risk Manager-compliant adapters, rules, and (optionally) tasks that enable security analysts to manage their enterprise from a single control point.

3.4.1 Adapters

Adapters are software processes that monitor event sources and convert the events generated from event sources into a standardized format that can be securely forwarded to the Tivoli Enterprise Console Event Server using the Tivoli Framework. An event source is anything capable of generating a security alert, such as firewall log file alerts generated from network and host-based intrusion detection systems, syslog messages from UNIX, event logs generated from Microsoft Windows NT, and antivirus alerts generated by desktop virus software. Tivoli Risk Manager supports the Intrusion Detection Exchange Format (IDEF) standard (an IETF draft) for alert sources to communicate event data to management systems. Standardizing on a common data format makes it easy for new event sources to leverage the distributed correlating, reporting, and decision support capabilities of Tivoli Risk Manager. New event sources can be easily integrated by the toolkit. Figure 10 on page 35 illustrates multiple event sources that use adapters to create IDEF-compliant messages.

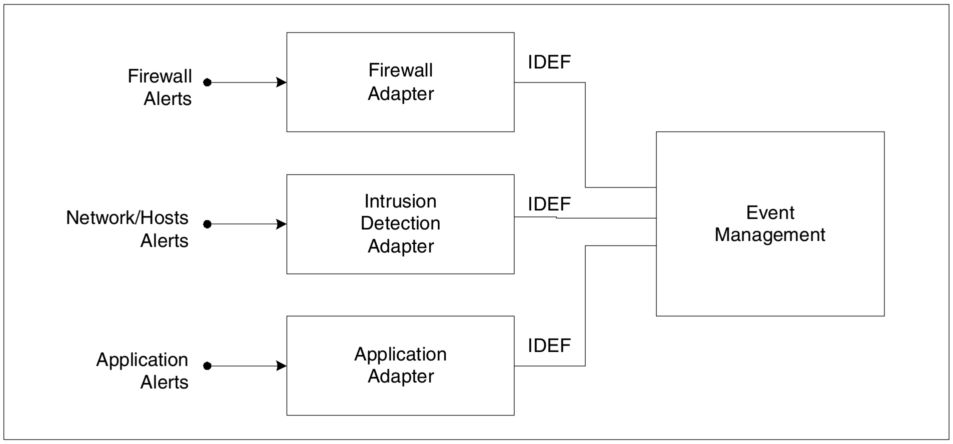


Figure 10. Adapters convert events and alerts into IDEF

3.4.2 Adapters and managed technologies

From a functional standpoint, adapters can be thought of as the *glue* that Tivoli Risk Manager uses to manage the technology components. Each managed technology requires an adapter. From a functional perspective, Tivoli Risk Manager supports three categories of managed technologies:

- Applications
- Systems
- Desktops

The applications category refers to applications, such as Web servers, firewalls, network intrusion detection systems, and custom and legacy applications, that are integrated using the toolkit. The systems category refers to UNIX and Windows NT servers, Cisco routers, and so on. The desktop category refers to managed desktop applications, such as virus tools.

3.4.3 Event management platform architecture

The event management platform is the set of event management services that provides the underlying infrastructure to manage the distributed alerts. The event management platform is built on flexibility, usability, and scalability. Flexibility refers to the ease with which new event sources can be integrated into the event management solution. New adapters can be easily built using IDEF and the toolkit. A scalable and highly performing event management platform ensures that security alerts can be filtered and correlated and that appropriate incident management and responses can be initiated in a timely fashion.

Enterprise event management is more than simply collecting and displaying events on a console for someone to view; it is a multifaceted, complex business process that requires analysis to determine how and where to filter, correlate, and route events and how to respond to the situations that event conditions represent in enterprise environments. It supports events from thousands of event sources: networks, servers, desktops, applications, and network management systems.

If the solution does not scale, alerts cannot be processed and correlated in real time. If the event management platform crashes, the organization is potentially vulnerable to threats and attacks.

The Tivoli Risk Manager event management platform is based on the new version of Tivoli Enterprise Console, a proven infrastructure and platform for event management. A new Java-based console helps level-one analysts watch consoles and also helps those who manage and maintain them. From a scalability perspective, a new AIM allows sophisticated filtering, routing, correlating, and automating to be performed anywhere in the event stream, so event management can scale to thousands of management nodes and adapt to business policies. AIM may be implemented virtually anywhere, as many as required, for tremendous flexibility and scalability. Its multitiered capabilities, tremendous flexibility, and scalability for the event stream result in better bandwidth utilization and more control over event flow, event storm protection, aggregation capabilities, and redundancy. With the new AIM, customers can easily process large volumes of events, re-route events based on any criteria, and duplicate event paths based on whatever policy has been established by the organization.

Event management enables all other IT processes, such as problem management and change management, and Tivoli Enterprise Console is uniquely suited to help IT organizations deliver flexible and scalable event management policies and processes. Tivoli Risk Manager exploits all the advanced capabilities of Tivoli Enterprise Console event management, and organizations quickly gain control of their environment and provide an integrated management of enterprise intrusions.

3.4.4 Correlation for enterprise risk management

Tivoli Risk Manager and the enterprise risk management correlation enable security analysts to establish relationships between multiple events and actions to run in response to the events, which clears the event condition and the event condition effects.

The distinction between rules and signatures causes confusion. Rules implement the logic needed to identify patterns of threats by correlating events from multiple sources. Signatures enlist misuse patterns that are used by intrusion detection systems to report events that match the signature criteria. New signatures need to be developed and updated for new attacks in a timely fashion; rules are independent of signatures and are updated during new product versions. Out-of-the-box rules are included for firewalls, intrusion detection systems, and routers. More details on the correlation engine can be found in the redbook *Tivoli SecureWay Risk Manager: Correlating Enterprise Risk Management*, SG24-6021.

3.4.5 Decision Support for enterprise risk management

Decision Support is a critical aspect of enterprise risk management. Enterprises deploy sophisticated security systems with the overall objective of lowering the risks to enterprise business assets. Decision Support is an invaluable tool for companies to understand, interpret, and quantify the business risks arising from threats, attacks, and intrusions. Using the capabilities of the Tivoli Decision Support product, enterprise alerts are analyzed in real time. Through a comprehensive set of enterprise risk management guides, security analysts can quantify business risks through an analytical decision-making process and proactively implement security policies quickly to eliminate the security vulnerability or exposure. Tivoli Risk Manager leverages the Tivoli Decision Support product to provide decision support for firewalls, vulnerability assessments, virus management, and intrusion detection.

Tivoli Risk Manager enterprise risk management guides (also known as Tivoli Decision Support Discovery Guides) provide a ready-to-use view of the wealth of data by transforming the intrusion and virus alert data into easily accessible business-relevant information. Analytical Decision Support enables high-level data analysis to answer the following questions:

- Which systems are most susceptible to virus attacks?
- Are the system, network, and application usage consistent with enterprise security policies?
- Is there a correlation between unauthorized access and intrusion attempts?

This information is presented in a variety of graphical formats that can be viewed interactively (for example, slice, dice, drill down, or drill through) or posted on a URL.

Tivoli Decision Support Discovery Guides are available for a number of products, including Tivoli Enterprise Console, Tivoli Inventory, Tivoli NetView, Tivoli Service Desk, Tivoli Software Distribution, and Tivoli Distributed Monitoring, and they provide easily accessible IT business-relevant information.

More detailed information on setting up and using Tivoli Decision Support can be found in Chapter 7, “Reporting using TDS for Enterprise Risk Management” on page 255.

3.5 The benefits of enterprise risk management

Risks are pervasive throughout the enterprise. Enterprise risk management lowers the overall risk to the enterprise by leveraging security intelligence across many different security products. There are four specific management disciplines to focus on:

- Firewall management
- Intrusion detection
- Risk assessment
- Virus management

3.5.1 Firewall management

Businesses today are deploying several firewalls to control access to their internal networks from the Internet and their extranet environment. Several resources manage firewalls and look at log files generated by firewalls, which contain a rich set of events crucial for enterprise risk management. Until now, security administrators had to manually sift through multiple firewall log files and look for intrusion data, an approach that is laborious, error-prone, and overwhelming to security administrators because of the sheer volume of log entries. The Tivoli Risk Manager Firewall Management feature enables customers to centrally manage their firewall log files. Tivoli Enterprise Console consolidates and monitors events from multiple firewalls. Customers can use Tivoli Enterprise Console as the centralized event management server to manage their firewall deployments. Tivoli Risk Manager monitors firewall log files in real time and forwards them to Tivoli Enterprise Console. Individual firewall alerts are grouped into event classes and archived in a relational database, making it easy for administrators to run various types of decision support queries using SQL.

Tivoli Risk Manager implements firewall rules that correlate and aggregate alerts issued by multiple firewalls and presents the alert information in an intuitive, easy-to-use, and manageable fashion. System administrators use the Tivoli desktop to manage firewall alerts, close open alerts, issue trouble tickets, and invoke predefined firewall tasks included with Tivoli Risk Manager. Role-based access control can be used to delegate specific firewall administration and management tasks to specific administrators.

For example, events from extranet and partner firewalls can be managed by one group, and Internet firewalls can be managed by a different group of administrators. Tivoli Risk Manager includes a number of tasks to automatically respond to firewall alerts, such as paging an administrator, invoking a firewall action to reset a TCP connection, or dynamically adding firewall filter rules to block networks or hosts from connecting to the enterprise.

Tivoli Risk Manager supports CheckPoint Firewall-1 and Cisco PIX Firewall. High-level toolkits are available to integrate other firewalls into Tivoli Risk Manager.

3.5.1.1 Managing CheckPoint Firewall-1

Tivoli Risk Manager supports CheckPoint Firewall-1 and VPN-1 virtual private networks. The firewall adapter for CheckPoint monitors the firewall log files on the Firewall-1 management station in real time, formats the log file events into IDEF, and forwards the events to the Tivoli Enterprise Console server through secure Framework communications.

Events from multiple Firewall-1 and VPN-1 deployments are aggregated and consolidated into an event group within Tivoli Enterprise Console. Firewall-1 alerts are grouped into event group categories, such as Firewall-1 communication messages, encryption engine messages, connection attempts, and critical alerts messages. Tivoli Plus modules for CheckPoint Firewall-1 allow customers to centrally manage and distribute VPN-1 and Firewall-1, such as new adapter versions and configuration data.

3.5.1.2 Managing Cisco PIX Firewall

Tivoli Risk Manager supports Cisco PIX Firewall. The firewall adapter for Cisco PIX Firewall monitors the firewall log files on the Cisco management station in real time, formats the log file events into IDEF, and forwards the events to the Tivoli Enterprise Console server using secure Framework communications. Events from multiple Cisco firewalls are aggregated and stored in a separate event group within Tivoli Enterprise Console.

3.5.2 Intrusion detection

Intrusion detection is an essential prerequisite to enterprise risk management. Customers are beginning to deploy several variants of intrusion detection systems:

- Network intrusion detection systems are being deployed to monitor unauthorized access and network-level intrusions.
- Host intrusion detection systems are being deployed to deal with host-level intrusions.
- Application-level intrusion detection is gaining popularity for detecting specific intrusions at the application level that are not detected by the network or host-level components. For example, Web servers are likely to have a real-time intrusion detection engine for HTTP (or HTTPS) application traffic.

Tivoli Risk Manager supports leading network intrusion detection solutions from ISS (network and host) and Cisco. In addition, Tivoli Risk Manager includes optional network and host-level intrusion detection and real-time application-level intrusion detection for Web servers.

3.5.2.1 Managing ISS RealSecure Network Engine

Tivoli Risk Manager supports both ISS RealSecure Network Intrusion Detection and the ISS RealSecure Host Intrusion Detection System. The RealSecure adapter monitors the log files generated by RealSecure in real time, formats the log file events into IDEF, and forwards the events to the Tivoli Enterprise Console server using secure Framework communications. Alerts from multiple RealSecure Intrusion Detection Systems are consolidated into an event group within Tivoli Enterprise Console and tagged with the appropriate critical level. System administrators can use the familiar and easy-to-use Tivoli desktop console to manage their diverse intrusion detection alerts with a single console rather than having to learn and use a new console for each intrusion detection system. More importantly, alerts from RealSecure are used by the Enterprise Intrusion Detection feature that enables system administrators to precisely identify patterns of threats, reduce false alarms, and manage their intrusions with a higher degree of assurance.

In addition to managing alerts, the Tivoli Plus module for RealSecure allows customers to centrally manage distribution and deployment of the intrusion detection engine from the Tivoli desktop console.

3.5.2.2 Managing Cisco Secure IDS

Tivoli Risk Manager supports the Cisco Secure IDS (formerly NetRanger) Network Intrusion Detection System. The Cisco Secure IDS adapter monitors the log files generated by RealSecure in real time, formats the log file events into IDEF, and forwards the events to the Tivoli Enterprise Console. Alerts from multiple Cisco Secure IDS Intrusion Detection Systems are consolidated in a separate event group within Tivoli Enterprise Console. System administrators can use the familiar and easy-to-use Tivoli desktop console to manage their diverse intrusion detection alerts with a single console rather than having to learn and use a new console for each intrusion detection system. More importantly, the Enterprise Intrusion Detection feature uses alerts from Cisco Secure IDS to help system administrators precisely identify patterns of threats, reduce false alarms, and manage intrusions with a higher degree of assurance using enterprise correlation.

3.5.3 Application intrusion detection management

As more applications are Web-enabled, the probability of attacks and intrusions on these applications increases. Web servers, Java applications, and databases must be secured and monitored to ensure their integrity and availability. Also, attacks increasingly use a secure transport, such as SSL, to render traditional network intrusion detection systems and firewalls incapable of defending against them. This opens up a new class of application-level intrusion detection systems that understand the application-level protocol and can monitor threats and intrusions on these applications.

3.5.3.1 Managing Web server intrusions using Web IDS

In today's e-business environment, protecting the Web infrastructure is one of the most serious challenges facing enterprises. Building a loyal customer base requires the Web infrastructure to be secure, highly available, and performing, and it must ensure the confidentiality, integrity, and privacy of customer transactions. High-profile denial of service attacks on Internet portal sites have shown how easily these threats can be carried out to destroy brand equity and cause a loss of customer confidence.

Tivoli Risk Manager includes an intrusion detection system feature called Web IDS. Web IDS is an essential component of enterprise risk management that enables organizations to monitor unauthorized intrusions and various forms of attacks on Web servers. Today, hackers use sophisticated tools that target URL-level attacks on public Web sites using HTTP or HTTPS (using HTTP over SSL). These type of attacks cannot be blocked by the firewall and frequently bypass monitoring by network intrusion detection tools. An application-level intrusion detection component, such as Web IDS, can detect these attacks and enable security administrators to implement incident management and containment.

Web IDS detects and manages attacks on a number of Web servers, including Netscape/iPlanet, Microsoft IIS, Domino, Apache, and Tivoli Policy Director. By integrating with Tivoli Policy Director, organizations allow authorized access for their business constituents and ensure that unauthorized access attempts, attacks, and intrusions are monitored and responded to in real time.

3.5.3.2 Virus management

One of an IT manager's top concerns is protecting the enterprise from virus threats. Although many organizations have some type of antivirus solution deployed, many organizations are still susceptible to virus attacks, such as the ILOVEYOU virus.

Vulnerabilities remain because of a lack of ongoing virus management to ensure that all desktops and systems have the most recent virus software, that virus signature files are updated, and that desktops not complying with enterprise virus policies are identified and acted upon immediately.

Managing Symantec Norton AntiVirus Client Alerts

Using the Tivoli Desktop feature in Tivoli Risk Manager, system administrators can manage Norton AntiVirus alerts. The Norton AntiVirus adapter uses the secure Framework communications to forward alerts from desktops to the Tivoli Enterprise Console server.

With Tivoli Risk Manager, security administrators can manage Symantec Norton AntiVirus alerts from Tivoli Enterprise Console. Examples of virus alerts include the following:

- Identify known viruses detected on different desktops
- Identify unknown viruses detected on different desktops
- Identify virus definitions that are out of date
- Identify virus-like activity

3.5.4 Managing host Intrusions using Tivoli Host IDS

Tivoli Host IDS is a host-level intrusion detection system that manages host-level intrusions throughout the enterprise.

3.5.4.1 Managing alerts from UNIX servers

Frequently, the syslog facility within UNIX can be configured to log useful information on different subsystems within UNIX, such as the UNIX kernel, user processes, TCP/IP subsystem, and devices. The events recorded by syslog form an important basis for detecting intrusions on host systems. With the syslog facility, Tivoli Risk Manager includes a UNIX adapter that monitors intrusions on UNIX systems. Events are forwarded to the Tivoli Enterprise Console server by secure Framework communications, and they are correlated with events from other adapters according to Tivoli Risk Manager rules.

3.5.4.2 Managing Windows NT servers

The event log facility within Windows NT can be configured to log useful information on different subsystems within Windows NT, such as the operating system, user processes, remote access, applications, TCP/IP subsystem, and devices. The events recorded by the event log facility form an important basis for detecting intrusions on Windows NT and Windows 2000 servers. The event log facility in Tivoli Risk Manager includes a Windows NT adapter that monitors for intrusions on servers. Events are forwarded to the Tivoli Enterprise Console server by secure Framework communications, and they are correlated with events from other adapters according to Tivoli Risk Manager rules.

3.5.5 Risk assessment

Correlation for enterprise risk management is the industry's first solution that provides cross-product, cross-platform intrusion management and risk assessment capability. This unique feature of Tivoli Risk Manager provides a correlated view of enterprise intrusions and violations. For example, a business has deployed 50 intrusion detection systems (a combination of network-based, host-based, and application-based engines). Using Tivoli Enterprise Console rules, events from several intrusion detection engines go through a process of duplicate elimination, alert summarization, and distributed correlation to identify patterns of threats. Each pattern of attack is referred to as a situation. By classifying thousands of alerts into a few precise situations, security administrators can quickly gain invaluable insight into threats and attack patterns that are monitored by different intrusion detection engines.

Security analysts can use the correlation for enterprise risk management feature to:

- Reduce or eliminate false positives by correlating alerts from different sources. Correlation provides a higher degree of assurance in reported alert information and weeds out misleading false alarms.

- Identify attack patterns (single high profile attacks and distributed denial of service attacks). Attacks are classified into situations that enable administrators to quickly pinpoint attack patterns.
- Provide a summary view of intrusion data that enables administrators to comprehend the alert data in a meaningful way.

3.5.5.1 Situations

A situation is the result of applying the Tivoli Enterprise Console rules to correlate events received from the different event sources throughout the enterprise. Situations identify patterns of threats that provide invaluable insight into how the enterprise is being targeted.

Situation 1

Situation 1 identifies a single critical alert that involves a single attack host and a single target. Examples of Situation 1 alerts are an attack host trying to obtain a password file from a UNIX machine, or an attack host launching a PHF attack on a Web server. Situation 1 identifies these situations through correlation and immediately forwards these alerts to the security administrator with a high severity.

Situation 2

Situation 2 identifies patterns of attacks between two machines, patterns of attacks launched on a destination, or patterns of attacks originating from a single machine to a set of targets. For example, an attacker trying to probe for vulnerabilities on a machine by launching a series of probes will be immediately identified and alerted by the correlation engine. This type of situation is difficult to detect on a manual basis, and identifying this situation early helps a security analyst quickly respond to the intrusions and disable the attack.

Situation 3

Situation 3 identifies more complex situations, such as a pattern of attacks launched against specific destinations (for example, a distributed denial of service attack launched on a Web server or an e-mail server). Situation 3 addresses the distributed pattern of attacks that involve multiple sources and multiple destinations.

3.5.6 Tasks for enterprise risk management

Tivoli Risk Manager includes a variety of tasks to quickly resolve security problems, such as:

- Inhibit a connection to/from a specific IP address on the firewall.

- Inhibit and close any existing connections to/from a specific IP address on the firewall.
- Cancel a previously enabled action on the firewall.
- Cancel all previously enabled actions on the firewall.
- Terminate a user process on a server.
- Suspend a user account on a server.
- Scan or delete a virus on a desktop.

3.5.7 The value of enterprise risk management

Finally, before we start going into the technical details with the next chapters, we want to summarize the basic Risk Manager values once again.

3.5.7.1 Modular deployment

Enterprise risk management offers flexibility for customers to pursue a modular approach to managing intrusions. For example, a customer interested in intrusion detection management can quickly leverage Tivoli Risk Manager to implement enterprise intrusion management as follows:

1. Install and configure a Tivoli Management Region (TMR) on one machine.
2. Install and configure Tivoli Enterprise Console.
3. Install and configure the Tivoli endpoint and the Tivoli Risk Manager adapters for the network intrusion systems that need to be managed using Tivoli Software Distribution (These steps have an estimated completion of three days, assuming five network intrusion systems need to be managed).

With the event management infrastructure in place, the power of an integrated risk management framework can now be demonstrated.

The steps required to integrate and manage additional servers, such as UNIX (50 UNIX servers) and Windows NT (100 Windows NT servers), are:

1. Distribute the Tivoli Management Agent and the Tivoli Host IDS (using the adapter profile) on the UNIX and Windows NT servers from the Tivoli desktop console.
2. Create and distribute the appropriate host security configuration on all the managed servers from the Tivoli desktop console (configuration settings control the intrusions detected and alerted by the Tivoli Host IDS system).

This illustrates the power of a scalable Framework across the enterprise. Customers can start with a small, manageable environment, such as managing intrusion detection systems or managing firewalls with a single TMR. With the risk management infrastructure in place, the solution can then be expanded to support managed technologies (using appropriate profile adapters), such as routers, Web servers, UNIX servers, and desktops.

> **Tivoli Framework security**
>
> In the past, there has been a lot of discussion about the Tivoli Framework security. This discussion was mainly about the secure communication between nodes or nodes and endpoints and the complexity of configuring management through firewalls.
>
> These topics have been addressed lately by introducing the Tivoli Management Framework Version 3.7.1, which is described in more detail in Appendix D, “Tivoli Management Framework 3.7.1 enhancements” on page 345.
>
> At the time this redbook was being finalized, Tivoli stated full support for using Risk Manager v3.7 in conjunction with the Tivoli Framework v3.7.1.

3.5.7.2 Tivoli integration

Tivoli Risk Manager integrates with the Tivoli Management Framework, Tivoli Enterprise Console, and Tivoli family of products. Integration benefits include:

- Tivoli Policy Director manages attacks and intrusions on e-business sites.
- Tivoli Security Manager quickly inspects and corrects security problems, such as virus infections or intrusion attempts.
- Tivoli Service Desk and Tivoli Remote Control manage security problems.
- Tivoli Global Business System Manager, Tivoli Distributed Monitoring, and Tivoli Application Performance Management tie together availability, performance, and security for your operation team.
- Tivoli Software Distribution and Tivoli Inventory help your change management team discover and resolve exposures due to outdated and misconfigured software.

3.5.7.3 Support for open standards

Tivoli Risk Manager actively promotes, supports, and contributes to the emerging open systems standards in the area of intrusion detection, including the following:

- The Common Vulnerabilities and Exposures (CVE)[1]

[1] http://www.cve.mitre.org

- The Intrusion Detection Exchange Format (IDEF)[2]

The CVE list is a dictionary of standardized names for vulnerability and other information. CVE standardizes the names for all publicly known vulnerabilities and security exposures.

IDEF is a common intrusion data model specification, which describes data formats that enable communication between intrusion detection systems and communication between intrusion detection systems and management systems.

Tivoli Risk Manager uses an IDEF-compliant protocol for communication with ID sensors. The IDEF standard integrates new security endpoints from multiple vendors into an enterprise risk management platform, such as Tivoli Risk Manager. An IDEF draft is available for review from the Intrusion Detection Working Group (IDWG) in the IETF.

3.5.7.4 Tivoli Risk Manager toolkit

Tivoli Risk Manager is built on top of Tivoli Enterprise Console, and it leverages the Tivoli Enterprise Console application programming interfaces (API) for integration.

To integrate with Tivoli Risk Manager, an alert generator:

1. Sends IDEF-compliant events to the Tivoli server via an event generator.
2. Provides response units to allow the administrator to react to attacks or resolve exposures.
3. Provides a Tivoli-compliant mechanism to install and configure the event generators and response units.

3.5.7.5 Conclusion

The knowledge economy is causing fundamental changes in enterprises as enterprises transform themselves to extend their traditional business models to the Web. Web companies are creating new ways of doing business on the Internet. All these changes are exciting, but fraught with challenges, and companies must understand the challenge of being on the Internet. The open Internet environment combined with lack of security makes companies unwitting targets of intrusions, such as virus threats, denial of service attacks, and unauthorized access. These threats are real. In the Computer Security Institute’s fifth annual Computer Crime and Security Survey[3], 85 percent of respondents detected computer viruses and 79 percent detected employee abuse of Internet access privileges. Companies can no longer deploy virus

[2] `http://www.ietf.org/html.charters/idwg-charter.html`

[3] Computer Security Institute (`http://www.gocsi.com`)

tools on all desktops or assume that virus threats can be mitigated. Managing virus policies, signatures, and compliance throughout the enterprise is crucial. A single user who does not comply with the virus policies becomes an unwitting participant in an ILOVEYOU virus threat that can bring down the company's e-mail system.

Integrated management of security alerts, practices, and policies is imperative to mitigating enterprise risks. An enterprise risk management solution, such as Tivoli Risk Manager, enables security analysts to centrally manage their enterprise security and use intelligent correlation and decision support to quickly identify users, networks, or hot spots (such as critical systems) and fix vulnerabilities. The business implications are significant if the company's e-mail servers or Web servers go down or are compromised. Having a single point of control to deploy an enterprise risk management solution for security across the enterprise helps mitigate risk, ensures business continuity, and is a compelling return on investment strategy that companies cannot ignore.

Chapter 4. Installation prerequisites and test environment

This chapter details the product installation order and prerequisites. It also introduces the test environment we are building for the remainder of this book.

4.1 Product installation order

This section covers the installation planning of Tivoli Risk Manager 3.7 and the respective prerequisite components. A basic overview is given about where (and why) to install the different components in terms of product prerequisites and dependencies and describes the test environment we used while working on this redbook. It provides detailed information on the machines, their setup, and the software installed.

You must install the following Tivoli or other products before you install the Risk Manager, as described in Section 5.2, “Installing Tivoli Risk Manager 3.7” on page 69:

1. Tivoli Management Framework (formerly TME/10 Management Enterprise Framework), Version 3.6.4.

New Framework version supported

At the time of finishing up the last lines of this book, Tivoli officially supports the Tivoli Framework Version 3.7.1 with Risk Manager. There are some interesting security implications with this new version, which are detailed in Appendix D, “Tivoli Management Framework 3.7.1 enhancements” on page 345.

```
# wlsinst -a
TME 10 Framework 3.6
Tivoli Framework Patch 3.6.1-TMF-0058 - 3.6.1A (w/reexec)
Tivoli Management Framework 3.6.4 Maintenance Release(build 08/10)
```

2. An external relational database management system (RDBMS) for use as the event database. We are using IBM DB2 Version 7.1.

```
# wgetrim tec
RIM Host:       tivoli
RDBMS User:     db2inst1
RDBMS Vendor:   DB2
Database ID:    tec
Database Home:  /usr/lpp/db2_07_01
Server ID:      tcpip
Instance Home:  /Tivoli/db2/db2inst1
```

3. Tivoli Enterprise Console (TEC) Version 3.7 Event Server

```
#wlsinst -p
TME 10 Framework 3.6
Tivoli Enterprise Console Server 3.7
```

4. TEC Version 3.7 User Interface (UI) Server

```
#wlsinst -p
TME 10 Framework 3.6
Tivoli Enterprise Console Server 3.7
Tivoli Enterprise Console User Interface Server 3.7
```

5. TEC Version 3.7 Sample Event Help

```
#wlsinst -p
..........
Tivoli Enterprise Console Server 3.7
Tivoli Enterprise Console User Interface Server 3.7
Tivoli Enterprise Console Sample Event Information 3.7
```

6. TEC Version 3.7 Event Console

```
#wlsinst -p
..............
Tivoli Enterprise Console Server 3.7
Tivoli Enterprise Console User Interface Server 3.7
Tivoli Enterprise Console Sample Event Information 3.7
Tivoli Enterprise Console 3.7
```

7. TEC Adapter Configuration Facility Version 3.7

ACF note

You have to install the ACF on the Tivoli Management Region (TMR) and endpoint gateways.

```
#wlsinst -p
...............
Tivoli Enterprise Console Server 3.7
Tivoli Enterprise Console User Interface Server 3.7
Tivoli Enterprise Console Sample Event Information 3.7
Tivoli Enterprise Console 3.7
Tivoli Enterprise Console Adapter Configuration Facility 3.7
```

8. TEC Event Integration Facility Version 3.7

```
#wlsinst -p
...............
Tivoli Enterprise Console Server 3.7
Tivoli Enterprise Console User Interface Server 3.7
Tivoli Enterprise Console Sample Event Information 3.7
Tivoli Enterprise Console Console 3.7
Tivoli Enterprise Console Adapter Configuration Facility 3.7
Tivoli Enterprise Console EIF 3.7
```

9. TEC patches (Patch 3.7-TEC-0001E (Early Release) and Patch 3.7-TEC-0004)

```
# wlsinst -P
..............
Tivoli Enterprise Console Server Patch 3.7-TEC-0001E (Early Release)
Tivoli Enterprise Console Server Patch 3.7-TEC-0004
Tivoli Enterprise Console Patch 3.7-TEC-0004 (Early Release)
Tivoli Enterprise Console ACF Patch 3.7-TEC-0004
Tivoli Enterprise Console User Interface Server Patch 4
```

10. The Tivoli Management Agent endpoint software (formerly LCF endpoint), Version 3.6.4

```
# wlsinst - P
...........
Gateway Enablement for Endpoint, Version 3.6.4 (build 08/13)
Tivoli Management Framework 3.6.4 Maintenance Release (build 08/10)
```

11. The Java for Tivoli 3.7 and Java Client Framework 3.7 (SIS 3.7 requirement).

TMF Version 3.7 CD required

The Java for Tivoli 3.7 and Java Client Framework 3.7 is located on the Tivoli Framework 3.7 CD (LK3T-5075-01) inside the JAVA subdirectory. Customers currently having access to the Framework 3.6.4 code only would need to order the Tivoli Framework 3.7 CD from their Tivoli sales representatives without charge.

```
# wlsinst -p
..........
Tivoli Java Client Framework 3.7
Java for Tivoli 3.7
..........
```

12. The Tivoli Software Installation Service (SIS), Version 3.7 and patches.

Note

The Software Installation Service Version 3.7 is located on the Tivoli Framework 3.7 CD (LK3T-5075-01) inside the SIS subdirectory. Customers currently having access to the Framework 3.6.4 code only would need to order the Tivoli Framework 3.7 CD from their Tivoli sales representatives without charge.

```
# wlsinst -a
...
Tivoli Software Installation Service Client, Version 3.7
Tivoli Software Installation Service Depot, Version 3.7
....
Tivoli SIS Client 3.7 Patch (3.7-SISCLNT-0002)
Tivoli SIS Depot 3.7 Patch (3.7-SISDEPOT-0002)
```

4.2 Product installation prerequisites

The information in this section is taken from the *.IND files that are included in the installation image. The applicable tags in these files regarding product prerequisites, dependencies, and registration are:

- patch_for

  The patch_for line indicates a dependency of the current TME package on an already installed version of the same product.

- patch_id

  The patch_id line is used to specify other products/patches that are included in this packaged imaged, and which are registered.

- depends

  The depends line is used to indicate dependencies between the current product/patch to be installed and other prerequisite products.

4.2.1 Tivoli Management Framework 3.6.4

The Tivoli Management Framework 3.6.4 can be installed as a new installation. The significant parts of the *.IND files, in terms of prerequisites, dependencies, and installation methods, are shown below:

```
TMF_3.6.4:description:Tivoli Management Framework 3.6.4 Maintenance Release
(build 08/10):TMF_3.6.4
TMF_3.6.4:patch_for:TMF
TMF_3.6.4:patch_id:TMF_3.6.4
TMF_3.6.4:patch_id:TMF_3.6.3
TMF_3.6.4:patch_id:TMF_3.6.2
TMF_3.6.4:patch_id:3.6.1-TMF-0002
TMF_3.6.4:patch_id:3.6.1-TMF-0003
.....
TMF_3.6.4:patch_id:3.2-TMF-0088
TMF_3.6.4:patch_id:3.2-TMF-0090
TMF_3.6.4:patch_id:TMF_364_0810_3.6.1
TMF_3.6.4:depends:TMF_3.6
```

Tivoli Framework 3.6 needs to be installed first with the Framework 3.6.4 maintenance release applied directly afterwards.

4.2.2 Java for Tivoli 3.7

Java for Tivoli 3.7 can be installed as a new installation. The significant parts of the *.IND files, in terms of prerequisites, dependencies, and installation methods, are shown below:

```
JRE:description:Java for Tivoli 3.7:JRE_1.1.8
JRE:revision:3.7
JRE:patch_id:JRE
JRE:depends:TMF_3.6
```

TMF_...:patch portions are registered with the installation.

4.2.2.1 Java Client Framework 3.7

Java Client Framework 3.7 can be installed as a new installation. The significant parts of the *.IND files, in terms of prerequisites, dependencies, and installation methods, are shown below:

```
JCF:description:Tivoli Java Client Framework 3.7:JCF_1.0
JCF:revision:3.7
JCF:patch_id:JCF
JCF:depends:TMF_3.6.1
JCF:depends:JRE
```

4.2.2.2 The SIS 3.7 Server Depot

The Software Installation Service 3.7 Server Depot can be installed as a new installation. The significant parts of the *.IND files, in terms of prerequisites, dependencies, and installation methods, are shown below:

```
SISDepot:description:Tivoli Software Installation Service Depot, Version
3.7:SIS
SISDepot:revision:3.7
.........
SISDepot:patch_id:SISDepot
SISDepot:patch_id:SIS_3.7
SISDepot:patch_id:SISDepot_3.7
SISDepot:depends:TMF_3.6.1
SISDepot:depends:3.6.1-TMF-0045
SISDepot:depends:JRE
SISDepot:depends:JCF
```

4.2.2.3 The SIS 3.7 Client

The Software Installation Service 3.7 Client can be installed as a new installation. The significant parts of the *.IND files, in terms of prerequisites, dependencies, and installation methods, are shown below:

```
SISCLNT:description:Tivoli Software Installation Service Client, Version
3.7:SISCLNT
SISCLNT:revision:3.7
.............
SISCLNT:patch_id:SISCLNT
SISCLNT:patch_id:SIS_3.7
SISCLNT:patch_id:SISCLNT_3.7
SISCLNT:patch_id:SIS_3.6.1
SISCLNT:patch_id:SIS_3.6
SISCLNT:patch_id:SIS_1.0
SISCLNT:patch_id:3.6.1-SIS-0005
............
SISCLNT:patch_id:1.0-SIS-0003
SISCLNT:patch_id:1.0-SIS-0004
```

```
SISCLNT:depends:TMF_3.6.1
SISCLNT:depends:3.6.1-TMF-0045
SISCLNT:depends:JRE
SISCLNT:depends:JCF
```

4.2.2.4 TEC Server 3.7

The Tivoli Enterprise Console Server 3.7 can be installed as a new installation. The significant parts of the *.IND files, in terms of prerequisites, dependencies, and installation methods, are shown below:

```
TEC_SERVER:description:Tivoli Enterprise Console Server 3.7:TEC_SERVER
TEC_SERVER:revision:3.7
TEC_SERVER:patch_id:TEC_SERVER
TEC_SERVER:patch_id:TEC_SERVER_3.7.0
TEC_SERVER:patch_id:FMT_EDITOR
TEC_SERVER:patch_id:RULE_BUILDER
TEC_SERVER:patch_id:TEC_CLI_3.7.0
TEC_SERVER:patch_id:TEC_SAMP_3.7.0
TEC_SERVER:depends:TMF_3.6.3
```

Tivoli Framework 3.6.3 or later is needed for the installation.

4.2.2.5 TEC User Interface Server 3.7

The Tivoli Enterprise Console User Interface Server 3.7 can be installed as a new installation. The significant parts of the *.IND files, in terms of prerequisites, dependencies, and installation methods, are shown below:

```
TEC_UI_SRVR:description:Tivoli Enterprise Console User Interface Server
3.7:TEC_UI_SRVR
TEC_UI_SRVR:revision:3.7
........
TEC_UI_SRVR:patch_id:TEC_UI_SRVR
TEC_UI_SRVR:patch_id:TEC_UI_SRVR_3.7
TEC_UI_SRVR:depends:TMF_3.6.3
```

Tivoli Framework 3.6.3 or later is needed for the installation.

4.2.2.6 TEC Adapter Configuration Facility 3.7

The Tivoli Enterprise Console Adapter Configuration Facility 3.7 can be installed as a new installation. The significant parts of the *.IND files, in terms of prerequisites, dependencies, and installation methods, are shown below:

```
ACF:description:Tivoli Enterprise Console Adapter Configuration Facility
3.7:ACF
ACF:revision:3.7
......
```

```
ACF:patch_id:ACF
ACF:patch_id:ACF_3.7.0
ACF:depends:TMF_3.6.2
```

Tivoli Framework 3.6.2 or later is needed for the installation.

4.2.2.7 Tivoli Risk Manager Server 3.7

The Tivoli Risk Manager Server 3.7 can be installed as a new installation. The significant parts of the *.IND files, in terms of prerequisites, dependencies, and installation methods, are shown below:

```
RISKMGR_CORR:description:Tivoli Risk Manager Server 3.7:RISKMGR_CORR
............
RISKMGR_CORR:patch_id:RISKMGR_CORR
RISKMGR_CORR:depends:TMF_3.6.3
RISKMGR_CORR:depends:TEC_SERVER_3.7.0
```

Tivoli Enterprise Console Server 3.7 is needed for the installation. The Tivoli Risk Manager Server 3.7 also needs TMF 3.6.3 or higher already installed.

4.2.2.8 Tivoli Risk Manager Event Integration Facility 3.7

The Tivoli Risk Manager Event Integration Facility 3.7 can be installed as a new installation. The significant parts of the *.IND files, in terms of prerequisites, dependencies, and installation methods, are shown below:

```
RISKMGR_EIF:description:Tivoli Risk Manager Event Integration Facility
3.7:RISKMGR_EIF
RISKMGR_EIF:revision:3.7
......
RISKMGR_EIF:patch_id:RISKMGR_EIF
RISKMGR_EIF:depends:TMF_3.6.4
```

Tivoli Management Framework 3.6.4 is needed for the installation.

4.2.2.9 Tivoli Risk Manager Adapter for Check Point FW-1 3.7

The Tivoli Risk Manager Adapter for Check Point FW-1 3.7 can be installed as a new installation. The significant parts of the *.IND files, in terms of prerequisites, dependencies, and installation methods, are shown below:

```
RISKMGR_CPFW:description:Tivoli Risk Manager Adapter for Check Point FW-1
3.7:RISKMGR_CPFW
RISKMGR_CPFW:revision:3.7
RISKMGR_CPFW:lcf_allow
..................
RISKMGR_CPFW:patch_id:RISKMGR_CPFW
```

```
RISKMGR_CPFW:depends:TMF_3.6.4
```

Tivoli Management Framework 3.6.4 is needed for the installation.

4.2.2.10 Tivoli Risk Manager Perl Support 3.7

The Tivoli Risk Manager Perl Support 3.7 can be installed as a new installation. The significant parts of the *.IND files, in terms of prerequisites, dependencies, and installation methods, are shown below:

```
RISKMGR_PERL:description:Tivoli Risk Manager Perl Support 3.7:RISKMGR_PERL
RISKMGR_PERL:revision:3.7
RISKMGR_PERL:lcf_allow
.................
RISKMGR_PERL:patch_id:RISKMGR_PERL
RISKMGR_PERL:depends:TMF_3.6.3
```

Tivoli Management Framework 3.6.3 or higher is needed for the installation.

4.2.2.11 Tivoli Risk Manager Adapter for Cisco Secure IDS 3.7

The Tivoli Risk Manager Adapter for Cisco Secure IDS 3.7 can be installed as a new installation. The significant parts of the *.IND files, in terms of prerequisites, dependencies, and installation methods, are shown below:

```
RISKMGR_NR:description:Tivoli Risk Manager Adapter for Cisco Secure IDS
3.7:RISKMGR_NR
RISKMGR_NR:revision:3.7
RISKMGR_NR:lcf_allow
.............
RISKMGR_NR:patch_id:RISKMGR_NR
RISKMGR_NR:depends:TMF_3.6.4
```

Tivoli Management Framework 3.6.4 is needed for the installation.

4.2.2.12 Tivoli Risk Manager Web IDS 3.7

The Tivoli Risk Manager Web Intrusion Detection System 3.7 can be installed as a new installation. The significant parts of the *.IND files, in terms of prerequisites, dependencies, and installation methods, are shown below:

```
RISKMGR_WEB:description:Tivoli Risk Manager Web Intrusion Detection System
3.7:RISKMGR_WEB
RISKMGR_WEB:revision:3.7
RISKMGR_WEB:lcf_allow
.................
RISKMGR_WEB:patch_id:RISKMGR_WEB
RISKMGR_WEB:depends:TMF_3.6.4
```

Tivoli Management Framework 3.6.4 is needed for the installation.

4.2.2.13 Tivoli Enterprise Console Java Console 3.7

The TEC Java Console 3.7 can be installed via the Tivoli Desktop install products mechanism, via SIS or as a non-TME application. We are using the SIS method in our approach.

For the SIS install method, the file Console.IND includes the following contents:

```
TEC_JCONSOLE:description:Tivoli Enterprise Console Console 3.7:TEC_JCONSOLE
....
TEC_JCONSOLE:patch_id:TEC_JCONSOLE
TEC_JCONSOLE:patch_id:TEC_JCONSOLE_3.7.0
TEC_JCONSOLE:depends:TMF_3.6.3
```

4.2.2.14 TEC Server patch 3.7-0001E

Perform an installation of TEC Patch 3.7-0001E (370TEC01.IND) as follows:

```
3.7-TEC-0001E:description:Tivoli Enterprise Console Server Patch
3.7-TEC-0001E (Early Release):3.7-TEC-0001E
3.7-TEC-0001E:patch_for:TEC_SERVER
............................
3.7-TEC-0001E:patch_id:3.7-TEC-0001E
3.7-TEC-0001E:depends:TEC_SERVER_3.7.0
```

Tivoli Enterprise Console Server 3.7 is needed for the installation.

4.2.2.15 TEC Server patch 3.7-0004

Perform an installation of TEC Patch 3.7-0004 (370SVR04.IND) as follows:

```
3.7-TEC-0004:description:Tivoli Enterprise Console Server Patch
3.7-TEC-0004:3.7-TEC-0004
3.7-TEC-0004:patch_for:TEC_SERVER
..........
3.7-TEC-0004:patch_id:3.7-TEC-0004
3.7-TEC-0004:patch_id:3.7-TEC-0001E
3.7-TEC-0004:patch_id:3.7-TEC-0002
3.7-TEC-0004:depends:TEC_SERVER_3.7.0
```

Tivoli Enterprise Console Server 3.7 is needed for the installation.

4.2.2.16 TEC User Interface Server patch 3.7-0004

Perform an installation of TEC Patch 3.7-0004 (370UIS04.IND) as follows:

```
3.7.0-TEC-UIS-0004:description:Tivoli Enterprise Console User Interface
Server Patch 4:3.7.0-TEC-UIS-0004
3.7.0-TEC-UIS-0004:patch_for:TEC_UI_SRVR
3.7.0-TEC-UIS-0004:revision:3.7
...........
3.7.0-TEC-UIS-0004:patch_id:3.7.0-TEC-UIS-0004
3.7.0-TEC-UIS-0004:patch_id:TEC_UI_SRVR_3.7
3.7.0-TEC-UIS-0004:depends:TMF_3.6.3
```

Tivoli Enterprise Management Framework 3.7 is needed for the installation.

4.2.2.17 TEC ACF patch 3.7-0004

Perform an installation of TEC Patch 3.7-0004 (370ACF04.IND) as follows:

```
3.7-TEC_ACF-0004:description:Tivoli Enterprise Console ACF Patch
3.7-TEC-0004:3.7-TEC_ACF-0004
3.7-TEC_ACF-0004:patch_for:ACF
...........
3.7-TEC_ACF-0004:patch_id:3.7-TEC_ACF-0004
3.7-TEC_ACF-0004:depends:ACF_3.7.0
```

Adapter Configuration Facility 3.7 is needed for the installation.

4.2.2.18 TEC Console patch 3.7-0004

Perform an installation of TEC Patch 3.7-0004 (370CON04.IND) as follows:

```
3.7-TEC-0004E:description:Tivoli Enterprise Console Patch 3.7-TEC-0004
(Early Release):3.7-TEC-0004E
3.7-TEC-0004E:patch_for:TEC_JCONSOLE
.............
3.7-TEC-0004E:patch_id:3.7-TEC-0004E
3.7-TEC-0004E:depends:TEC_JCONSOLE_3.7.0
```

Tivoli Enterprise Console 3.7 is needed for the installation.

4.2.2.19 Tivoli SIS Depot patch

Perform an installation of SIS Depot Patch 3.7 (SISDEPOT.IND) as follows:

```
3.7-SISDEPOT-0002:description:Tivoli Software Installation Service Depot
3.7 Patch (3.7-SISDEPOT-0002) :3.7-SISDEPOT-0002
3.7-SISDEPOT-0002:patch_for:SISDepot
............
3.7-SISDEPOT-0002:patch_id:3.7-SISDEPOT-0002
3.7-SISDEPOT-0002:depends:SISDepot
```

SIS Depot 3.7 is needed for the installation.

4.2.2.20 Tivoli SIS Client patch

Perform an installation of SIS Client Patch 3.7 (SISCLNT.IND) as follows:

```
3.7-SISCLNT-0002:description:Tivoli Software Installation Service Client
3.7 Patch (3.7-SISCLNT-0002) :3.7-SISCLNT-0002
3.7-SISCLNT-0002:patch_for:SISCLNT
.............
3.7-SISCLNT-0002:patch_id:3.7-SISCLNT-0002
3.7-SISCLNT-0002:depends:SISCLNT
```

SIS Client 3.7 is needed for the installation.

4.3 Test environment

This section gives a summary of the environment that was built and used to obtain the information in this redbook. One Tivoli Management Region has been set up. All installed Tivoli products are listed. In addition, a topological overview in terms of connectivity and installed software is given.

4.3.1 Tivoli Management Region

All of the tested hardware and software components are part of one single TMR.

4.3.2 Topological overview

Figure 11 on page 61 shows an overview of the topology with respect to the TMR Server, Gateway, Endpoint and Risk Manager infrastructure.

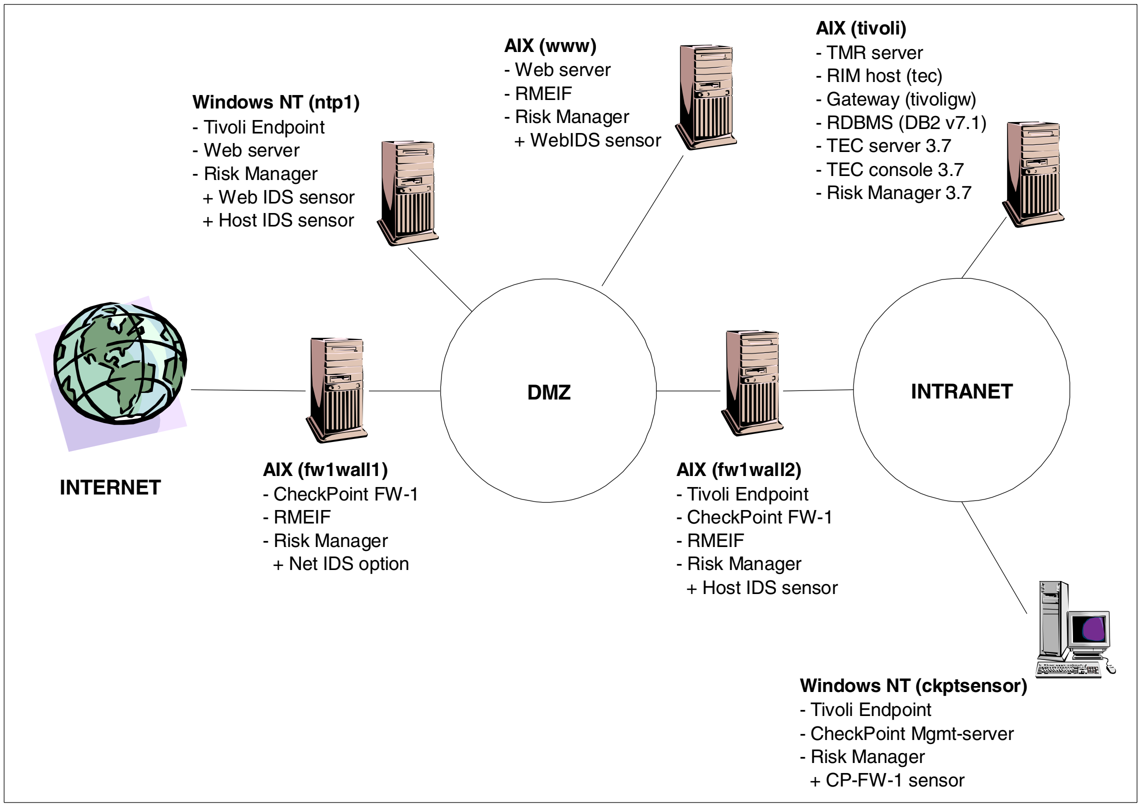


Figure 11. Basic topology of the test environment

The test environment includes the following components, either installed on separate machines or in combination of some kind:

- TMR Server
- TEC Server
- TEC Console
- Risk Manager Server
- Gateway
- RIM Host
- RDBMS server

Several endpoints and Risk Manager sensors and adapters are connected to these components. They will be used as target systems in order to create events for the Risk Manager server.

4.3.3 TMR server setup

The central machine in our TMR is set up as shown in Table 2. The following information is listed:

- Role(s) within the Tivoli environment
- System configuration
- Tivoli products and patches installed

Table 2. TMR Server configuration information

Host name	**tivoli.internal.itsorisc.com**
Roles within Tivoli	TMR Server Endpoint Manager Gateway (tivoli.gw) RIM Host (tec) TEC Server TEC Console Risk Manager Server SIS Depot Installation Repository (/ir) SIS Client RDBMS
System information ip-address: Operating system:	 10.30.30.2 AIX 4.3.3 (aix4-r1) IBM RS/6000

Host name	tivoli.internal.itsorisc.com
Products and patches installed	Tivoli Management Framework 3.6 TMF Maintenance release 3.6.4 Java for Tivoli 3.7 Tivoli Java Client Framework 3.7 Tivoli Software Installation Service Depot 3.7, Patch 3.7-SISDEPOT-0002 Tivoli Software Installation Service Client 3.7, Patch 3.7-SISCLNT-0002 Tivoli Enterprise Console ACF 3.7 TEC ACF 3.7 Patch 3.7-TEC-004 Tivoli Enterprise Console Server 3.7 TEC Server 3.7 Patch 3.7-TEC-004 TEC Using Interface Server 3.7 TEC UIS 3.7 Patch 4 Tivoli Enterprise Console 3.7 TEC Console 3.7 Patch 3.7-TEC-004 Tivoli Enterprise Console EIF 3.7 TEC Sample Event Information3.7 Tivoli SW Risk Manager Server 3.7 Tivoli SW Risk Manager EIF 3.7 Tivoli SW Risk Manager Perl Support 3.7 DB2 7.1

4.3.3.1 Tivoli Framework basic customization

In this section the basic Tivoli Framework customization, that later scenarios are based on, is port usage.

For all installations, the default ports have been used (see Table 3).

Table 3. Port usage

Tivoli role	Port
TMR Server (oserv)	94
Gateway	9494
Endpoints	9495

4.3.4 Tivoli endpoint setup

We are using two different approaches in utilizing the Risk Manager integration of event sensors. One is based on having a Tivoli Endpoint distributed to the system and therefore making it an active part of the TMR with all other benefits and side effects. The second option is to not deploy Tivoli Endpoints to these systems.

An example setup of an endpoint based system would look similar to the details specified in the Table 4.

Table 4. Endpoint configuration information

Host name	**rmnt37.internal.itsorisc.com**
Roles within Tivoli	Endpoint RM Sensor (TEC adapter)
System information: ip-address: Operating system:	 10.30.30.9 Windows NT 4.0 Server SP 5/6 IBM PC Netfinity 3000
Products and patches installed:	Tivoli Management Agent endpoint software (formerly LCF endpoint) Version 3.6.4 Risk Manager Web Intrusion Detection System installation package Tivoli Risk Manager Perl Support 3.7 Risk Manager Event Integration Facility 3.7

This concludes the details on the Tivoli Framework prerequisites for the Risk Manager 3.7 installation, configuration, and sensor deployments.

Part 3. Deploying an e-business Risk Management solution

Chapter 5. Deploying Tivoli Risk Manager

Based on the topology described in Section 4.3, “Test environment” on page 60, we will install and set up a centralized Tivoli Risk Manager solution. We provide you with more detailed configuration information for each of the components used in this scenario. Although we will not cover all of Risk Manager’s single items and capabilities, you will be able to understand all of the following steps involved in setting up this scenario:

- Planning for deploying Risk Manager components
- Configuration of the features used
- Using the centralized correlation engine
- Developing your own Risk Manager sensor

5.1 Implementation overview

In the following sections, we will guide you through the individual components configuration, as depicted in Figure 11 on page 61.

Risk Manager can be an integral part of the Tivoli Framework and therefore follows all rules and concepts defined by this framework. Major advantages of the Risk Management solution are the scalability and extensibility. Therefore, it takes a relatively short time period to learn the product and concepts, and existing Tivoli resources can be used to integrate this product into the existing Tivoli Framework.

The Risk Manager centerpiece, the event correlation engine, is based on the Tivoli Enterprise Console. Tivoli Risk Manager contains the following TEC Event Server components:

- Risk Manager
- TEC correlation rule files
- Prolog files
- Configuration files

Risk Manager collects events from a variety of different sensors and adapters that are supporting a wide range of products, as listed in Section 5.1.1, “Platforms support” on page 68. The machines running those sensors and adapters can also be integrated into the Tivoli Management Framework by installing an endpoint on them. But they can also be integrated into the Risk

Manager event framework without knowing anything about the underlying TMF infrastructure.

This capability gives you a variety of choices on how to best deploy the Risk Manager solution.

5.1.1 Platforms support

The Tivoli Risk Manager management infrastructure (Console, Server, Intermediate Managers, and SNMP/Logfile Adapters) components are available for the following platforms:

- Solaris 2.6 and 2.7
- Windows NT Version 4.0 (workstation and server)
- AIX 4.3.3

Tivoli Risk Manager supports the following sensor/adapter endpoints directly out of the box (with no additional prerequisites, such as Plus Modules):

- Servers
  - Windows NT 4.0
  - Windows 2000
  - AIX 4.3.3
  - Solaris 2.6 and 2.7
- Web servers
  - Apache 1.3
  - Microsoft Internet Information Server 4.0
  - iPlanet Web Server, Enterprise Edition 4.1 (formerly also known as Netscape Enterprise Server 4)
  - Lotus Domino R5 using HTTPD
  - Tivoli Policy Director WebSEAL (since the WebSEAL HTTP engine creates standard Web server log file, it can be directly supported by Risk Manager Web IDS)
- Firewalls
  - CheckPoint FW-1
  - Cisco PIX Firewall 5.1 model 506
- Network Devices
  - Cisco Routers

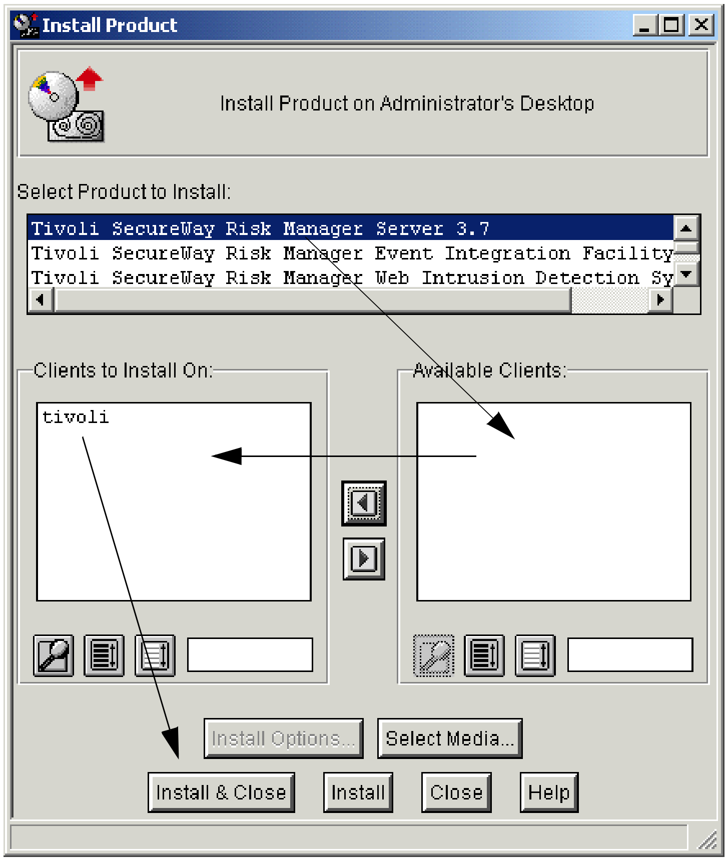
- Intrusion Detection Systems
  - ISS Real Secure 3.2
  - Cisco Secure IDS 2.2.1
- Desktop Security
  - Symantec Norton AntiVirus 7

For an explanation of the Tivoli Risk Manager 3.7 installation pre-requisites, please refer to Section 4.1, “Product installation order” on page 49 and Section 4.2, “Product installation prerequisites” on page 52.

5.2 Installing Tivoli Risk Manager 3.7

In this section, we walk you through the specific steps necessary to get Tivoli Risk Manager up and running in the sample scenario.

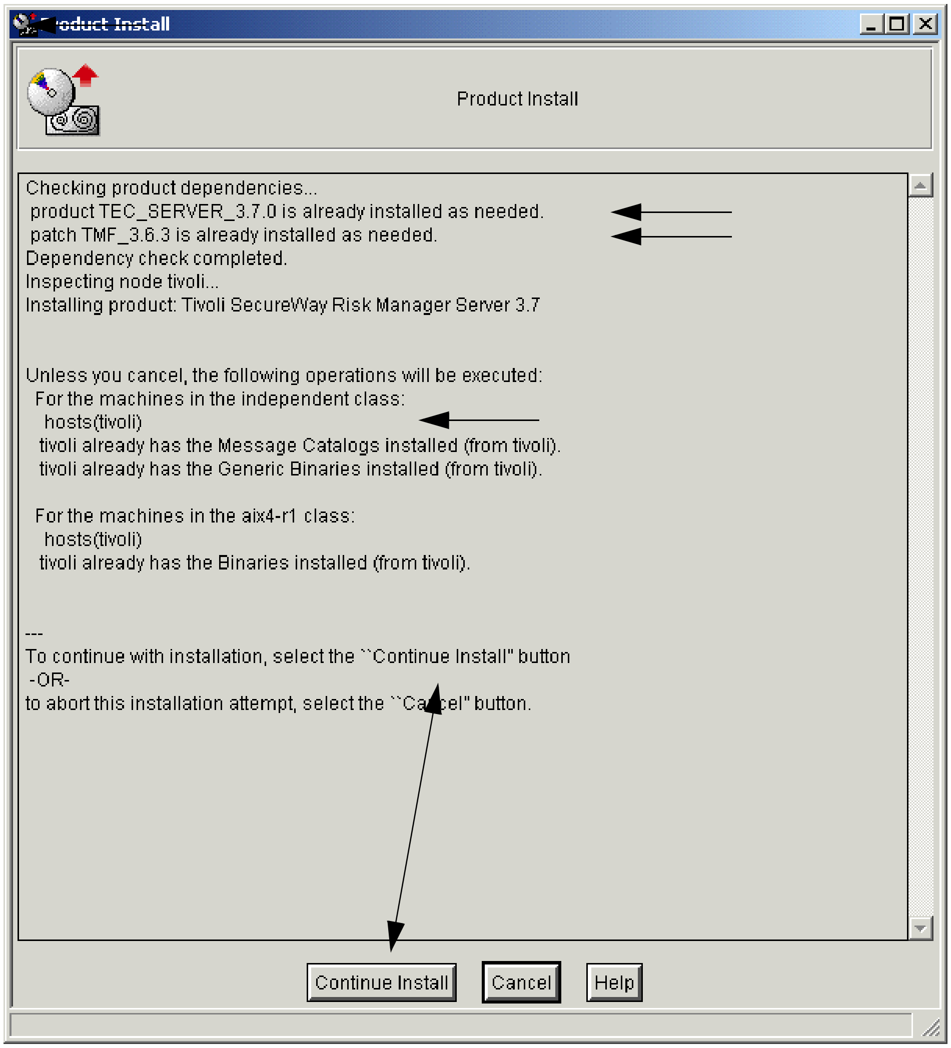
1. On the Tivoli Desktop, open the Install Product panel and select the product Tivoli Risk Manager Server 3.7, as shown in Figure 12 on page 70.


Install Product
Install Product on Administrator's Desktop
Select Product to Install:

Tivoli SecureWay Risk Manager Server 3.7
Tivoli SecureWay Risk Manager Event Integration Facility
Tivoli SecureWay Risk Manager Web Intrusion Detection Sy

Figure 12. Install Product panel

2. Chose the appropriate client from the Client to Install On panel and select Install & Close. This opens the Products Install panel, as shown in Figure 13 on page 71.



```
Checking product dependencies...
 product TEC_SERVER_3.7.0 is already installed as needed.
 patch TMF_3.6.3 is already installed as needed.
Dependency check completed.
Inspecting node tivoli...
Installing product: Tivoli SecureWay Risk Manager Server 3.7


Unless you cancel, the following operations will be executed:
  For the machines in the independent class:
    hosts(tivoli)
   tivoli already has the Message Catalogs installed (from tivoli).
   tivoli already has the Generic Binaries installed (from tivoli).

  For the machines in the aix4-r1 class:
    hosts(tivoli)
   tivoli already has the Binaries installed (from tivoli).


---
To continue with installation, select the ``Continue Install'' button
 -OR-
to abort this installation attempt, select the ``Cancel'' button.
```

Figure 13. Product Install Panel

3. Select Continue Install and Tivoli Risk Manager 3.7 will successfully install.
4. After completion, check the log file on the TMR Server to verify success. By default, this log file is located in /tmp/tivoli.cinstall for UNIX.

Risk Manager provides an installable package that you can use to distribute the following Risk Manager TEC correlation and Tivoli event server components:

- Risk Manager .baroc files

```
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/cpfw.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/crouter_snmp.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/klaxon.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/netranger.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/nids.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/os.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/pix.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/realsecure.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/riskmgr.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/rmvirus.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/sensor_abstract.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/sensor_generic.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/webids.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/root.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/tec.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/riskmgr.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/sensor_abstract.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/sensor_generic.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/klaxon.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/realsecure.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/webids.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/netranger.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/cpfw.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/crouter_snmp.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/os.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/pix.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/rmvirus.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/nids.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/.rbtargets/EventServer/TEC_CLASSES/root.bar
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/realsecure.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/riskmgr.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/rmvirus.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/sensor_abstract.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/sensor_generic.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/webids.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/root.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/tec.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/riskmgr.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/sensor_abstract.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/sensor_generic.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/klaxon.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/realsecure.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/webids.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/netranger.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/cpfw.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/crouter_snmp.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/os.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/pix.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/rmvirus.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_CLASSES/nids.baroc
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/.rbtargets/EventServer/TEC_CLASSES/root.bar
/Tivoli/Tivoli/tivoli.db/tec/rb_dir/TEC_CLASSES/realsecure.baroc
/Tivoli/Tivoli/tivoli.db/tec/rb_dir/TEC_CLASSES/webids.baroc
/Tivoli/Tivoli/tivoli.db/tec/rb_dir/TEC_CLASSES/netranger.baroc
/Tivoli/Tivoli/tivoli.db/tec/rb_dir/TEC_CLASSES/cpfw.baroc
/Tivoli/Tivoli/tivoli.db/tec/rb_dir/TEC_CLASSES/crouter_snmp.baroc
/Tivoli/Tivoli/tivoli.db/tec/rb_dir/TEC_CLASSES/os.baroc
/Tivoli/Tivoli/tivoli.db/tec/rb_dir/TEC_CLASSES/pix.baroc
/Tivoli/Tivoli/tivoli.db/tec/rb_dir/TEC_CLASSES/rmvirus.baroc
/Tivoli/Tivoli/tivoli.db/tec/rb_dir/TEC_CLASSES/nids.baroc
```

- Risk Manager .pro files

```
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/riskmgr_categories.pro
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/riskmgr_hosts.pro
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/riskmgr_links.pro
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/riskmgr_parameters.pro
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/riskmgr_thresholds.pro
```

- Risk Manager .rls files

```
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/boot.rls
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/normalization.rls
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/sensorevent.rls
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/situation.rls
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/timer.rls
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_RULES/normalization.rls
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_RULES/sensorevent.rls
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_RULES/situation.rls
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_RULES/timer.rls
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_RULES/boot.rls
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_RULES/tec_r.normalization.rls
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_RULES/tec_r.sensorevent.rls
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_RULES/tec_r.situation.rls
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_RULES/tec_r.timer.rls
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec/TEC_RULES/tec_r.boot.rls
/Tivoli/bin/aix4-r1/TME/TEC/contrib/rules/security/security_default.rls
/Tivoli/bin/aix4-r1/TME/TEC/default_rb/.rbtargets/EventServer/TEC_RULES/from_sem.rls
/Tivoli/bin/aix4-r1/TME/TEC/default_rb/.rbtargets/EventServer/TEC_RULES/log_default.
rls
/Tivoli/bin/aix4-r1/TME/TEC/default_rb/.rbtargets/EventServer/TEC_RULES/ov_defaul.rl
s
```

- Risk Manager .fmt files

```
/Tivoli/bin/aix4-r1/RISKMGR/adapters/etc/webids.fmt
/Tivoli/bin/generic_unix/RISKMGR/ACF_REP/netranger.fmt
/Tivoli/bin/generic_unix/RISKMGR/ACF_REP/os_aix.fmt
/Tivoli/bin/generic_unix/RISKMGR/ACF_REP/os_nt.fmt
/Tivoli/bin/generic_unix/RISKMGR/ACF_REP/os_solaris.fmt
/Tivoli/bin/generic_unix/RISKMGR/ACF_REP/pix.fmt
/Tivoli/bin/generic_unix/RISKMGR/ACF_REP/pix_nt.fmt
/Tivoli/bin/generic_unix/RISKMGR/ACF_REP/rmnav.fmt
/Tivoli/bin/generic_unix/RISKMGR/ACF_REP/webids.fmt
/Tivoli/bin/generic_unix/RISKMGR/ACF_REP/webids.nt.fmt
```

- Risk Manager .cds and .oid files

```
/Tivoli/bin/generic_unix/RISKMGR/ACF_REP/tecad_snmp.cds
/Tivoli/bin/generic_unix/TME/ACF_REP/tecad_snmp.cds
/Tivoli/tecad/etc/tecad_logfile.cds
/Tivoli/bin/generic_unix/RISKMGR/ACF_REP/tecad_snmp.oid
/Tivoli/bin/generic_unix/TME/ACF_REP/tecad_snmp.oid
```

- Risk Manager configuration files

```
/Tivoli/bin/aix4-r1/RISKMGR/adapters/etc/webids.cfg
/Tivoli/bin/generic_unix/RISKMGR/ACF_REP/webids.cfg
```

5.2.1 Risk Manager task library

Before or after installing the Tivoli Risk Manager Server 3.7 installation package on an AIX or Solaris TEC event server, make sure that the cpp program is installed. The cpp program is used when creating the task library for Risk Manager when the post-installation script file calls the TEC `wtll` command. The `cpp` command must be installed at the following location (or supply a softlink):

```
/usr/ccs/lib/cpp
```

The directory in which the `cpp` command resides can also be added to the systems PATH environment variable.

```
# ls -l /usr/ccs/lib/cpp
-r-xr-xr-x   1 bin      bin       516962 Aug 26 1998  cpp
```

In rare situations, the Tivoli Management Framework commands to create the Tasks for Enterprise Risk Management item in the TEC-Region policy region might fail.

If the task library is not created, or is created but does not contain the full set of Risk Manager tasks, run the following command to create the task library manually:

```
wtll -r -p TEC-Region -P $CPP_LOCATION $BINDIR
/RISKMGR/corr/tasks/rmt_tasks.tll -P
```

In our scenario, we would use the following commands:

```
# cp /cdrom/patch/rmt_tasks.tll
/Tivoli/bin/aix4-r1/RISKMGR/corr/tasks
# ls *.tll
# rmt_tasks.tll
# cd /Tivoli/bin/aix4-r1/bin/wtll
# cd /Tivoli/bin/aix4-r1/bin/
# wtll -r -p TEC-Region -P  /usr/ccs/lib/cpp
/Tivoli/bin/aix4-r1/RISKMGR/corr/tasks/rmt_tasks.tll -P
```

5.2.2 Running the TEC correlation script file

Run the TEC correlation script file called rmcorr_cfg in order for Risk Manager to configure the Tivoli event server to accept, correlate, and display Risk Manager events.

Note

Do not change the rule set provided with Risk Manager. To install the Risk Manager correlation rule base, run the rmcorr_cfg program.

To create a new rule base, run the following command:

```
rmcorr_cfg -install -dir directory -new new_rulebase
```

where:

directory Specifies the directory where you want to place the new rule base files.

new_rulebase The name of the newly created rule base.

In our example, we execute the following:

```
# cd /Tivoli/bin/aix4-r1/RISKMGR/corr
# ./rmcorr_cfg.sh - install $BINDIR/RISKMGR/corr/tec -new RM37RB.
```

To obtain the currently active rule base, run:

```
# wlscurrb
The currently used rule base was loaded from the
rule base named 'RM37RB'.
```

To verify the complete status of the Risk Manager components, the output created by the `rmcorr_cfg -status` command will look similar to the following:

```
# ./rmcorr_cfg -status
rmcorr_cfg:Info:---------------------------------------------
rmcorr_cfg:Info:Checking Status of Risk Manager Components...
rmcorr_cfg:Info:---------------------------------------------
rmcorr_cfg:Info:The Tivoli Enterprise Console Server is running.
rmcorr_cfg:Info:TMR Host: tivoli
rmcorr_cfg:Info:TMR install dir: /Tivoli/bin/aix4-r1
rmcorr_cfg:Info:Region name: tivoli-region
rmcorr_cfg:Info:Risk Mgr install dir: /Tivoli/bin/aix4-r1/RISKMGR/corr
rmcorr_cfg:Info:Current rulebase: RM37RB
rmcorr_cfg:Info: Current rulebase path:
/Tivoli/bin/aix4-r1/RISKMGR/corr/tec
rmcorr_cfg:Info:Event cache size: 1000
rmcorr_cfg:Info:Class RM_SensorEvent is defined
rmcorr_cfg:Info:Event source RISKMGR is defined
rmcorr_cfg:Info:Rules files in rulebase:
Rule Set files
normalization.rls
sensorevent.rls
situation.rls
timer.rls
boot.rls
```

5.2.2.1 Risk Manager BAROC files

In order to verify that the Risk Manager BAROC files are correctly compiled into the rule base, you have to use the `wlsrbclass -hostname` command:

```
# wlsrbclass RM37RB
```

```
..........
NIDS_SCAN
NIDS_CONFIG
NIDS_AUTH
NIDS_BACKDOOR
NIDS_STEALTH
NIDS_GOPHER
NIDS_Loki
NIDS_TFTP_PW_File
NIDS_WWW_Shell
NIDS_IntelBuffOverflow
NIDS_RS6KBuffOverflow
NIDS_SparcBuffOverflow
NIDS_SendMailPipeBug1
NIDS_SendMailPipeBug2
NIDS_SendMailPipeBug3
NIDS_DefaultUserLogin
```

The above command will list all classes in the rule base.

The different classes for various Risk Manager components can be identified by the starting strings shown in Table 5.

Table 5. Description of classes in the rule base

Risk Manager components	Beginning strings
Web IDS	WW_
RealSecure	RS_
Secure IDS	NR_
CheckPoint	CPFW_
Norton Antivirus	RMV_
Cisco Router	CR_
Host IDS	OS_
Cisco PIX	PIX_
Network IDS	NIDS_

5.2.2.2 Risk Manager rules files

In order to verify that the Risk Manager rules files are correctly compiled into the rule base, you have to use the `wlsrbrules -hostname` command:

```
# wlsrbrules RM37RB
Rule Set files
```

```
--------------
normalization.rls
sensorevent.rls
situation.rls
timer.rls
boot.rls
```

5.2.3 TEC console configuration

In this section, we cover different aspects of configuring the TEC console for Windows NT to the specific needs of the Risk Manager administrator or security officer.

We create Risk Manager event groups and the associated filters that we use when we define a new Risk Manager specific TEC console.

We also take a closer look at verifying the functionality of our installation by sending and receiving basic events, checking the available RDBMS database space, handling TEC errors, and debugging TEC correlation.

5.2.3.1 Create TEC Console event groups and filters

To create the TEC Console event groups and filters, follow these steps:

1. Start the TEC Console 3.7, as shown in Figure 14 on page 78.

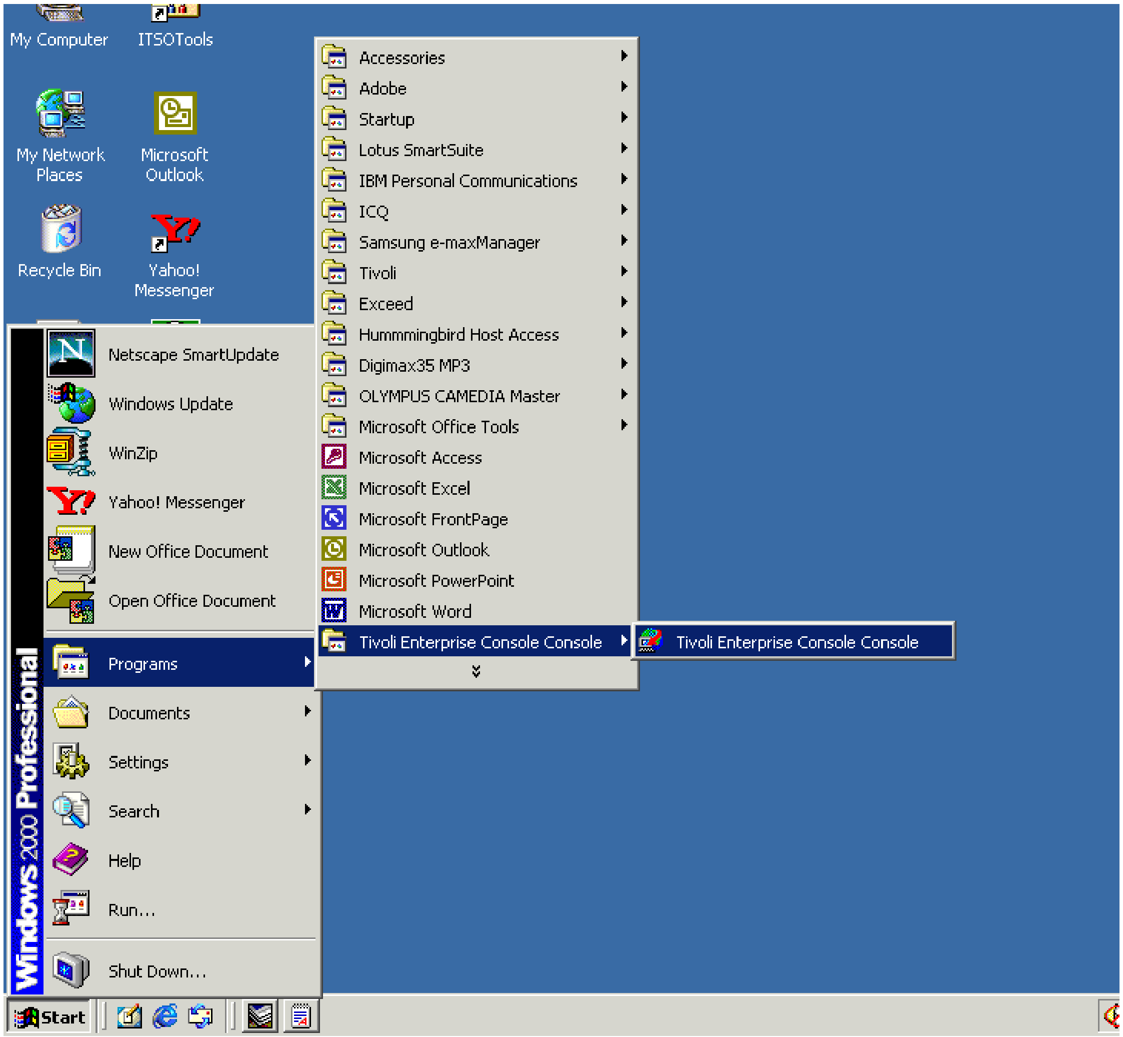
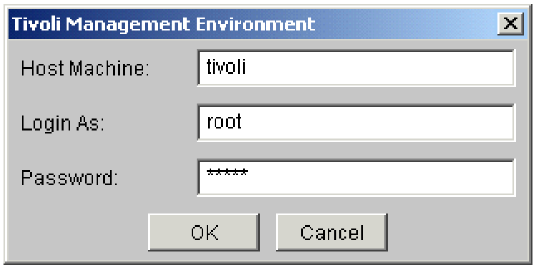


Figure 14. TEC Console 3.7 start from the user's workstation

The Tivoli Management Environment login panel is displayed, as shown in Figure 15 on page 79.



Host Machine: tivoli

Login As: root

Password: *****

Figure 15. Java Console login panel

2. Enter the host name of the appropriate Managed Node, your Tivoli Administrator ID and password, and press OK.

   The Tivoli Enterprise Console panel will be launched, as shown in Figure 16.

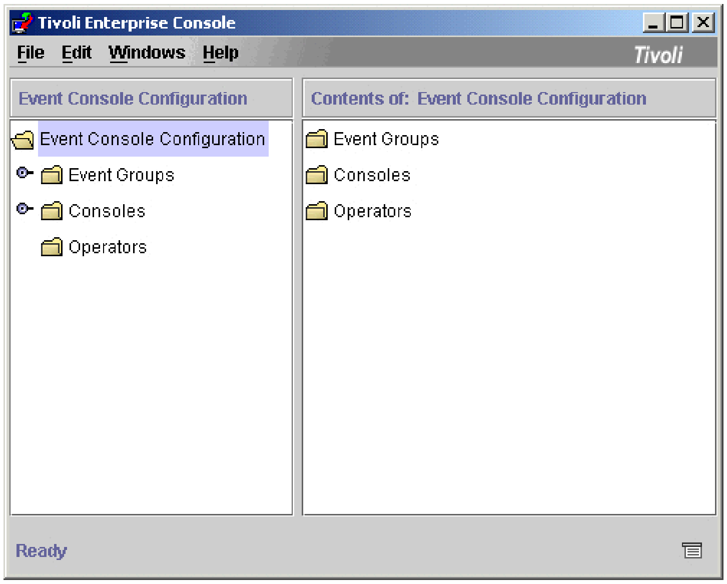

Tivoli Enterprise Console
File
Edit
Windows
Help
Tivoli
Event Console Configuration
Event Console Configuration
Event Groups
Consoles
Operators
Contents of: Event Console Configuration
Event Groups
Consoles
Operators
Ready

Figure 16. Enterprise Console panels for a TEC Console operator

3. Create Risk Manager event groups and associated filters for the TEC console. From the Configuration panel, select **File -> Import**, as shown in Figure 17 on page 80.

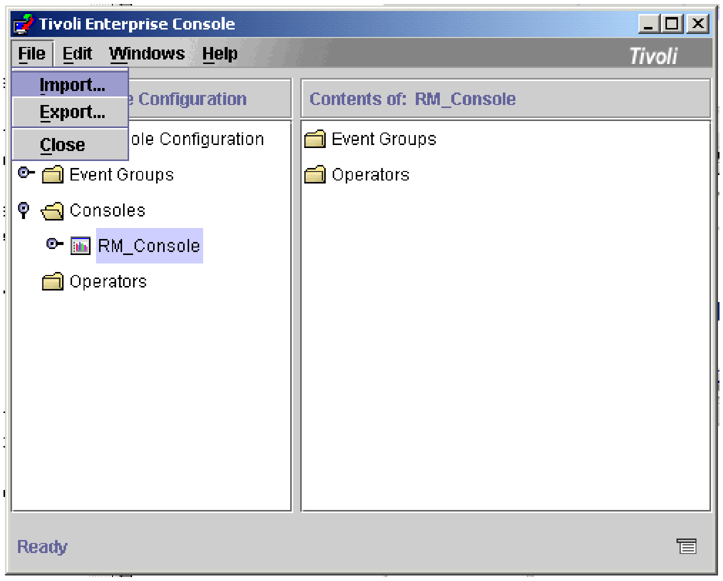


Figure 17. Import from the Configuration panel

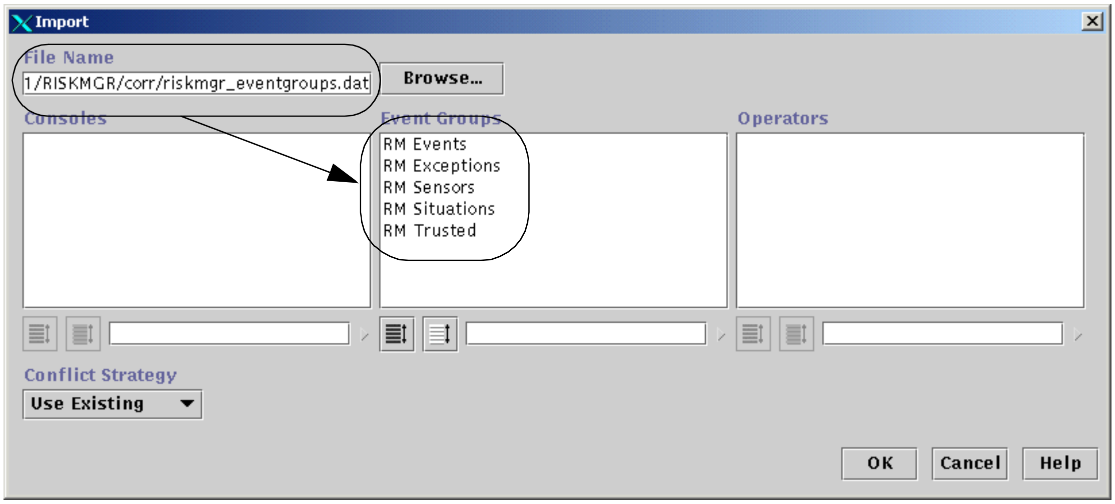
4. The Import panel will then be displayed. Use the Browse button to select the riskmgr_eventgroups.dat file that is located on the TEC server at the following operating system specific locations:

   Windows NT *%BINDIR%*\RISKMGR\corr

   UNIX *$BINDIR*\RISKMGR\corr

   Where BINDIR is the directory where the event server binaries are located.

   This will display a panel similar to the one in Figure 18 on page 81.


Import

File Name

1/RISKMGR/corr/riskmgr_eventgroups.dat

Event Groups

RM Events
RM Exceptions
RM Sensors
RM Situations
RM Trusted

Conflict Strategy

Use Existing

Figure 18. Import panel

5. Select all of the five event groups that are displayed in the Event Groups panel:
   - RM Events
   - RM Exceptions
   - RM Sensor
   - RM Situations
   - RM Trusted
6. Select the desired option for Conflict Strategy, as shown in Figure 19 on page 82. Selecting the Change Names option is safest, because it renames the groups (if they already exist).

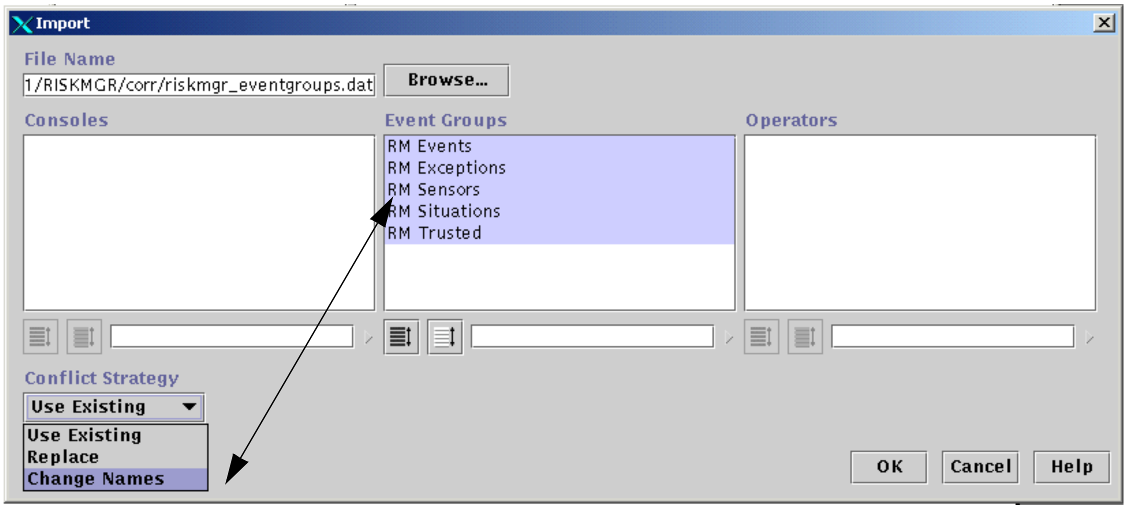
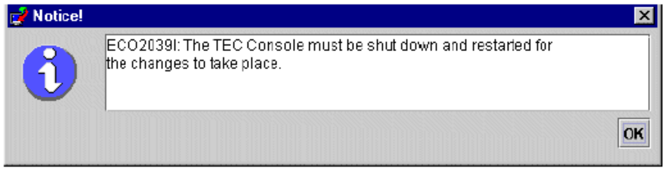


Figure 19. Selecting the desired option for Conflict Strategy

7. Click on OK and the Notice panel will be displayed, as shown in Figure 20.



ECO2039I: The TEC Console must be shut down and restarted for the changes to take place.

Figure 20. Notice panels

8. Press the OK button in the Notice panel. This will return you to the main Configuration panel and restart the TEC Console.

5.2.3.2 Create new TEC console

In order to create a new TEC console, follow these steps:

1. From the Configuration panel, select the TEC Console option by clicking the left mouse button. Now press the right mouse button and select the Create Console option, as shown in Figure 21 on page 83.

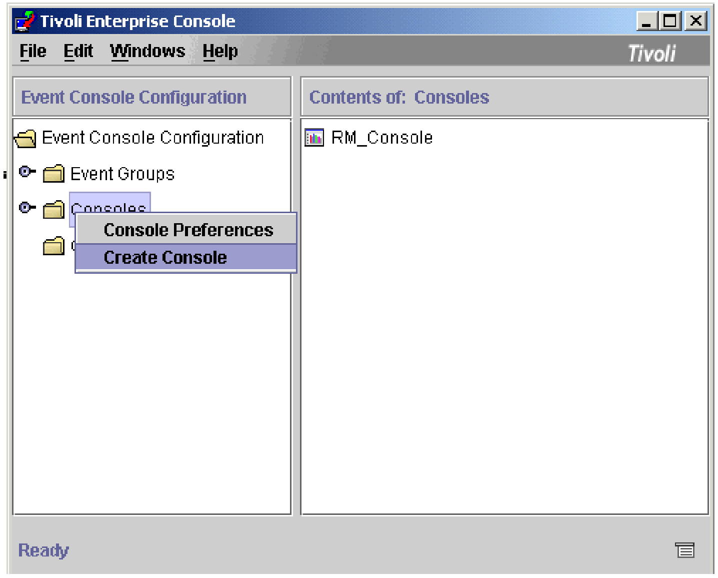
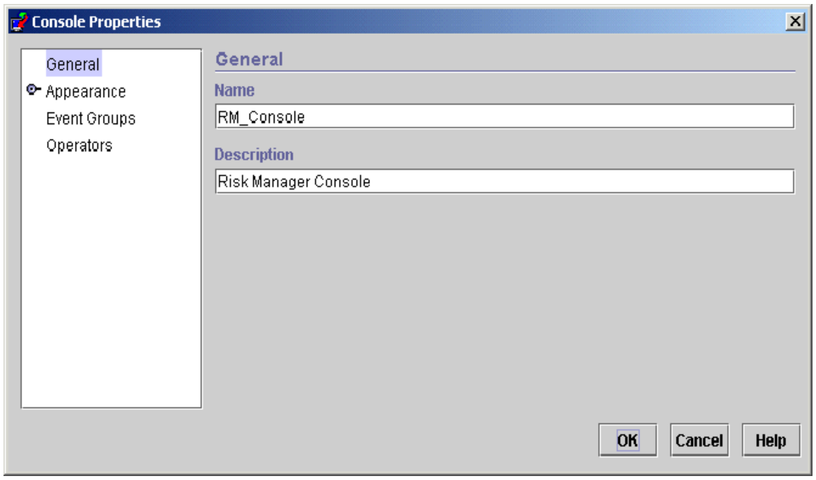


Figure 21. Selecting the Create Console option

2. The Console Properties dialog will be displayed next. Enter the name of the new TEC Console and a brief description of the purpose of the TEC Console definition, as depicted In Figure 22.

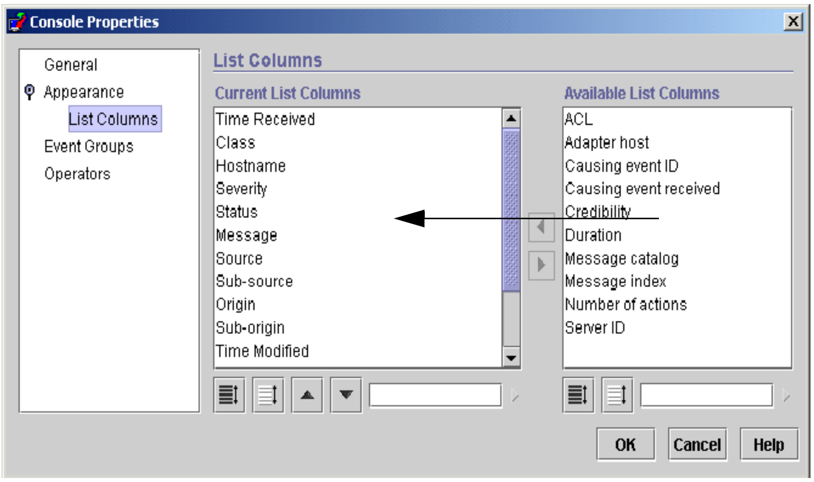


Name: RM_Console

Description: Risk Manager Console

Figure 22. Create Console panel

3. To select the columns you want to have displayed on the TEC Console, select the List Columns, a sub-option of Appearance, as shown in Figure 23.



Current List Columns

- Time Received
- Class
- Hostname
- Severity
- Status
- Message
- Source
- Sub-source
- Origin
- Sub-origin
- Time Modified

Available List Columns

- ACL
- Adapter host
- Causing event ID
- Causing event received
- Credibility
- Duration
- Message catalog
- Message index
- Number of actions
- Server ID

Figure 23. Customizing the information that will appear on the console

4. Now select the Event Groups option in the left panel, as shown in Figure 24.

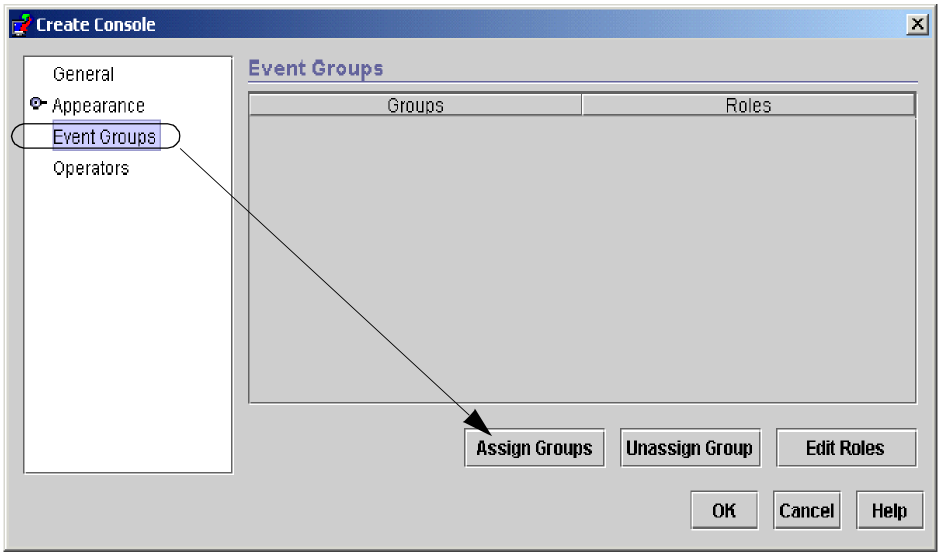
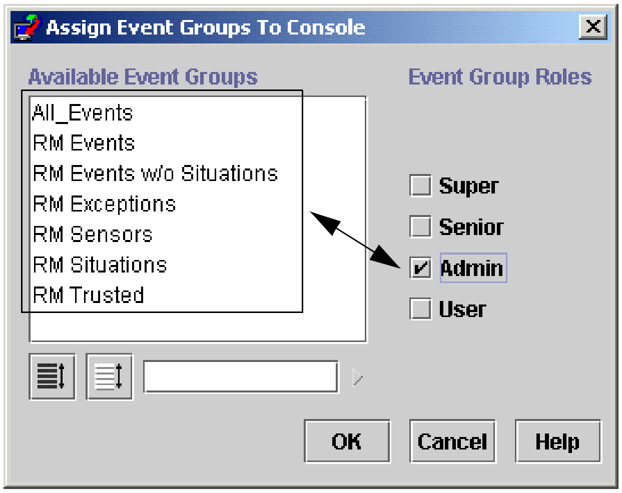


Figure 24. Event Group panel

5. Click on the Assign Groups button to display the Assign Event Groups To Console panel. This panel will display all available Event Groups and the roles than can be assigned to the TEC Console. Figure 25 shows how to assign the Event Group called RM_* with a TEC role of Admin to the TEC Console.



Available Event Groups

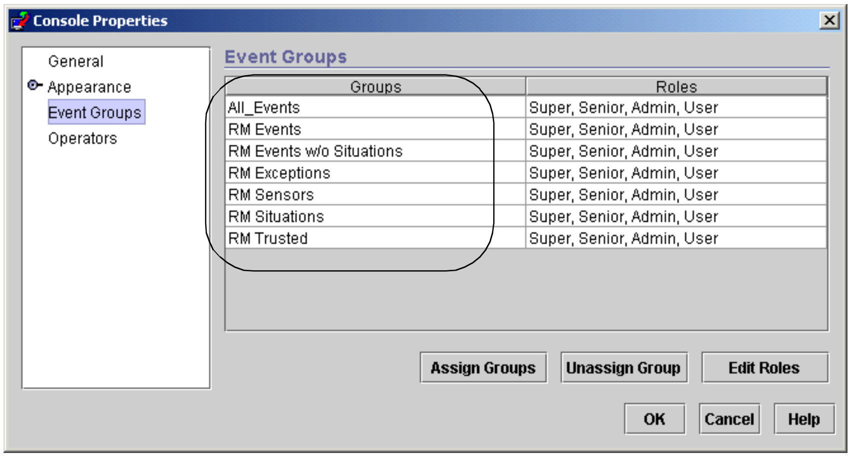
All_Events
RM Events
RM Events w/o Situations
RM Exceptions
RM Sensors
RM Situations
RM Trusted

Event Group Roles

□ Super
□ Senior
☑ Admin
□ User

Figure 25. Assigning the RM_* Event Groups to the RM_Console

6. When you click on the OK button, the panel shown in Figure 26 will be displayed.



Event Groups

Groups	Roles
All_Events	Super, Senior, Admin, User
RM Events	Super, Senior, Admin, User
RM Events w/o Situations	Super, Senior, Admin, User
RM Exceptions	Super, Senior, Admin, User
RM Sensors	Super, Senior, Admin, User
RM Situations	Super, Senior, Admin, User
RM Trusted	Super, Senior, Admin, User

Figure 26. Events Groups currently assigned to a console

Additional Event Groups can be assigned if required by clicking on the **Assign Groups** button again.

7. Finally, select the Operators option in the left view of the Console Properties panel. This will allow you to specify the operators assigned to this Console. Figure 27 depicts how, in this example, we are assigning the Root_tivoli-region operator to the TEC Console.

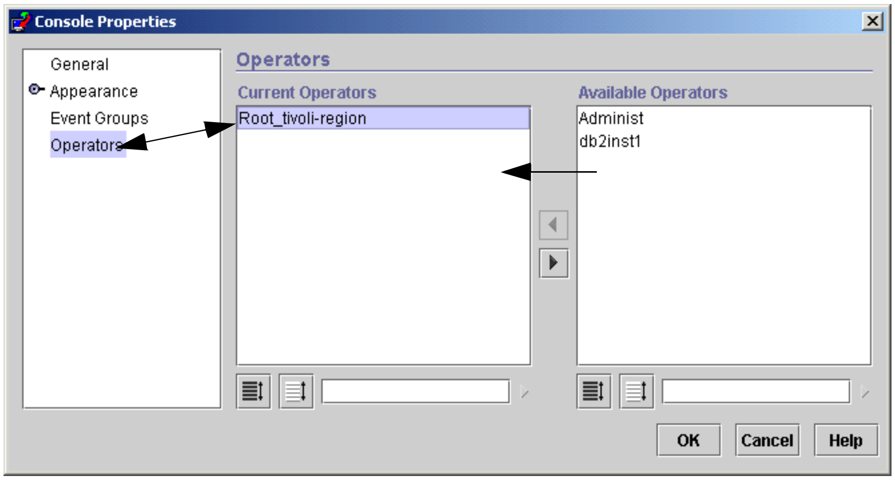


Figure 27. Assigning an operator to the console

8. Before an operator can be created from the Configuration panel, select the Operators option by selecting it with the left mouse button. Now press the right mouse button and the panel will show the Create Operators option, as shown in Figure 28 on page 87.

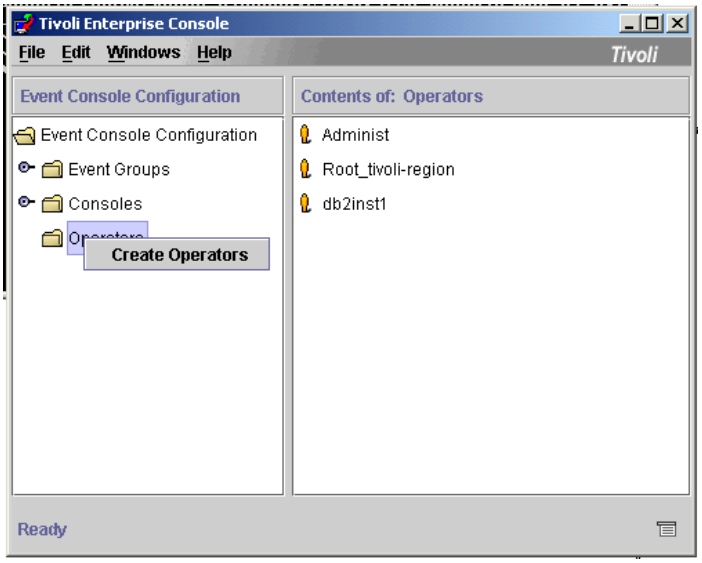


Figure 28. Create the TEC Console Operator

The Create Operator panel is displayed, as shown in Figure 29. The Select Tivoli Administrators panel, on the left part of the panel, is a list of Tivoli Administrators who do not currently have a TEC Console associated with their Tivoli account. The Assign to a Console panel, on the right of the panel, is the list of defined Consoles.

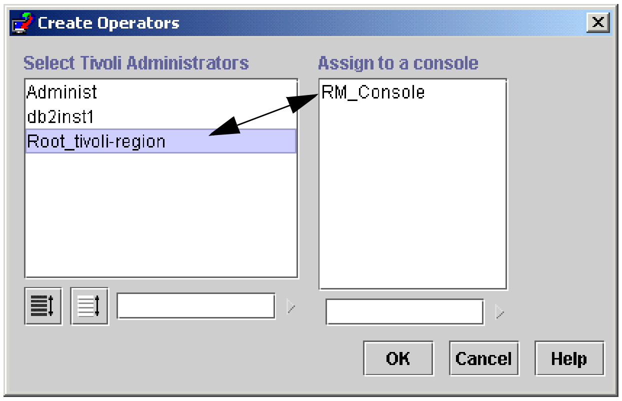


Figure 29. Create Operator panel

Figure 30 on page 88 shows the Configuration panel after creating the TEC operator Root_tivoli-region.

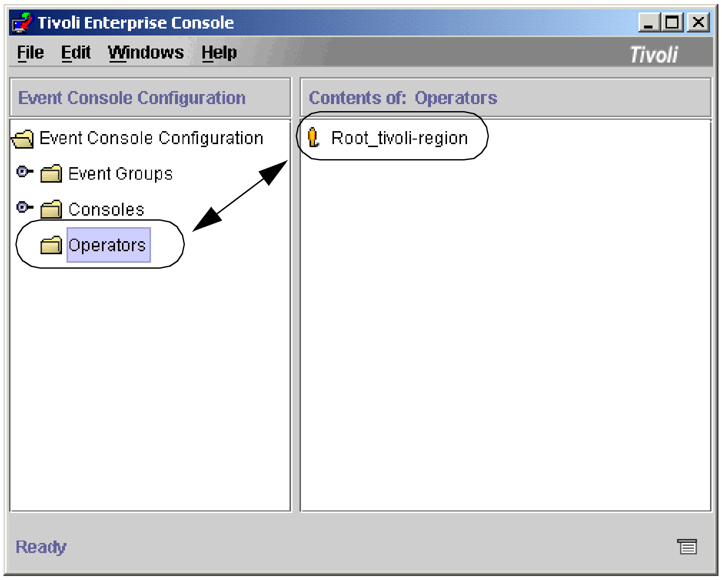


Figure 30. Configuration panel after creating the operator

5.2.3.3 Verify that the TEC event server is working

The `postemsg` command can be used on UNIX or NT to send events to the TEC server. Create a text file called config_file with the following lines (if you are sending to an NT server, uncomment the server port line):

```
ServerLocation=b01yaix.austin.lab.tivoli.com
#ServerPort=5529
```

Run the command:

```
postemsg -f config_file -r WARNING -m This_is_a_test TEC_DB TEC
```

You should see the event arrive at the TEC server by doing a `wtdumprl` on the server console. Note that the `postemsg` command is located in the $BINDIR/bin directory on the server. It is placed on a client when a TEC logfile adapter is installed.

5.2.3.4 Verify event repository

To verify that events are going to the event repository, run:

```
wtdumper -o DESC
```

This command shows events in the event repository in descending order (that is, newer first).

Some sample data from the previous command is:

```
# wtdumper -o DESC
.................
Mar 6 09:49:17~
CONFIG SERVER protocol ERROR Data: HTTP/1.1 403 Forbidden\0d\0aDate: Tue,
06 Mar
 2001 15:49:26 GMT\0d\0aServer: IBM_HTTP_Server/1.3.6.1 Apache/1.3.7-dev
(Unix)\
0d~
N/A~0~
0~0~ES~1~983893131(Mar 06 09:38:51 2001)~1~NIDS_SCAN~
RISKMGR~IDSEVENT~10.20.20.1~NIDS~fw1_sec_net~N/A~CLOSED~
~[ admin]~WARNING~
Mar 6 09:38:52~
SCAN ICMP - Echo Pkt~
N/A~0~
0~0~ES~1~983893082(Mar 06 09:38:02 2001)~1~NIDS_SCAN~
RISKMGR~IDSEVENT~10.20.20.1~NIDS~fw1_sec_net~N/A~CLOSED~
~[ admin]~WARNING~
Mar 6 09:38:03~
SCAN ICMP - Echo Pkt~
```

Watch your database

If the TEC database is full, events will not get written to the event repository. TEC provides a `wtdbspace` command to check the space available in the TEC DB. Since this command is not supported with DB2, we will take a closer look at this issue in the following section.

5.2.3.5 Checking and resizing the DB2 database

When the TEC database is running out of space to store events, it will simply freeze the TEC server. No more incoming events will be stored or displayed on the TEC console. You should set up a mechanism that informs the administrator that the DB2 database running low on space for the TEC database in order to give you ample time to resize or take other actions.

In order to work with the DB2 database, you need to obtain the Tivoli RIM information by using the `wgetrim` command:

```
# wgetrim tec
RIM Host:       tivoli
RDBMS User:     db2inst1
RDBMS Vendor:   DB2
Database ID:    tec
Database Home:  /usr/lpp/db2_07_01
Server ID:      tcpip
Instance Home:  /Tivoli/db2/db2inst1
```

In order to delete all the events in the TEC database, you can use the following TEC commands:

```
# wtdumper -o DESC | grep -c RISKMGR
5430
# wtdbclear -el -t 0
# wtdumper -o DESC | grep -c RISKMGR
0
```

The command `wtdumper` shows the current number of records in the TEC database and the command `wtdbclear` deletes it.

The following steps outline the resizing of the DB2 database, because in most cases, you do not want to just delete your TEC database:

1. Connect to DB2 (TEC database):

   ```
   # su - db2inst1
   $ db2 connect to tec user db2inst1 using tivoli

      Database Connection Information

    Database server        = DB2/6000 7.1.0
    SQL authorization ID   = DB2INST1
    Local database alias   = TEC
   $
   ```

2. Check the available space in the TEC database:

   ```
   $ db2 list tablespaces show detail
   Detailed explanation:-03-05-14.01.14.199893
   Normal2inst1   No
   Total pages                           = 19593200838mp
   PID:25542(db2agent (TEC))
    Usable pages = 1959b2inst1.010303200838t   Probe:830   Database
    Used pages = 19590   Database:TECg   Probe:792   Database:TEC
    Free pages = Not applicable
   High water mark (pages)               =542
   ```

```
 Name = TEMPSPACE1tance:db2inst1   Node:000/db2/db2inst1/sqllib/db2d
 Type = Database managed spacepid:*LOCAL.db2inst1.010303200838mp

2001-03-05-14.01.08.01006
 Contents = System Temporary dataocateExtent   Probe:830
Database:TECdb2agent (TEC))   Appid
 State = 0x0000ablespace 2(USERSPACE1) is fullt={2;14}, EM=r
 High water mark (pages)              = 64
 Page size (bytes)                    = 4096
 Extent size (pages)                  = 32
 Prefetch size (pages)                = 32
 Number of containers                 = 1

Tablespace ID                        = 2
 Name                                 = USERSPACE1
 Type                                 = Database managed space
 Contents                             = Any data
 State                                = 0x0000
   Detailed explanation:
     Normal
 Total pages                          = 25000
 Useable pages                        = 24992
 Used pages                           = 12768
 Free pages                           = 12224
 High water mark (pages)              = 12768
 Page size (bytes)                    = 4096
 Extent size (pages)                  = 32
 Prefetch size (pages)                = 32
 Number of containers                 = 1

$
```

3. Increase the available space in the TEC database:

   ```
   $ db2 alter tablespace userspace1 resize (all 50000)
   ```

For more information on handling DB2, databases refer to the DB2 user's guides.

5.2.3.6 Verify events arriving in TEC

All events received at the TEC event server are recorded in the TEC reception log.

To verify that events are actually getting to the event server, use the following command:

```
wtdumprl -o DESC
```

It shows events in the reception log in descending order (that is, newer first).

Here is some sample data using the `wtdumprl` command:

```
# wtdumprl -o DESC
................
## EVENT ###
NIDS_SCAN;date='Mar 6
09:38:52';hostname=fwall1;rm_SensorHostname=fw1_sec_net;rm
_SensorIPAddr=10.20.20.1;rm_NameData=1060;rm_Timestamp=0x3aa50489;rm_Sourc
eIPAdd
r=9.3.240.16;rm_DestinationIPAddr=10.30.30.1;rm_NameType=CVE;rm_NameID=N/A
;rm_Si
gnature=SCAN;msg='SCAN ICMP - Echo Pkt';END

### END EVENT ###
PROCESSED

1~311~1~983893082(Mar 06 09:38:02 2001)
### EVENT ###
NIDS_SCAN;date='Mar 6
09:38:03';hostname=fwall1;rm_SensorHostname=fw1_sec_net;rm
_SensorIPAddr=10.20.20.1;rm_NameData=1060;rm_Timestamp=0x3aa5045a;rm_Sourc
eIPAdd
r=9.3.240.16;rm_DestinationIPAddr=10.20.20.1;rm_NameType=CVE;rm_NameID=N/A
;rm_Si
gnature=SCAN;msg='SCAN ICMP - Echo Pkt';END
```

5.2.3.7 Handling TEC correlation errors

There are three internal error messages that are provided for TEC correlation. These messages include:

- RM_InputErr

  You receive this error message when there is a problem processing a configuration file or processing an incoming raw event.

  User Response: Evaluate the message for the event or configuration file that is causing the error message to determine and correct the problem.

- RM_SituationErr

  You receive this error message when the application of the correlation algorithm failed on the event.

  User Response: Identify the event from the TME adapter event log message and send this message to the customer support for BAROC files or rules file updates. The message should contain the date and other information that is available about the origin of the internal error.

- RM_PrologErr

  You receive this error message when there is a Prolog failure.

  User Response: When this happens, you must determine which file, which version of the file, or which predicate has caused the failure. This information is available in the event.

  Identify the event from the TME adapter event log message and send this message to the customer support for BAROC files or rules file updates. The message should contain the date and other information that is available about the origin of the internal error.

5.2.3.8 Checking the size of the event cache

In the Tivoli Enterprise Console (TEC) environment, rules are applied to events that are stored in an event cache. When the cache fills up, events are purged or they are no longer processed by the rules. A full event cache affects correlation results, so you have to check the size of the event cache.

To check the size of the TEC event cache, run:

```
# wlsesvrcfg
Time allowed for server initialization: 300 seconds
Maximum number of events buffered in memory: 500 events
Time to keep logged events in reception log: 86400 seconds
Event cache size: 1000 events
Time to keep closed events in cache: 86400 seconds
Time to keep non-closed events: 15552000 seconds
Trace rule execution:  No
Rule trace output file: /tmp/rules.trace
```

The recommended value for the size of the TEC cache is 3000 entries. To change the size of the event cache, run:

```
# wsetesvrcfg -c 3000
```

5.2.3.9 Debugging correlation

If situation alarms are not being generated, first make sure that the Risk Manager rules are incorporated into the currently active rule base. (This is shown in Section 5.2.2.1, “Risk Manager BAROC files” on page 75 and Section 5.2.2.2, “Risk Manager rules files” on page 76.)

To enable tracing on the rule base, you must recompile the rule base with the tracing option. In order to do this, apply the following configuration:

1. On the Tivoli desktop, open the TEC server icon so that the rule bases are depicted as in Figure 31 on page 94.

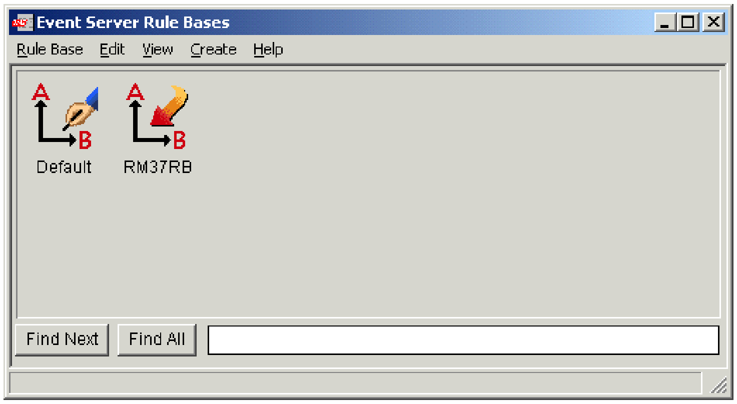


Figure 31. Event Server Rule bases panel

2. Right-click on the rule base for which you want to enable tracing, as shown in Figure 32. Select Compile from the pop-up menu.

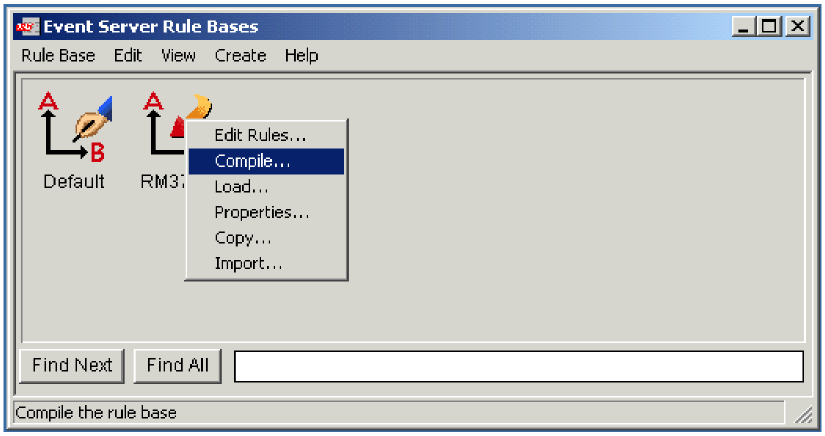


Figure 32. Event Server rule bases panel and drop menu

3. In the following dialog, shown in Figure 33 on page 95, select the Trace check box and click on Compile.

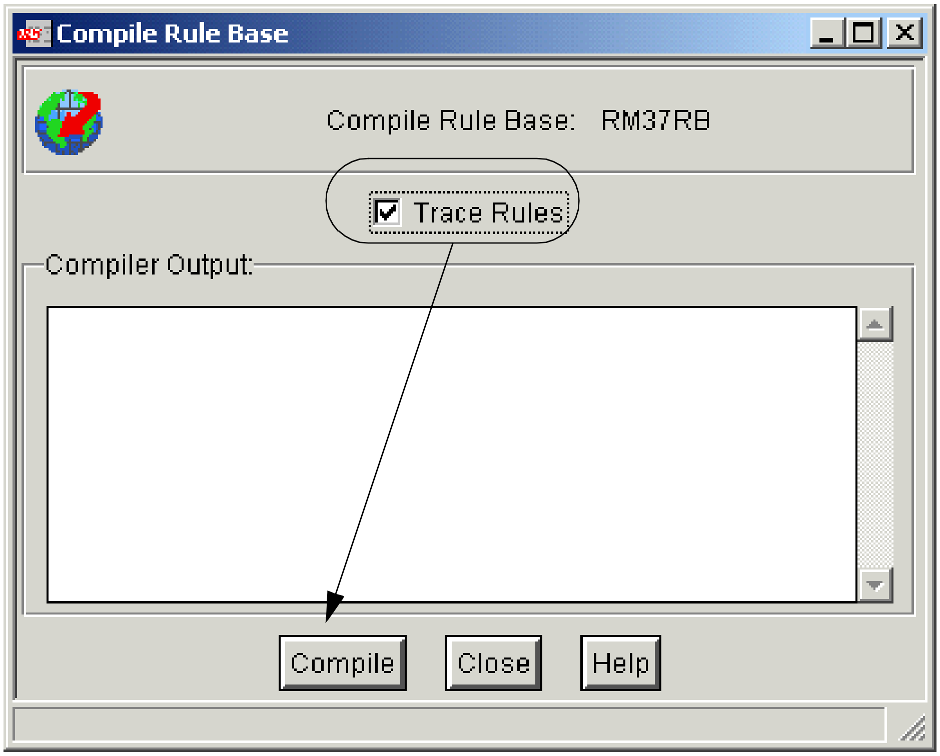


Figure 33. Compile Rule Base dialog

Once finished, close the dialog and close the Event Server Rules Base panel

4. Right-click on the Event Server icon and select Parameters, as shown in Figure 34 on page 96.

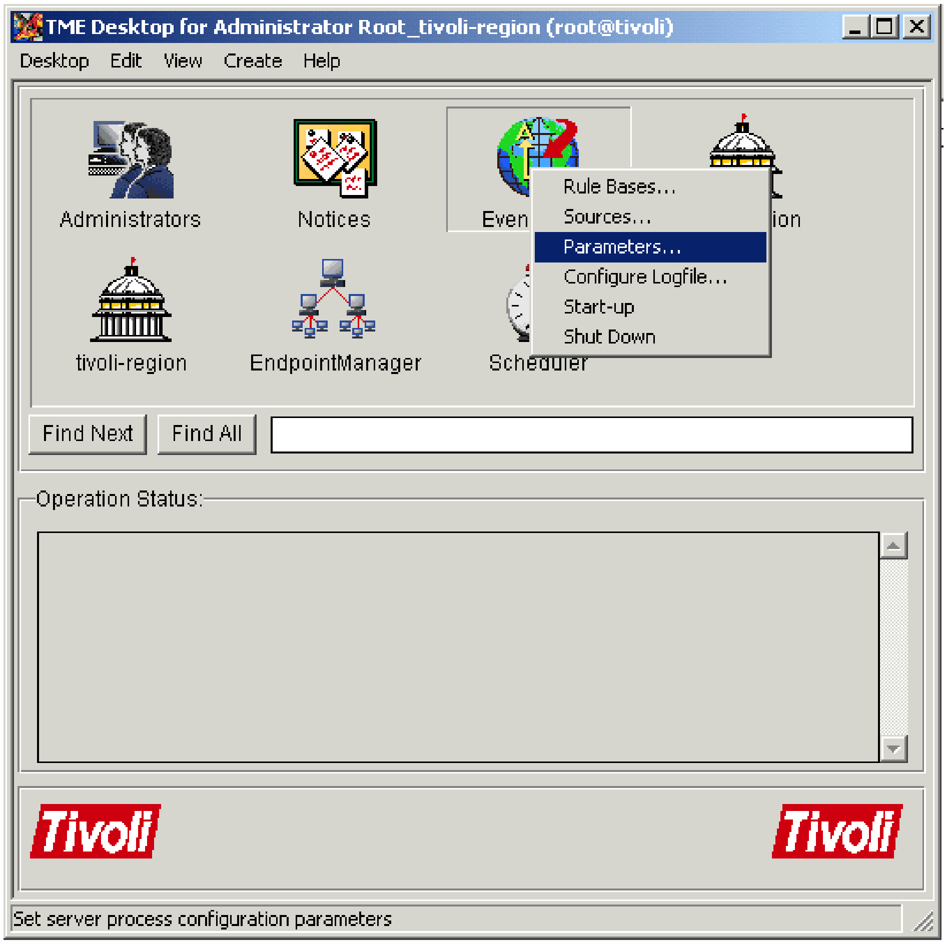
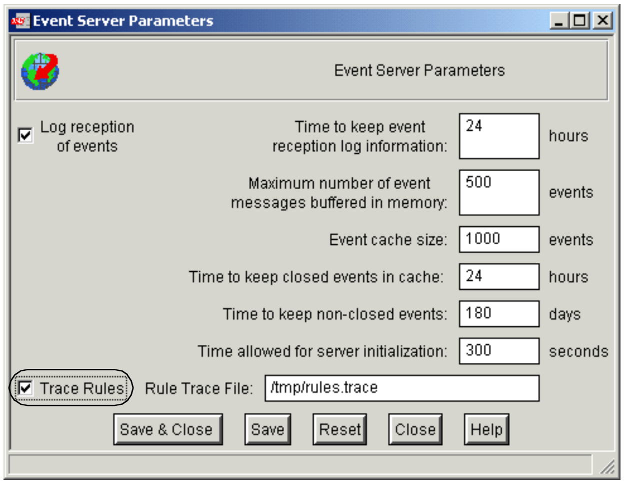


Figure 34. Changing Event Server parameters

5. Figure 35 on page 97 shows you to check the Trace Rules box and fill in a name for the Rule Trace File. The default file name is /tmp/rules.trace.



Event Server Parameters

Event Server Parameters

☑ Log reception of events

Time to keep event reception log information: 24 hours

Maximum number of event messages buffered in memory: 500 events

Event cache size: 1000 events

Time to keep closed events in cache: 24 hours

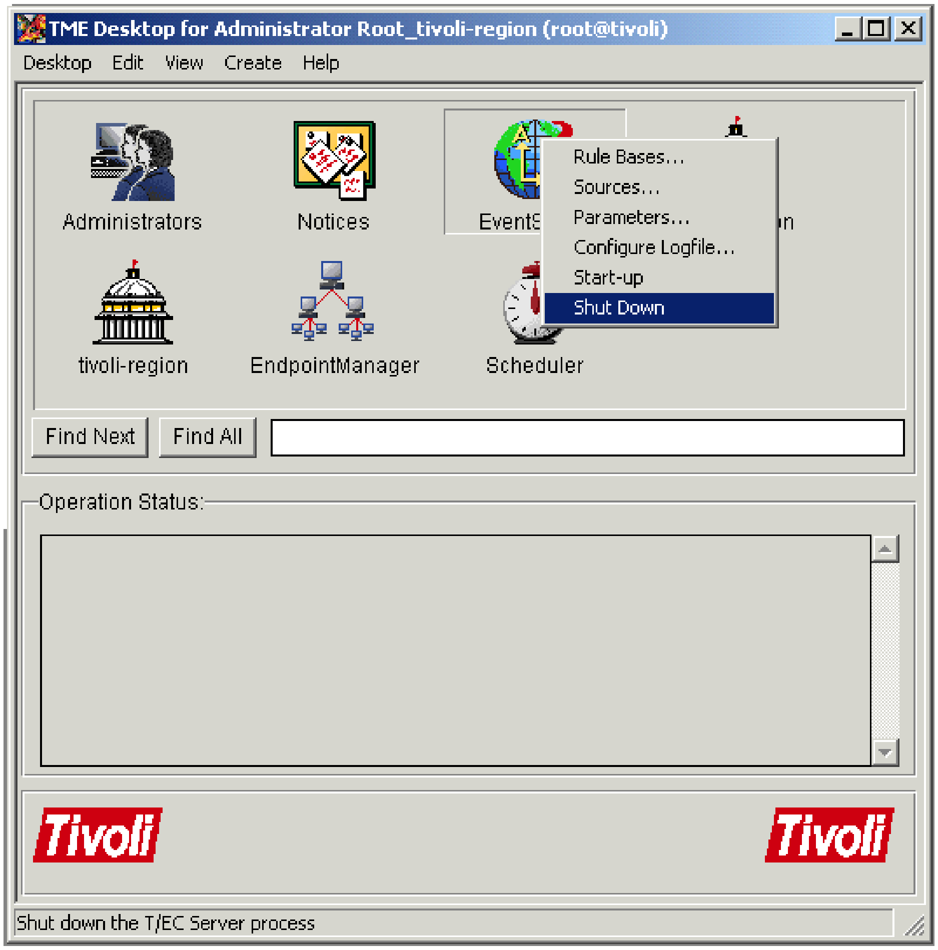
Time to keep non-closed events: 180 days

Time allowed for server initialization: 300 seconds

☑ Trace Rules Rule Trace File: /tmp/rules.trace

Figure 35. Changing Event Server parameters (continued)

6. Click on Save & Close and stop and restart the event server (see Figure 36 on page 98).



Shut down the T/EC Server process

Figure 36. Shut down the Event Server

7. Try to reproduce the problem you are having. Once done, save the trace file for further investigations.

5.2.4 Event Viewer configuration

In order to administer Risk Manager in a productive and efficient way for the TEC console operator, you need to configure the Event Viewer to your special needs.

To start displaying events, the TEC console operator selects **Windows > Event Viewer,** as shown in Figure 37 on page 99.

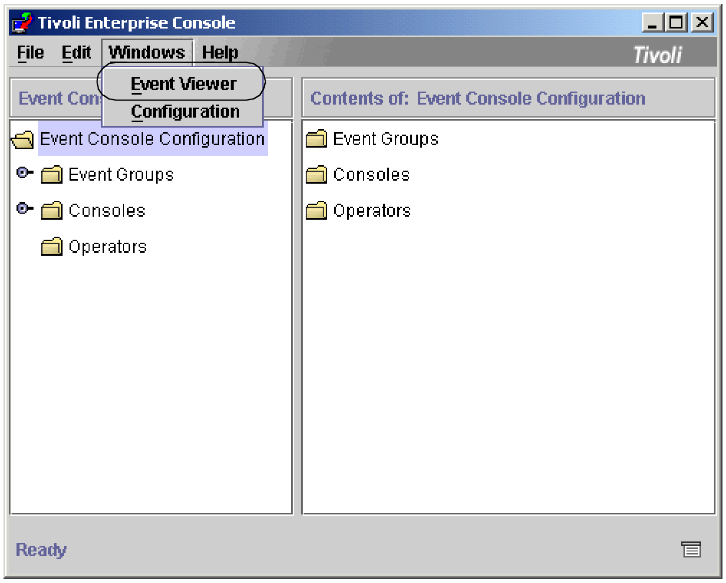


Figure 37. Starting Event Viewer

The Event Summary panel, displaying all the Event Groups assigned to this operator, is shown in Figure 38 on page 100.

The number 15, which is shown in the bar graph, represents the total number of HARMLESS events in the Event Group RM Events w/o Situations that are in the OPEN state. Moving the mouse over the other boxes will display the number of events open with other severities.

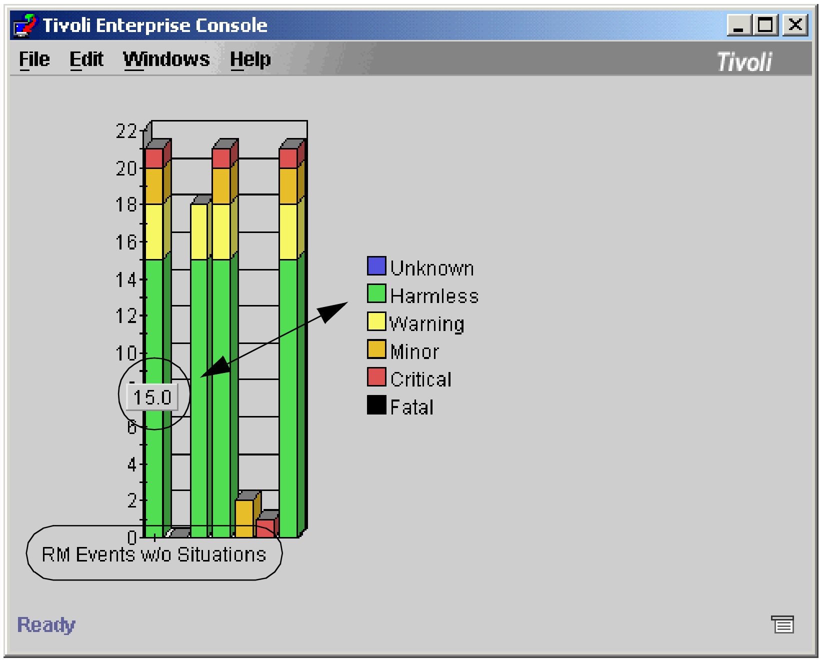
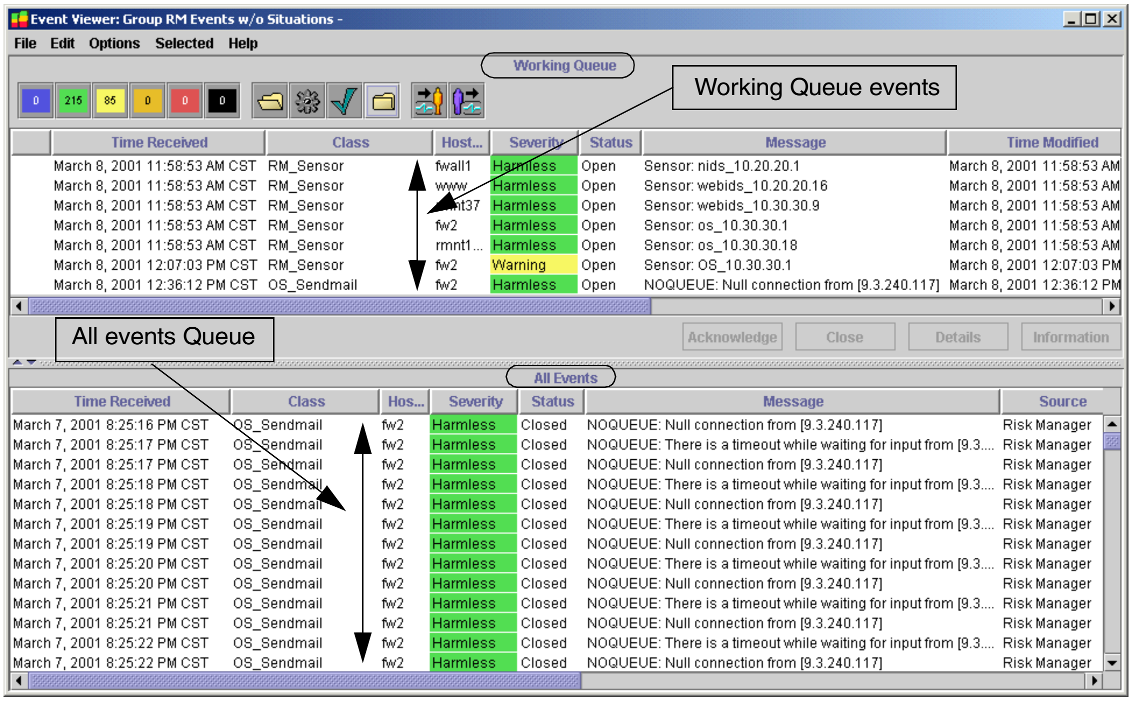


Figure 38. Event summary panel

Click anywhere inside the status boxes for an Event Group to display events associated with that Event Group. Figure 39 on page 101 shows an example of RM Events w/o Situations.



	Time Received	Class	Host...	Severity	Status	Message	Time Modified
	March 8, 2001 11:58:53 AM CST	RM_Sensor	fwall1	Harmless	Open	Sensor: nids_10.20.20.1	March 8, 2001 11:58:53 AM
	March 8, 2001 11:58:53 AM CST	RM_Sensor	www	Harmless	Open	Sensor: webids_10.20.20.16	March 8, 2001 11:58:53 AM
	March 8, 2001 11:58:53 AM CST	RM_Sensor	rmnt37	Harmless	Open	Sensor: webids_10.30.30.9	March 8, 2001 11:58:53 AM
	March 8, 2001 11:58:53 AM CST	RM_Sensor	fw2	Harmless	Open	Sensor: os_10.30.30.1	March 8, 2001 11:58:53 AM
	March 8, 2001 11:58:53 AM CST	RM_Sensor	rmnt1...	Harmless	Open	Sensor: os_10.30.30.18	March 8, 2001 11:58:53 AM
	March 8, 2001 12:07:03 PM CST	RM_Sensor	fw2	Warning	Open	Sensor: OS_10.30.30.1	March 8, 2001 12:07:03 PM
	March 8, 2001 12:36:12 PM CST	OS_Sendmail	fw2	Harmless	Open	NOQUEUE: Null connection from [9.3.240.117]	March 8, 2001 12:36:12 PM

Time Received	Class	Hos...	Severity	Status	Message	Source
March 7, 2001 8:25:16 PM CST	OS_Sendmail	fw2	Harmless	Closed	NOQUEUE: Null connection from [9.3.240.117]	Risk Manager
March 7, 2001 8:25:17 PM CST	OS_Sendmail	fw2	Harmless	Closed	NOQUEUE: There is a timeout while waiting for input from [9.3....	Risk Manager
March 7, 2001 8:25:17 PM CST	OS_Sendmail	fw2	Harmless	Closed	NOQUEUE: Null connection from [9.3.240.117]	Risk Manager
March 7, 2001 8:25:18 PM CST	OS_Sendmail	fw2	Harmless	Closed	NOQUEUE: There is a timeout while waiting for input from [9.3....	Risk Manager
March 7, 2001 8:25:18 PM CST	OS_Sendmail	fw2	Harmless	Closed	NOQUEUE: Null connection from [9.3.240.117]	Risk Manager
March 7, 2001 8:25:19 PM CST	OS_Sendmail	fw2	Harmless	Closed	NOQUEUE: There is a timeout while waiting for input from [9.3....	Risk Manager
March 7, 2001 8:25:19 PM CST	OS_Sendmail	fw2	Harmless	Closed	NOQUEUE: Null connection from [9.3.240.117]	Risk Manager
March 7, 2001 8:25:20 PM CST	OS_Sendmail	fw2	Harmless	Closed	NOQUEUE: There is a timeout while waiting for input from [9.3....	Risk Manager
March 7, 2001 8:25:20 PM CST	OS_Sendmail	fw2	Harmless	Closed	NOQUEUE: Null connection from [9.3.240.117]	Risk Manager
March 7, 2001 8:25:21 PM CST	OS_Sendmail	fw2	Harmless	Closed	NOQUEUE: There is a timeout while waiting for input from [9.3....	Risk Manager
March 7, 2001 8:25:21 PM CST	OS_Sendmail	fw2	Harmless	Closed	NOQUEUE: Null connection from [9.3.240.117]	Risk Manager
March 7, 2001 8:25:22 PM CST	OS_Sendmail	fw2	Harmless	Closed	NOQUEUE: There is a timeout while waiting for input from [9.3....	Risk Manager
March 7, 2001 8:25:22 PM CST	OS_Sendmail	fw2	Harmless	Closed	NOQUEUE: Null connection from [9.3.240.117]	Risk Manager

Figure 39. View of events in the RM Events w/o Situations Event Group

By default, two slightly different views are displayed:

- Working queue events
- All events

The details about these views are as follows:

- All events

  This queue displays all events received from the event group. The number of actual events displayed is defined by the maximum number of events in the Event View option. This defaults to 1000, but can be set by the user.

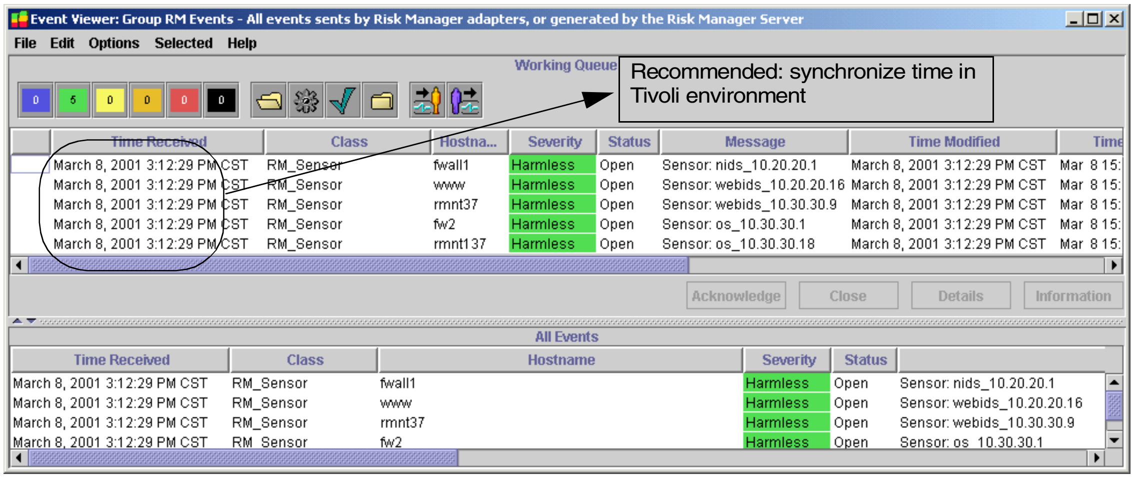
- Working queue

  This initially displays the same events as in the All events panel. As soon as an event is highlighted in this view, it remains in focus.

If new events arrive, they will appear in the All events panel and a globe icon will appear in the top left corner of the panel, indicating new events have arrived. To see these new events in the Working Queue view, click on this icon.

5.2.4.1 Obtaining details on an event

The first change the operator will see on the TEC Console is the message appearing in the Working Queue and All events views, as shown in Figure 40.


Event Viewer: Group RM Events - All events sents by Risk Manager adapters, or generated by the Risk Manager Server
File
Edit
Options
Selected
Help
Working Queue
0
5
0
0
0
0
Acknowledge
Close
Details
Information
All Events

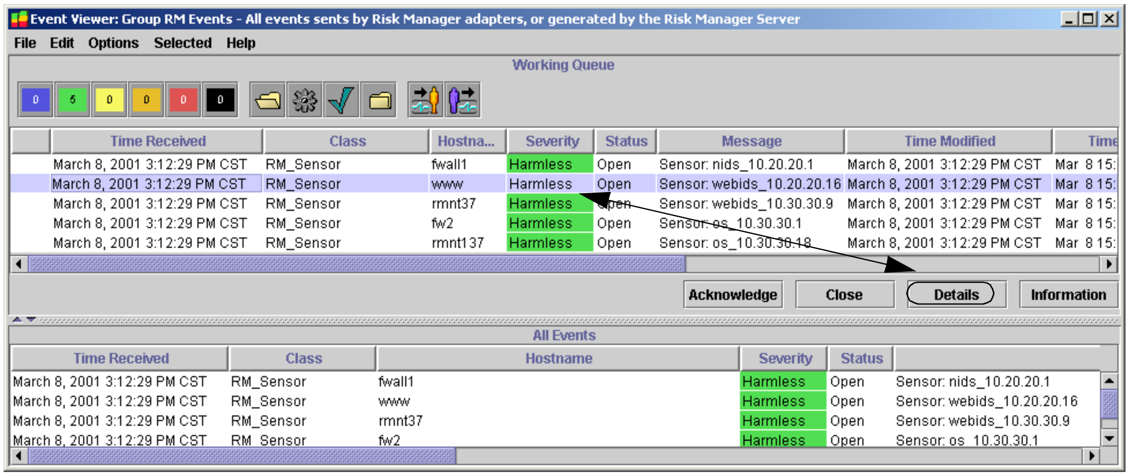
Recommended: synchronize time in Tivoli environment

Time Received	Class	Hostna...	Severity	Status	Message	Time Modified	Time
March 8, 2001 3:12:29 PM CST	RM_Sensor	fwall1	Harmless	Open	Sensor: nids_10.20.20.1	March 8, 2001 3:12:29 PM CST	Mar 8 15:
March 8, 2001 3:12:29 PM CST	RM_Sensor	www	Harmless	Open	Sensor: webids_10.20.20.16	March 8, 2001 3:12:29 PM CST	Mar 8 15:
March 8, 2001 3:12:29 PM CST	RM_Sensor	rmnt37	Harmless	Open	Sensor: webids_10.30.30.9	March 8, 2001 3:12:29 PM CST	Mar 8 15:
March 8, 2001 3:12:29 PM CST	RM_Sensor	fw2	Harmless	Open	Sensor: os_10.30.30.1	March 8, 2001 3:12:29 PM CST	Mar 8 15:
March 8, 2001 3:12:29 PM CST	RM_Sensor	rmnt137	Harmless	Open	Sensor: os_10.30.30.18	March 8, 2001 3:12:29 PM CST	Mar 8 15:

Time Received	Class	Hostname	Severity	Status	
March 8, 2001 3:12:29 PM CST	RM_Sensor	fwall1	Harmless	Open	Sensor: nids_10.20.20.1
March 8, 2001 3:12:29 PM CST	RM_Sensor	www	Harmless	Open	Sensor: webids_10.20.20.16
March 8, 2001 3:12:29 PM CST	RM_Sensor	rmnt37	Harmless	Open	Sensor: webids_10.30.30.9
March 8, 2001 3:12:29 PM CST	RM Sensor	fw2	Harmless	Open	Sensor: os 10.30.30.1

Figure 40. Event on operator's console

The operator selects the event in the Working Queue panel by clicking on the event entry with the left mouse button, as shown in Figure 41.

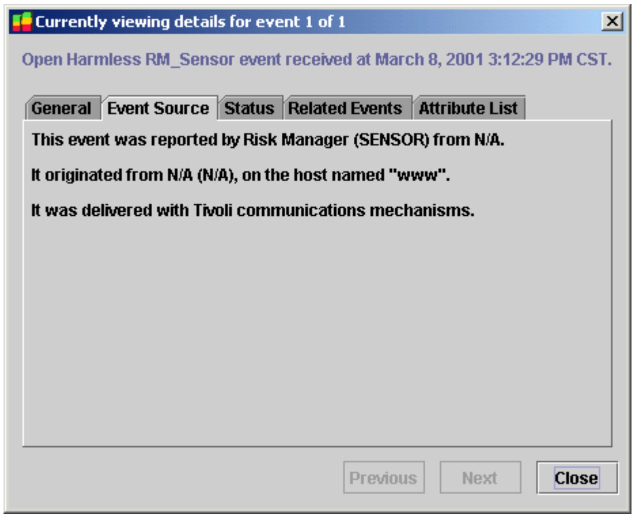

Event Viewer: Group RM Events - All events sents by Risk Manager adapters, or generated by the Risk Manager Server
File
Edit
Options
Selected
Help
Working Queue
0
5
0
0
0
0
Acknowledge
Close
Details
Information
All Events

Time Received	Class	Hostna...	Severity	Status	Message	Time Modified	Time
March 8, 2001 3:12:29 PM CST	RM_Sensor	fwall1	Harmless	Open	Sensor: nids_10.20.20.1	March 8, 2001 3:12:29 PM CST	Mar 8 15:
March 8, 2001 3:12:29 PM CST	RM_Sensor	www	Harmless	Open	Sensor: webids_10.20.20.16	March 8, 2001 3:12:29 PM CST	Mar 8 15:
March 8, 2001 3:12:29 PM CST	RM_Sensor	rmnt37	Harmless	Open	Sensor: webids_10.30.30.9	March 8, 2001 3:12:29 PM CST	Mar 8 15:
March 8, 2001 3:12:29 PM CST	RM_Sensor	fw2	Harmless	Open	Sensor: os_10.30.30.1	March 8, 2001 3:12:29 PM CST	Mar 8 15:
March 8, 2001 3:12:29 PM CST	RM_Sensor	rmnt137	Harmless	Open	Sensor: os_10.30.30.18	March 8, 2001 3:12:29 PM CST	Mar 8 15:

Time Received	Class	Hostname	Severity	Status	
March 8, 2001 3:12:29 PM CST	RM_Sensor	fwall1	Harmless	Open	Sensor: nids_10.20.20.1
March 8, 2001 3:12:29 PM CST	RM_Sensor	www	Harmless	Open	Sensor: webids_10.20.20.16
March 8, 2001 3:12:29 PM CST	RM_Sensor	rmnt37	Harmless	Open	Sensor: webids_10.30.30.9
March 8, 2001 3:12:29 PM CST	RM Sensor	fw2	Harmless	Open	Sensor: os 10.30.30.1

Figure 41. Selecting an event to work on

Pressing the Details button displays some general information about the event, as shown in Figure 42 on page 103.



Open Harmless RM_Sensor event received at March 8, 2001 3:12:29 PM CST.

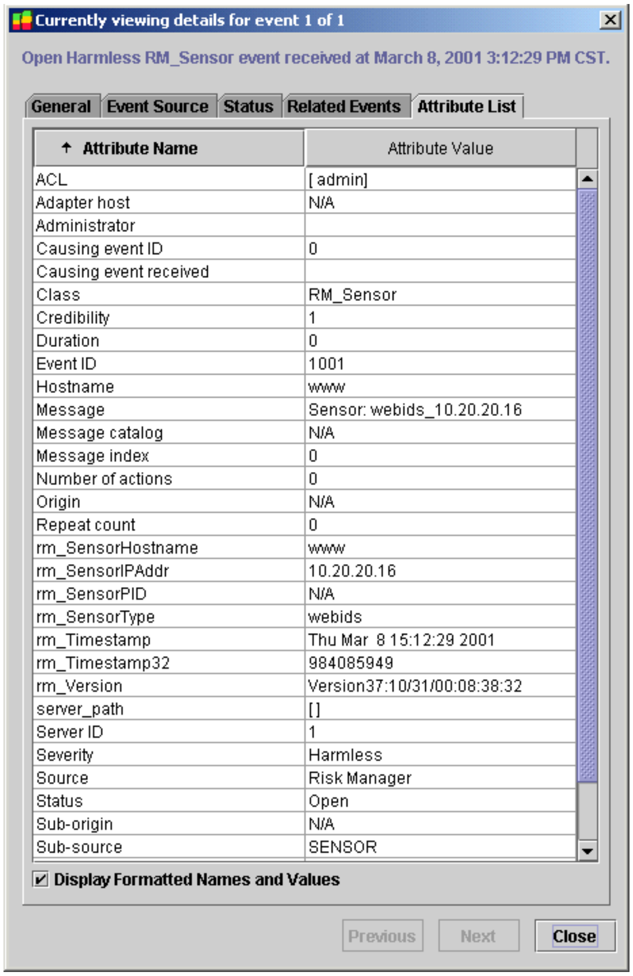
This event was reported by Risk Manager (SENSOR) from N/A.

It originated from N/A (N/A), on the host named "www".

It was delivered with Tivoli communications mechanisms.

Figure 42. Details of an event

To toggle between views in this panel, the user would click on the appropriate tab with the left mouse button. Figure 43 on page 104 shows the Attribute List of the selected event.



Open Harmless RM_Sensor event received at March 8, 2001 3:12:29 PM CST.

Attribute Name	Attribute Value
ACL	[admin]
Adapter host	N/A
Administrator	
Causing event ID	0
Causing event received	
Class	RM_Sensor
Credibility	1
Duration	0
Event ID	1001
Hostname	www
Message	Sensor: webids_10.20.20.16
Message catalog	N/A
Message index	0
Number of actions	0
Origin	N/A
Repeat count	0
rm_SensorHostname	www
rm_SensorIPAddr	10.20.20.16
rm_SensorPID	N/A
rm_SensorType	webids
rm_Timestamp	Thu Mar 8 15:12:29 2001
rm_Timestamp32	984085949
rm_Version	Version37:10/31/00:08:38:32
server_path	[]
Server ID	1
Severity	Harmless
Source	Risk Manager
Status	Open
Sub-origin	N/A
Sub-source	SENSOR

☑ Display Formatted Names and Values

Figure 43. Attributes of a event (RM Sensor)

The following list provides a brief summary of each view available in the Currently viewing details for event 1 of 1 panel:

- General

  Displays the message, time of arrival, the number of duplicates, when it was last modified, and information on any automatic response that has been executed.

- Related events

  Displays the events that were the cause for this one (if there is one) and any events that are symptom events of this event. More details of cause and effect events can be obtained by clicking on the Details button in this view.

- Attribute list

  Displays a list of all the event attributes and their values.

- Event source

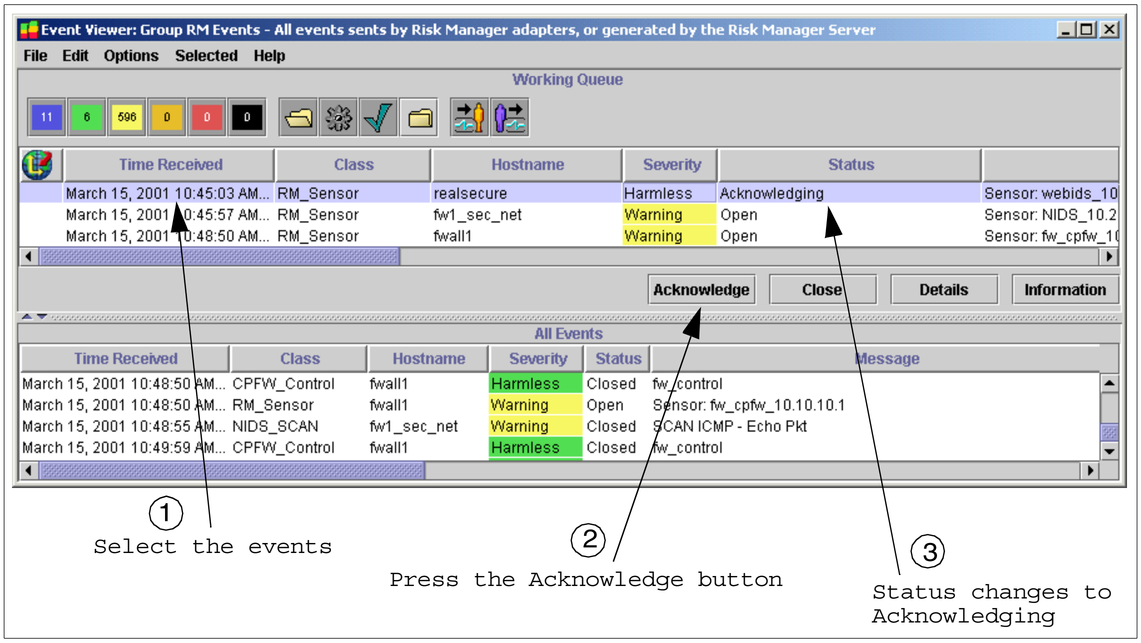
  Displays the source name of the event, its origin, and whether it is a TME or non-TME event.

- Status

  Displays the current status, for example, Open, how long it has been open, and which operator it is currently assigned.

5.2.4.2 Acknowledging an event

As shown in Figure 44, select the event to acknowledge in the Working Queue view and then click the Acknowledge button with the left mouse button. The status of the event then changes from Open to Acknowledging.



Event Viewer: Group RM Events - All events sents by Risk Manager adapters, or generated by the Risk Manager Server

Working Queue

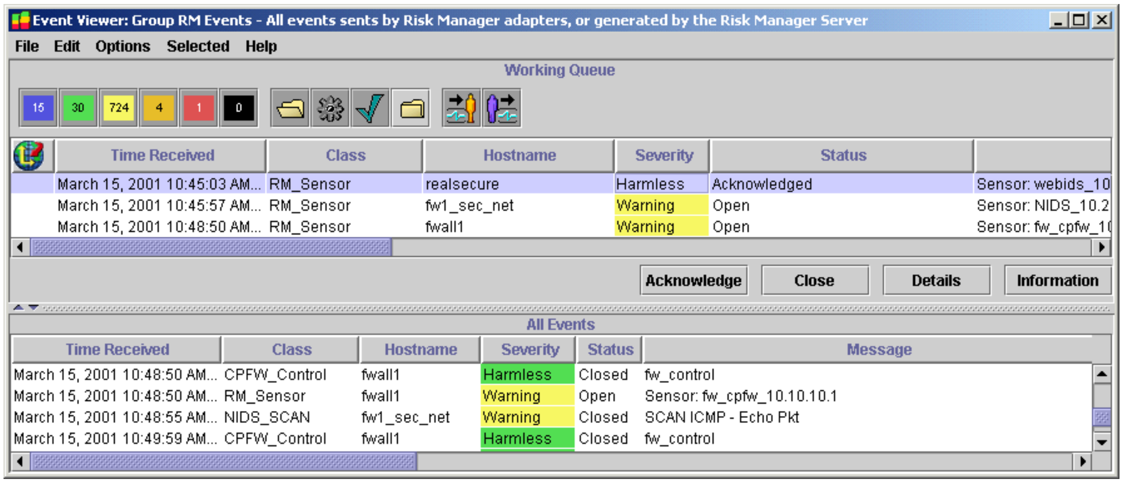
Time Received	Class	Hostname	Severity	Status	
March 15, 2001 10:45:03 AM...	RM_Sensor	realsecure	Harmless	Acknowledging	Sensor: webids_10
March 15, 2001 10:45:57 AM...	RM_Sensor	fw1_sec_net	Warning	Open	Sensor: NIDS_10.2
March 15, 2001 10:48:50 AM...	RM_Sensor	fwall1	Warning	Open	Sensor: fw_cpfw_1(

All Events

Time Received	Class	Hostname	Severity	Status	Message
March 15, 2001 10:48:50 AM...	CPFW_Control	fwall1	Harmless	Closed	fw_control
March 15, 2001 10:48:50 AM...	RM_Sensor	fwall1	Warning	Open	Sensor: fw_cpfw_10.10.10.1
March 15, 2001 10:48:55 AM...	NIDS_SCAN	fw1_sec_net	Warning	Closed	SCAN ICMP - Echo Pkt
March 15, 2001 10:49:59 AM...	CPFW_Control	fwall1	Harmless	Closed	fw_control

Figure 44. Event Viewer panel while an event is being acknowledged

When the Refresh Time timer expires, the status changes to Acknowledged, as shown in Figure 45 on page 106, but the event still remains highlighted.



Event Viewer: Group RM Events - All events sents by Risk Manager adapters, or generated by the Risk Manager Server

Working Queue

Time Received	Class	Hostname	Severity	Status	
March 15, 2001 10:45:03 AM...	RM_Sensor	realsecure	Harmless	Acknowledged	Sensor: webids_10
March 15, 2001 10:45:57 AM...	RM_Sensor	fw1_sec_net	Warning	Open	Sensor: NIDS_10.2
March 15, 2001 10:48:50 AM...	RM_Sensor	fwall1	Warning	Open	Sensor: fw_cpfw_1(

All Events

Time Received	Class	Hostname	Severity	Status	Message
March 15, 2001 10:48:50 AM...	CPFW_Control	fwall1	Harmless	Closed	fw_control
March 15, 2001 10:48:50 AM...	RM_Sensor	fwall1	Warning	Open	Sensor: fw_cpfw_10.10.10.1
March 15, 2001 10:48:55 AM...	NIDS_SCAN	fw1_sec_net	Warning	Closed	SCAN ICMP - Echo Pkt
March 15, 2001 10:49:59 AM...	CPFW_Control	fwall1	Harmless	Closed	fw_control

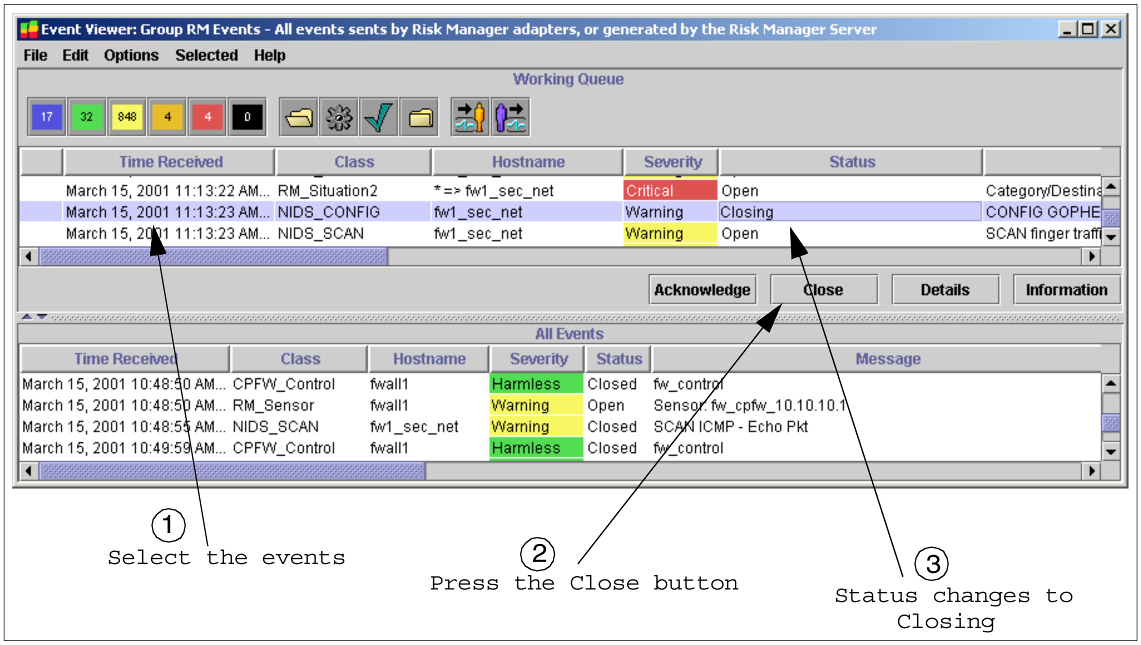
Figure 45. Event Viewer panel after an event has been acknowledged

Note

The minimum value for the Refresh Time timer is set to one minute by default. An operator cannot set the value to be any lower than this value. However, the TEC Console Administrator can change it.

5.2.4.3 Closing an event

Select the event in the Working Queue view you wish to close, then press Close with the left mouse button. The status of the event then changes from Acknowledged to Closing, as shown Figure 46 on page 107.



Event Viewer: Group RM Events - All events sents by Risk Manager adapters, or generated by the Risk Manager Server

Working Queue

	Time Received	Class	Hostname	Severity	Status	
	March 15, 2001 11:13:22 AM...	RM_Situation2	* => fw1_sec_net	Critical	Open	Category/Destina
	March 15, 2001 11:13:23 AM...	NIDS_CONFIG	fw1_sec_net	Warning	Closing	CONFIG GOPHE
	March 15, 2001 11:13:23 AM...	NIDS_SCAN	fw1_sec_net	Warning	Open	SCAN finger traffi

All Events

Time Received	Class	Hostname	Severity	Status	Message
March 15, 2001 10:48:50 AM...	CPFW_Control	fwall1	Harmless	Closed	fw_control
March 15, 2001 10:48:50 AM...	RM_Sensor	fwall1	Warning	Open	Sensor: fw_cpfw_10.10.10.1
March 15, 2001 10:48:55 AM...	NIDS_SCAN	fw1_sec_net	Warning	Closed	SCAN ICMP - Echo Pkt
March 15, 2001 10:49:59 AM...	CPFW_Control	fwall1	Harmless	Closed	fw_control

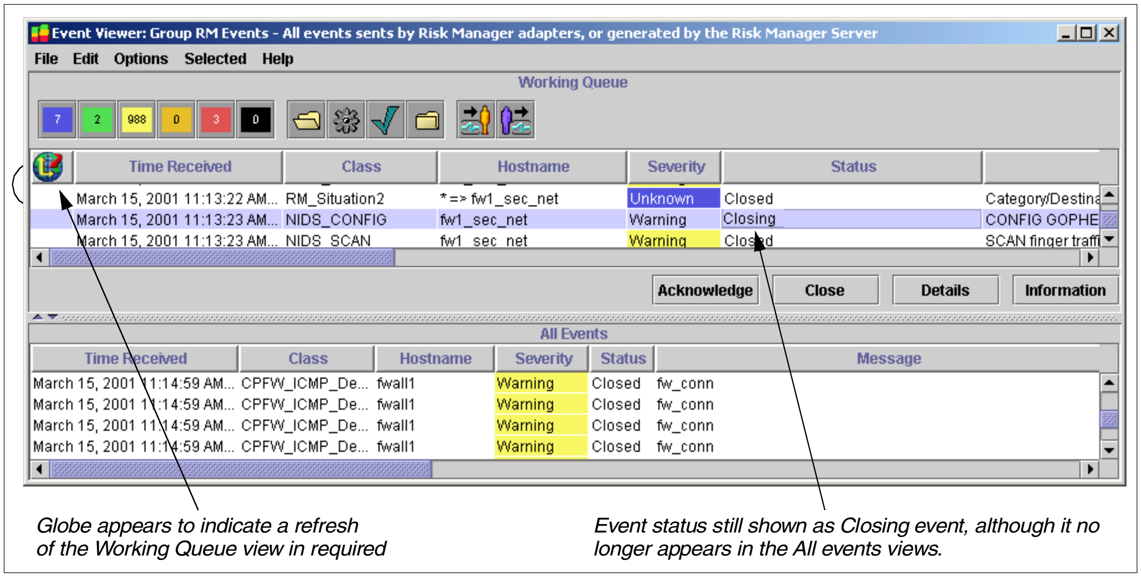
① Select the events

② Press the Close button

③ Status changes to Closing

Figure 46. Event Viewer panel while an event is being closed

When the Refresh Time timer expires, the TEC globe appears at the top left of the Working Queue view. The globe indicates that the Working Queue panel needs to be refreshed. Note that the event has already vanished from the All events view.



Event Viewer: Group RM Events - All events sents by Risk Manager adapters, or generated by the Risk Manager Server
File Edit Options Selected Help
Working Queue
7 2 988 0 3 0
Acknowledge
Close
Details
Information
All Events

Time Received	Class	Hostname	Severity	Status	
March 15, 2001 11:13:22 AM...	RM_Situation2	* => fw1_sec_net	Unknown	Closed	Category/Destina
March 15, 2001 11:13:23 AM...	NIDS_CONFIG	fw1_sec_net	Warning	Closing	CONFIG GOPHE
March 15, 2001 11:13:23 AM...	NIDS_SCAN	fw1_sec_net	Warning	Closed	SCAN finger traffi

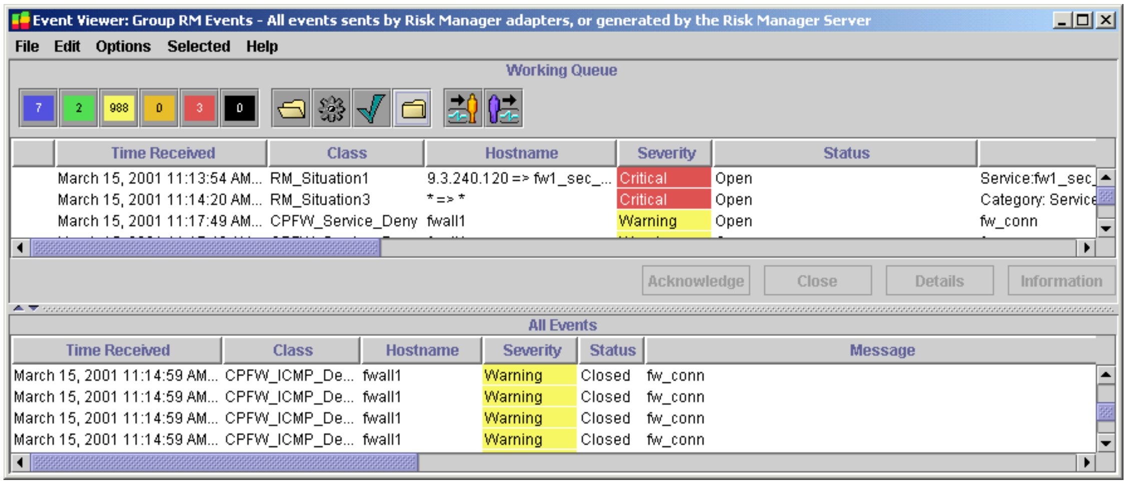
Time Received	Class	Hostname	Severity	Status	Message
March 15, 2001 11:14:59 AM...	CPFW_ICMP_De...	fwall1	Warning	Closed	fw_conn
March 15, 2001 11:14:59 AM...	CPFW_ICMP_De...	fwall1	Warning	Closed	fw_conn
March 15, 2001 11:14:59 AM...	CPFW_ICMP_De...	fwall1	Warning	Closed	fw_conn
March 15, 2001 11:14:59 AM...	CPFW_ICMP_De...	fwall1	Warning	Closed	fw_conn

Globe appears to indicate a refresh of the Working Queue view in required

Event status still shown as Closing event, although it no longer appears in the All events views.

Figure 47. Event Viewer panel after an event has been closed successfully

Clicking on the globe results in the panel being updated, as shown in Figure 48. Notice the event has also disappeared from the Working Queue view.



Event Viewer: Group RM Events - All events sents by Risk Manager adapters, or generated by the Risk Manager Server
File Edit Options Selected Help
Working Queue
7 2 988 0 3 0
Acknowledge
Close
Details
Information
All Events

Time Received	Class	Hostname	Severity	Status	
March 15, 2001 11:13:54 AM...	RM_Situation1	9.3.240.120 => fw1_sec_...	Critical	Open	Service:fw1_sec_
March 15, 2001 11:14:20 AM...	RM_Situation3	* => *	Critical	Open	Category: Service
March 15, 2001 11:17:49 AM...	CPFW_Service_Deny	fwall1	Warning	Open	fw_conn

Time Received	Class	Hostname	Severity	Status	Message
March 15, 2001 11:14:59 AM...	CPFW_ICMP_De...	fwall1	Warning	Closed	fw_conn
March 15, 2001 11:14:59 AM...	CPFW_ICMP_De...	fwall1	Warning	Closed	fw_conn
March 15, 2001 11:14:59 AM...	CPFW_ICMP_De...	fwall1	Warning	Closed	fw_conn
March 15, 2001 11:14:59 AM...	CPFW_ICMP_De...	fwall1	Warning	Closed	fw_conn

Figure 48. Event Viewer panel after pressing the globe icon

Note

By default, all closed events in the Event Viewer panel will be removed immediately. An operator can set his own value by selecting **Edit > Preferences** from the Event Viewer panel and changing the “Maximum age of closed events to display setting.” The change will not take effect until the Event Viewer panel is restarted.

5.2.5 Risk Manager Event Integration Facility

The Risk Manager Event Integration Facility (RMEIF) is the default method of delivering events to the TEC event server. Alternative methods of delivering events to the TEC event server include the following:

- TEC Event Integration Facility
- Logfile adapter (UNIX syslogd)
- Windows NT Event Log adapter
- SNMP adapter

The Risk Manager Event Integration Facility contains an event Application Programming Interface (API) library for use by C or Perl programs.

The Risk Manager Web IDS and the adapter for CheckPoint FireWall-1 use the Risk Manager Event Integration Facility APIs for sending Risk Manager related events to the TEC event server. Instead of using the API library for use with the C programming language, you can use the Perl module interface provided with the RMEIF for your Risk Manager adapters. As an example, Risk Manager uses the Perl module interface for Web IDS (see Figure 49 on page 110).

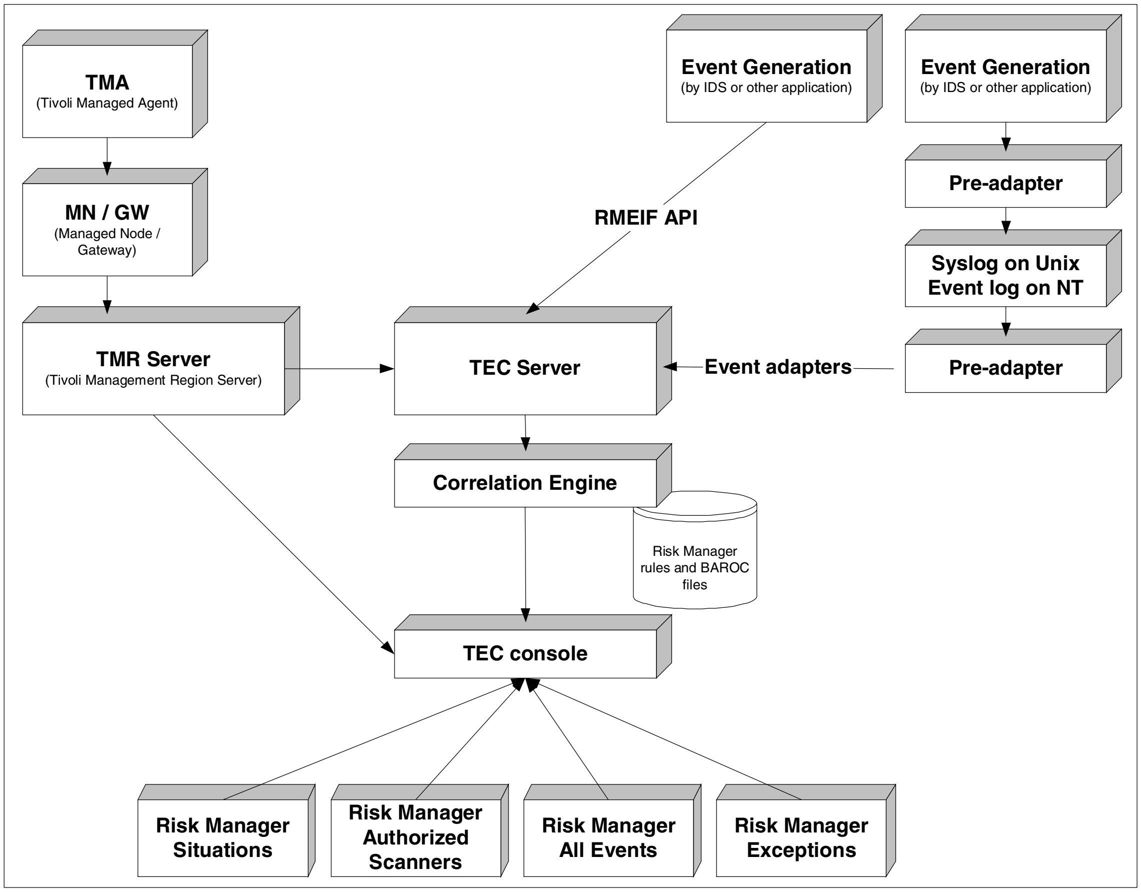


Figure 49. Risk Manager architecture

The Risk Manager Event Integration Facility daemon automatically initializes and then runs as a standalone process. The daemon must be running for the Risk Manager adapters to communicate with the event server.

The first application on a system that calls the RMEIF APIs causes the Risk Manager Event Integration Facility daemon to start. Subsequent applications that use the RMEIF share the same instance of the daemon. The daemon receives event information from the Risk Manager Event Integration Facility shared library that, in turn, forwards the information to the event server.

The RMEIF provides a version of its daemon for Tivoli Endpoint and Non-Tivoli environments.

The RMEIF contains an event application programming interface (API) library for use with the C programming language. The Risk Manager Event Integration Facility shared library provides the interfaces necessary to enable Risk Manager adapters to send events to the event server.

The adapters provided with Risk Manager that use the RMEIF already link with this library. When creating your own adapter for Risk Manager, be sure to link the RMEIF shared library.

5.2.5.1 Adapter files

An adapter uses various files for its operations. Table 6 provides a brief description of the types of files that can be used.

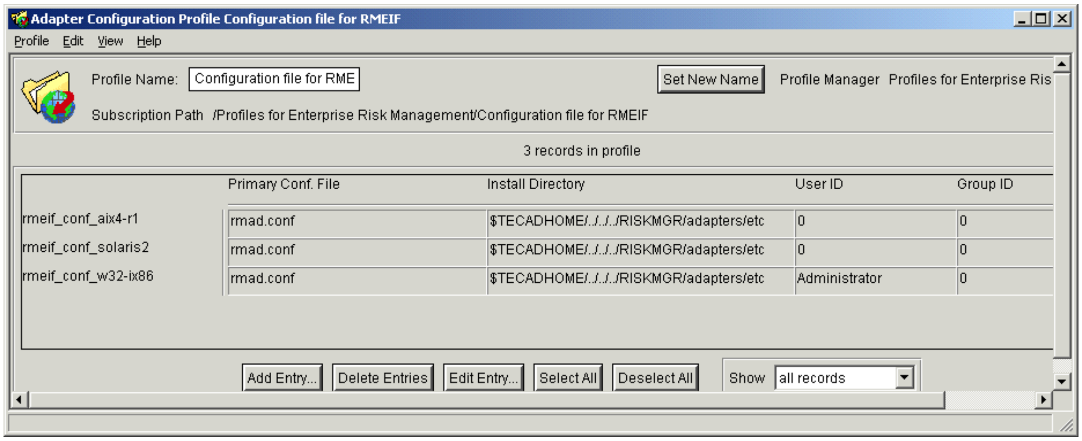
Table 6. Adapters descriptions files

File type	Description
Basic recorder of objects in C (BAROC)	Defines event classes to the event server. Installed at the TEC event server.
Class definition statement (CDS)	Defines event class definitions to the adapter.
Configuration	Defines configuration options for adapters.
Error	Defines error logging and tracing options for the adapter.
Format	Defines the format of messages and matches them to event classes for the UNIX logfile adapter (syslogd) and the Windows NT Event Log adapter.

5.2.5.2 Configuration file

The RMEIF uses a configuration file that contains configuration options and filters. This file is read by the Risk Manager Event Integration Facility daemon when it is started. By changing this file, you can reconfigure the RMEIF at any time. To have your configuration changes take effect, stop, and restart the Risk Manager Event Integration Facility.

The default name for the RMEIF configuration file is rmad.conf. More details are shown in Figure 50 on page 112.



Profile Name: Configuration file for RME

Profile Manager Profiles for Enterprise Ris

Subscription Path /Profiles for Enterprise Risk Management/Configuration file for RMEIF

3 records in profile

	Primary Conf. File	Install Directory	User ID	Group ID
rmeif_conf_aix4-r1	rmad.conf	$TECADHOME/../../../RISKMGR/adapters/etc	0	0
rmeif_conf_solaris2	rmad.conf	$TECADHOME/../../../RISKMGR/adapters/etc	0	0
rmeif_conf_w32-ix86	rmad.conf	$TECADHOME/../../../RISKMGR/adapters/etc	Administrator	0

Show all records

Figure 50. Adapter Configuration Profile for RMEIF

5.2.5.3 Windows NT file location

By default, the Risk Manager Event Integration Facility expects its Windows NT configuration file to be located, as shown in Table 7. For Windows NT, the syntax shown is correct when running the Bash interpreter, which Tivoli provides with the Tivoli Enterprise Console.

Table 7. Windows NT Locations files

Adapter type	Node type	Location
Tivoli	Endpoint	$LCFROOT/bin/$*INTER*P/RISKMGR/adapters/etc
Non-Tivoli	Not applicable	$LCFROOT/bin/$*INTER*P/RISKMGR/adapters/etc

This concludes the configuration of our Risk Manager environment. In the following sections, we describe how to install and set up the other components in our test scenario.

5.3 CheckPoint FireWall-1 integration

This section describes how the CheckPoint Firewall-1 and its Tivoli Risk Manager adapter are installed and configured in our lab scenario.

Other firewall support

We have randomly picked CheckPoint’s Firewall-1 product to be included in the Risk Manager scenario. Another firewall product directly supported with Risk Manager is Cisco Secure PIX Firewall.

The IBM Firewall 4.2.1 will support Risk Manager by supplying an adapter for this specific release of the product.

For our purposes, the firewall served mostly as a source of alerts for the Risk Manager. Therefore, the steps listed below describe only how to set up a minimally functional firewall. For a more rigorous review of the process of setting up a firewall for business use, refer to the redbook *CheckPoint VPN-1 / FireWall-1 on AIX: A Cookbook for Stand-Alone and High Availability Solutions*, SG24-5492. An excellent Web site for more details on the CheckPoint Firewall-1 is:

`http://www.phoneboy.com`

Additional details can be obtained from the book *Check Point Firewalls: An Administration Guide*, by Goncalves.

Tivoli Risk Manager provides an adapter for CheckPoint FireWall-1 that maps CheckPoint FireWall-1 log entries into events that it then forwards to the Tivoli Event Server. Unlike many products and sensors that write events into syslog, CheckPoint uses its own rule set in a proprietary format. Special code is required to read the firewall logs.

The adapter for CheckPoint FireWall-1 (CheckPoint adapter) uses the CheckPoint Open Platform for Secure Enterprise Connectivity (OPSEC™) server and Log Export API (LEA) to read the firewall log into the adapter. After the adapter formats the events for use by Tivoli, the Risk Manager Event Integration Facility (RMEIF) is used to forward events to the Event Server.

The Log Export API

- Retrieves real-time and historical log information from VPN-1/FireWall-1 in a secure manner.
- Provides for security event analysis and reporting.
- Allows integration with enterprise event management, such as Risk Manager.
- Performs usage monitoring and reporting.

Using the CheckPoint APIs, any of the following connection types can be established with VPN-1/FireWall-1:

- Clear connection

  The CheckPoint adapter and VPN-1/FireWall-1 transfer data without any restrictions.

- Authenticated connection

  The CheckPoint adapter and VPN-1/FireWall-1 must verify each other's identities before the transfer of any data takes place. The CheckPoint adapter uses a shared key, exchanged by the `opsec_putkey` command, to authenticate the OPSEC host with VPN-1/FireWall-1.

- Encrypted connection by using Secure Sockets Layer (SSL)

  The CheckPoint adapter encrypts the data transferred between VPN-1/FireWall-1 and the OPSEC application by using a 3DES key. The CheckPoint adapter performs the encryption only after it authenticates the OPSEC host with VPN-1/FireWall-1.

We chose to establish an authenticated connection between the CheckPoint adapter and the firewall.

In our lab configuration, the CheckPoint adapter is installed on a Windows NT 4 server. This is because the OPSEC LEA, needed by the adapter to read the logs from the firewall, is available on NT and Solaris only, not AIX.

Through the CheckPoint adapter, Tivoli administrators can evoke TEC tasks that use the CheckPoint Suspicious Activity Monitor (SAM) to closely monitor or block connections from hosts that the Tivoli Risk Manager identifies as potentially threatening. The TEC tasks evoke the `rmt_cpfw` command on the NT machine with parameters describing the host/s to block or monitor. The adapter in the NT machine then forwards the request to the firewall via its sam_server connection. More detail on using this capability can be found in Section 5.3.3, “Automated Risk Manager firewall action” on page 161.

Protect the SAM function

There is nothing preventing someone with access to the NT machine from invoking the `rmt_cpfw` command manually with malicious intent, perhaps to block access to the root name servers. Misused, the SAM function can be an effective Denial of Service tool. Restrict access to the NT machine just as you would to the firewall itself.

Also, the NT machine must be hardened following the current "best practices." Leaving known vulnerabilities uncorrected will expose your systems to abuse.

5.3.1 Firewall installation

In this section, we take a closer look at how to prepare and execute the installation of the CheckPoint Firewall-1 on an AIX machine. We also describe the configuration of the software and show how to define basic firewall policies.

5.3.1.1 Before installing VPN-1/FireWall-1

Follow these steps in order to be well prepared for a firewall installation:

1. Install AIX 4.3.3 on the RS/6000.
2. Ensure that there is adequate file space for the install and normal operation of the firewall.
3. In order for the X/Motif GUI to function properly, the LANG environment variable must be defined.

Security advice

You should also consider if you need the X/Motif GUI on the firewall machine at all, because normal operations will be performed on a remote management console.

4. Confirm the routing is correctly configured on the gateway. If there are problems with routing, resolve them before continuing with the install.
5. Make a note of the names and IP addresses of all the gateways's interfaces. You will need this information later when you define your Security Policy.
6. Confirm that the gateway's name, as given in the /etc/hosts file, corresponds to the IP address of the gateway's external interface. If you fail to do so, IKE encryption (among other features) may not work properly.
7. If IP Forwarding is enabled, the gateway will route packets to other IP addresses. Ensure that this does not occur while VPN-1/FireWall-1 is not running; you will be exposing your network. Make sure that it is not turned on in one of the .rc scripts during boot. Turn it on (with the `no -o ipforwarding=1` command) in the fwstart script after VPN-1/FireWall-1 starts enforcing the Security Policy, and turn it off (with the `no -o ipforwarding=0` command) in the fwstop script just before

VPN-1/FireWall-1 stops. This is outlined in Section 5.3.1.3, “Basic configuration of FireWall-1” on page 118.

8. Harden the operating system. Review the services running on the FireWall-1 machine and remove any service that is not required. You can get some guidance on this by referring to the "Hardening the AIX Operating System" chapter in the redbook *CheckPoint VPN-1/Firewall-1 on AIX: A Cookbook for Stand-Alone and High Availability Solutions,* SG24-5492*.*

9. DNS on a firewall is not recommended. Therefore, you may want to force AIX not to use DNS by doing the following:

   ```
   # echo "hosts=local" > /etc/netsvc.conf
   # mv /etc/resolv.conf /etc/resolv.conf.old
   ```

10. You should have the current VPN-1/FireWall-1 software on a CD-ROM. Download any new patches from the CheckPoint Web site:

    `http://www.checkpoint.com/support`

    or obtain them from your reseller.

11. Familiarize yourself with the concepts of the Management module, Master and firewalled host by reading Chapter 1, "Pre-Installation Configuration", of the *VPN-1/FireWall-1 Administration Guide*.

12. Determine which VPN-1/FireWall-1 component is to be installed on each computer. You must decide which computer(s) will host your management server, which will host your enforcement point(s), and which will host your GUI client.

13. When installing a VPN-1/FireWall-1 component, verify that there are no other VPN-1/FireWall-1 components running.

14. You are provided a certificate key from your CheckPoint reseller. Contact `http://license.checkpoint.com` to obtain the license (evaluation or permanent). Instead of typing all the license information at the prompt or in the cpconfig menus, it is much more useful to put it in a script in /usr/local/fw1 on your AIX machine; you will need it again in the future (for entering the license after updates, for example). The easiest way is to copy the license command that you received from the license Web site or by e-mail to a file called fw1lic (Remember to put all commands on one line!):

    ```
    # cd /usr/local/fw1
    # cat > fw1lic  fw putlic 10.1.1.1 3719c801-d3de94bf-4f5f8401 pfmx
    connect vpnstrong srunlimit c ontrolx oseu motif embedded vpnstrong
    srunlimit ram1
    ```

```
CTRL-D
# chmod +x fw1lic
```

5.3.1.2 CheckPoint VPN-1/FireWall-1 installation steps

CheckPoint VPN-1/FireWall-1 4.1 can be installed in two different ways. There is an install script (INSTALLU) that will completely guide you through the installation process by prompting you for your input data. After the script is completed, your firewall is ready to run. The second procedure uses SMIT to install and configure the VPN-1/FireWall-1 product. This procedure is lined out in more detail in the following:

1. Insert the CheckPoint 2000 CD-ROM into the CD-ROM drive and enter:

   ```
   # cd /mnt
   # mkdir cdrom
   # cd /
   # mount /dev/cd0 mnt/cdrom
   ```

2. Execute:

   ```
   # smitty install_latest
   ```

3. Enter /mnt/cdrom/aix/CPfw1-41 in "INPUT device/directory for software" and press Enter once.
4. Press F4 to list the available software
5. Scroll down using the arrow keys on the keyboard. Select 4.1.0.0 CheckPoint FireWall-1 for AIX, 4.1.0.0 by pressing F7. Press Enter twice to return to the menu. At this point, change any of the install options displayed as appropriate.
6. Press Enter to start the installation process. If the install process detects any missing prerequisites, then you must:
   a. Remove the FireWall-1 CD-ROM.
   b. Install the appropriate CD-ROM.
   c. Install the appropriate prerequisite software.
   d. Return to step 1 to repeat the install steps.
7. When the installation completes, exit SMIT by pressing Enter twice.
8. Edit the /etc/environment file to:
   a. Add a line containing FWDIR=/usr/lpp/CPfw1-41.
   b. Append $FWDIR/bin to the PATH statement.

5.3.1.3 Basic configuration of FireWall-1

To do the basic configuration of FireWall-1, follow these steps:

1. If cpconfig does not detect a previous VPN-1/FireWall-1 installation, cpconfig asks you to confirm your consent to the license agreement:

   ```
   Do you accept all the terms of this license agreement (y/n) ? y
   ```

2. cpconfig then configures VPN-1/FireWall-1 by asking you a series of questions. First, the following screen is displayed:

   ```
   Choosing Installation
   --------------------------------
   (1) VPN-1 & FireWall-1 Stand alone Installation
   (2) VPN-1 & FireWall-1 Distributed Installation

   Option (1) will install VPN-1 and FireWall-1 Internet Gateway Management
   Server and Enforcement Module on a single machine.
   Option (2) will allow you to install specific components of the VPN-1 &
   FireWall-1 Enterprise Products on Different Machines.
   Enter your selection (1-2): 1
   ```

   To install all the VPN-1/FireWall-1 components, choose (1) VPN-1 & FireWall-1 Stand alone Installation.

   In this case, the Management Server and Enforcement Module will both be installed on this machine, and the Management Module will be unable to manage Enforcement Modules on other machines. You can install the GUI Client on any machine.

   To install the FireWall-1 components on different machines, choose (2) VPN-1 & FireWall-1 Distributed Installation. In this case, the Management Server and Enforcement Modules can both be installed on this machine, and the Management Module will be able to manage Enforcement Modules on other machines.

3. If you choose (2) VPN-1 & FireWall-1 Distributed Installation, the following screen is displayed

   ```
   Which of the following VPN-1 & FireWall-1 options do you wish to
   install/configure:
   ----------------------------------------------------------------------
   -------------------
   (1) VPN-1 & FireWall-1 Enterprise Management and Gateway/Server Module
   (2) VPN-1 & FireWall-1 Gateway/Server Module
   (3) VPN-1 & FireWall-1 Enterprise Management
   ```

   If you choose VPN-1 & FireWall-1 Enterprise Management, then proceed to step 5, which automatically prompts you regarding starting FireWall-1 at startup.

If you choose VPN-1 & FireWall-1 Gateway/Server Module or VPN-1 & FireWall-1 Enterprise Management and Gateway/Server Module, then continue.

4. Choose one of the following:

   ```
   Which Module would you like to install?
   ------------------------------------------------------------
   (1) VPN-1 & FireWall-1 - Limited Hosts (25, 50, 100,  or 250)
   (2) VPN-1 & FireWall-1 - Unlimited Hosts
   (3) VPN-1 & FireWall-1 - SecureServer
   ```

   Choose the number of hosts that will be licensed for the SecureServer. SecureServer is an internal VPN-1/FireWall-1 Module that encrypts with VPN-1 SecureClients.

5. Next you are asked whether you wish to automatically start VPN-1 & FireWall-1 at boot time:

   ```
   Do you wish to start VPN-1 & FireWall-1 automatically from /etc/rc.net
   y/n [y]? y
   ```

   Type y if you want VPN-1 and FireWall-1 to automatically start each time the system boots.

6. Next you are asked to enter group names:

   ```
   Please specify group name [<ret> for no group permissions]:
   ```

   Usually the FireWall-1 module is given group permission for access and execution. You may now name such a group or instruct the installation procedure to give no group permissions to the FireWall-1 module. If you have not yet set up a VPN-1 & FireWall-1 group or choose not to, press <Return>. This results in only a Super-User being able to access and execute the FireWall-1 module.

7. Next, you are asked if you have a VPN-1 & FireWall-1 license.

   If you have not yet obtained your license(s), see step 14. on page 116.

   If you have already obtained your license, enter y, and enter your license key when prompted. If you have not yet obtained your license, then enter n. You may complete the installation process and add your license later, as outlined in step 14. on page 116.

8. Next, you are asked to enter a list of administrators, that is, people who are allowed to use the GUI clients (computers) to administer the VPN-1 & FireWall-1 Security Policy on the Management Server:

   ```
   You may now define administrators that are allowed to use the GUI
   clients (for example, the Windows GUI).
   ```

```
At any later time you can modify administrators and passwords by running
fwm -a
You must define at least one administrator in order to use the GUI
Clients.
```

If you choose not to define any administrators now, you will not be able to use the VPN-1 & FireWall-1 client/server configuration until you do so (using the fwm program).

9. Next, you are asked to enter a list of trusted GUI clients.

   ```
   You should now enter a list of trusted hosts that may be used as GUI
   clients (for example, on which you may run the Windows GUI). At any
   later time you can add hosts to this list by modifying
   $FWDIR/conf/gui-clients
   ```

   At least one GUI client must be defined if you wish to use the VPN-1 & FireWall-1 client/server configuration. If you do not define one now, you can do so later by modifying the file $FWDIR/conf/gui-clients. This file consists of IP addresses or resolvable names, one per line.

10. If you have installed a Management Module on this computer, you must specify the remote VPN-1 & FireWall-1 modules for which this Management Module is defined as Master.

    Enter the IP addresses or resolvable names of all hosts this Management Module controls.

    Enter a single IP address or resolvable name on each line, then terminate the list with a Ctrl-D or your EOF character.

11. The screen will show your entries and ask you for confirmation:

    ```
    Is this correct y/n [y] ?
    ```

    If the list of hosts on the screen is correct, press <Return>. If it is incorrect, type n, and make the necessary corrections.

12. Next, you are asked to configure the SMTP security server. Modify if appropriate.

13. Next, you are asked to configure the SNMP daemon. Modify if appropriate.

14. If you have only installed a Management Server (Module) on this computer, you must specify the name(s) of the machine(s) that will be considered the Master(s).

    a. Enter the IP addresses or resolvable names of all hosts allowed to perform control operations on this host.

    b. Enter a single IP address or resolvable name on each line, then terminate the list with a Ctrl-D or your EOF character.

c. A host name is the name returned by the `hostname` command.

15. The screen will show your entries and ask you for confirmation:

    ```
    Is this correct y/n [y] ?
    ```

    If the list of hosts on the screen is correct, press <Return>. If it is incorrect, type n, and make the necessary corrections.

16. If you have installed only a FireWall-1 gateway module on this computer, specify whether this gateway is a member of a high availability configuration:

    ```
    Would you like to install the High Availability product (y/n) [n] ? n
    ```

    If you answer yes, you must configure the machine's IP and MAC addresses accordingly. See the "Expanding the FW-1 implementation to high availability" chapter in the redbook *CheckPoint VPN-1/Firewall-1 on AIX: A Cookbook for Stand-Alone and High Availability Solutions,* SG24-5492.

17. You are now asked to perform a short random keystroke session. The random data collected in this session will be used for generating Certificate Authority keys.

18. If you are installing a Management Module or a FireWall-1 module, you are asked to specify an authentication password to be used by the Management and FireWall-1 Modules to validate communications between them.

    Enter the same authentication password for all hosts and gateways managed by the same Management Module. For additional information, see "Distributed Configurations" on page 69 of the *VPN-1 & FireWall-1 Administration Guide*.

19. Execute /usr/local/fw1/fw1lic and FW-1 accepts your license:

    ```
    # ./fw1lic
    This is VPN-1(TM) & FireWall-1 Version xxxxxxxxxxxxxxxxxxxxxxxxxxx
    Type  Expiration Ver    Features
    10.10.10.1xxxxxxxxxx4.xcxxxxxxxxxxxxxxxxxxxxx
    motif embed
    License file updated
    #
    ```

20. You have now reached the end of the installation procedure

You still need to customize the firewall start and stop scripts because VPN-1/FireWall-1 does not support controlling ipforwarding on AIX. This fact is documented under the heading "Special Notes for IBM AIX" in the Quick Start Guide. Please read them now unless you have done so already.

For this reason, we need to enable ipforwarding after starting VPN-1/FireWall-1 and disable it before stopping VPN-1/FireWall-1. We created the scripts start-fw1 and stop-fw1 to be used instead of fwstart and fwstop (to prevent them from being used, we removed the execute permissions). This is what we did:

```
# cd /usr/lpp/CPfw1-41/bin/
# chmod -x fwstart fwstop
# ./fwstart
/bin/ksh: ./fwstart: 0403-006 Execute permission denied.
# ./fwstop
/bin/ksh: ./fwstop: 0403-006 Execute permission denied.
#
# mkdir /usr/local/bin
# cd /usr/local/bin
#
# cat > stop-fw1
/usr/sbin/no -o ipforwarding=0
/usr/sbin/no -a | grep ipforwarding
csh -f /usr/lpp/CPfw1-41/bin/fwstop
CTRL-D
#
# cat > start-fw1
csh -f /usr/lpp/CPfw1-41/bin/fwstart
/usr/sbin/no -o ipforwarding=1
/usr/sbin/no -a | grep ipforwarding
CTRL-D
# chmod 770 stop-fw1 start-fw1
```

You should also add a line containing /usr/local/bin/start-fw1 to /etc/rc.local to automatically start the firewall in the boot process and test it to ensure that fwstart and fwstop work as expected:

```
# echo "/usr/local/bin/start-fw1" >> /etc/rc.local
# start-fw1
FW-1: driver installed
FireWall-1: Starting fwd
FireWall-1: Starting fwm (Remote Management Server)
fwm: FireWall-1 Management Server is running

FireWall-1: Fetching Security Policy from localhost

Trying to fetch Security Policy from localhost:
Failed to load Security Policy: No State Saved
Fetching Security Policy from local host failed
FireWall-1 started
ipforwarding = 1
```

```
# stop-fw1
ipforwarding = 0
fwm: FireWall-1 Management Server going to die on sig 15
Uninstalling Security Policy from all.all@fw3
Done.
FW-1: driver removed
#
```

At this point, you should back up your system (before proceeding to update FireWall-1). If you have a tape device, and want to create a backup, do the following:

1. Insert a tape that is not write-protected in to the tape drive.
2. Execute:

   ```
   # smitty mksysb
   ```

3. Enter your tape device (for example, /dev/rmt0) and press Enter.

After the backup is done, check if there are any new FireWall-1 service packs or patches available. If there are, install them now. You should follow the installation instructions that came with the service pack as closely as possible.

5.3.1.4 Creating VPN-1/FireWall-1 Security Policies

This section makes you familiar with the VPN-1/FireWall-1 Graphical User Interface (GUI) and shows you the common mistakes that are made while using it to create VPN-1/FireWall-1 Security Policies (also called rule sets). This section does not contain any AIX-specific information.

The following steps only cover the configuring of a basic rule set. It illustrates how to create network objects, modify an initial set of rules, modify the global policy properties, and configure anti-spoofing. The areas not covered are: High Availability, NAT, VPN, Authentication methods, etc. These advanced topics are documented in depth in the redbook *CheckPoint VPN-1/Firewall-1 on AIX: A Cookbook for Stand-Alone and High Availability Solutions,* SG24-5492.

Installation of the VPN-1/FireWall-1 GUI

Now it is time to install the VPN-1/FireWall-1 GUI client software on the GUI workstation.

If you are using a Windows OS (Windows 9x, Windows NT, or Windows 2000), installation is done by executing \windows\CPMgmtClnt\setup.exe on the CD-ROM and clicking the Next button a couple of times. You do not have to reboot your machine. If you have your CD autostart feature enabled, setup.exe will automatically start when you insert the CD into your CD-drive.

All VPN-1/FireWall-1 documentation is provided in PDF format on the VPN-1/FireWall-1 CD-ROM in the \Docs\FireWall-1 directory. You will find the Adobe Acrobat Reader for the supported operating systems in the directory \Docs\PDFRead on the CD-ROM.

It may be a good idea to install the reader and copy the PDF files and the installation directories for later use to the local hard disk of the GUI workstation.

Creating a simple rule set with VPN-1/FireWall-1

This section covers the steps to create a simple rule set for the firewall. The rule set should be kept as short and as simple as possible. This will improve the performance of the firewall and reduce the complexity of the configuration and troubleshooting.

Complete the following steps to create a simple rule set:

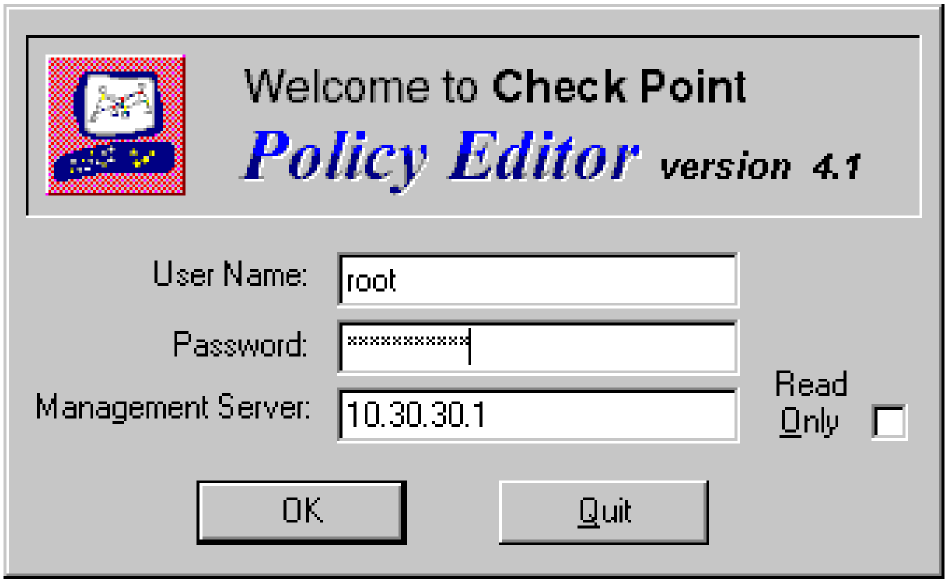
1. Start VPN-1/FireWall-1 on the firewall server with the `start-fw1` command:

   ```
   # start-fw1
   ```

2. Ping the firewall from the GUI workstation:

   ```
   d:\>ping 10.30.30.1
   Pinging 10.30.30.1 with 32 bytes of data:
   Reply from 10.30.30.1: bytes=32 time<10ms TTL=254
   Reply from 10.30.30.1: bytes=32 time<10ms TTL=254
   Reply from 10.30.30.1: bytes=32 time<10ms TTL=254
   Reply from 10.30.30.1: bytes=32 time<10ms TTL=254
   ```

3. Start the FireWall-1 GUI by selecting **Start -> Programs -> CheckPoint Management Clients -> Policy Editor 4.1**.
4. A pop-up box, shown in Figure 51 on page 125, asks you for a User Name, Password, and Management Server. Enter the FireWall-1 administrator account name, password, and the IP address of the firewall.


Welcome to Check Point Policy Editor version 4.1

User Name: root

Password: ************

Management Server: 10.30.30.1

Read Only □

Figure 51. Sign-in panel

5. You get an empty rule base panel. Now, we go step-by-step through adding a first rule that will drop and log everything. This is called the cleanup rule.

6. From the menu bar, select **Edit -> Add Rule -> Bottom**, as shown in Figure 52 on page 126.

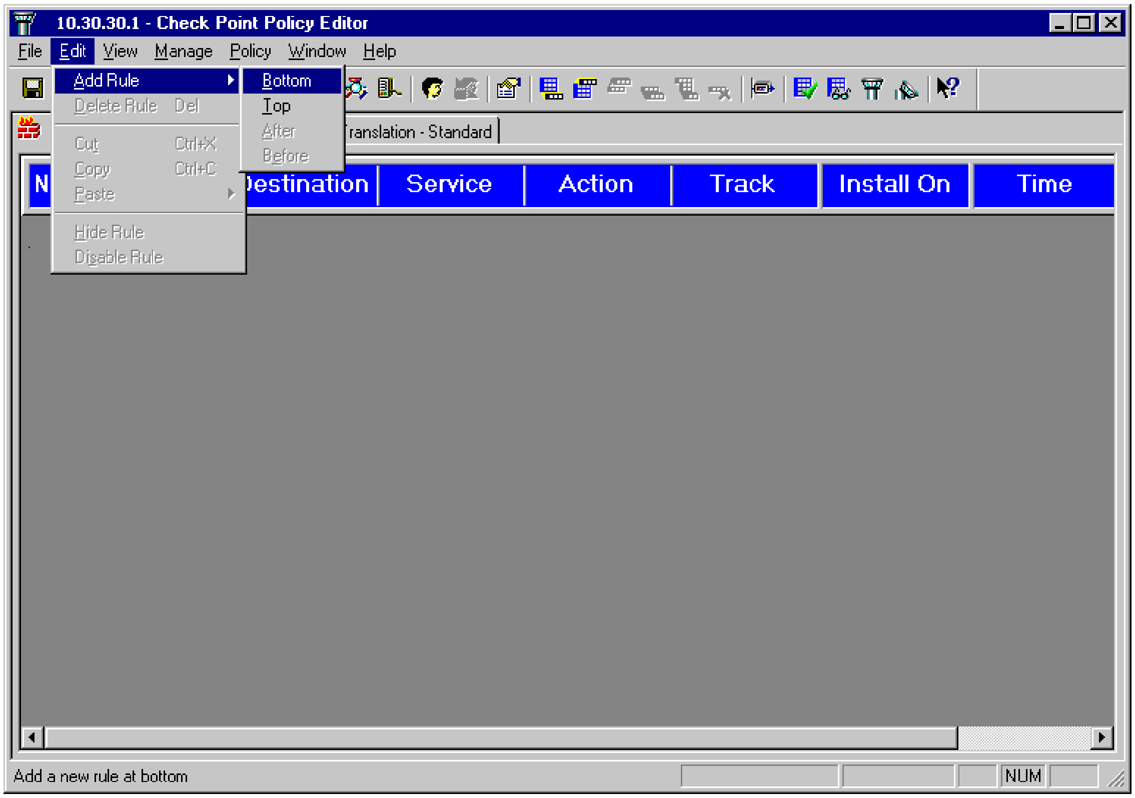


Figure 52. Add first rule

7. See Figure 53 on page 127 on how to right-click in the blank box under TRACK and change the option from blank to Long.

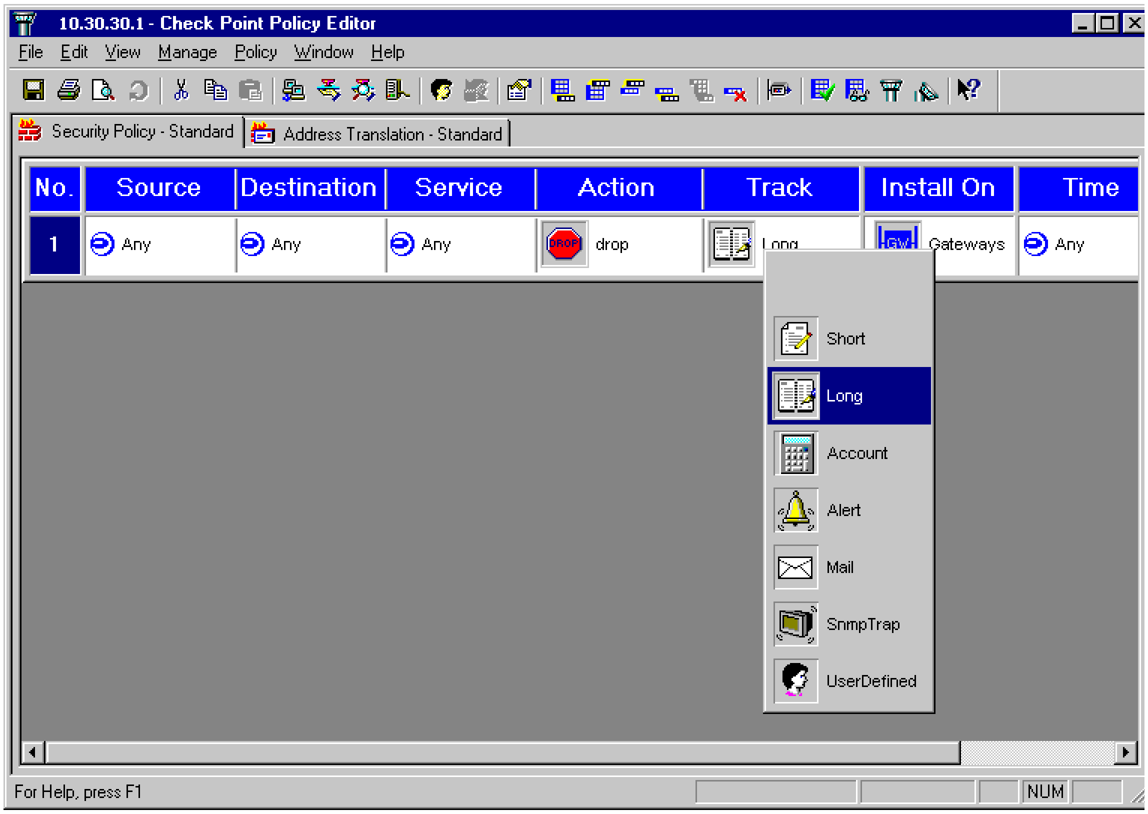


Figure 53. Set Track to LONG

8. Next, Figure 54 on page 128 shows how to create your firewall's network object. From the menu bar, select **Manage -> Network Objects**.

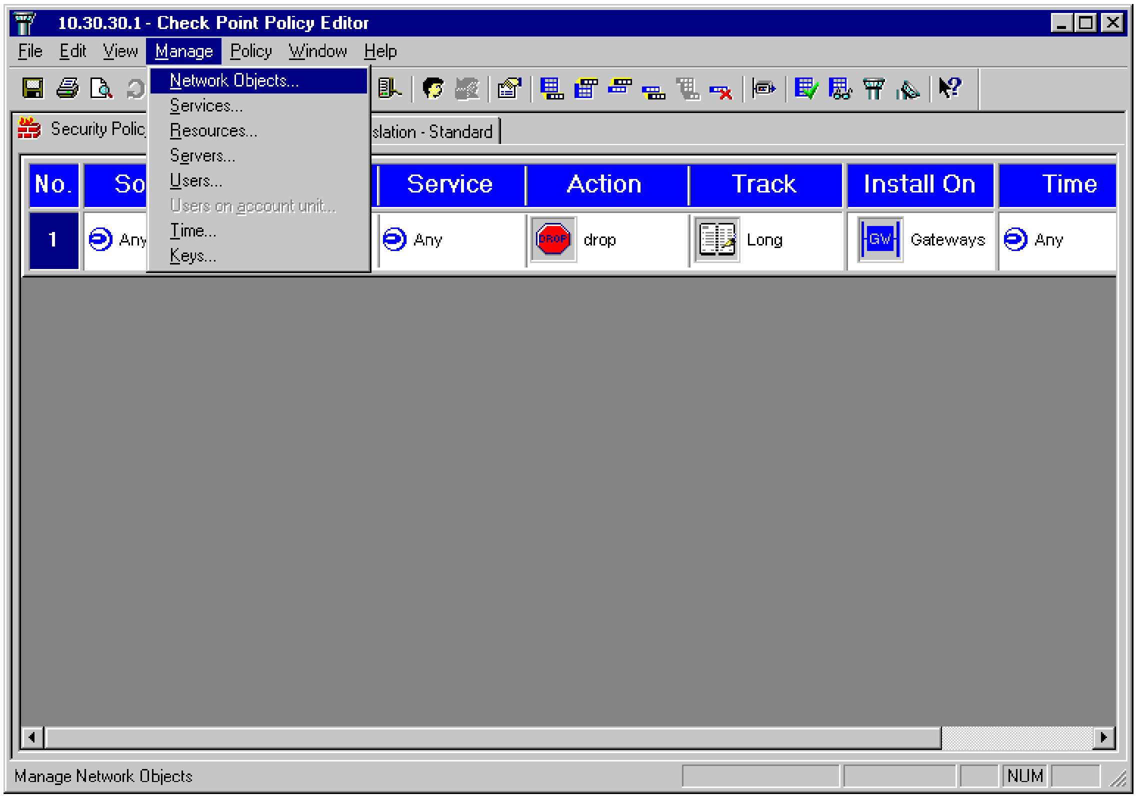


Figure 54. Manage->Network Objects

9. The Network Objects dialog box appears, as seen in Figure 55 on page 129. Select **New -> Workstation**.

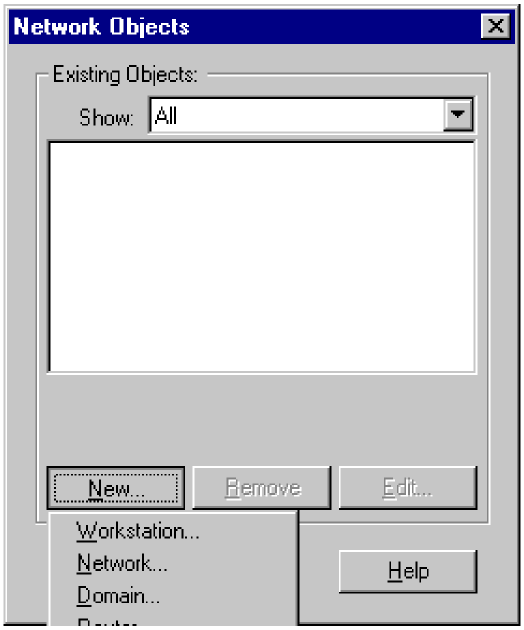
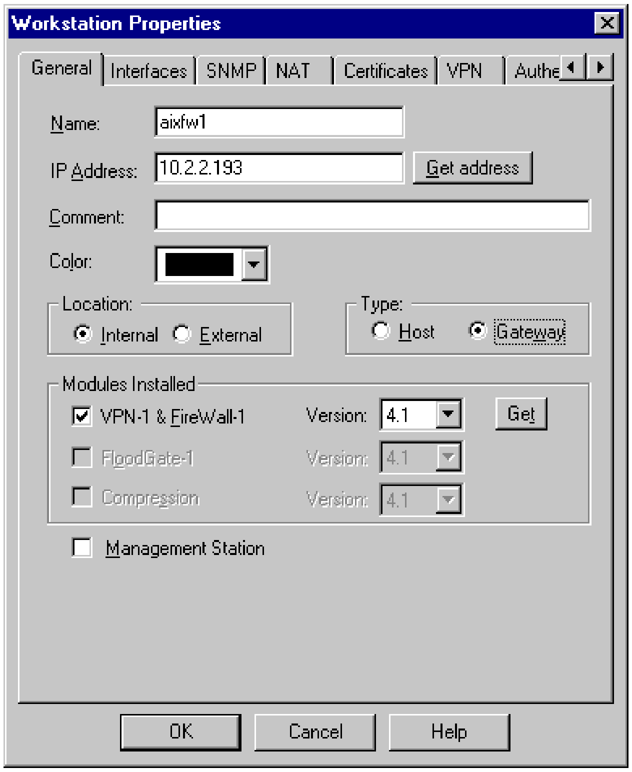


Figure 55. New->Workstation

10. Type in the host name of the firewall in the Name field of the pop-up box. Click the Get Address button. The external IP address of the firewall should automatically appear in the IP Address field. Change the Type: from Host to Gateway. Click on Modules installed: VPN-1 & FireWall-1.

    Please note that Gateway always means some kind of firewall in VPN-1/FireWall-1 terms. It is used in the rules because, by default, rules are installed on gateways. Look in your rule set at the second column from the right. The heading is Install On and your rule selects Gateways.

    At this point, you should put some consideration into the color scheme you wish to use for your network objects. Perhaps green for internal, blue for the DMZ, and red for external. The choices are yours to make, but this makes for easy eye catchers when viewing the rule set.



Name: aixfw1

IP Address: 10.2.2.193

Comment:

Color: ■

Location: ● Internal ○ External

Type: ○ Host ● Gateway

Modules Installed

☑ VPN-1 & FireWall-1 Version: 4.1

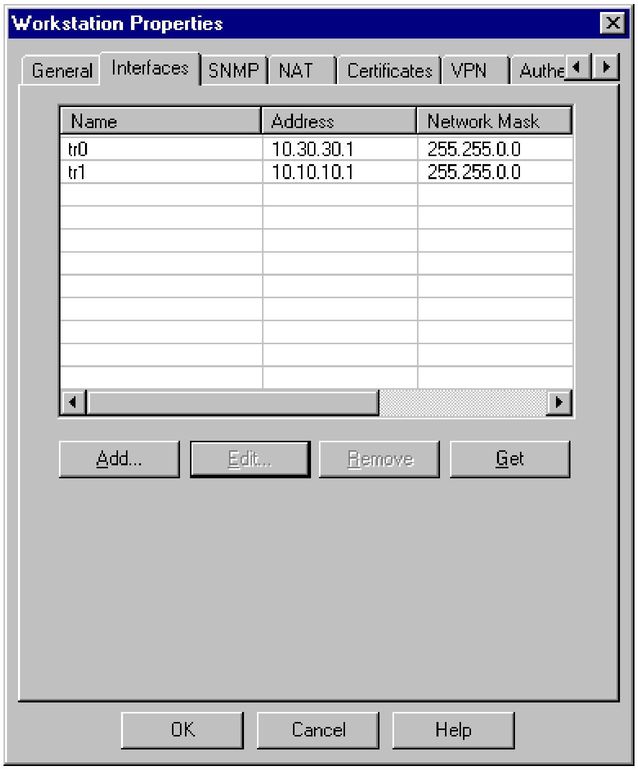
□ FloodGate-1 Version: 4.1

□ Compression Version: 4.1

□ Management Station

Figure 56. Firewall properties

11. Click on the Interfaces Tab. Click on the Get button to retrieve the interface configuration for fw1-snmp. You can configure IP spoofing later (in step 19. on page 137) by double-clicking the interface names. Do not do that now, just click OK.



Name	Address	Network Mask
tr0	10.30.30.1	255.255.0.0
tr1	10.10.10.1	255.255.0.0

Figure 57. Firewall interfaces

12. Take a look at the icon of the firewall gateway object. If it looks different than the one shown in the panel, you either forgot to check the VPN-1 & FireWall-1 modules installed check box or you did not change the type to Gateway. To fix it, click the Edit button and make the necessary changes. If it looks OK, then click Close.

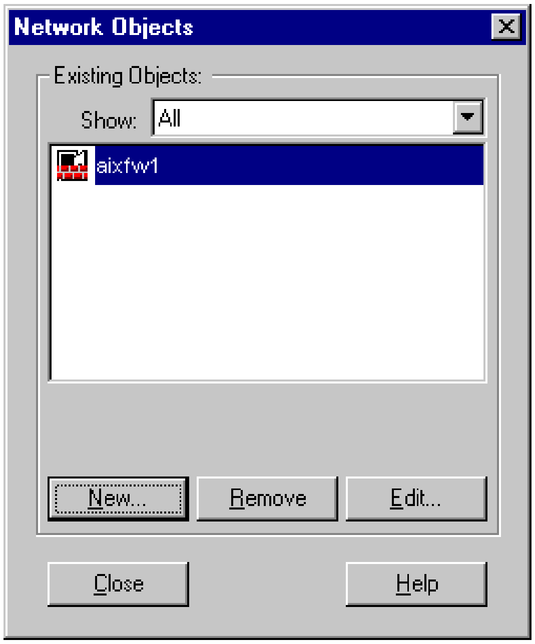


Figure 58. Network objects

13. Next, look at the menu and click on **Policy -> Install**, as shown in Figure 59 on page 133.

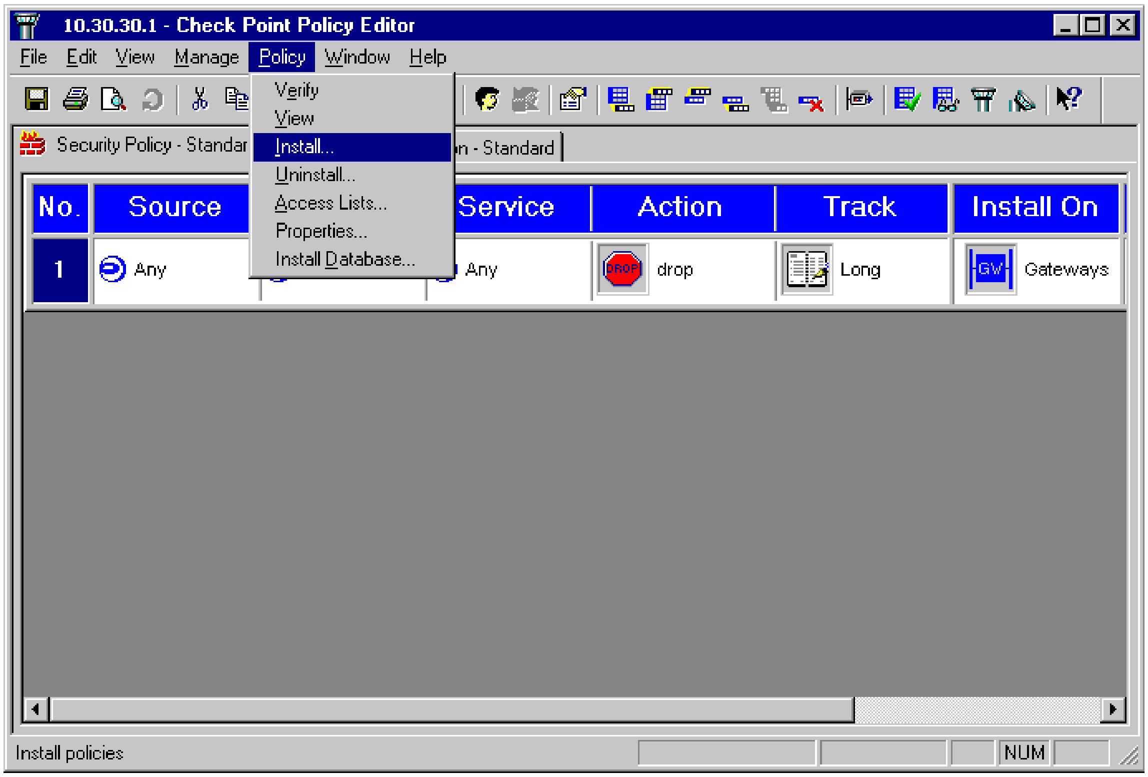
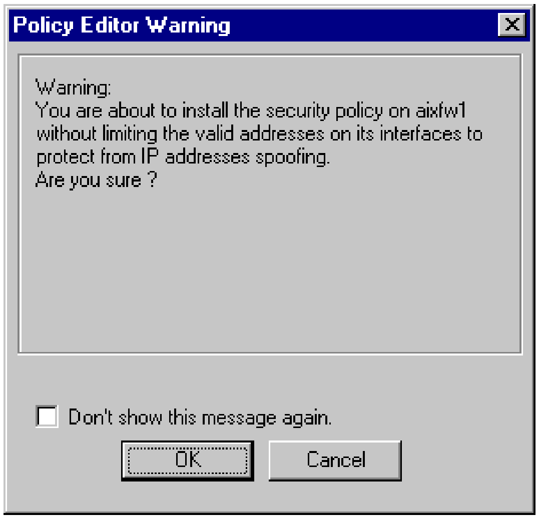


Figure 59. Policy install

14. You will get a warning message that you did not edit the implied security policy properties, which are a real security threat. You will have to take care of this later, but for now click OK.

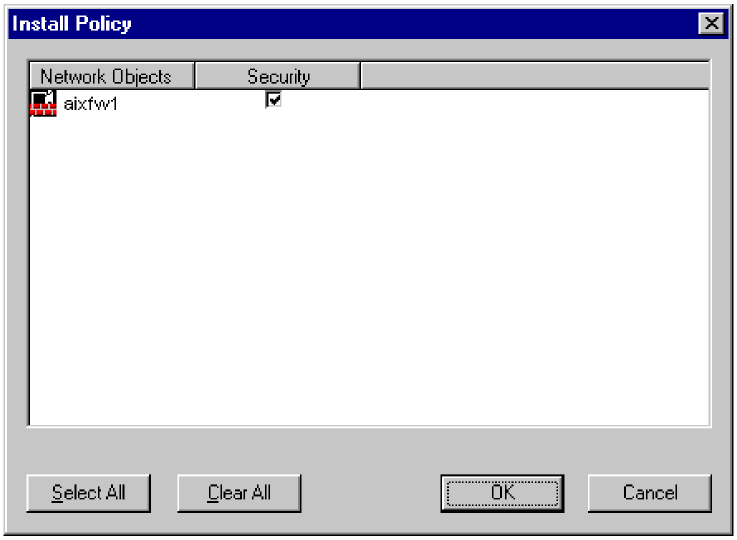


Policy Editor Warning

Warning:
You are about to install the security policy on aixfw1
without limiting the valid addresses on its interfaces to
protect from IP addresses spoofing.
Are you sure ?

Figure 60. Policy editor warning

15. You are shown the list of gateways that your security policy will be installed to. If your firewall does not show up, you probably forgot to change its type from host to gateway. Click OK to install the security policy.

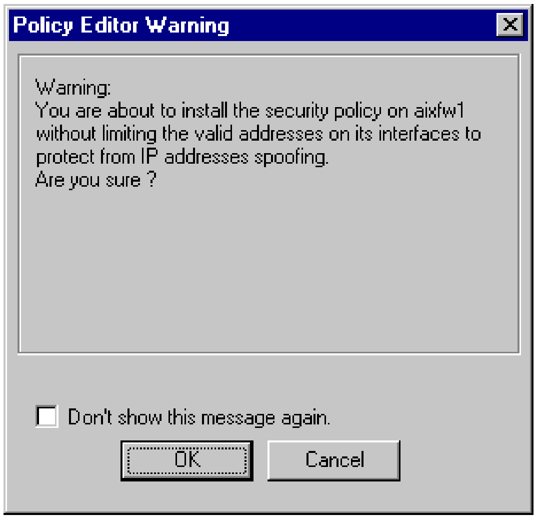


Install Policy

Network Objects	Security
aixfw1	☑

Figure 61. Install policy

16. You will get another warning that you are not secured against IP spoofing. You have to take care of this also, but not now. Click OK.

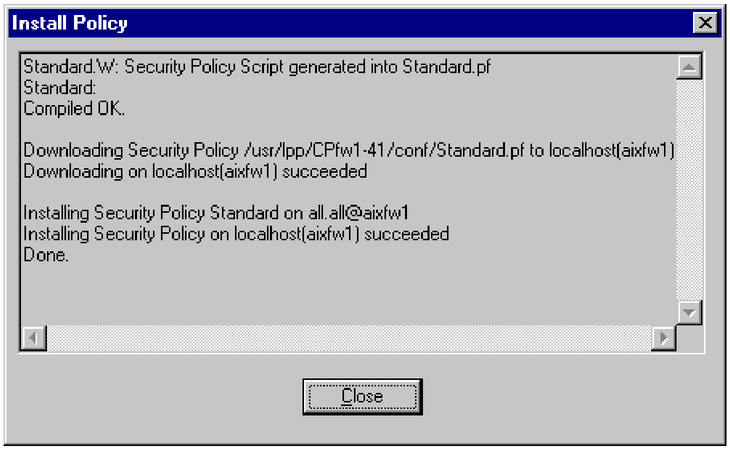


Warning:
You are about to install the security policy on aixfw1 without limiting the valid addresses on its interfaces to protect from IP addresses spoofing.
Are you sure ?

☐ Don't show this message again.

Figure 62. Spoofing warning

17. Your security policy is being compiled and then installed on the VPN-1/FireWall-1 module. Notice how the button changes from Abort to Close. Do not click it before it changes to Close or you will stop the installation of the policy.



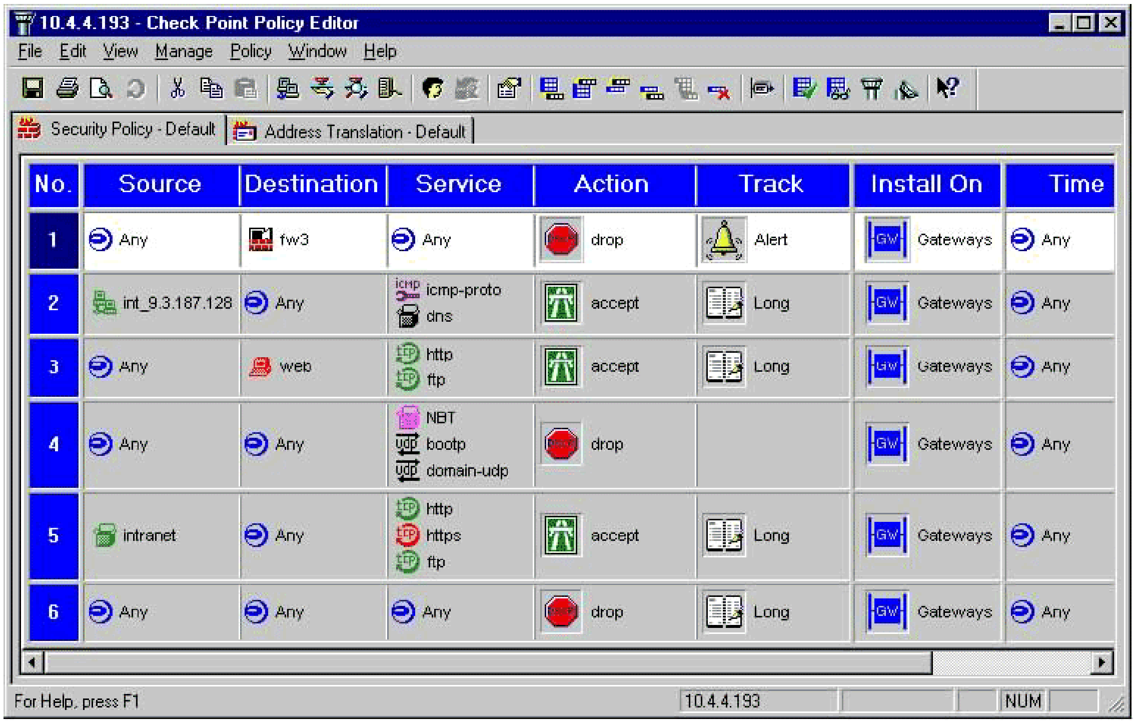
```
Standard.W: Security Policy Script generated into Standard.pf
Standard:
Compiled OK.

Downloading Security Policy /usr/lpp/CPfw1-41/conf/Standard.pf to localhost(aixfw1)
Downloading on localhost(aixfw1) succeeded

Installing Security Policy Standard on all.all@aixfw1
Installing Security Policy on localhost(aixfw1) succeeded
Done.
```

Figure 63. Policy installation complete

18. A simple firewall rule set is shown in Figure 64 on page 136.


10.4.4.193 - Check Point Policy Editor
File Edit View Manage Policy Window Help
Security Policy - Default
Address Translation - Default
For Help, press F1
10.4.4.193
NUM

No.	Source	Destination	Service	Action	Track	Install On	Time
1	Any	fw3	Any	drop	Alert	Gateways	Any
2	int_9.3.187.128	Any	icmp-proto dns	accept	Long	Gateways	Any
3	Any	web	http ftp	accept	Long	Gateways	Any
4	Any	Any	NBT bootp domain-udp	drop		Gateways	Any
5	intranet	Any	http https ftp	accept	Long	Gateways	Any
6	Any	Any	Any	drop	Long	Gateways	Any

Figure 64. Sample rule set

Where:

Rule 1: The stealth rule. It prevents any users (internal or external) from connecting to the firewall. Protecting the firewall in this manner makes it transparent. In most cases the stealth rule, in order to fully protect your firewall from port scanning, should be placed above all other rules. However, authentication and encryption rules always go above the stealth rule.

Rule 2: Any internal user or server can do an external ping or DNS lookup.

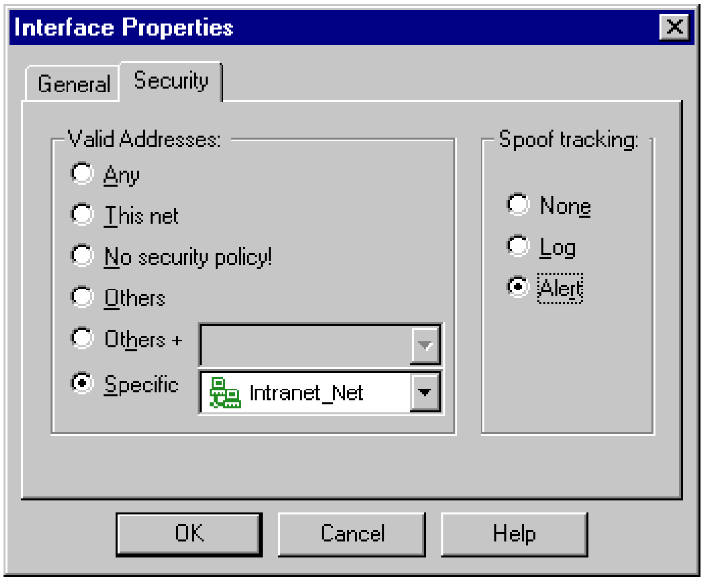
Rule 3: Any user (internal or external) can access the internal Web server (in the DMZ).

Rule 4: Any NetBIOS, bootp, or domain-UDP packets are explicitly dropped and not logged. This removes unwanted entries in the log viewer.

Rule 5: Intranet users can access any Internet hosts via http, https, and ftp. Surfing is allowed.

Rule 6: Cleanup rule. Any communication packets that are not accepted, dropped, or rejected by the prior rules are explicitly dropped and logged.

19. Configure anti-spoofing by double-clicking (or click on Edit, as seen in step 11. on page 130). Click on the Security tab and you will see Figure 65 below. Modify the Valid Addresses entries. FireWall-1 examines the incoming packets to validate that these addresses are valid for the network from which they come. Also, select the Alert radio button to allow alert messages to pop up on the administrator GUI.



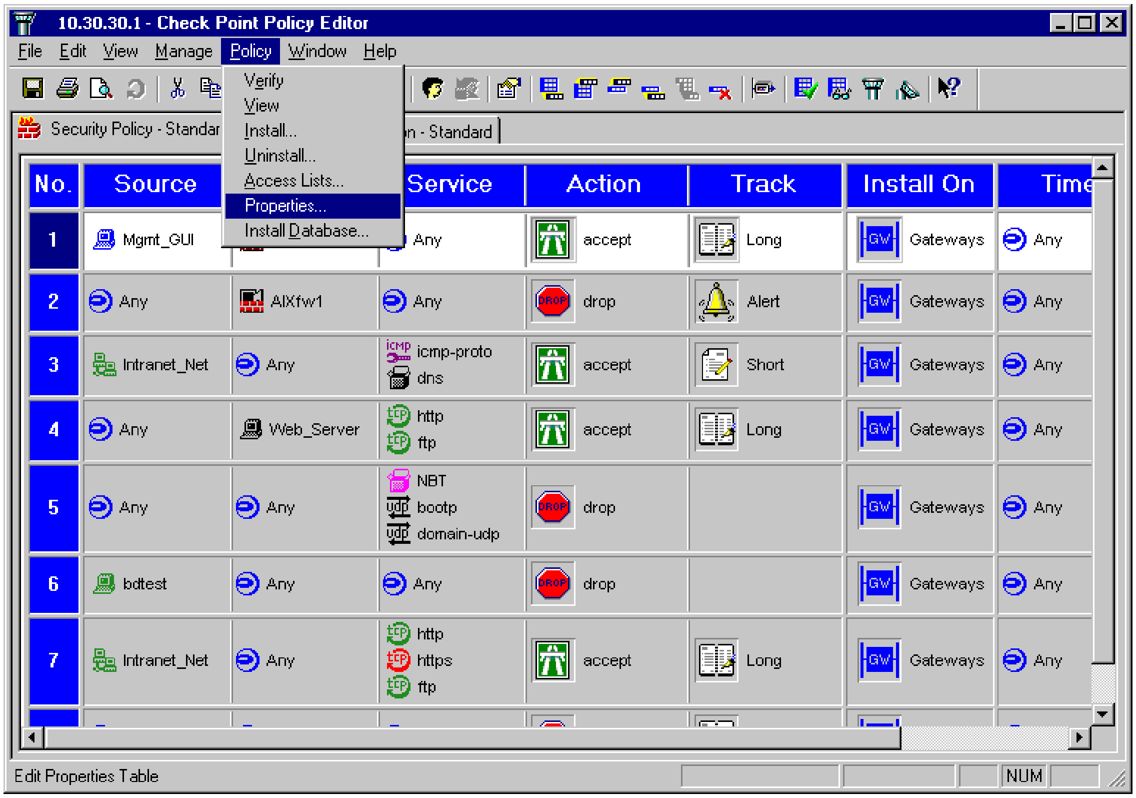
Interface Properties

Valid Addresses:
○ Any
○ This net
○ No security policy!
○ Others
○ Others +
● Specific: Intranet_Net

Spoof tracking:
○ None
○ Log
● Alert

Figure 65. Interface properties

20. Some of the Policy Properties should be modified. From the Menu bar, select **Policy->Properties**, as shown in Figure 66 on page 138.



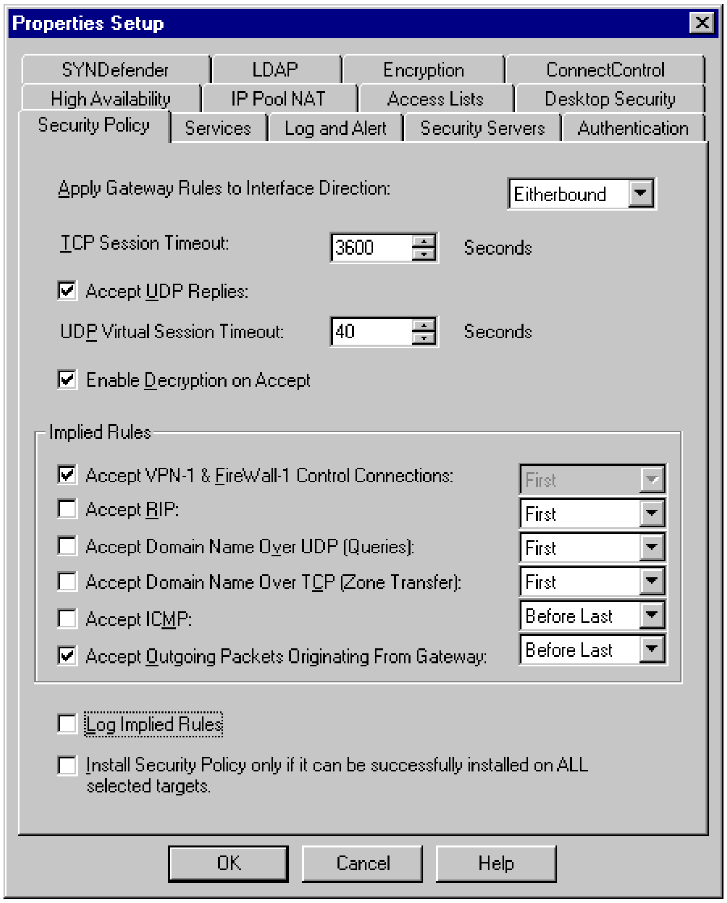
No.	Source		Service	Action	Track	Install On	Time
1	Mgmt_GUI		Any	accept	Long	Gateways	Any
2	Any	AIXfw1	Any	drop	Alert	Gateways	Any
3	Intranet_Net	Any	icmp-proto dns	accept	Short	Gateways	Any
4	Any	Web_Server	http ftp	accept	Long	Gateways	Any
5	Any	Any	NBT bootp domain-udp	drop		Gateways	Any
6	bdtest	Any	Any	drop		Gateways	Any
7	Intranet_Net	Any	http https ftp	accept	Long	Gateways	Any

Figure 66. Policy properties

21. Modify the Security Policy as appropriate, as shown in Figure 67 on page 139. Some suggestions are:

    a. Change Apply Gateway Rules to Interface Direction to Inbound (Eitherbound examines packet both into and out of the firewall).

    b. Select Log Implied Rules.



Apply Gateway Rules to Interface Direction: Eitherbound

TCP Session Timeout: 3600 Seconds

☑ Accept UDP Replies:

UDP Virtual Session Timeout: 40 Seconds

☑ Enable Decryption on Accept

Implied Rules

☑ Accept VPN-1 & FireWall-1 Control Connections: First

□ Accept RIP: First

□ Accept Domain Name Over UDP (Queries): First

□ Accept Domain Name Over TCP (Zone Transfer): First

□ Accept ICMP: Before Last

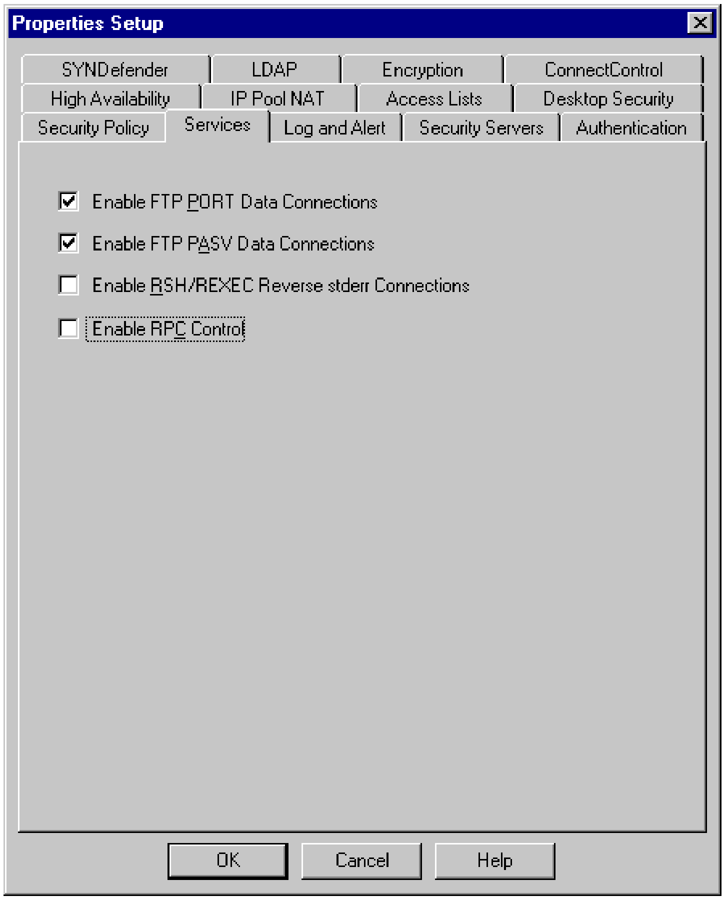
☑ Accept Outgoing Packets Originating From Gateway: Before Last

□ Log Implied Rules

□ Install Security Policy only if it can be successfully installed on ALL selected targets.

Figure 67. Properties setup - Security Policy tab

22. Click the Services tab and modify as appropriate, as shown in Figure 68 on page 140. A suggestion is to remove the check box beside Enable RPC Control when you do not have DCE RPC components communicating through the firewall.



☑ Enable FTP PORT Data Connections

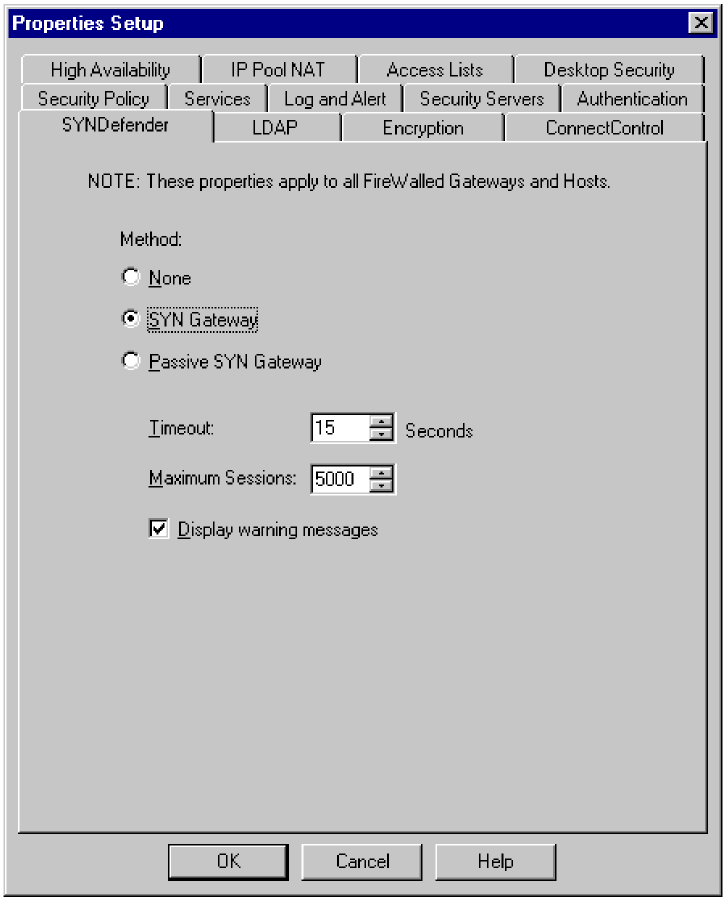
☑ Enable FTP PASV Data Connections

□ Enable RSH/REXEC Reverse stderr Connections

□ Enable RPC Control

Figure 68. Properties setup - Services tab

23. Click the SYNDefender tab. Select either SYN Gateway or Passive SYN Gateway and modify the Timeout and Maximum Sessions fields as appropriate, as shown in Figure 69 on page 141. For further information, see "What is a TCP SYN Flooding Attack?" on page 617 of the *VPN-1/FireWall-1 Administration Guide.* Click OK.



NOTE: These properties apply to all FireWalled Gateways and Hosts.

Method:

○ None

● SYN Gateway

○ Passive SYN Gateway

Timeout: 15 Seconds

Maximum Sessions: 5000

☑ Display warning messages

Figure 69. Properties setup SYNDefender tab

Access violation

If you try to login with the FireWall-1 GUI, and you get the following error message in a pop-up box:

```
Someone else (root@gui) is using FireWall-1 Security Policy Editor -
Information is locked. You can either retry connecting when root@gui
using fwm logs out, or login again in read-only mode.
```

then either somebody else is already logged in or the lock file for the management access was not correctly removed (for example, the VPN-1/FireWall-1 GUI client unexpectedly died when the GUI workstation rebooted or crashed for some reason).

After you make sure that there is nobody else logged in, you can manually delete the /usr/lpp/CPfw1-41/log/manage.lock file with `rm` and log in again

5.3.2 Installing the Risk Manager adapter

The next section talks about how the CheckPoint adapter and the Risk Manager Event Integration Facility can be installed in two different ways, depending on the configuration of the actual machine:

- Non-TME method

  If the machine is not part of a Tivoli managed region, we have to install the software manually.

- TME based method

  If the machine is configured as a Tivoli endpoint in a Tivoli managed region, the software has to be distributed using the Tivoli Software Installation Services (SIS) method and the adapter will be configured using the Tivoli Adapter Configuration Facility (ACF).

Both approaches will be described here. The non-TME based method describes all the necessary steps to set up and configure the components. The TME based method starts with the installation of the Tivoli endpoint software and then briefly describes how to deploy the components using Tivoli SIS.

5.3.2.1 Non-TME method

The Risk Manager adapter for CheckPoint Firewall-1 is installed on a Windows NT platform. This is because the OPSEC LEA it uses to read the logs from the firewall is available on NT and Solaris only, not AIX.

The adapter uses the Risk Manager Event Integration Facility APIs (RMEIF) to send Risk Manager-related events to the TEC Event Server. Both the Risk Manager CheckPoint adapter and the RMEIF must be installed on the same machine and in the same directory. A utility to decompress .zip files is required.

The minimum service level for the Windows NT machine is SP5.

The CheckPoint adapter will forward to the event server ONLY those firewall log entries that are identified as ALERT. That is to say, if you want log entries generated by a firewall rule to appear in the Event Server, the TRACK option of the rule must be ALERT, not just LONG or SHORT.

Note

The NT machine must be hardened following current "best practices." Leaving known vulnerabilities uncorrected will expose your systems to abuse. Secure this machine as you would the firewall itself.

The adapter enables the Risk Manager to send Suspicious Activity Monitor (SAM) commands to the firewall to closely monitor or block traffic. You have to protect the environment against unauthorized use of the SAM function. It could be used against the firewall as an effective Denial of Service tool.

Before installing the adapter, be sure to add a rule to the CheckPoint Firewall-1 rule base to allow the SAM and LEA services. The rule should have the following parameters:

Source	Risk Manager adapter
Destination	Firewall
Service	FW1_sam and FW1_lea

To actually install the adapter, follow these steps:

1. Log on to the NT machine with a user ID that has Administrator authority.
2. Open a command panel and create a directory to hold all the adapter-related files, then `cd` to that directory:

   ```
   C:\>mkdir \target_dir
   C:\>cd \target_dir
   C:\target_dir>
   ```

   Leave the command panel open.

3. Put the Tivoli Secure Way Risk Manager CD-ROM in the Windows NT machine and, using Windows Explorer, navigate to the RMadapters sub-directory.

4. Unzip the rmeif_nt_non_TME.zip and cpfw_nt.zip files from the RMadapters subdirectory, in that order, into the target_dir directory. When unzipping cpfw_nt.zip, allow pre-existing files in the target_dir directory to be replaced.

5. In the command panel, run the configuration scripts for EIF and the CheckPoint adapter in this order:

   ```
   C:\target_dir>rma_eif-cfg.cmd
   C:\target_dir>rma_cpfw-cfg.cmd
   Attempting to install service: rma_cpfw
   Service installed: rma_cpfw
   The Risk Manager CheckPoint FW-1 Adapter service is starting.
   The Risk Manager CheckPoint FW-1 Adapter service was started
   successfully.

   C:\target_dir>
   ```

   Navigate to **Start>Settings>Control Panel>Services**. Scroll down to the Risk Manager Common Adapter and change the start method from Manual to Automatic.

6. Edit \target_dir\bin\w32-ix86\RISKMGR\adapters\etc\rmad.conf. On the line that begins ServerLocation, replace the text @EventServer with the IP address of the Event Server. Then add the ConnectionMode line. See page 135 of the *Risk Manager User's Guide* for details about the ConnectionMode. Basically, you want to specify "connection_oriented," which causes the EIF to use a single TCP session to send firewall log records to the Risk manager server rather than one TCP session per record.

   Edit as follows:

   ```
   ServerLocation=x.x.x.x
   ConnectionMode=connection_oriented
   EventMaxSize=4096
   RmadLogging=NO
   ```

   where x.x.x.x is the IP address of the Risk Manager Event Server

7. Edit \target_dir\bin\w32-ix86\RISKMGR\adapters\etc\rma_cpfw.conf. The following lines should appear in the file; others should be removed or commented out by placing a # in the first column:

   ```
   lea_server ip x.x.x.x
   lea_server auth_port 18184
   ```

```
lea_server auth_type auth_opsec

sam_server ip x.x.x.x
sam_server auth_port 18183
sam_server auth_type auth_opsec
```

where x.x.x.x is the secure interface of the firewall.

8. On the firewall, edit $FWDIR/conf/fwopsec.conf. The following lines should appear in the file; others should be removed or commented out by placing a # in the first column:

```
lea_server auth_port 18184
lea_server auth_type auth_opsec

sam_server auth_port 18183
sam_server auth_type auth_opsec

sam_allow_remote_requests yes
```

9. On the firewall, issue these commands to set the security keys for communication with the RM adapter on the NT machine:

```
# fw putkey -opsec x.x.x.x
Enter secret key: yyyyyyyy
Again secret key: yyyyyyyy
#
```

Where x.x.x.x is the IP address of the NT machine and yyyyyyyy is a key of your choice. The key must be at least 6 characters long.

10. On the Windows NT machine, issue these commands to complete the setup of keys for communication between the RM adapter and the firewall:

```
c:\>cd \target_dir\bin\w32-ix86\RISKMGR\adapters\etc
c:\target_dir\bin\w32-ix86\RISKMGR\adapters\etc>..\bin\opsec_putkey
x.x.x.x
Please enter secret key: yyyyyyyy
Please enter secret key again: yyyyyyyy
OPSEC: Received new control security key from x.x.x.x
Authentication with x.x.x.x initialized

c:target_dir\bin\w32-ix86\RISKMGR\adapters\etc\>
```

Where x.x.x.x is the IP address of the secure interface of the firewall and yyyyyyyy is the same key used with the `fw putkey -opsec` command.

Note

One result of this step is the creation of a file called authkeys.C. When the step is finished verify that authkeys.C is in the \target_dir\bin\w32-ix86\RISKMGR\ adapters\etc directory. It *must* be in that directory or the adapters will not work. If it is not, you did not run the `../bin/opsec_putkey` command while the current directory was \target_dir\bin\w32-ix86\RISKMGR\adapters\etc, as specified in the first two commands of this step. Redo step 9. on page 145 (where you issue the `fw putkey` command in AIX) and this time, ensure that you are in the correct directory on the NT machine.

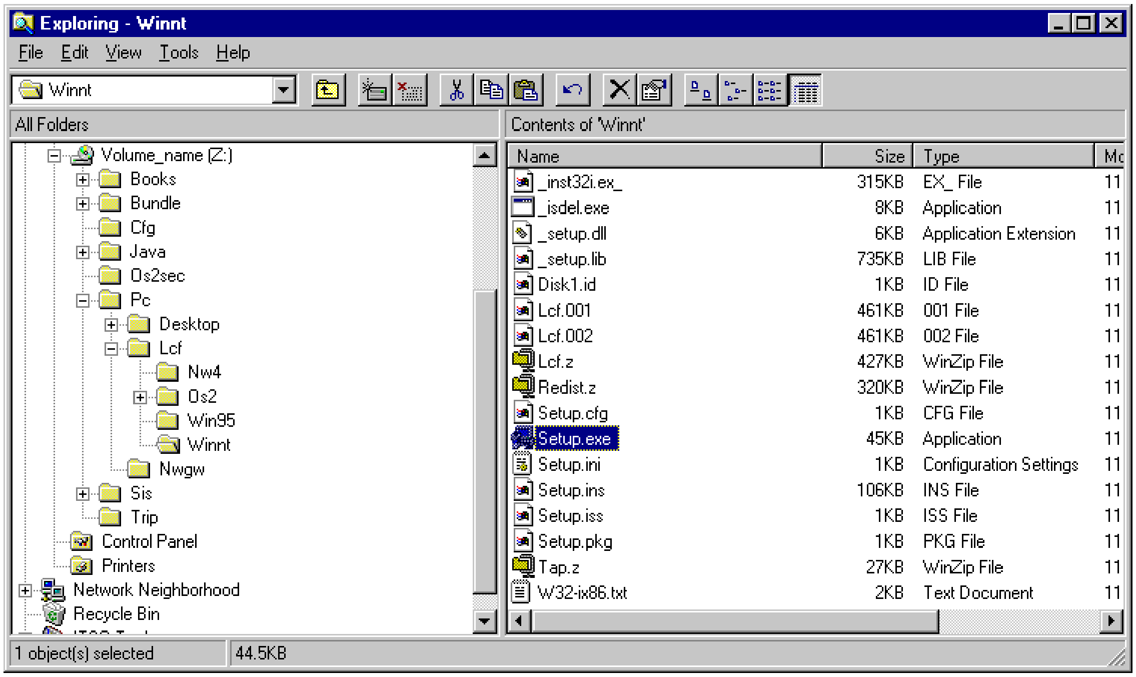
5.3.2.2 Installation steps for the Tivoli endpoint

Note

Before you begin installation, ensure all host names and IP addresses are resolvable through facilities like DNS or hosts files (/etc/hosts for AIX or c:\winnt\system32\drivers\etc\hosts for NT).

The installation steps for the Tivoli Endpoint are as follows:

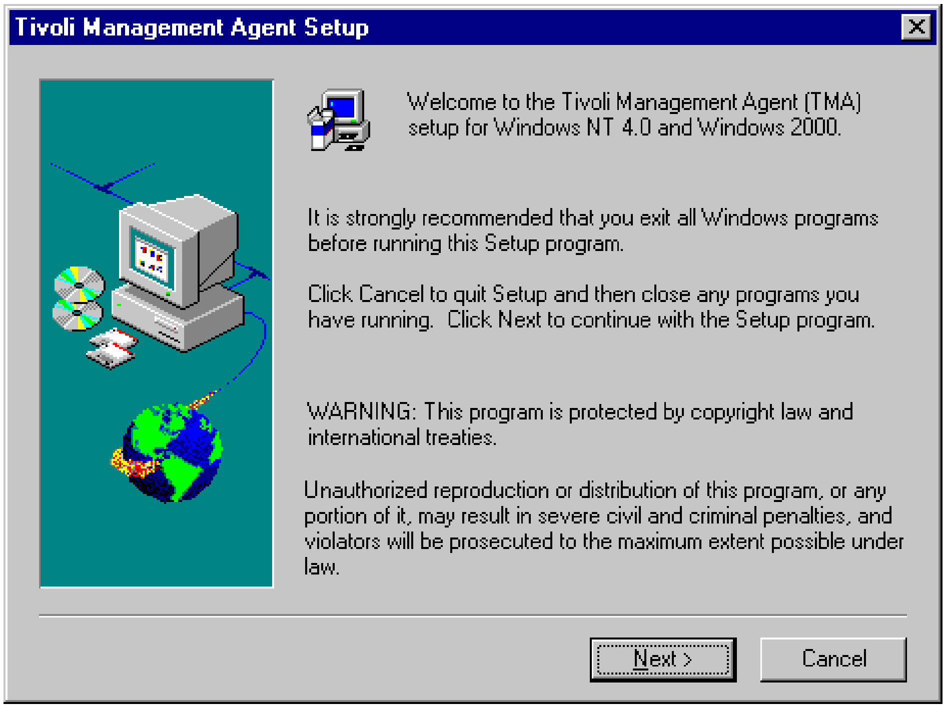
1. Log on to the Windows NT machine with a user ID that has Administrator authority.
2. Put the Tivoli Management Framework CD-ROM in the NT machine and, using Windows Explorer, navigate to the CD's PC\Lcf\Winnt sub-directory. Double-click the Setup.exe file to begin the Installation (see Figure 70 on page 147).



Name	Size	Type	Mc
inst32i.ex	315KB	EX_ File	11
_isdel.exe	8KB	Application	11
_setup.dll	6KB	Application Extension	11
_setup.lib	735KB	LIB File	11
Disk1.id	1KB	ID File	11
Lcf.001	461KB	001 File	11
Lcf.002	461KB	002 File	11
Lcf.z	427KB	WinZip File	11
Redist.z	320KB	WinZip File	11
Setup.cfg	1KB	CFG File	11
Setup.exe	45KB	Application	11
Setup.ini	1KB	Configuration Settings	11
Setup.ins	106KB	INS File	11
Setup.iss	1KB	ISS File	11
Setup.pkg	1KB	PKG File	11
Tap.z	27KB	WinZip File	11
W32-ix86.txt	2KB	Text Document	11

Figure 70. CD-ROM image

3. Click Next on the panel titled Tivoli Management Agent Setup (see Figure 71 on page 148).



Welcome to the Tivoli Management Agent (TMA) setup for Windows NT 4.0 and Windows 2000.

It is strongly recommended that you exit all Windows programs before running this Setup program.

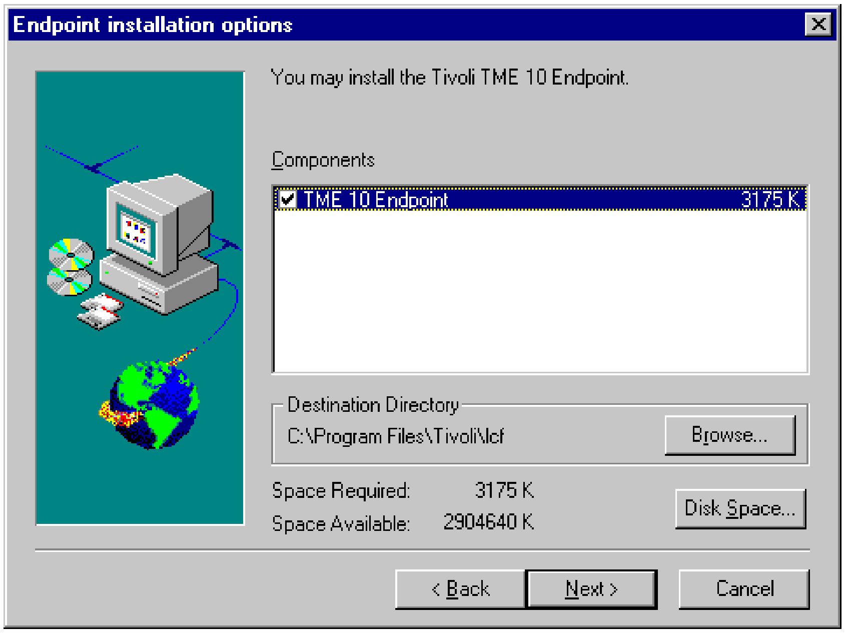
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and violators will be prosecuted to the maximum extent possible under law.

Figure 71. First setup panel

4. On the License Agreement panel, click Next.
5. You *must* change the Destination Directory on the Endpoint installation options panel (see Figure 72 on page 149). Click Browse.



Endpoint installation options

You may install the Tivoli TME 10 Endpoint.

Components

☑ TME 10 Endpoint 3175 K

Destination Directory

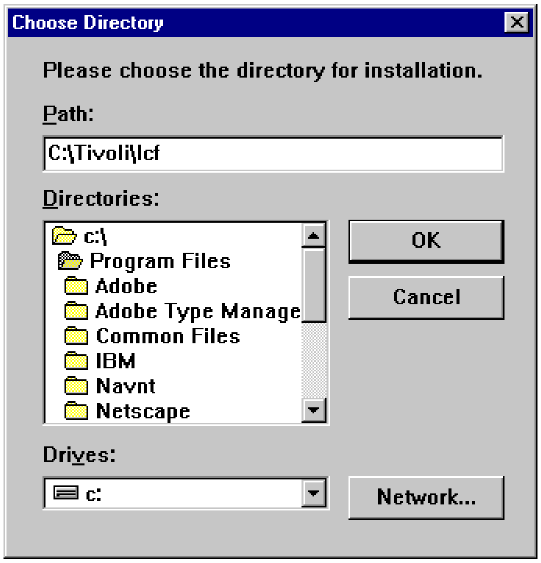
C:\Program Files\Tivoli\lcf

Space Required: 3175 K

Space Available: 2904640 K

Figure 72. Installation options

A panel appears on which you select the Path for the installation directory. Remove the Program Files portion of the suggested file name so that the path is C:\Tivoli\lcf. Click OK.



Choose Directory

Please choose the directory for installation.

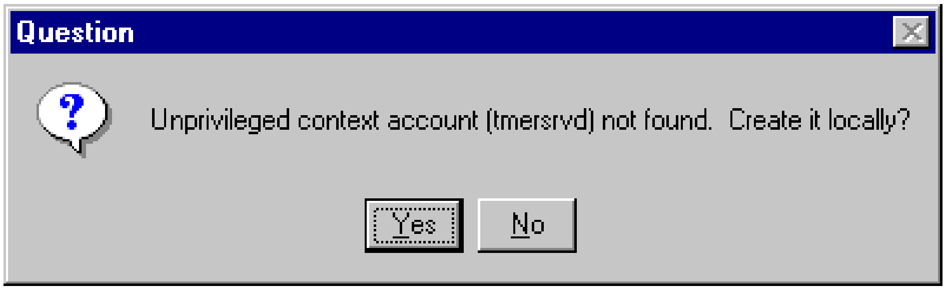
Path: C:\Tivoli\lcf

Directories:

Drives: c:

Figure 73. Installation directory

6. Answer Yes to the question "The directory C:\Tivoli\lcf does not exist. Do you want the directory to be created?"
7. Click Yes on the next panel (see Figure 74).

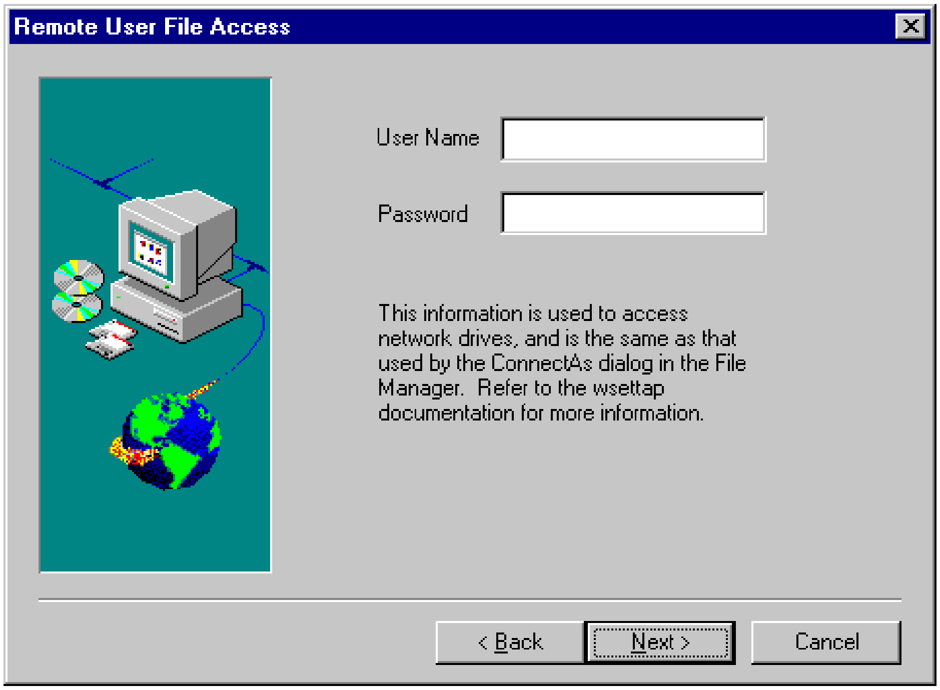


Question

Unprivileged context account (tmersrvd) not found. Create it locally?

Figure 74. Unprivileged context account question

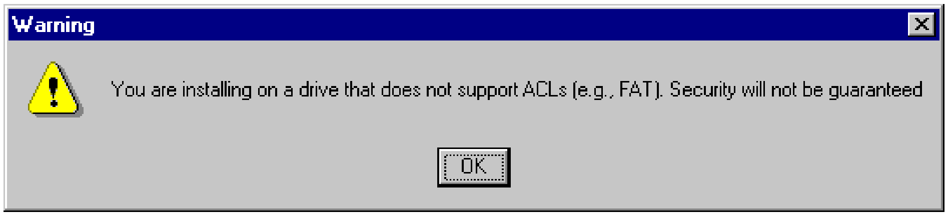
8. Leave the User Name and Password fields blank on the Remote User File Access panel (see Figure 75 on page 151). Click Next.



This information is used to access network drives, and is the same as that used by the ConnectAs dialog in the File Manager. Refer to the wsettap documentation for more information.

Figure 75. Remote user panel

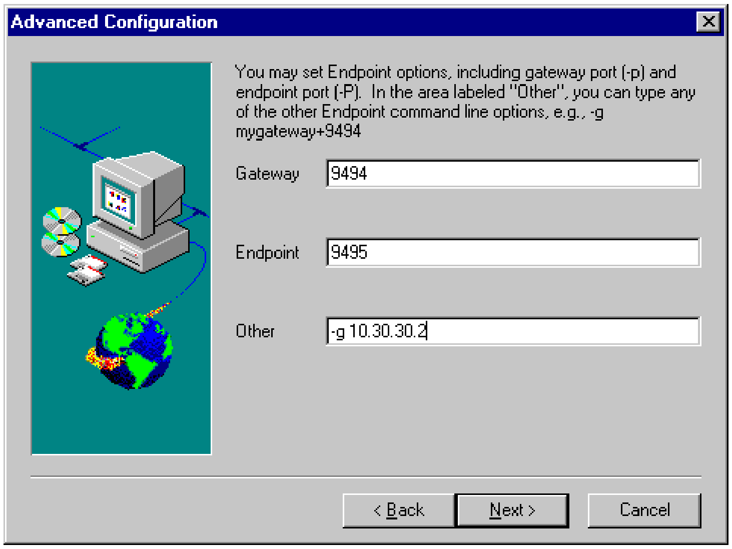
9. If you are installing on a drive formatted as FAT, you will see the panel shown in Figure 76. Click OK.



You are installing on a drive that does not support ACLs (e.g., FAT). Security will not be guaranteed

Figure 76. No ACLs warning panel

10. The Advanced Configuration panel will appear as shown in Figure 77 on page 152. In the Other field, type -g x.x.x.x where x.x.x.x is the IP address of the Tivoli Gateway. Click Next.



Advanced Configuration

You may set Endpoint options, including gateway port (-p) and endpoint port (-P). In the area labeled "Other", you can type any of the other Endpoint command line options, e.g., -g mygateway+9494

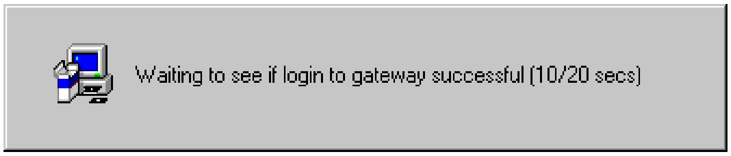
Gateway: 9494

Endpoint: 9495

Other: -g 10.30.30.2

Figure 77. Advanced configuration panel

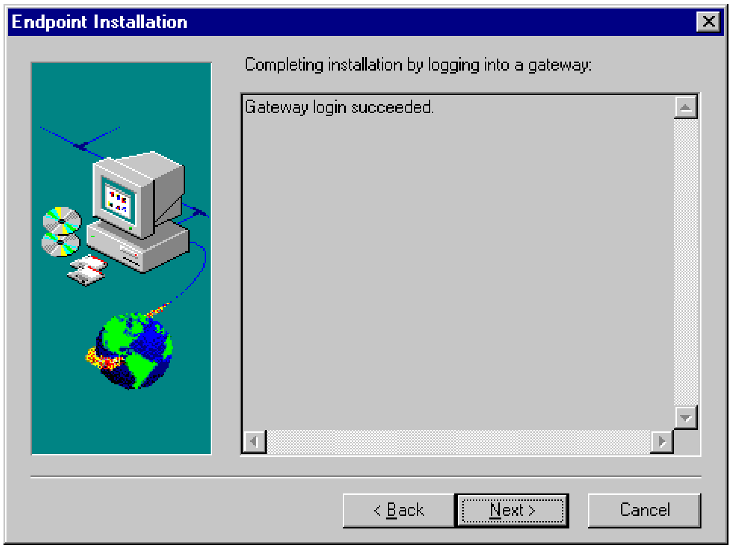
11. The panel in Figure 78 will appear, indicating that the endpoint is trying to connect to the Tivoli Gateway.



Waiting to see if login to gateway successful (10/20 secs)

Figure 78. Login attempt panel

A few seconds later the panel in Figure 79 on page 153 will appear if the connection was successful. Click Next.

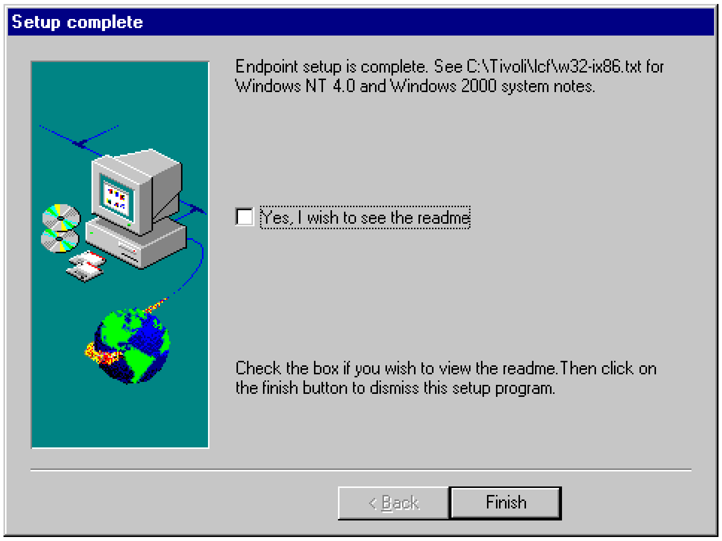

Endpoint Installation

Completing installation by logging into a gateway:

Gateway login succeeded.

Figure 79. Connection successful

12. Click **Finish** (see Figure 80).


Setup complete

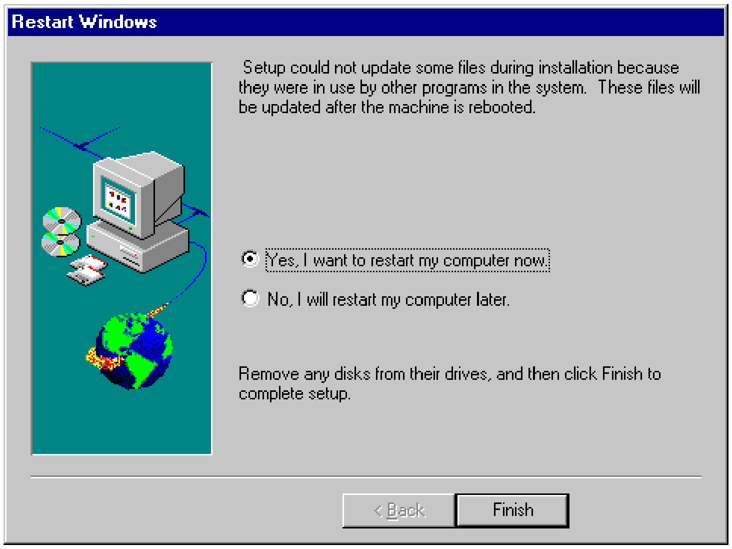
Endpoint setup is complete. See C:\Tivoli\lcf\w32-ix86.txt for Windows NT 4.0 and Windows 2000 system notes.

□ Yes, I wish to see the readme

Check the box if you wish to view the readme. Then click on the finish button to dismiss this setup program.

Figure 80. Setup complete

13. The Windows NT machine must be restarted. Click Yes then Finish (see Figure 81 on page 154).



Restart Windows

Setup could not update some files during installation because they were in use by other programs in the system. These files will be updated after the machine is rebooted.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

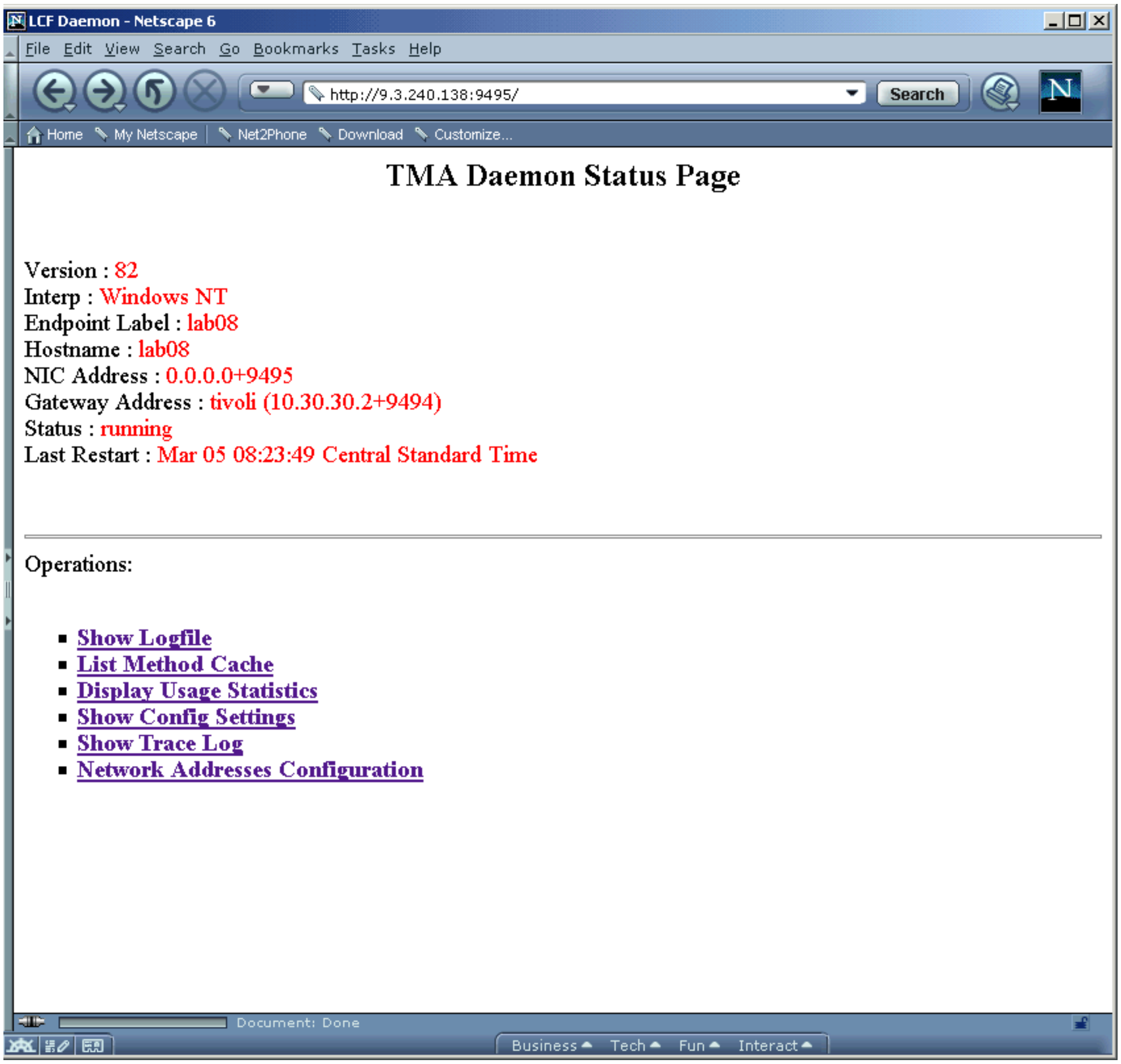
Remove any disks from their drives, and then click Finish to complete setup.

Figure 81. Restart required

14. After rebooting, you can check the status of the endpoint by accessing it with a Web browser. The URL is:

    `http://end_point_ip_address:9495.`

    Note that the Status field should show "running", as shown in Figure 82 on page 155.


LCF Daemon - Netscape 6
File Edit View Search Go Bookmarks Tasks Help
http://9.3.240.138:9495/
Search
Home My Netscape Net2Phone Download Customize...
Document: Done
Business Tech Fun Interact

TMA Daemon Status Page

Version : 82
Interp : Windows NT
Endpoint Label : lab08
Hostname : lab08
NIC Address : 0.0.0.0+9495
Gateway Address : tivoli (10.30.30.2+9494)
Status : running
Last Restart : Mar 05 08:23:49 Central Standard Time

Operations:

- Show Logfile
- List Method Cache
- Display Usage Statistics
- Show Config Settings
- Show Trace Log
- Network Addresses Configuration

Figure 82. Web based endpoint status

If you need to reinstall the Tivoli endpoint, first run the uninstall program from the install directory C:\Tivoli\lcf\uninst.bat. Also, the endpoint must be removed from the gateway before the reinstallation is attempted. This is done on the gateway with the command:

```
wdelep end_point_name
```

5.3.2.3 TME-based method

Next, we need to install the CheckPoint Adapter and the Risk Manager EIF using the Tivoli Software Installation Services on the Risk Manager server. Follow these steps:

1. On the TMR server, start up the SIS GUI by issuing:

   ```
   #wsisgui
   ```

   Enter your user ID and password.

   After entering the user ID and password, the dialog box shown in Figure 83 will appear. Click on the Worksheet pull-down menu and select the option Select machines.

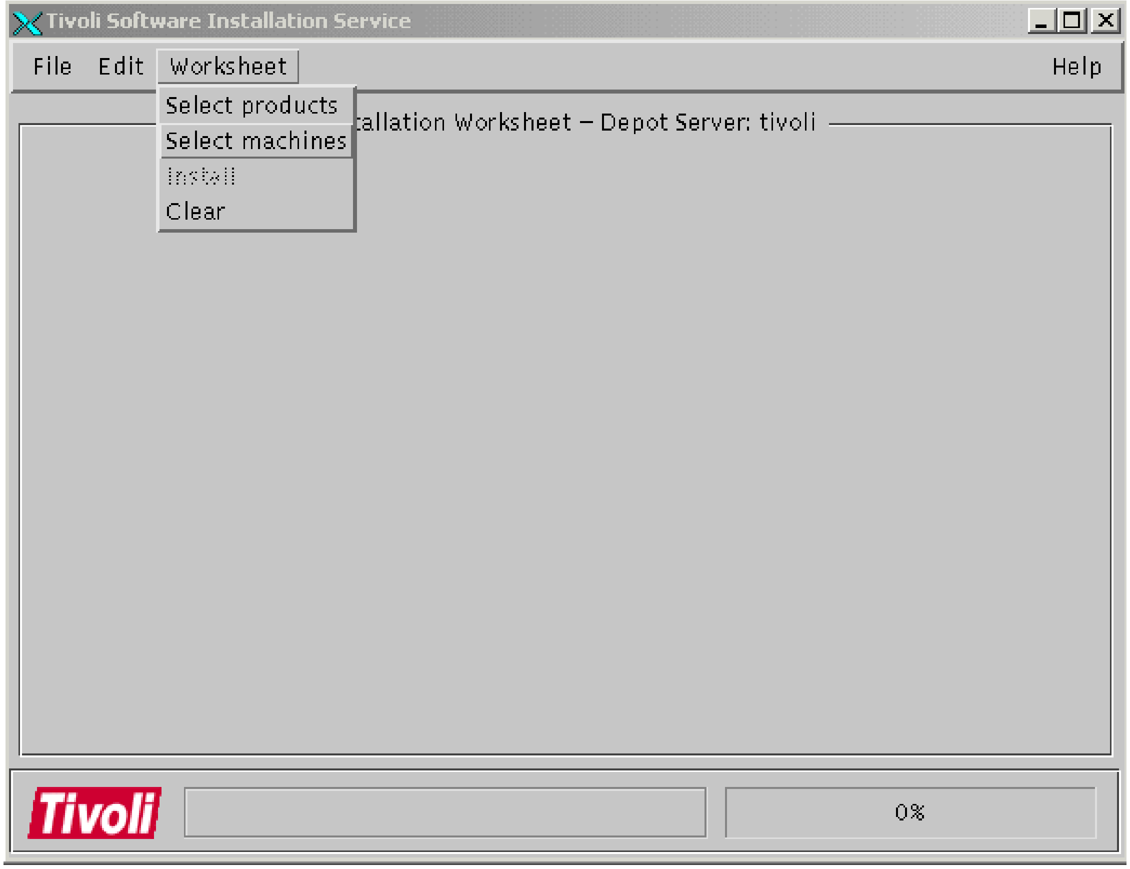
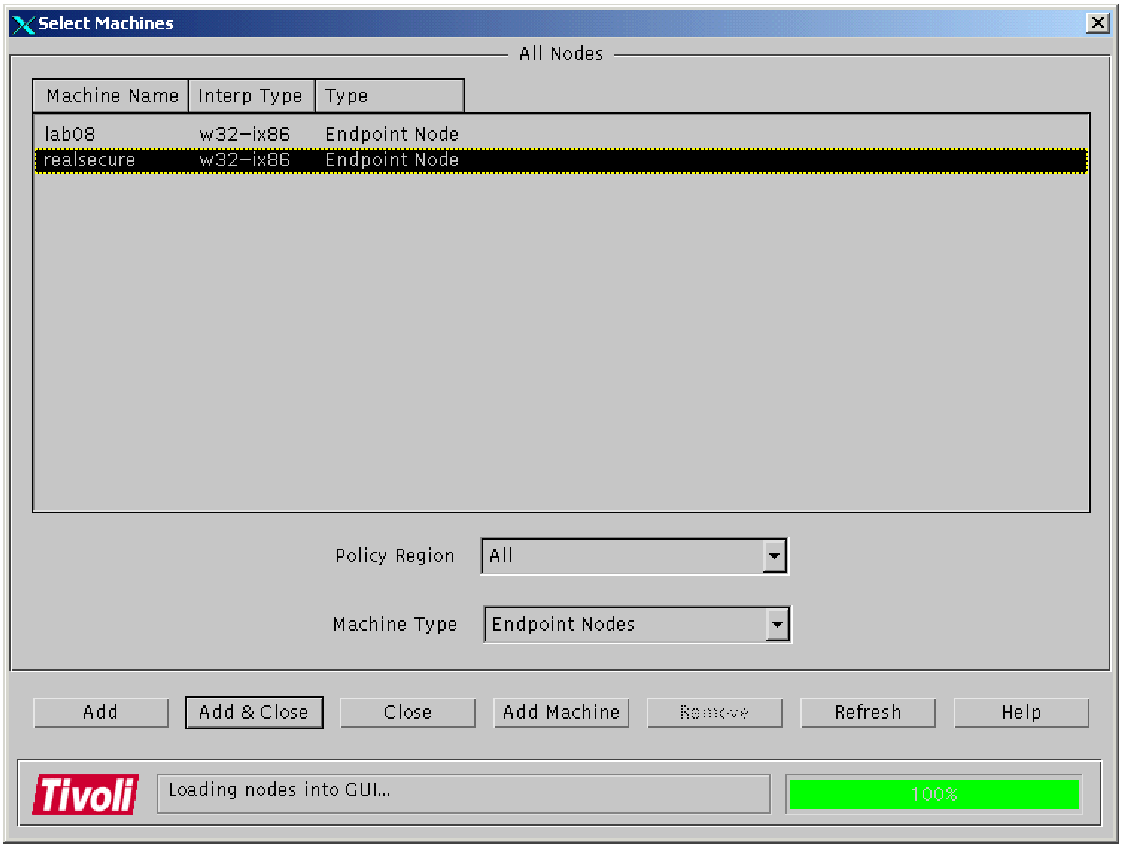

Tivoli Software Installation Service
File
Edit
Worksheet
Help
Select products
Select machines
Install
Clear
tallation Worksheet – Depot Server: tivoli
Tivoli
0%

Figure 83. SIS startup panel

2. Change the Machine Type drop-down list to Endpoint Nodes. Select the appropriate endpoint from the list, as shown in Figure 84 on page 157.



Machine Name	Interp Type	Type
lab08	w32-ix86	Endpoint Node
realsecure	w32-ix86	Endpoint Node

Policy Region: All

Machine Type: Endpoint Nodes

Loading nodes into GUI... 100%

Figure 84. SIS - Selecting an endpoint

3. After selecting the endpoint(s) we want to install the software packages on, close this panel using the button Add & Close as shown in Figure 84. In the next step, we have to select the components or products we want to install.

4. The Select Products option is what we choose from the next dialog box in Figure 85 on page 158.

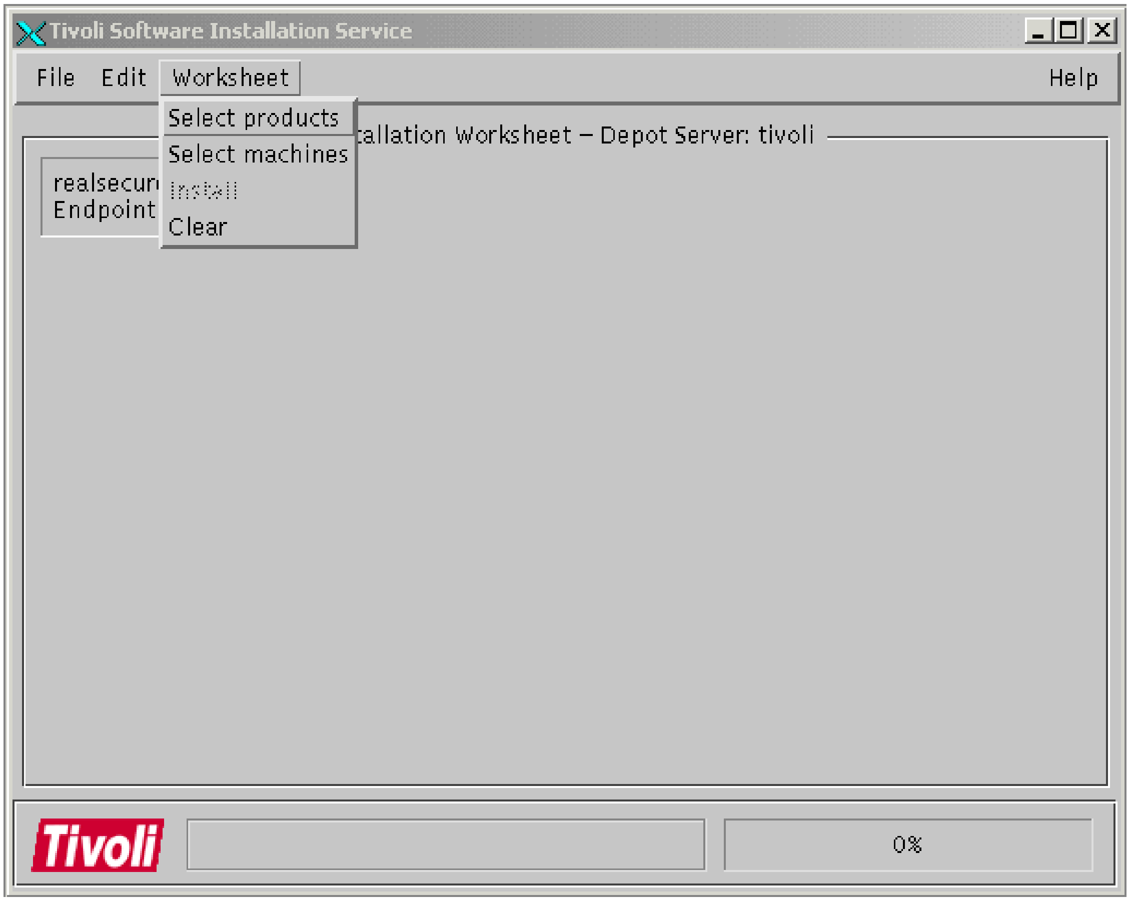
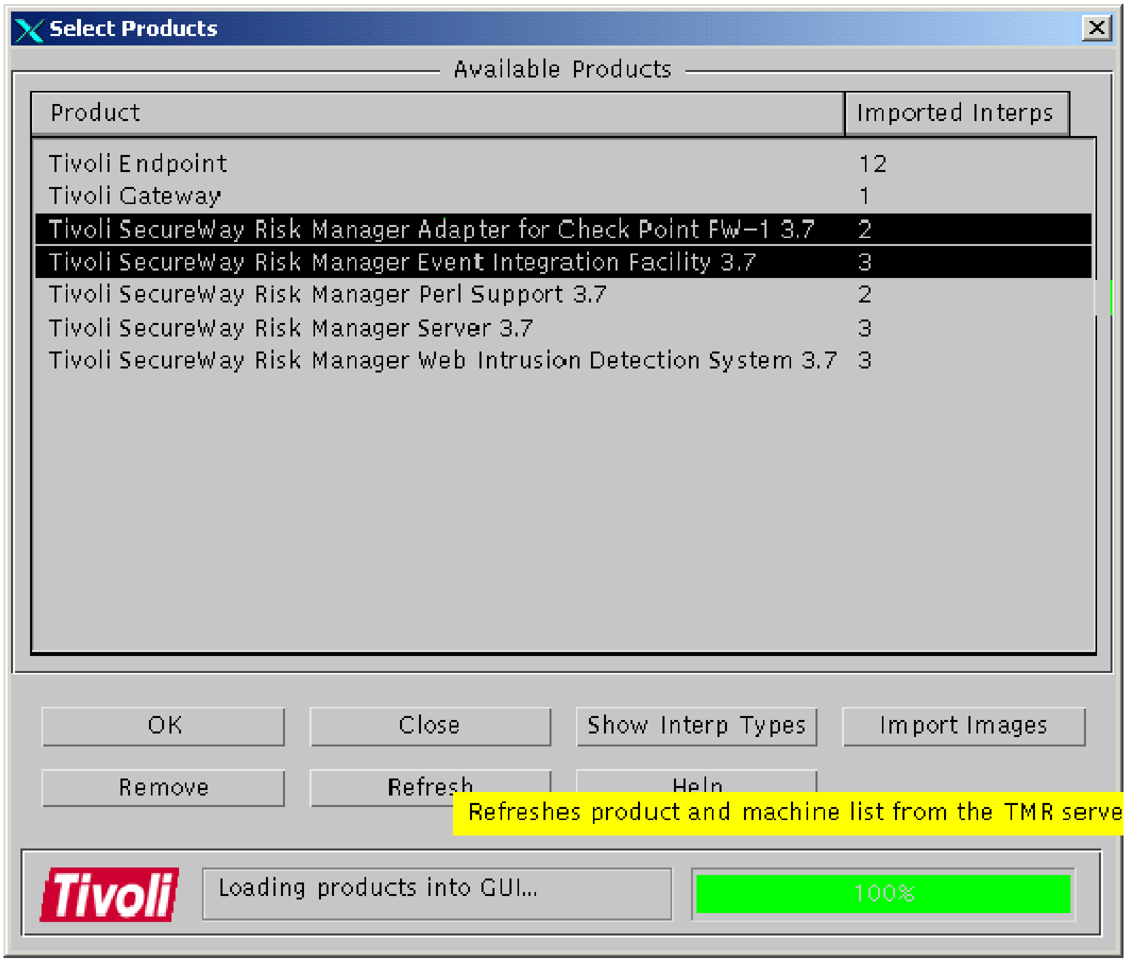


Figure 85. SIS - Select products

5. Select the following products from the product list shown in Figure 86 on page 159:
   a. Tivoli Risk Manager Event Integration Facility 3.7
   b. Tivoli Risk Manager Adapter for Check Point FW-1 3.7



Product	Imported Interps
Tivoli Endpoint	12
Tivoli Gateway	1
Tivoli SecureWay Risk Manager Adapter for Check Point FW-1 3.7	2
Tivoli SecureWay Risk Manager Event Integration Facility 3.7	3
Tivoli SecureWay Risk Manager Perl Support 3.7	2
Tivoli SecureWay Risk Manager Server 3.7	3
Tivoli SecureWay Risk Manager Web Intrusion Detection System 3.7	3

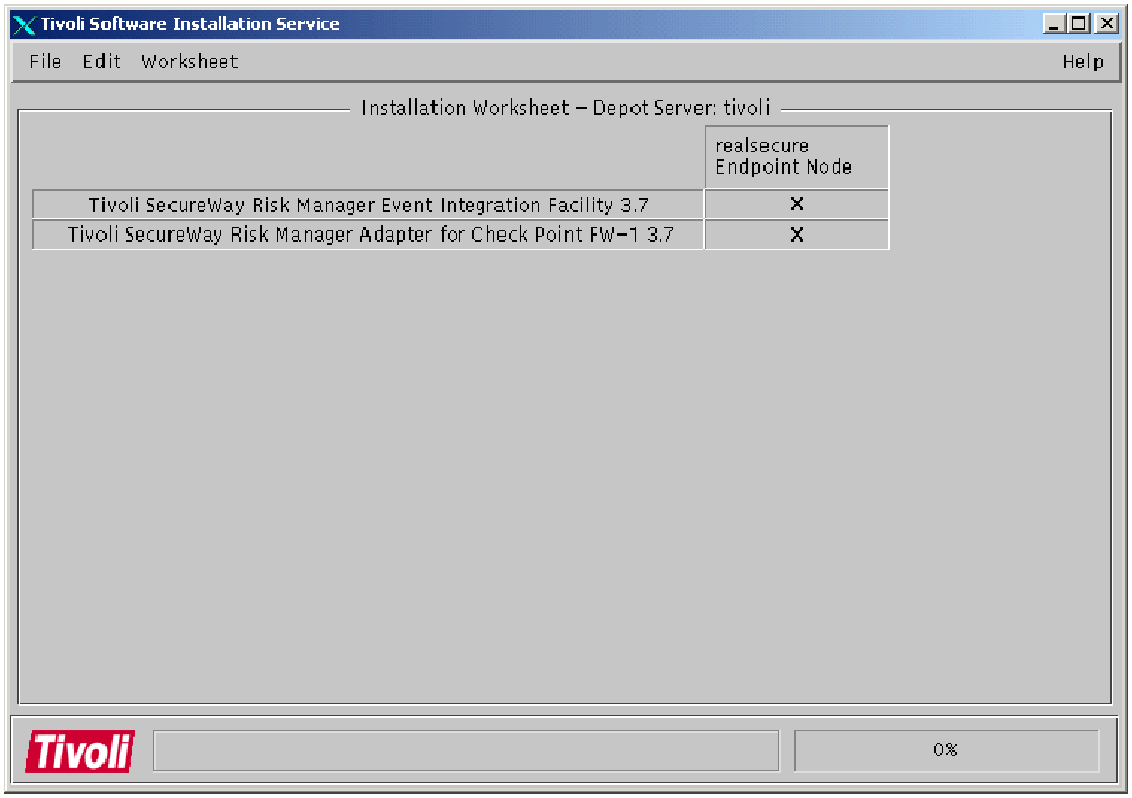
Refreshes product and machine list from the TMR serve

Loading products into GUI...

100%

Figure 86. SIS - Select products continued

Check the two components and select OK. The dialog box shown in Figure 87 on page 160 shows the installation worksheet with your selected components.

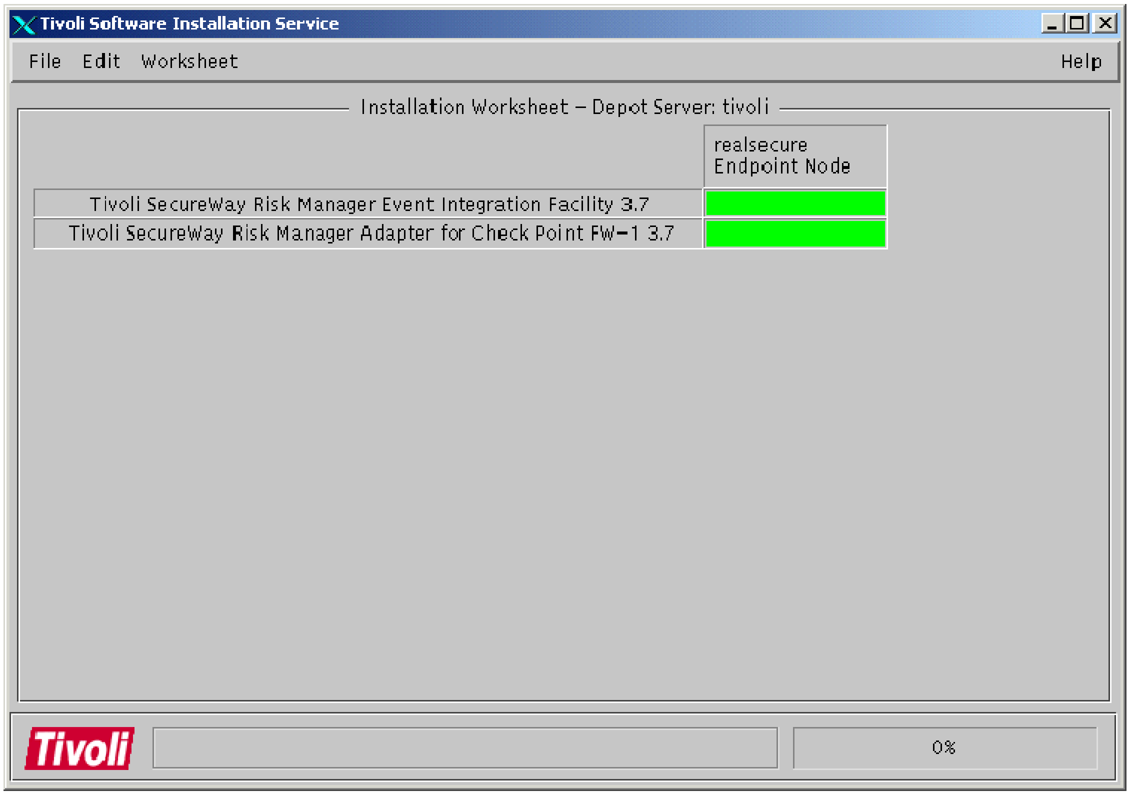


Installation Worksheet – Depot Server: tivoli

	realsecure Endpoint Node
Tivoli SecureWay Risk Manager Event Integration Facility 3.7	X
Tivoli SecureWay Risk Manager Adapter for Check Point FW–1 3.7	X

Figure 87. SIS - Installation worksheet

6. Click on the Worksheet pull-down menu and select Install.



Installation Worksheet – Depot Server: tivoli

	realsecure Endpoint Node
Tivoli SecureWay Risk Manager Event Integration Facility 3.7	🟩
Tivoli SecureWay Risk Manager Adapter for Check Point FW-1 3.7	🟩

Figure 88. SIS - Installation success

7. A green bar, as shown in Figure 88, is indicating the successfully distributed two adapters. At the endpoint, a new directory is created (..\tivoli\lcf\bin\w32-ix86\riskmgr\), and individual adapter folders have been added.

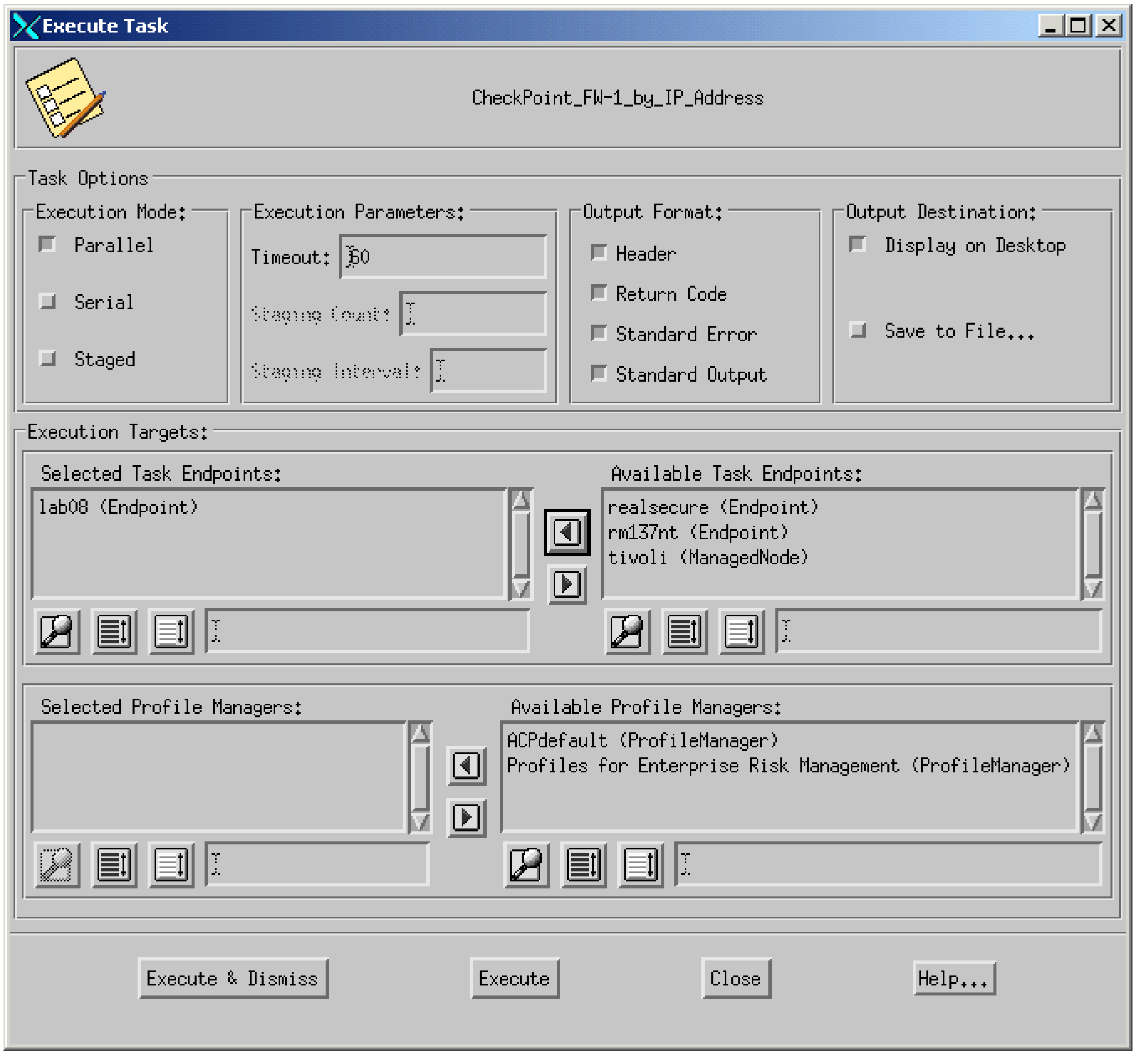
5.3.3 Automated Risk Manager firewall action

One of the main functions of Risk Manager is to identify suspicious activity. The Risk Manager and the CheckPoint VPN1/Firewall-1 also provide a way to respond to that suspicious activity in an automated fashion. Risk Manager provides TEC Tasks that can be used to monitor or block traffic at the firewall.

Follow these steps:

1. On the Tivoli desktop, navigate to **TEC Region -> Tasks for Enterprise Risk Management**. You will see a panel listing TEC Tasks. Double-click the icon labeled CheckPoint_FW-1_by_IP_Address.

2. An Execute Task panel will appear, as shown in Figure 89. Choose a CheckPoint adapter endpoint from the Available Task Endpoints area, click Display on Desktop from the Output Destination area, then click Execute.



CheckPoint_FW-1_by_IP_Address

Timeout: 60

Selected Task Endpoints:
lab08 (Endpoint)

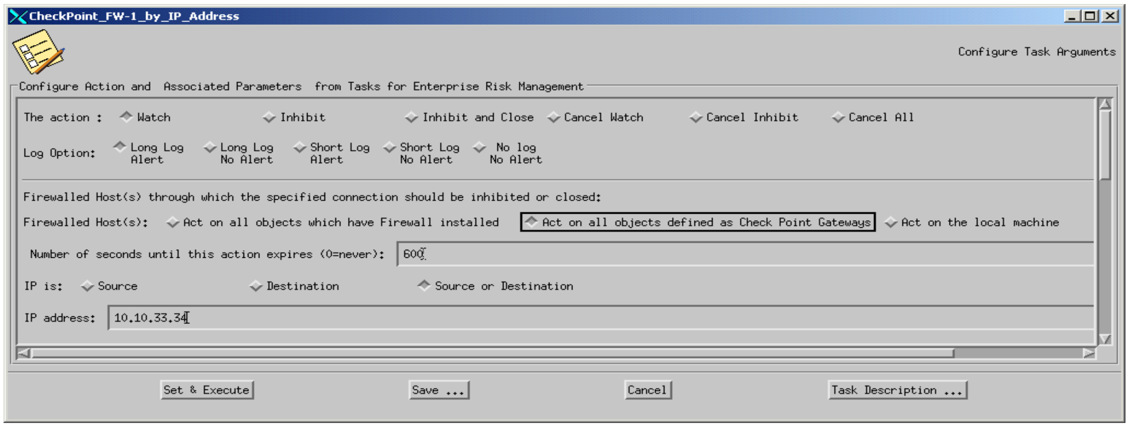
Available Task Endpoints:
realsecure (Endpoint)
rm137nt (Endpoint)
tivoli (ManagedNode)

Available Profile Managers:
ACPdefault (ProfileManager)
Profiles for Enterprise Risk Management (ProfileManager)

Figure 89. Execute Task panel

3. You will see a panel called CheckPoint_FW-1_by_IP_Address, as shown in Figure 90 on page 163. In this example, we will monitor all activity from one IP address - 10.10.33.34. Click WATCH, click Long Log Alert, click Act on all objects defined as CheckPoint Gateways, fill in a duration of 600

seconds in this case, click Source or Destination, and fill in the IP address of the host. Finally, click Set and Execute.



CheckPoint_FW-1_by_IP_Address

Configure Task Arguments

Configure Action and Associated Parameters from Tasks for Enterprise Risk Management

The action : ◆ Watch ◇ Inhibit ◇ Inhibit and Close ◇ Cancel Watch ◇ Cancel Inhibit ◇ Cancel All

Log Option: ◆ Long Log Alert ◇ Long Log No Alert ◇ Short Log Alert ◇ Short Log No Alert ◇ No log No Alert

Firewalled Host(s) through which the specified connection should be inhibited or closed:

Firewalled Host(s): ◇ Act on all objects which have Firewall installed ◆ Act on all objects defined as Check Point Gateways ◇ Act on the local machine

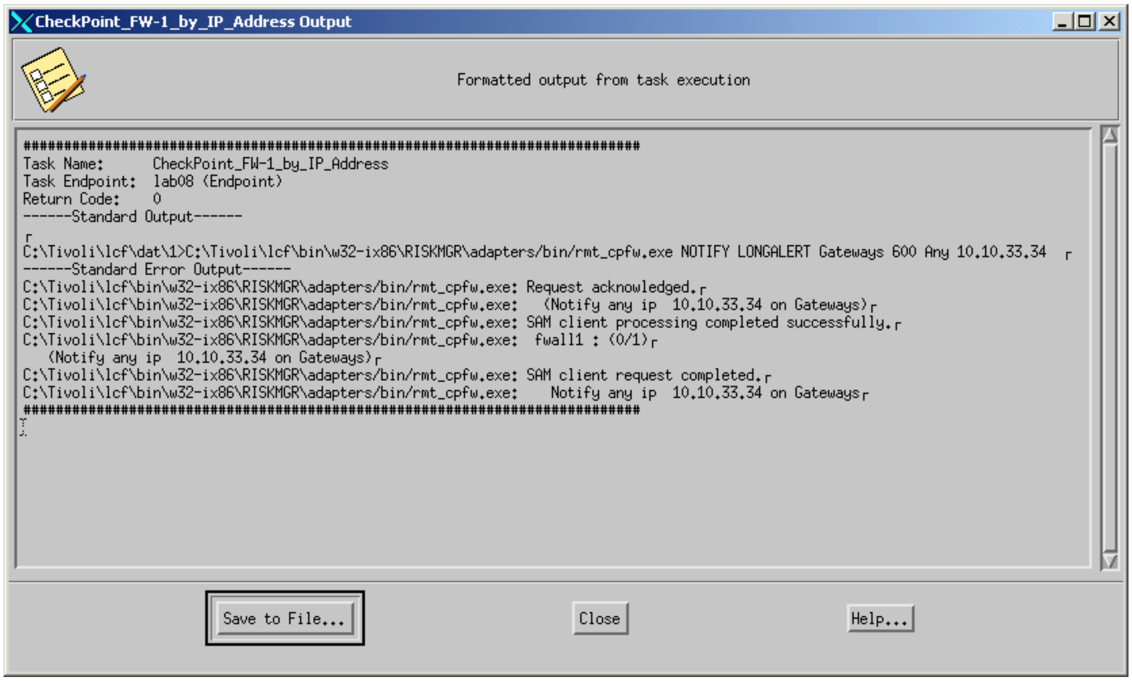
Number of seconds until this action expires (0=never): 600

IP is: ◇ Source ◇ Destination ◆ Source or Destination

IP address: 10.10.33.34

Figure 90. CheckPoint_FW-1_by_IP_Address

4. A panel, as seen in Figure 91, will appear showing the success or failure of the TEC task.



CheckPoint_FW-1_by_IP_Address Output

Formatted output from task execution

```
############################################################################
Task Name:      CheckPoint_FW-1_by_IP_Address
Task Endpoint:  lab08 (Endpoint)
Return Code:    0
------Standard Output------
┌
C:\Tivoli\lcf\dat\1>C:\Tivoli\lcf\bin\w32-ix86\RISKMGR\adapters/bin/rmt_cpfw.exe NOTIFY LONGALERT Gateways 600 Any 10.10.33.34  ┌
------Standard Error Output------
C:\Tivoli\lcf\bin\w32-ix86\RISKMGR\adapters/bin/rmt_cpfw.exe: Request acknowledged.┌
C:\Tivoli\lcf\bin\w32-ix86\RISKMGR\adapters/bin/rmt_cpfw.exe:   (Notify any ip  10.10.33.34 on Gateways)┌
C:\Tivoli\lcf\bin\w32-ix86\RISKMGR\adapters/bin/rmt_cpfw.exe: SAM client processing completed successfully.┌
C:\Tivoli\lcf\bin\w32-ix86\RISKMGR\adapters/bin/rmt_cpfw.exe:  fwall1 : (0/1)┌
   (Notify any ip  10.10.33.34 on Gateways)┌
C:\Tivoli\lcf\bin\w32-ix86\RISKMGR\adapters/bin/rmt_cpfw.exe: SAM client request completed.┌
C:\Tivoli\lcf\bin\w32-ix86\RISKMGR\adapters/bin/rmt_cpfw.exe:    Notify any ip  10.10.33.34 on Gateways┌
############################################################################
```

Figure 91. Output panel

Entries will appear in the CheckPoint firewall log and in the Tivoli Event Server for each packet the firewall sees with a source or destination of 10.10.33.34.

The packets can be blocked by choosing INHIBIT instead of WATCH on the CheckPoint_FW-1_by_IP_Address panel.

5.4 Tivoli Network Intrusion Detection System (NIDS) integration

Network Intrusion Detection quickly alerts network managers to intrusion-detection problems so that they can invoke adequate responses. Intrusion detection helps a network manager determine whether an unusual network traffic pattern is actually an attack or simply a random event that is occurring for non-malicious reasons.

The software included in this package is based on work done in the IBM Research Labs to develop better Network Intrusion Detection Systems to protect a customer's e-business infrastructure. The Tivoli NIDS is available for Tivoli Risk Manager customers as an optional add on. Currently, it is only supported on AIX, but it is Tivoli’s stated intention that future releases will be supported on Linux as well.

The following sections cover the installation and testing of NIDS as well as the integration with Tivoli Risk Manager. This implementation uses the Non-TME deployment method. Alternatively, you can use the TME method to install the Tivoli logfile adapter, but the NIDS installation has to be done by the AIX native install (`installp`), as shown in Figure 92 on page 165. The steps for this are detailed in the *Tivoli Risk Manager 3.7 Network Intrusion Detection Option User Guide*. Certain steps may vary according to your situation.

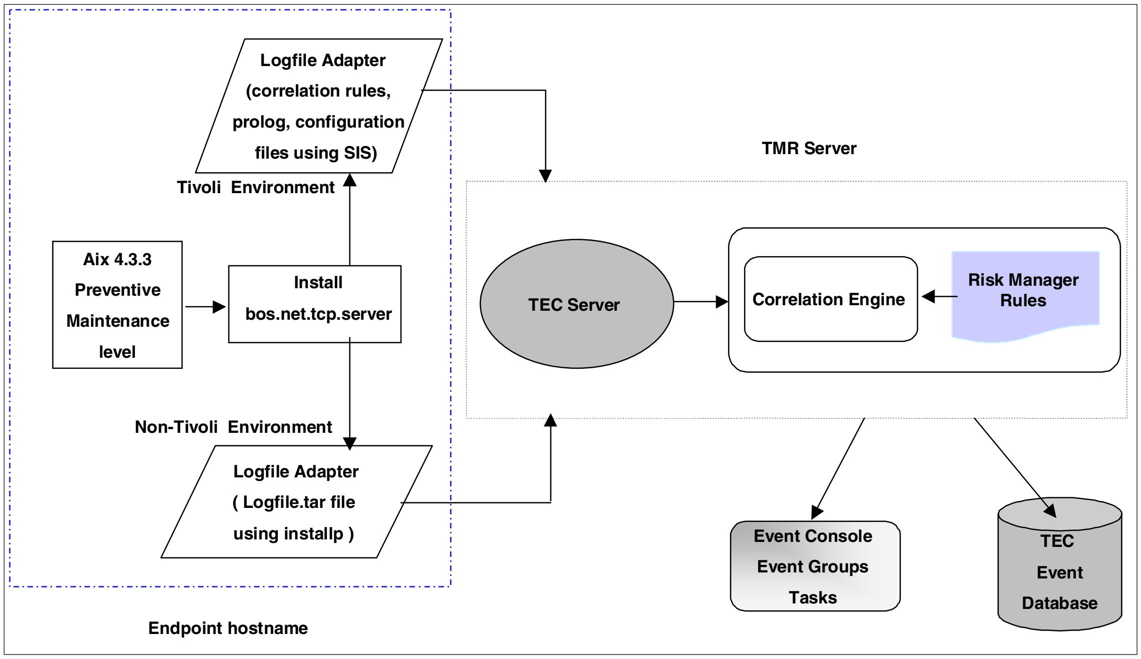


Figure 92. NIDS configuration

5.4.1 Installing the OS

The first step is to prepare AIX for Tivoli NIDS:

1. Install AIX 4.3.3 (refer to the AIX Installation Guide).
2. Install bos.net.tcp.server 4.3.3 using SMIT.
3. Install the latest AIX Preventive Maintenance Level (this can be obtained through your local IBM Customer Support).

5.4.2 Installing NIDS (non-TME install method)

To install NIDS using the non-TME install method, follow these steps:

1. Before installing the NIDS, remember to download the latest patches for NIDS from

   `http://www.tivoli.com/support/secure_download_bridge.html`

   This is a protected site, so ask your local Tivoli support for the user ID and password.
2. Ensure that /usr has at least 2 MB of free disk space available.

3. Insert the Tivoli Risk Manager 3.7: Network Intrusion Detection Option CD-ROM.
4. Type:

   ```
   smit install_latest
   ```

   This should bring up the following screen:

   ```
   Install and Update from LATEST Available Software

   Type or select values in entry fields.
   Press Enter AFTER making all desired changes.

                                                           [Entry Fields]
   * INPUT device / directory for software               /dev/cd0
   * SOFTWARE to install                                [_all_latest]+
     PREVIEW only? (install operation will NOT occur)    no                       +
     COMMIT software updates?                            yes                      +
     SAVE replaced files?                                no                       +
     AUTOMATICALLY install requisite software?           yes                      +
     EXTEND file systems if space needed?                yes                      +
     OVERWRITE same or newer versions?                   no                       +
     VERIFY install and check file sizes?               no                       +
     Include corresponding LANGUAGE filesets?            yes                      +
     DETAILED output?                                    no                       +
     Process multiple volumes?                           yes                      +


   F1=Help     F2=Refresh     F3=Cancel      F4=List
   F5=Reset    F6=Command     F7=Edit        F8=Image
   F9=Shell    F10=Exit       Enter=Do
   ```

5. To test the installation, type:

   ```
   # cd /usr/opt/Tivoli/nids
   # ./nids
   ```

   You should see an output similar to:

   ```
   Tivoli Network Intrusion Detection System

   Version 3.7  Build: 11/06/2000-10:56:21-EST

   Licensed Materials - Property of IBM
   5698-RMG
   (C) Copyright IBM Corp. 1996, 1997, 1998, 1999, 2000
   All Rights Reserved.

   # NIDS:Mon Feb 19 14:42:48 2001 Starting
   Got device type 9
   ./nids: listening on tr0
   ```

From the output above, we can see that the NIDS is running and listening on the token ring adapter. For an ethernet adapter, you would see an en0 instead of tr0.

6. To test it, start another telnet session to the host and logon as root but enter an incorrect password. The output of the NIDS should be similar to:

```
Alert Level: 3 Date: Mon Feb 19 14:57:48 2001 Sig: N/A AUTH login
failure Host: 10.30.30.2:23 to 10.20.20.16:32775 Data: 3004-007 You
entered an invalid login name or password.\0d
```

5.4.3 Installing and configuring the TEC adapters

A complete guide of installing TEC adapters can be found in the *Tivoli Enterprise Console Adapter Guide*. In this implementation, we will assume that TECADHOME =/usr/tecad, but you may use any directory you desire. However, the following is the tested way of installing and configuring the TEC adapters in a Non-TME environment:

1. Insert the Tivoli Enterprise Console 3.7 CD-ROM in the server
2. Type:

```
# mount /cdrom
```

3. Type the following to copy the files in the /usr/tecad directory:

```
# mkdir /usr/tecad
# cd /usr/tecad
# tar -xvf /cdrom/NON_TME/AIX4-R1/LOGFILE.TAR
```

4. When this is done, you should get three directories within /usr/tecad:

```
# ls
etc      codeset  etc
```

5. To configure the adapters, you would have to copy the tecad_logfile.fmt file from TECADHOME/etc/lang to TECADHOME/etc directory, such as:

```
# cp /usr/tecad/etc/C/tecad_logfile.fmt /usr/tecad/etc
```

6. The next step is to merge the format files together so that the TEC adapter will understand the NIDS events and send them to the TEC server, such as:

```
# cat /usr/opt/Tivoli/nids/nids.fmt >> /usr/tecad/etc/tecad_logfile.fmt
```

7. Now we have to configure the TEC adapter to talk to the TEC server. This is accomplished by running the `tecad_logfile.cfg` command. Do not forget to export the TECADHOME variable. When prompted for the TEC server host name, enter the host name or the IP address:

```
# export TECADHOME=/Tivoli/tecad
# /usr/tecad/bin/tecad_logfile.cfg
+ PATH=/usr/bin:/etc:/usr/sbin:/usr/ucb:/usr/bin/X11:/sbin:/usr/ucb
+ export PATH
+ APPNAME=Tivoli Enterprise Console Logfile Adapter
+ PROD=tecad_logfile
+ get_tme_env
+ get_interp_env
+ AS=1
+ export AS
+ configure_tecad /Tivoli/tecad tecad_logfile

Enter the host name where your TEC Server is running:
tivolirm
+ configure_removal_script /Tivoli/tecad logfile
+ [ FALSE = TRUE ]
+ TECAD_START=/Tivoli/tecad/bin/init.tecad_logfile
+ set +e
+ remove_rc_files FALSE 1 /Tivoli/tecad/bin/init.tecad_logfile
tecad_logfile aix4-r1
+ config_non_tme_autostart FALSE 1 /Tivoli/tecad/bin/init.tecad_logfile
tecad_logfile aix4-r1
/etc/rc.nfs is already configured to autostart this adapter
+ unset CHILD_OF_OSERV
+ [ FALSE = TRUE ]
+ /Tivoli/tecad/bin/logfile_gencds /Tivoli/tecad/etc/tecad_logfile.fmt
+ 1> /Tivoli/tecad/etc/tecad_logfile.cds
warning: in Printer_Error_Cleared dropping inherited map `msg $3'
warning: in Printer_Powerup dropping inherited map `msg $3'
warning: in Printer_Toner_Low dropping inherited map `msg $3'
warning: in Printer_Page_Punt dropping inherited map `msg $3'
warning: in Printer_Offline dropping inherited map `msg $3'
warning: in Printer_Output_Full dropping inherited map `msg $3'
warning: in Printer_Paper_Out dropping inherited map `msg $3'
warning: in Printer_Paper_Jam dropping inherited map `msg $3'
warning: in Printer_Door_Open dropping inherited map `msg $3'
warning: in Oserv_IPC_Dispatch_Failed dropping inherited map `msg $5'
warning: in Oserv_Graceful_Exit dropping inherited map `msg $5'
+ [ FALSE = TRUE ]
+ /Tivoli/tecad/bin/init.tecad_logfile start
tivoli:root in /Tivoli/tecad/bin
# Starting TME 10 Enterprise Console Logfile Adapter ...
cd /Tivoli/tecad
bin/tecad_logfile -n  -c /Tivoli/tecad/etc/tecad_logfile.conf
Refreshing syslogd...
0513-095 The request for subsystem refresh was completed successfully.
# export TECADHOME=/Tivoli/tecad
# /usr/tecad/bin/tecad_logfile.cfg
```

```
+ PATH=/usr/bin:/etc:/usr/sbin:/usr/ucb:/usr/bin/X11:/sbin:/usr/ucb
+ export PATH
+ APPNAME=Tivoli Enterprise Console Logfile Adapter
+ PROD=tecad_logfile
+ get_tme_env
+ get_interp_env
+ AS=1
+ export AS
+ configure_tecad /Tivoli/tecad tecad_logfile

Enter the host name where your TEC Server is running:
tivolirm
+ configure_removal_script /Tivoli/tecad logfile
+ [ FALSE = TRUE ]
+ TECAD_START=/Tivoli/tecad/bin/init.tecad_logfile
+ set +e
+ remove_rc_files FALSE 1 /Tivoli/tecad/bin/init.tecad_logfile
tecad_logfile aix4-r1
+ config_non_tme_autostart FALSE 1 /Tivoli/tecad/bin/init.tecad_logfile
tecad_logfile aix4-r1
/etc/rc.nfs is already configured to autostart this adapter
+ unset CHILD_OF_OSERV
+ [ FALSE = TRUE ]
+ /Tivoli/tecad/bin/logfile_gencds /Tivoli/tecad/etc/tecad_logfile.fmt
+ 1> /Tivoli/tecad/etc/tecad_logfile.cds
warning: in Printer_Error_Cleared dropping inherited map `msg $3'
warning: in Printer_Powerup dropping inherited map `msg $3'
warning: in Printer_Toner_Low dropping inherited map `msg $3'
warning: in Printer_Page_Punt dropping inherited map `msg $3'
warning: in Printer_Offline dropping inherited map `msg $3'
warning: in Printer_Output_Full dropping inherited map `msg $3'
warning: in Printer_Paper_Out dropping inherited map `msg $3'
warning: in Printer_Paper_Jam dropping inherited map `msg $3'
warning: in Printer_Door_Open dropping inherited map `msg $3'
warning: in Oserv_IPC_Dispatch_Failed dropping inherited map `msg $5'
warning: in Oserv_Graceful_Exit dropping inherited map `msg $5'
+ [ FALSE = TRUE ]
+ /Tivoli/tecad/bin/init.tecad_logfile start
tivoli:root in /Tivoli/tecad/bin
# Starting TME 10 Enterprise Console Logfile Adapter ...
cd /Tivoli/tecad
bin/tecad_logfile -n  -c /Tivoli/tecad/etc/tecad_logfile.conf
Refreshing syslogd...
0513-095 The request for subsystem refresh was completed successfully.
```

From the output above, we can see a couple of warning messages. Do not worry as this format file (tecad_logfile.fmt) caters to many products and events (including printers). The TEC logfile adapter is now started.

8. For maintenance purposes, the following commands are used to stop and start the TEC adapters. For debugging purposes, use the -d flag.

   To stop the TEC adapter, type:

   ```
   # $TECADHOME/init.tecad_logfile stop
   ```

   To start the TEC adapter, type:

   ```
   # $TECADHOME/init.tecad_logfile start
   ```

5.4.4 Risk Manager server configuration

The following are the steps to add the Network Intrusion Detector Sensor into the Tivoli Risk Manager Server. We assume that the Risk Manager Server is installed, configured, and tested.

Note

There are additional steps to further customize and fine tune the Risk Manager Server, which can be found in the *Risk Manager 3.7 User's Guide*.

1. In the Risk Manager server, look for the file riskmgr_hosts.pro and add the following two lines to the file. Do not forget to back up the original file (Do not forget the full stops in the end):

   ```
   set_host('10.30.30.3', nids_sensor.xxx.com).
   set_sensor('nids', '10.30.30.3', 'nids_sensor.xxx.com').
   ```

   These steps register the NIDS server as a host and a sensor in the Risk Manager configuration.

2. Next, we have to reconfigure Risk Manager and activate the changes by executing the following command:

   ```
   rmcorr_cfg -reconfig
   ```

5.4.5 Risk Manager and NIDS verification

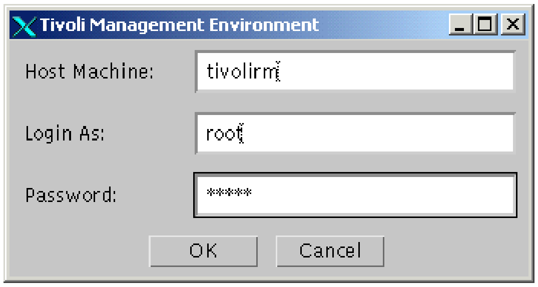
After doing the steps in Section 5.4.4, “Risk Manager server configuration” on page 170, we need to verify that the setup is working correctly. We need to use some insecure connections to any network. The test that is going to be done below is a simple telnet password failure. You can also use any network scanning tool available in the market, such as the Network Services Auditor (NSA) (available from IBM), to test the effectiveness of your NIDS.

Do the following steps:

1. Telnet to the host three times and enter a wrong password each time.
2. On the Risk Manager Server, start up the Tivoli Enterprise Console by issuing:

```
#tec_console &
```

3. The password dialogue in Figure 93 will be shown. Enter your user ID and password.



Host Machine: tivolirm

Login As: root

Password: *****

Figure 93. TEC console login

4. After entering the password, the TEC console shown in Figure 94 will appear. Select **Windows -> Event Viewer**.

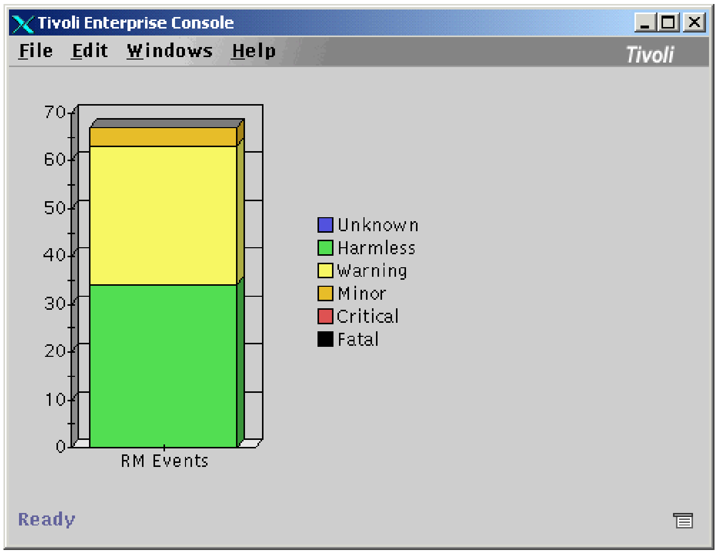
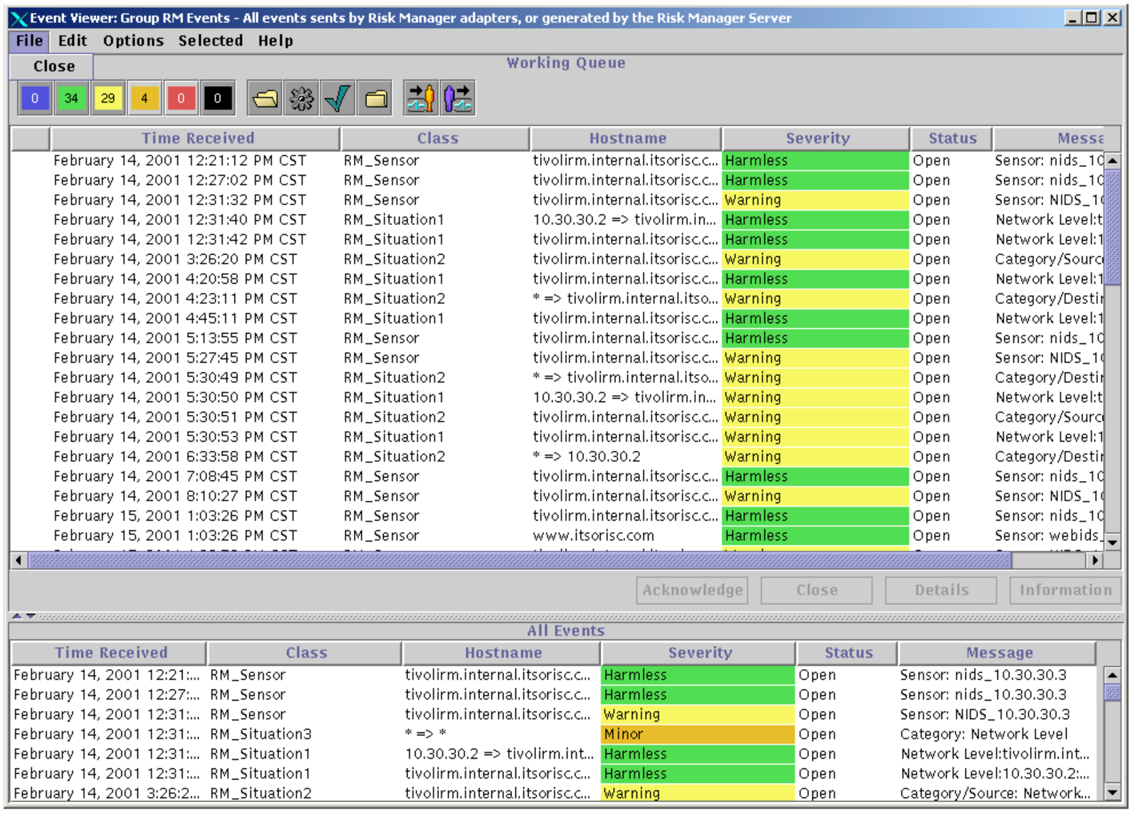


Figure 94. Tivoli Enterprise Console initial panel

5. Click on any portion of the bar chart and the Event Viewer panel, depicted in Figure 95, will appear. You should see some events with the sensor name on it. Although it is not clear in the picture, some NIDS events are shown on the panel and these are the events that have to be shown. The other events shown here are a result of network scanning from the Network Services Auditor tool.


Event Viewer: Group RM Events - All events sents by Risk Manager adapters, or generated by the Risk Manager Server
File
Edit
Options
Selected
Help
Close
Working Queue
0
34
29
4
0
0
Acknowledge
Close
Details
Information
All Events

	Time Received	Class	Hostname	Severity	Status	Messa
	February 14, 2001 12:21:12 PM CST	RM_Sensor	tivolirm.internal.itsorisc.c...	Harmless	Open	Sensor: nids_10
	February 14, 2001 12:27:02 PM CST	RM_Sensor	tivolirm.internal.itsorisc.c...	Harmless	Open	Sensor: nids_10
	February 14, 2001 12:31:32 PM CST	RM_Sensor	tivolirm.internal.itsorisc.c...	Warning	Open	Sensor: NIDS_10
	February 14, 2001 12:31:40 PM CST	RM_Situation1	10.30.30.2 => tivolirm.in...	Harmless	Open	Network Level:t
	February 14, 2001 12:31:42 PM CST	RM_Situation1	tivolirm.internal.itsorisc.c...	Harmless	Open	Network Level:1
	February 14, 2001 3:26:20 PM CST	RM_Situation2	tivolirm.internal.itsorisc.c...	Warning	Open	Category/Source
	February 14, 2001 4:20:58 PM CST	RM_Situation1	tivolirm.internal.itsorisc.c...	Harmless	Open	Network Level:1
	February 14, 2001 4:23:11 PM CST	RM_Situation2	* => tivolirm.internal.itso...	Warning	Open	Category/Destir
	February 14, 2001 4:45:11 PM CST	RM_Situation1	tivolirm.internal.itsorisc.c...	Harmless	Open	Network Level:1
	February 14, 2001 5:13:55 PM CST	RM_Sensor	tivolirm.internal.itsorisc.c...	Harmless	Open	Sensor: nids_10
	February 14, 2001 5:27:45 PM CST	RM_Sensor	tivolirm.internal.itsorisc.c...	Warning	Open	Sensor: NIDS_10
	February 14, 2001 5:30:49 PM CST	RM_Situation2	* => tivolirm.internal.itso...	Warning	Open	Category/Destir
	February 14, 2001 5:30:50 PM CST	RM_Situation1	10.30.30.2 => tivolirm.in...	Warning	Open	Network Level:t
	February 14, 2001 5:30:51 PM CST	RM_Situation2	tivolirm.internal.itsorisc.c...	Warning	Open	Category/Source
	February 14, 2001 5:30:53 PM CST	RM_Situation1	tivolirm.internal.itsorisc.c...	Warning	Open	Network Level:1
	February 14, 2001 6:33:58 PM CST	RM_Situation2	* => 10.30.30.2	Warning	Open	Category/Destir
	February 14, 2001 7:08:45 PM CST	RM_Sensor	tivolirm.internal.itsorisc.c...	Harmless	Open	Sensor: nids_10
	February 14, 2001 8:10:27 PM CST	RM_Sensor	tivolirm.internal.itsorisc.c...	Warning	Open	Sensor: NIDS_10
	February 15, 2001 1:03:26 PM CST	RM_Sensor	tivolirm.internal.itsorisc.c...	Harmless	Open	Sensor: nids_10
	February 15, 2001 1:03:26 PM CST	RM_Sensor	www.itsorisc.com	Harmless	Open	Sensor: webids_

Time Received	Class	Hostname	Severity	Status	Message
February 14, 2001 12:21:...	RM_Sensor	tivolirm.internal.itsorisc.c...	Harmless	Open	Sensor: nids_10.30.30.3
February 14, 2001 12:27:...	RM_Sensor	tivolirm.internal.itsorisc.c...	Harmless	Open	Sensor: nids_10.30.30.3
February 14, 2001 12:31:...	RM_Sensor	tivolirm.internal.itsorisc.c...	Warning	Open	Sensor: NIDS_10.30.30.3
February 14, 2001 12:31:...	RM_Situation3	* => *	Minor	Open	Category: Network Level
February 14, 2001 12:31:...	RM_Situation1	10.30.30.2 => tivolirm.int...	Harmless	Open	Network Level:tivolirm.int...
February 14, 2001 12:31:...	RM_Situation1	tivolirm.internal.itsorisc.c...	Harmless	Open	Network Level:10.30.30.2:...
February 14, 2001 3:26:2...	RM_Situation2	tivolirm.internal.itsorisc.c...	Warning	Open	Category/Source: Network...

Figure 95. TEC Event Viewer

After these steps are followed, you should get a working Network Intrusion Detector Sensor. For further tasks and tuning, please consult the *Tivoli Risk Manager 3.7 Network Intrusion Detection Option User's Guide*.

5.5 Web IDS setup

The Web Intrusion Detection System (Web IDS) is a Perl based tool that is provided with Risk Manager. This tool uses the actual access log files generated by a Web server to perform an analysis to detect Web server attacks.

The following sections cover the installation and testing of Web IDS as well as the integration with Tivoli Risk Manager. This implementation uses the TME and Non-TME method on IBM HTTPD Server on Windows NT. The steps for this are detailed in the *Tivoli Risk Manager 3.7 User Guide*.

Web IDS can monitor intrusion detection events on the following different Web servers:

- Apache Web Server for Windows NT and AIX
- Lotus Domino Server on Windows NT, AIX, and Solaris
- IBM HTTP Server on Windows NT, AIX, and Solaris
- Tivoli Policy Director WebSEAL Server on Windows NT, AIX and Solaris

The overview of setting up the sensor (TME and non-TME) is shown in Figure 96.

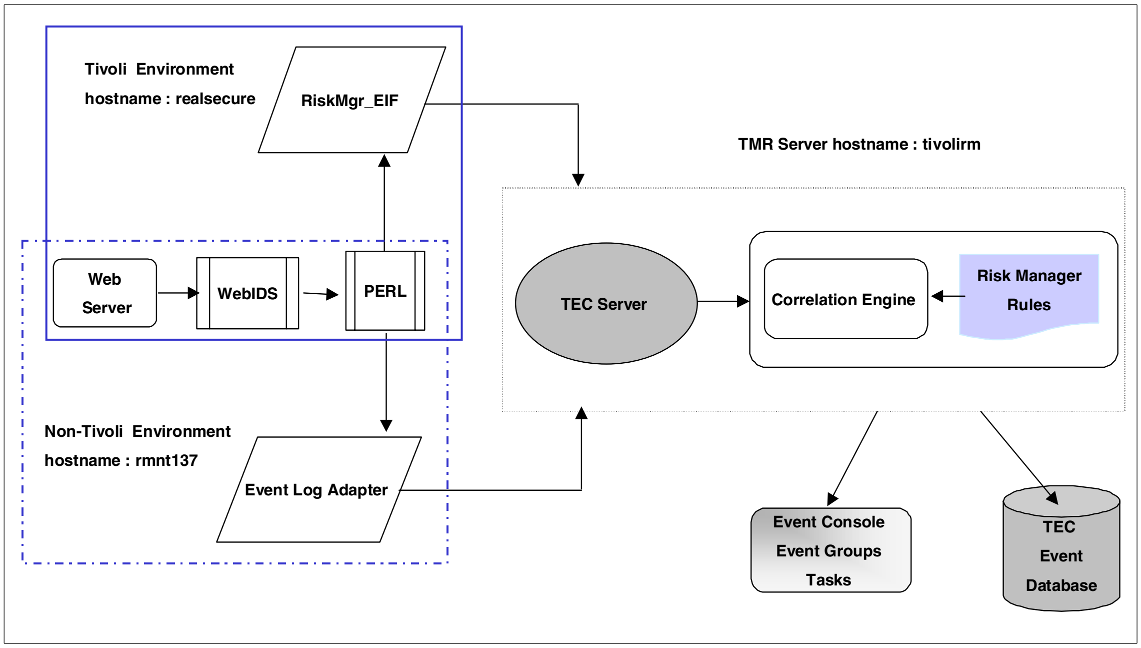


Figure 96. Web IDS configuration

5.5.1 Installation in a Non-Tivoli environment

To install Web IDS, Perl support, and the Risk Manager Event Log Adapter in a non-Tivoli environment, we use the .tar or .zip files. This implementation uses the Non-TME method using Risk Manger Log Adapter on Windows NT. The steps are detailed in the Tivoli Risk Manager 3.7 user guide.

5.5.1.1 Windows NT and Risk Manager components installation

Now we are installing the Risk Manger components in a non-Tivoli environment.

1. The first step is to prepare Windows NT for Tivoli Web IDS.
   a. Install Windows NT Server 4.0.
   b. Install service pack version 5.0 or higher.
   c. Install IBM HTTP server.

   Make sure that you are logged on to the Windows NT system as Administrator and also be sure that you have the Risk Manager CD inserted in the CD-ROM drive. Extract the adapter files from the directory x:\rmadapters (x:\ CD-ROM drive).

2. Create the directory to contain the Risk Manger component files:

```
mkdir webids_nt
mkdir perl_nt
```

3. Extract the Risk Manger adapter files from the .zip file on the CD

   webids_nt.zip This file contains the Risk Manager Web IDS for installation on Windows NT. Extract it into the directory c:\webids_nt on host: rmnt37.

   perl_nt.zip This file contains the Perl distribution for installation on Windows NT that is used with the Risk Manager Web IDS and Risk Manager Event Log Adapter components. Extract it into the directory c:\perl_nt\ on host: rmnt37.

5.5.1.2 Installation of the NT Event Log Adapter

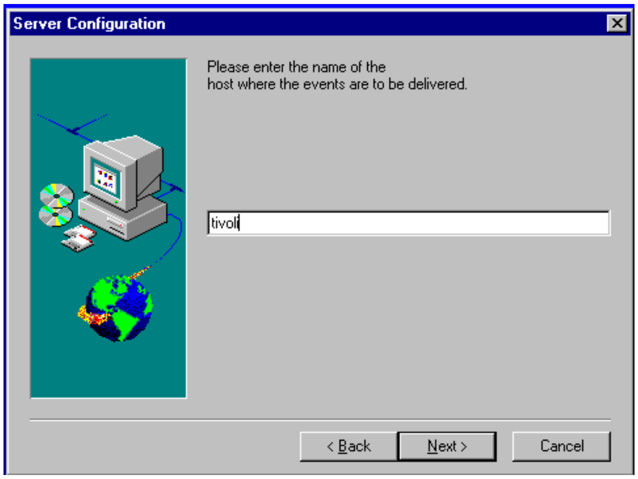
In this section, we are installing the Windows NT Event Log Adapter on the rmnt37 machine.

Do the following:

1. Insert the Tivoli Enterprise Console Version 3.7 CD-ROM
   a. Select the folder x:\NON_TME\w32-ix86\installnt\ (x:\ cd_rom drive).
   b. Double-click setup.exe.

2. Click the Next button in order to complete the installation.

3. Provide the host name of the TEC server, as shown in Figure 97.

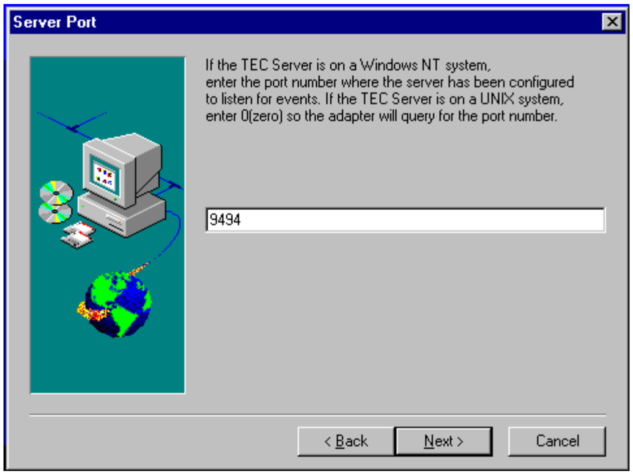


Please enter the name of the host where the events are to be delivered.

tivoli

Figure 97. NTEvent Log Adapter host name

4. Provide the port number of the TEC Server, as shown in Figure 98.

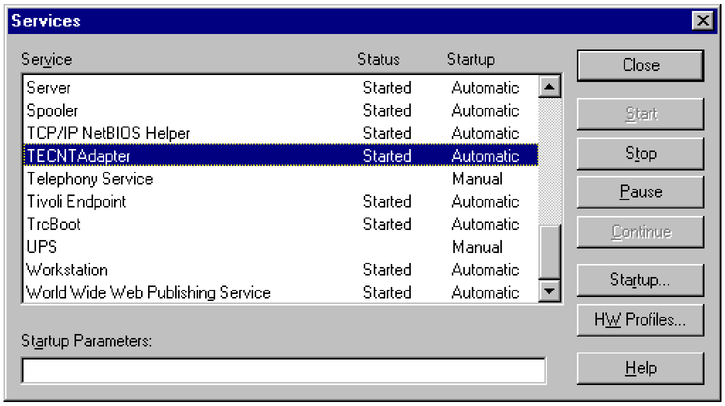


If the TEC Server is on a Windows NT system, enter the port number where the server has been configured to listen for events. If the TEC Server is on a UNIX system, enter 0(zero) so the adapter will query for the port number.

9494

Figure 98. NTEvent Log Adapter Installation Provide TEC Server Port Number

5. After successful installation of the Windows NT logfile adapter, a TECNTAdapter service is added to the Windows NT system services, as shown in Figure 99 on page 176.



Service	Status	Startup
Server	Started	Automatic
Spooler	Started	Automatic
TCP/IP NetBIOS Helper	Started	Automatic
TECNTAdapter	Started	Automatic
Telephony Service		Manual
Tivoli Endpoint	Started	Automatic
TrcBoot	Started	Automatic
UPS		Manual
Workstation	Started	Automatic
World Wide Web Publishing Service	Started	Automatic

Figure 99. NT event log adapter installation complete

5.5.1.3 Configure the Web IDS sensor

After installing the Web IDS Sensor on host rmnt37, we have to finalize the setup with some configurations:

1. Set the Environment Path on Windows NT. Add the Perl path to the environment (C:\perl_nt\bin\w32-ix86\riskmgr\adapters\perl\bin).

2. Make a backup of the files C:\tecnt\etc\c\tecad_nt.fmt and C:\tecnt\etc\tecad_nt.cds.

3. Copy the content of the file C:\webids_nt\bin\w32-ix86\RiskMgr\adapters\etc\webids.fmt to the end of the file C:\tecnt\etc\c\tecad_nt.fmt.

4. Execute the following command and make sure that everything is entered on one line:

   ```
   C:\tecnt\bin\nt_gencds C:\tecnt\etc\c\tecad_nt.fmt
   C:\tecnt\etc\tecad_nt.cds
   ```

5. Stop the TEC adapter service and restart it by starting the command prompt, changing the directory to c:\tecnt\bin, and entering the following commands:

   ```
   net stop TECNTadapter
   net start TECNTadapter
   ```

Check the command

Use the `postemsg` command to test if the TEC adapter is configured properly:

```
postemsg -f <conf file name> -m <message> <class> <source>
```

For example:

```
postemsg -f x:\tecnt\etc\tecad_nt.conf -m test tecdb tec
```

6. Add the Log sources at the end of the file c:\tecnt\etc\tec_nt.conf:
   a. LogSources=c:\progra~1\IBMHTT~1\logs\access.log.
   b. Stop the IBM HTTP Server and restart the services.
7. Execute the following command sequence:
   a. Change the directory to c:\webids_nt\bin\w32-ix86\riskmgr\adapters\bin\.
   b. Execute the command:

      ```
      webids -lp c:\progra~1\IBMHTT~1\logs\access.log
      ```

   c. Keep this process running. It will forward all the real time log entries to the TEC server and TEC console.
8. To configure the Risk Manager Server, refer to Section 5.4.4, “Risk Manager server configuration” on page 170.
9. Use the `webids test.log` command to test if Web IDS is properly configured:
   a. Change the directory to c:\webids_nt\bin\w32_ix86\riskmgr\adapters\bin.
   b. Execute the command:

      ```
      webids test.log
      ```

   c. The output is printed on standard output.

In order to verify the successful installation of this component, refer to Section 5.5.2.4, “Risk Manager and Web IDS verification” on page 188.

5.5.2 Installation in a Tivoli environment

Be sure that the Risk Manager Web Intrusion Detection system installation package is installed on endpoints in a Tivoli environment. This package contains the SIS-enabled installation support for Web IDS for Windows NT, AIX, and Solaris. This package also contains the webids.baroc file, the correlation rules and prolog files, the webids.fmt and webids.nt.fmt format files, and the default configuration files (sig.nefarious) that are required for Web IDS.

5.5.2.1 Installing a Tivoli Endpoint

The installation process of the Tivoli Endpoint software on host realsecure, as shown in Figure 96 on page 173, can be described in four steps:

1. The first step is to prepare Windows NT for Tivoli Web IDS:
   a. Install Windows NT Server 4.0.
   b. Install Service pack version 5.0 or higher.
   c. Install IBM HTTP Server.

Watch the file system

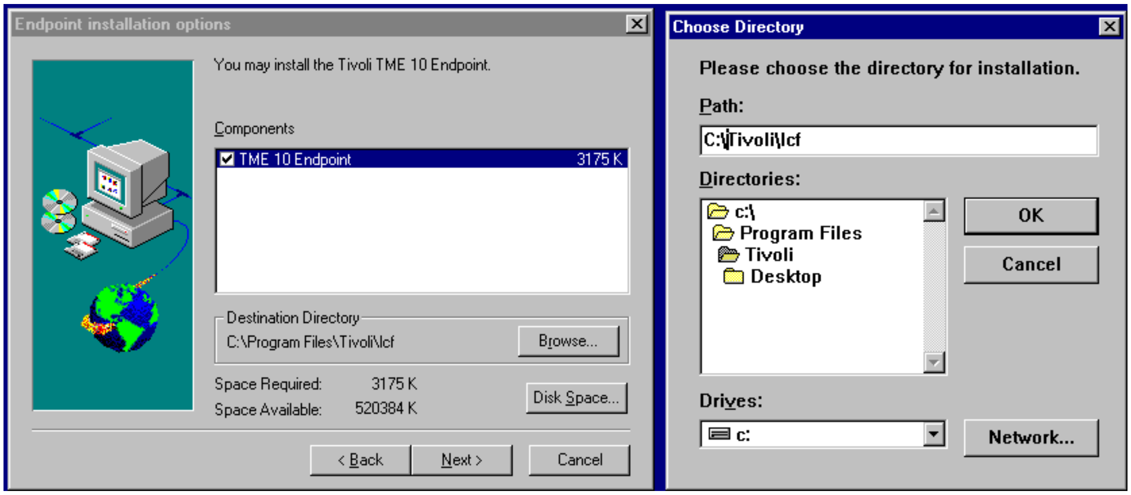
Check the file system used on your hard disk; it should be formatted with the NTFS. If the file system of the hard disk is FAT, then convert it using the following command:

```
c:> convert volume /fs:ntfs
```

2. Insert the Tivoli Management Framework version 3.7 RevisionB CD:
   a. Choose the folder x:\pc\lcf\winnt (x: is the CD Drive).
   b. Double-click the setup.exe.

Change the directory

Please change the default installation directory c:\program files\Tivoli\lcf\ to c:\tivoli\lcf for NT based installations, as depicted in Figure 100 on page 179.



Endpoint installation options

You may install the Tivoli TME 10 Endpoint.

Components

☑ TME 10 Endpoint 3175 K

Destination Directory

C:\Program Files\Tivoli\lcf

Space Required: 3175 K

Space Available: 520384 K

Choose Directory

Please choose the directory for installation.

Path: C:\Tivoli\lcf

Directories:

c:\
Program Files
Tivoli
Desktop

Drives: c:

Figure 100. Endpoint Installation changing default directory

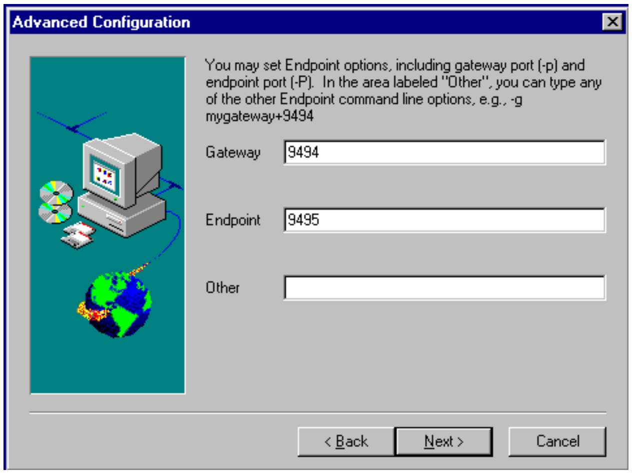
3. Enter the host name and IP address of the TEC server and local host in the file c:\winnt\system32\dirvers\etc\hosts.

4. In the Advanced Configuration panel, shown in Figure 101 on page 180, you need to enter the TME Gateway and Endpoint port number that will be used. By default, the Other option is null. If there are multiple gateways in your TME environment, then provide a specific gateway using the Other option in either of two ways:

```
-g Host name+portnumber
```

or

```
-g ipaddress+portnumber
```



You may set Endpoint options, including gateway port (-p) and endpoint port (-P). In the area labeled "Other", you can type any of the other Endpoint command line options, e.g., -g mygateway+9494

Gateway: 9494

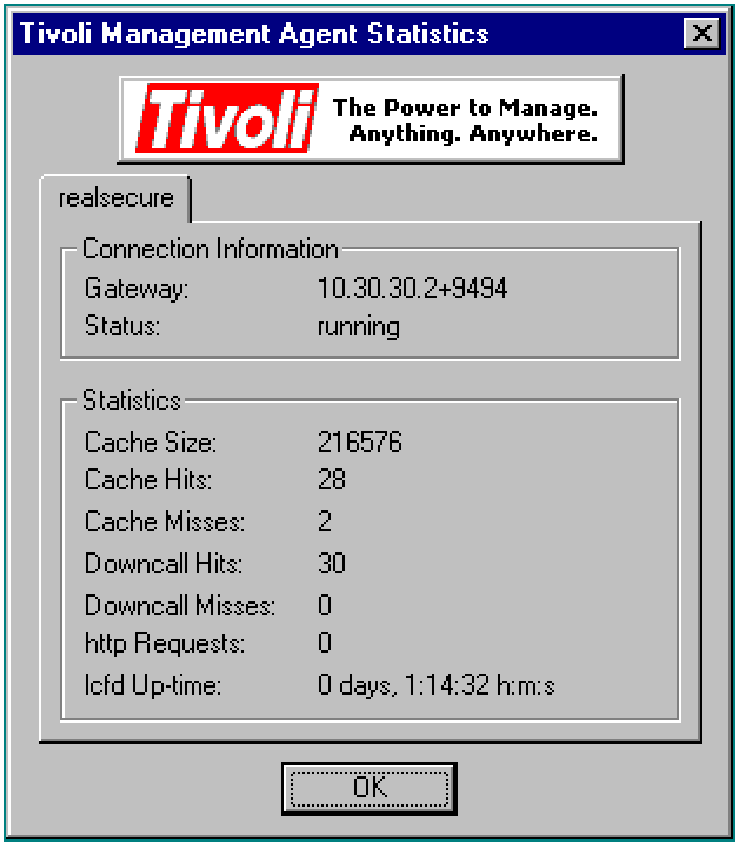
Endpoint: 9495

Other:

Figure 101. Endpoint installation

5. After successful installation, a Tivoli Icon is added to the taskbar and the endpoint statistics are available, as shown in Figure 102 on page 181. More information about the endpoint will be available using the local host’s IP address in a standard URL, for example:

```
http://ipaddress:9495
```


Tivoli Management Agent Statistics
Tivoli
The Power to Manage. Anything. Anywhere.
realsecure
OK

Connection Information

Gateway:	10.30.30.2+9494
Status:	running

Statistics

Cache Size:	216576
Cache Hits:	28
Cache Misses:	2
Downcall Hits:	30
Downcall Misses:	0
http Requests:	0
lcfd Up-time:	0 days, 1:14:32 h:m:s

Figure 102. Endpoint installation statistics

5.5.2.2 Web IDS adapter installation

To install the Web IDS adapter on a Tivoli Endpoint, we use the Software Installation Services (SIS) on the TMR server. For Web IDS, we distribute Web IDS, Perl support, and the Risk Manager Even Integration Facility to the destination machine, as depicted in Figure 96 on page 173.

Follow these steps:

1. On the TMR server, start up the SIS GUI by issuing `#wsisgui` and entering your password

   After entering the password, the dialog in Figure 103 on page 182 will appear. Select **Worksheet -> Select machines**.

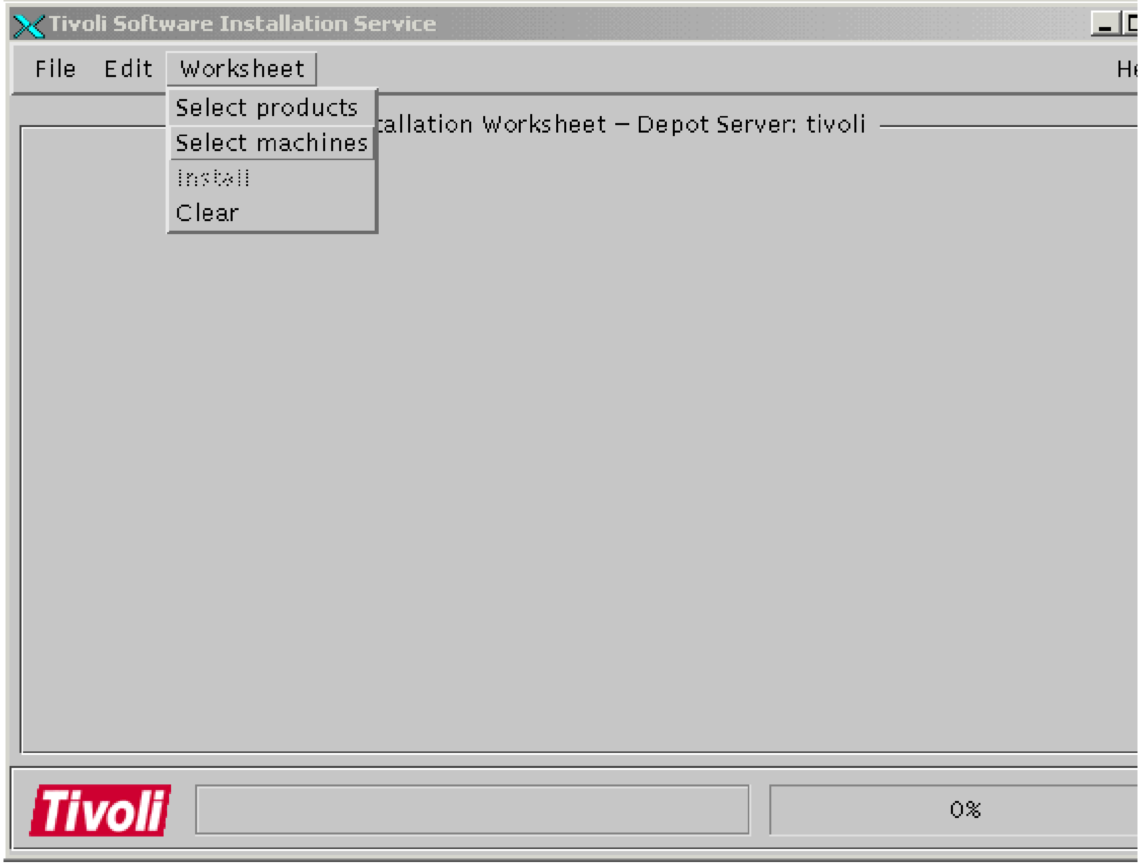
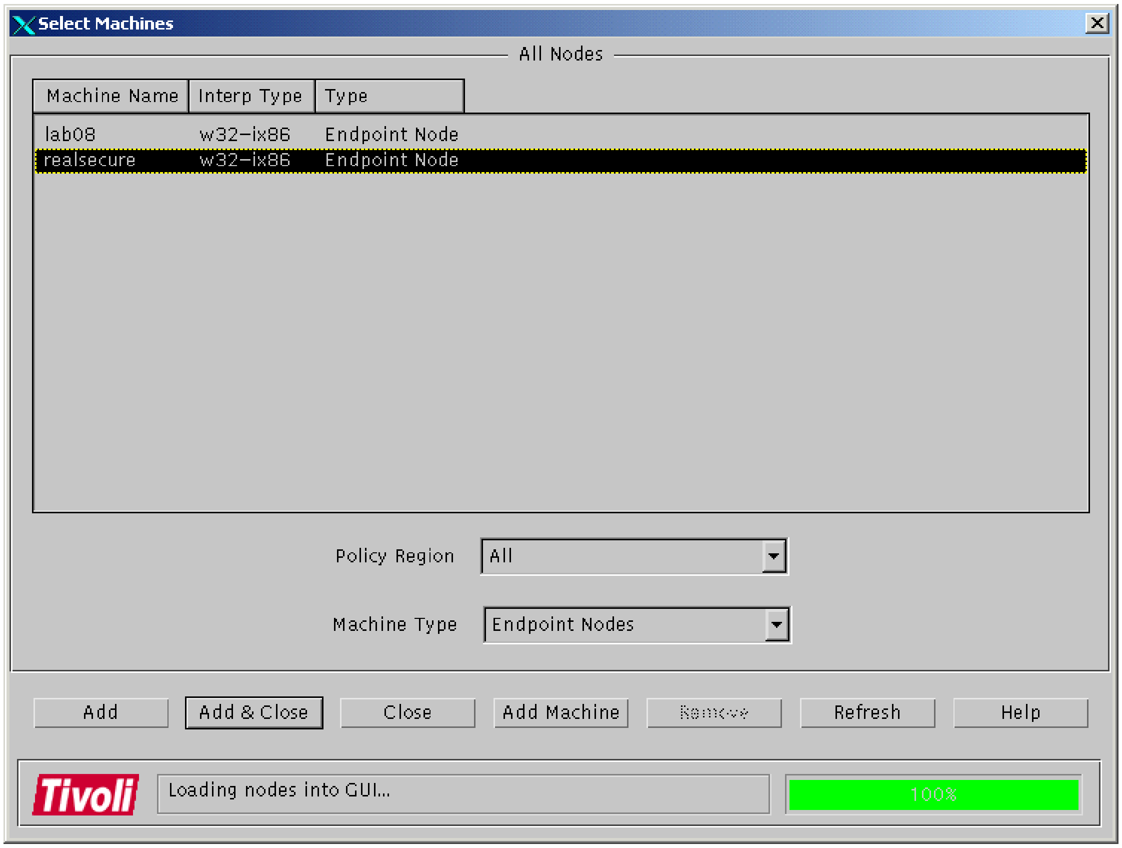

Tivoli Software Installation Service
File
Edit
Worksheet
He
Select products
Select machines
Install
Clear
tallation Worksheet – Depot Server: tivoli
Tivoli
0%

Figure 103. Tivoli Software Installation Service GUI

2. Change the Machine Type drop-down list to Endpoint Nodes. Select the appropriate endpoint from the list, as shown in Figure 104 on page 183.



Select Machines

All Nodes

Machine Name	Interp Type	Type
lab08	w32-ix86	Endpoint Node
realsecure	w32-ix86	Endpoint Node

Policy Region: All

Machine Type: Endpoint Nodes

Loading nodes into GUI...

100%

Figure 104. Select the endpoint (SIS)

3. After selecting the endpoint(s) we want to install the software packages on, we close this panel using the button Add & Close. In the next step, we select the components or products we want to install. Choose the Select Products option shown in Figure 105 on page 184.

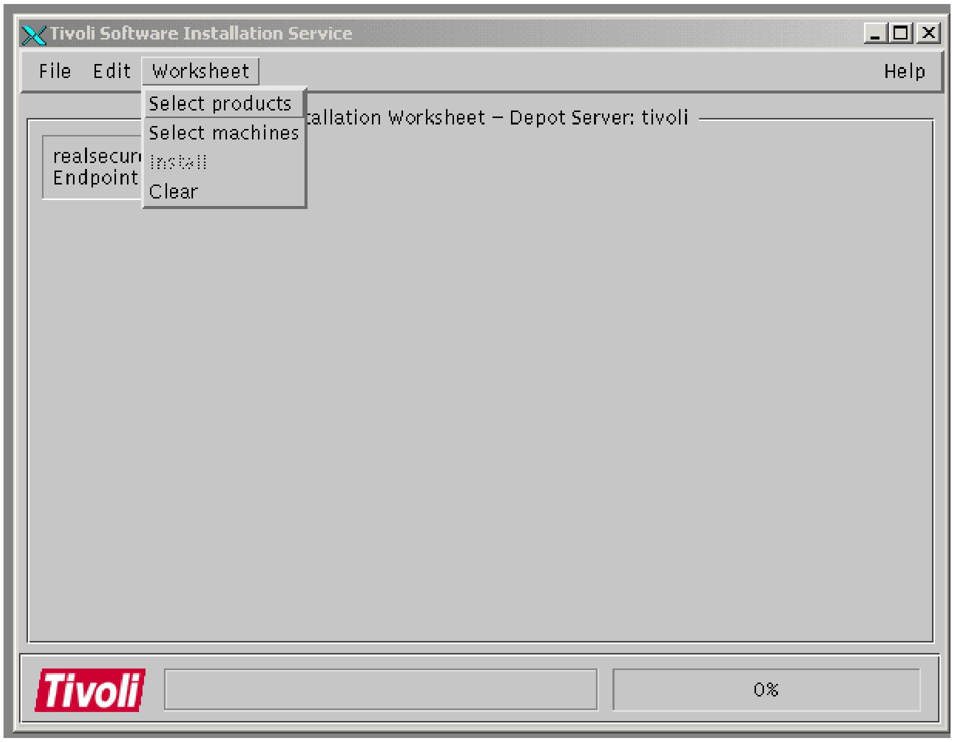


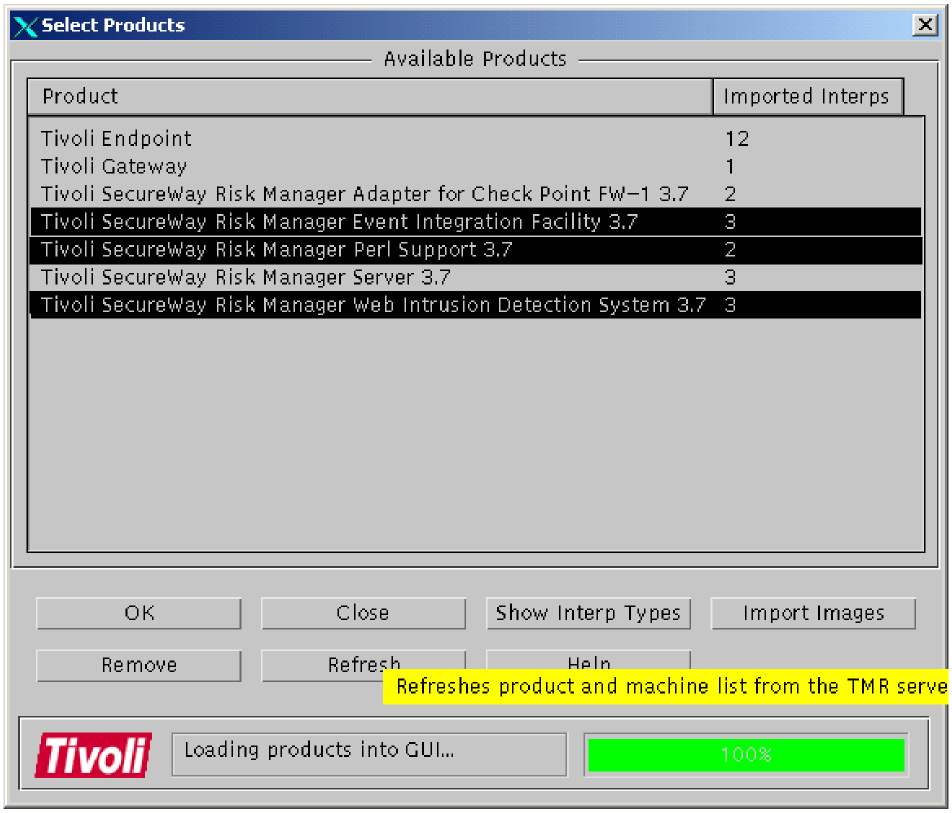
Figure 105. Select Products option (SIS)

4. Select the following products from the product list shown in Figure 106 on page 185:

   a. Tivoli Risk Manager Perl Support 3.7

   b. Tivoli Risk Manager Event Integration Facility 3.7

   c. Tivoli Risk Manager Web Intrusion Detection System 3.7



Select Products

Available Products

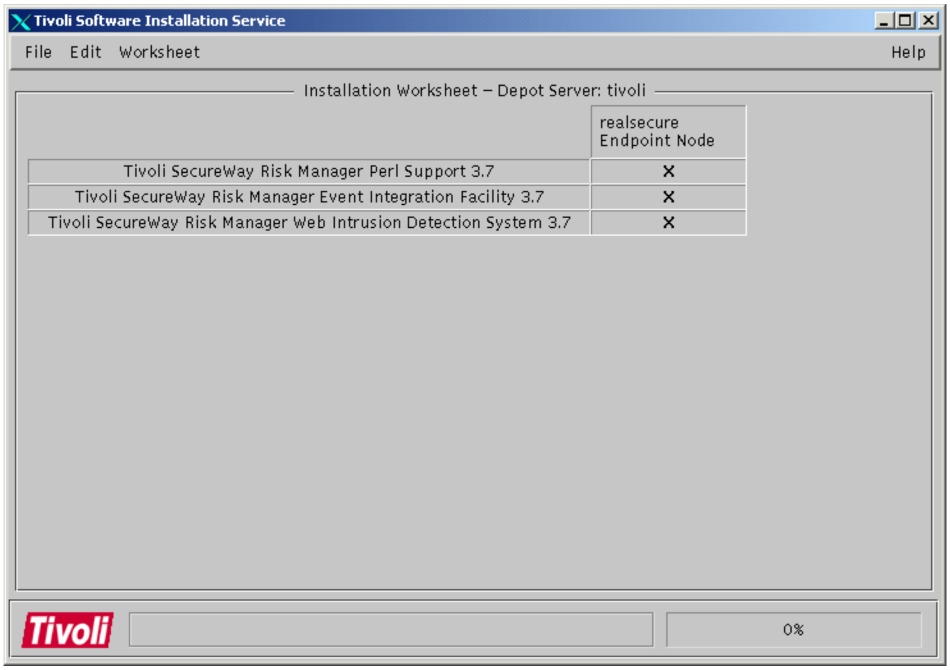
Product	Imported Interps
Tivoli Endpoint	12
Tivoli Gateway	1
Tivoli SecureWay Risk Manager Adapter for Check Point FW–1 3.7	2
Tivoli SecureWay Risk Manager Event Integration Facility 3.7	3
Tivoli SecureWay Risk Manager Perl Support 3.7	2
Tivoli SecureWay Risk Manager Server 3.7	3
Tivoli SecureWay Risk Manager Web Intrusion Detection System 3.7	3

Refreshes product and machine list from the TMR serve

Loading products into GUI...

Figure 106. Product list (SIS)

5. Check the three components and select OK. Figure 107 on page 186 shows the worksheet with your selected components.



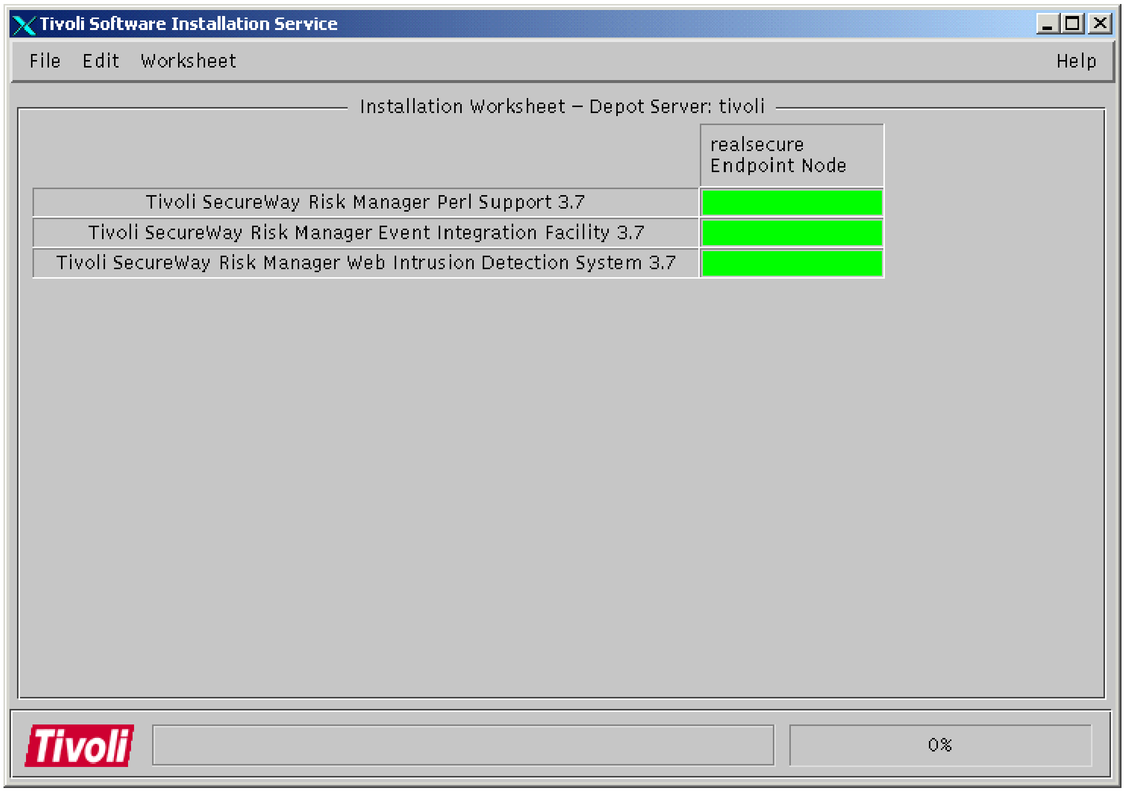
Installation Worksheet – Depot Server: tivoli

	realsecure Endpoint Node
Tivoli SecureWay Risk Manager Perl Support 3.7	✕
Tivoli SecureWay Risk Manager Event Integration Facility 3.7	✕
Tivoli SecureWay Risk Manager Web Intrusion Detection System 3.7	✕

Figure 107. Components worksheet (SIS)

6. Select **Worksheet -> Install**.

   A green bar, shown in Figure 108 on page 187, is indicating the successfully distributed three adapters. At the endpoint, a new directory is created (..\tivoli\lcf\bin\w32-ix86\riskmgr\), and individual adapter folders have been added.



Installation Worksheet – Depot Server: tivoli

	realsecure Endpoint Node
Tivoli SecureWay Risk Manager Perl Support 3.7	🟩
Tivoli SecureWay Risk Manager Event Integration Facility 3.7	🟩
Tivoli SecureWay Risk Manager Web Intrusion Detection System 3.7	🟩

Figure 108. Successful installation of components

5.5.2.3 Configure the Web sensor

Next we configure the Web sensor on the Windows NT system realsecure, as shown in Figure 96 on page 173.

1. Set the following environment path:

   Perl path C:\tivoli\lcf\bin\w32-ix86\riskmgr\adapters\perl\bin

   DLL path C:\tme\lcf\bin\w32-ix86\mrt

2. Set the adapter path. Execute the following command files:

```
c:\winnt\tivoli\lcf\rma_eif_env.cmd
c:\winnt\tivoli\lcf\rma_perl_env.cmd
c:\winnt\tivoli\lcf\rma_web_env.cmd
```

3. Copy the content of the file C:\tivoli\lcf\bin\w32-ix86\riskmgr\adapters\etc\webids_nt.fmt to the end of the file C:\tivoli\lcf\bin\w32-ix85\riskmgr\adapters\bin\rmad.fmt (create a new text file if rmad.fmt does not exists)

Important

Take care while concatenating the files. Use Notepad to open the files and do not include spaces between the lines.

4. Execute the following command and make sure that everything is entered on one line:

   ```
   c:\tivoli\lcf\bin\w32-ix86\riskmgr\adapters\bin\riskmgr_gencds rmad.fmt
   >rmad.cds
   ```

5. Stop the End Point service and restart it.

   a. Start a command prompt, change the directory to C:\tivoli\lcf\bin\w32-ix86\tme\tec\adapters\bin\ and enter the following commands:

   ```
   net stop Endpoint Service
   net start Endpoint Service
   ```

   b. Execute the following command:

   ```
   webids -lp c:\progra~1\IBMHTT~1\logs\access.log
   ```

5.5.2.4 Risk Manager and Web IDS verification

After executing the steps in Section 5.5.2.3, "Configure the Web sensor" on page 187, we need to verify that the setup is working correctly.

Do these steps:

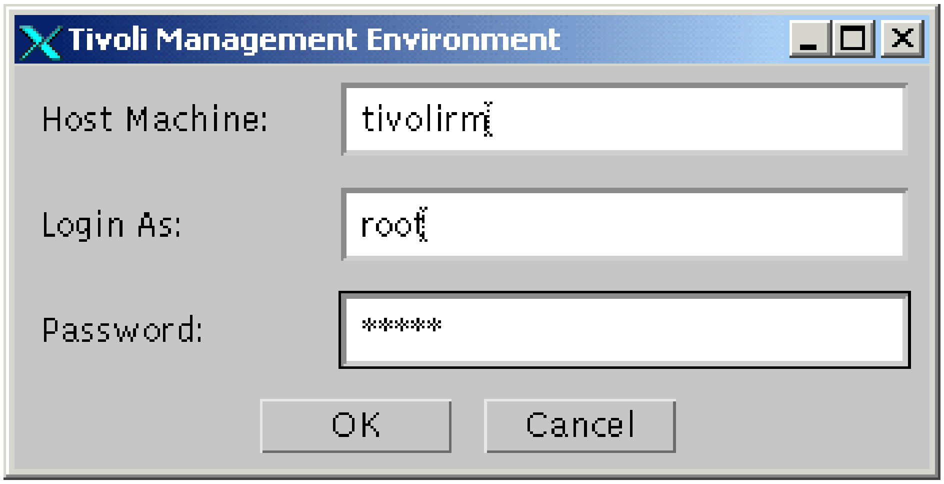
1. In order to generate HTTP log file entries you need to point your browser to the URL:

   ```
   http://localhost/../
   ```

2. On the Risk Manager Server, start up the Tivoli Enterprise Console by issuing:

   ```
   # tec_console &
   ```

3. The password field will be shown. Enter your user ID and password, as shown in Figure 109 on page 189.



Tivoli Management Environment

Host Machine: tivolirm

Login As: root

Password: ******

Figure 109. Tivoli Console login dialog

4. After entering the password, select **Windows -> Event Viewer** (see Figure 110).

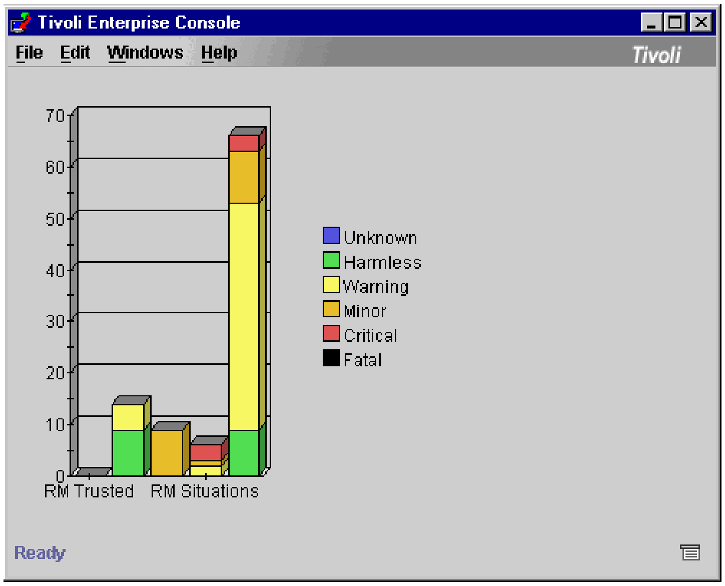
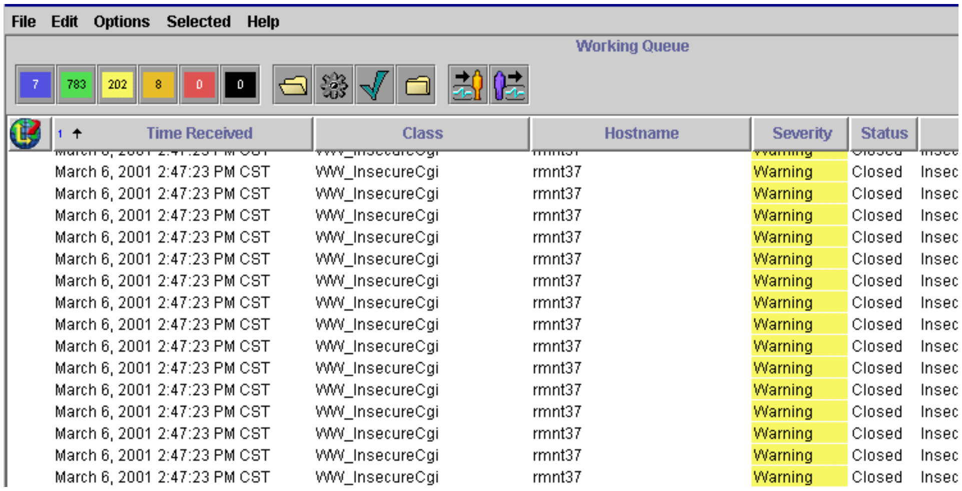


Figure 110. Tivoli Enterprise Console Event Viewer

5. Click on the bar chart and the TEC Event Viewer panel will appear, as seen in Figure 111. Some Web IDS events of the class WW_InsecureCgi are shown on the panel as a result of the Web Sensor.



Time Received	Class	Hostname	Severity	Status	
March 6, 2001 2:47:23 PM CST	WW_InsecureCgi	rmnt37	Warning	Closed	Insec
March 6, 2001 2:47:23 PM CST	WW_InsecureCgi	rmnt37	Warning	Closed	Insec
March 6, 2001 2:47:23 PM CST	WW_InsecureCgi	rmnt37	Warning	Closed	Insec
March 6, 2001 2:47:23 PM CST	WW_InsecureCgi	rmnt37	Warning	Closed	Insec
March 6, 2001 2:47:23 PM CST	WW_InsecureCgi	rmnt37	Warning	Closed	Insec
March 6, 2001 2:47:23 PM CST	WW_InsecureCgi	rmnt37	Warning	Closed	Insec
March 6, 2001 2:47:23 PM CST	WW_InsecureCgi	rmnt37	Warning	Closed	Insec
March 6, 2001 2:47:23 PM CST	WW_InsecureCgi	rmnt37	Warning	Closed	Insec
March 6, 2001 2:47:23 PM CST	WW_InsecureCgi	rmnt37	Warning	Closed	Insec
March 6, 2001 2:47:23 PM CST	WW_InsecureCgi	rmnt37	Warning	Closed	Insec
March 6, 2001 2:47:23 PM CST	WW_InsecureCgi	rmnt37	Warning	Closed	Insec
March 6, 2001 2:47:23 PM CST	WW_InsecureCgi	rmnt37	Warning	Closed	Insec
March 6, 2001 2:47:23 PM CST	WW_InsecureCgi	rmnt37	Warning	Closed	Insec
March 6, 2001 2:47:23 PM CST	WW_InsecureCgi	rmnt37	Warning	Closed	Insec
March 6, 2001 2:47:23 PM CST	WW_InsecureCgi	rmnt37	Warning	Closed	Insec

Figure 111. TEC Event Viewer

After these steps are completed, you should get a working Web Intrusion Detector sensor.

5.6 Host IDS setup

Risk Manager provides an adapter for Host Intrusion Detection (Host IDS) that can be deployed on secured systems to strengthen the security of the basic operating system.

Host IDS maps events that are detected and logged by the Windows NT, AIX, and Solaris operating systems into TEC events. It uses the Tivoli logfile adapter (syslogd) (for AIX and Solaris) or the Tivoli NT Event Log Adapter (for Windows NT) to send events to the TEC server in order to get correlated by Risk Manager with other events from different sources.

The following sections cover the installation and testing of Host IDS, as well as the integration with Tivoli Risk Manager. This implementation uses the TME and Non-TME method on Windows NT. The steps for this are detailed in the *Tivoli Risk Manager 3.7 User Guide*.

The different ways of setting up the sensor, (in a TME versus a non-TME environment) are shown in Figure 112 on page 191.

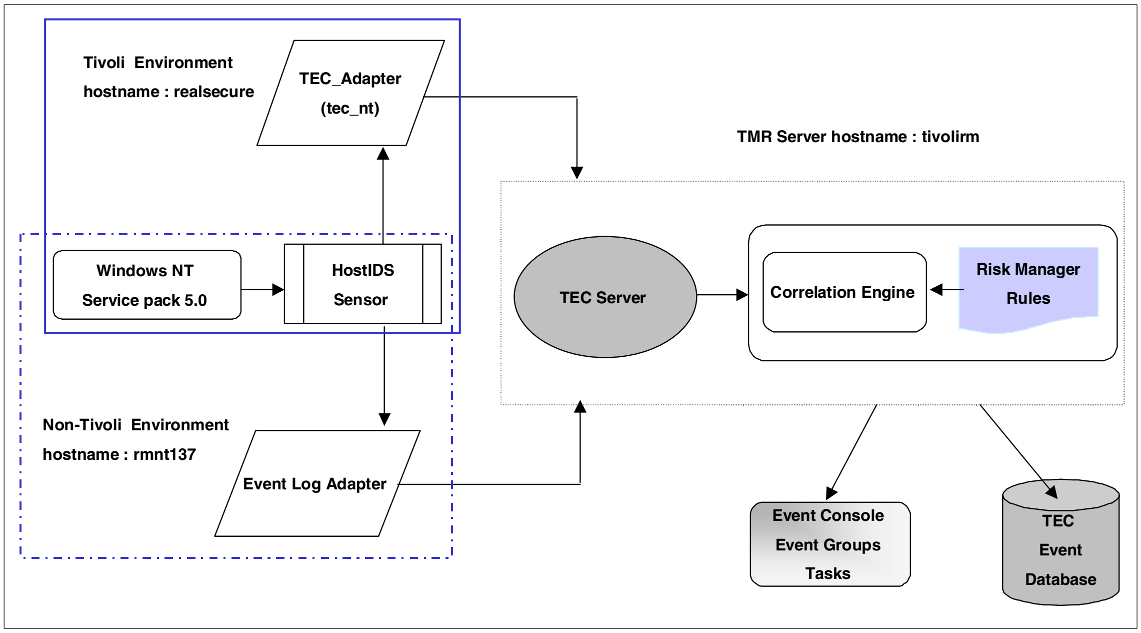


Figure 112. Host IDS configuration

5.6.1 Installation in a Non-Tivoli environment

To install Host IDS in a non-Tivoli environment, we use the .tar or .zip files. These steps are stated in the *Tivoli Risk Manager 3.7 User Guide*.

5.6.1.1 Windows NT and Risk Manager components installation

We install the Risk Manager components in a non-Tivoli environment on the Windows NT host rm137nt, as shown in Figure 112.

Do the following:

1. Make sure that you are logged on to the Windows NT system as Administrator and also be sure that you have the Risk Manager CD-ROM inserted in the CD-ROM drive. Extract the adapter files from the directory x:\rmadapters (x:CD-ROM drive).
2. Create the directory to extract the Risk Manager component files:

```
mkdir Hostids_nt
```

3. Extract the Risk Manager adapter files from the rm_adapter_cfg.zip file on the CD-ROM.

5.6.1.2 Event log adapter installation

For a detailed description of the NT event log adapter installation, refer to Section 5.5.1.2, “Installation of the NT Event Log Adapter” on page 174.

5.6.1.3 Configure Host IDS sensor

We now configure Host IDS on the Windows NT host rm137nt as shown in Figure 112 on page 191.

Do the following:

1. Make a backup of the following files:
   a. C:\tecnt\etc\c\tecad_nt.fmt
   b. C:\tecnt\etc\tecad_nt.cds
2. Copy the content of the file C:\hostids\riskmgr\acf_rep\os_nt.fmt to the end of the file C:\tecnt\etc\c\tecad_nt.fmt.
3. Execute the following command and make sure that everything is entered on one line:

   ```
   C:\tecnt\bin\nt_gencds C:\tecnt\etc\c\tecad_nt.fmt
   C:\tecnt\etc\tecad_nt.cds
   ```

4. Stop the TEC adapter and restart it.

   Start a command prompt, change the directory to C:\tecnt\bin, and enter the following commands:

   ```
   net stop TECNTadapter
   net start TECNTadapter
   ```

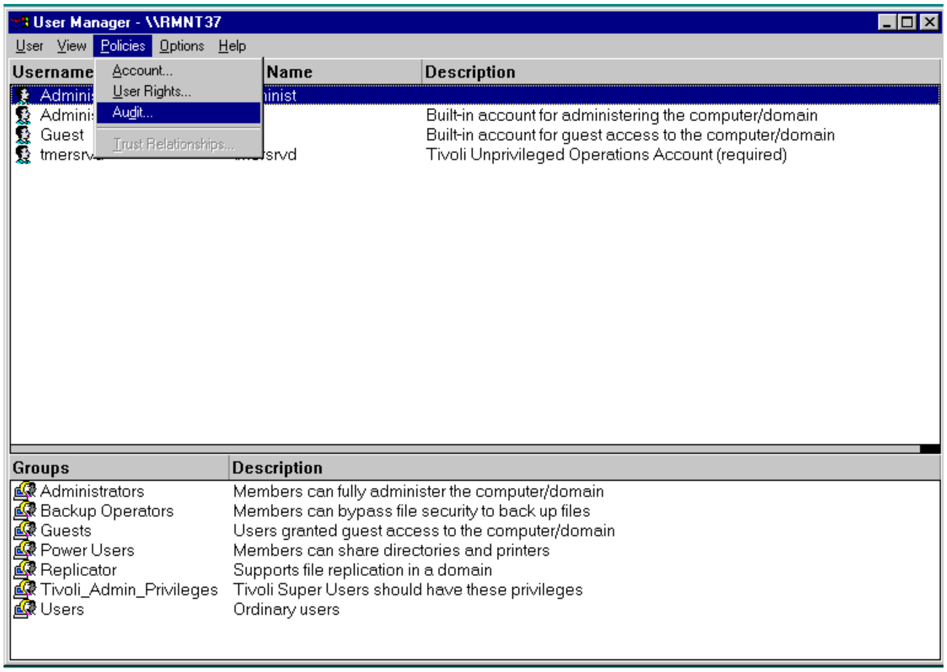
5. Using the command `postemsg`, we test if the TEC adapter is properly configured:

   ```
   postemsg -f <conf file name > -m message <class> <source>
   ```

   For example:

   ```
   postemsg -f x:\tecnt\etc\tecad_nt.conf -m test tecdb tec
   ```

6. We need to explicitly enable auditing of security events for the Windows NT system rm137nt using the User Manager. Select **Start -> Programs -> Administrative Tools -> User Manager for Domains**, and the User Manager panel will appear, as shown in Figure 113 on page 193.

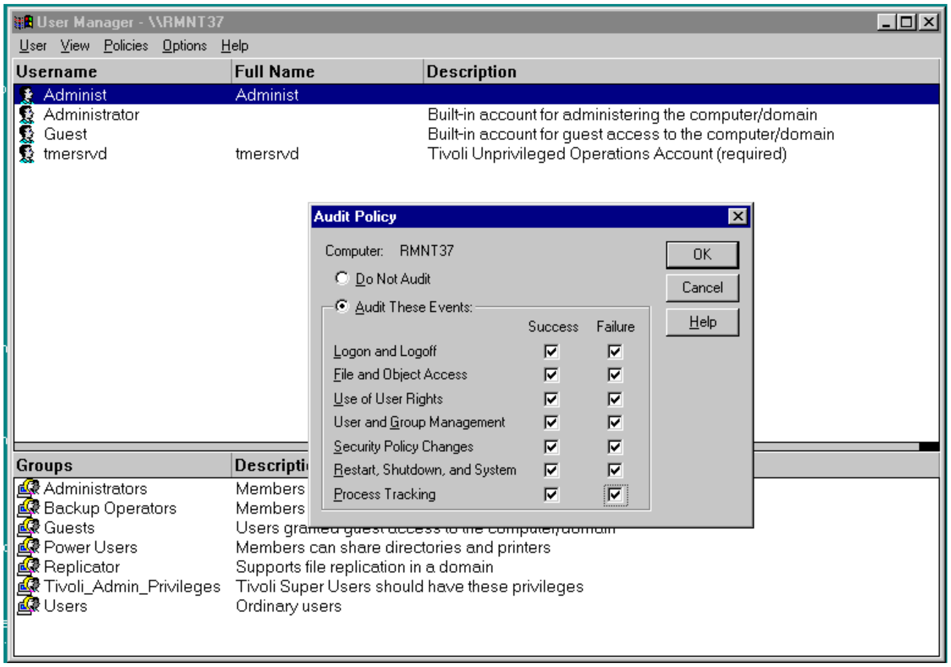


Username	Full Name	Description
Admini	inist	
Admini		Built-in account for administering the computer/domain
Guest		Built-in account for guest access to the computer/domain
tmersrv	rsrvd	Tivoli Unprivileged Operations Account (required)

Groups	Description
Administrators	Members can fully administer the computer/domain
Backup Operators	Members can bypass file security to back up files
Guests	Users granted guest access to the computer/domain
Power Users	Members can share directories and printers
Replicator	Supports file replication in a domain
Tivoli_Admin_Privileges	Tivoli Super Users should have these privileges
Users	Ordinary users

Figure 113. Select Audit option

7. Select **Policies -> Audit** and check all the events you want to audit, as depicted in Figure 114 on page 194.



Username	Full Name	Description
Administ	Administ	
Administrator		Built-in account for administering the computer/domain
Guest		Built-in account for guest access to the computer/domain
tmersrvd	tmersrvd	Tivoli Unprivileged Operations Account (required)

Audit Policy

Computer: RMNT37

○ Do Not Audit

● Audit These Events:

	Success	Failure
Logon and Logoff	☑	☑
File and Object Access	☑	☑
Use of User Rights	☑	☑
User and Group Management	☑	☑
Security Policy Changes	☑	☑
Restart, Shutdown, and System	☑	☑
Process Tracking	☑	☑

Groups	Descripti
Administrators	Members
Backup Operators	Members
Guests	Users granted guest access to the computer/domain
Power Users	Members can share directories and printers
Replicator	Supports file replication in a domain
Tivoli_Admin_Privileges	Tivoli Super Users should have these privileges
Users	Ordinary users

Figure 114. Check the events to audit

When you are done, click OK and close the User Manager dialog.

In order to test the successful installation of this component, refer to Section 5.6.2.4, “Risk Manager and Host IDS verification” on page 201.

5.6.2 Installation in a Tivoli environment

The Risk Manager adapter for Host IDS consists of a format file that is specifically designed to work in conjunction with the Tivoli logfile adapter so that it captures and forwards the events that are logged by the operating systems.

5.6.2.1 Installing a Tivoli Endpoint

The installation process of the Tivoli Endpoint software is described in Section 5.5.2.1, “Installing a Tivoli Endpoint” on page 178.

5.6.2.2 Adapter installation

We install the Host IDS adapter using the Adapter Configuration Facility (ACF) from the host tivolirm to the destination machine realsecure, as depicted in Figure 112 on page 191.

Do the following:

1. Create a new profile for Host IDS on the TMR Server tivolirm.

   a. Set the path using the command:

   ```
   # . /etc/Tivoli/setup_env.sh
   ```

   b. Start up the Tivoli Management Framework by issuing:

   ```
   #tivoli
   ```

2. After the Framework is started, as shown in Figure 115, double-click on the TEC-Region icon.

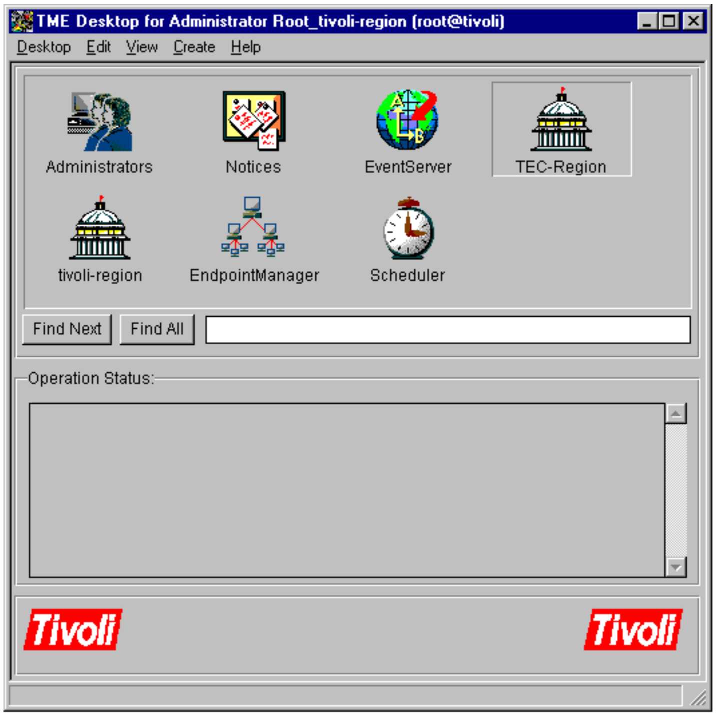


Figure 115. TME Desktop

3. Double-click on the Profiles for Enterprise Risk Management, as shown in Figure 116 on page 196.

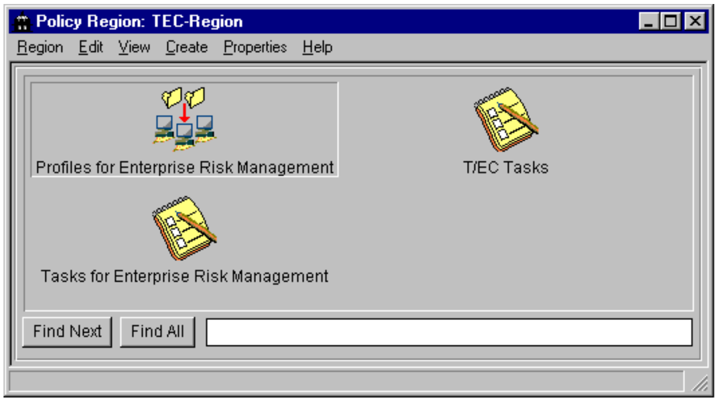

Policy Region: TEC-Region
Region Edit View Create Properties Help
Profiles for Enterprise Risk Management
T/EC Tasks
Tasks for Enterprise Risk Management
Find Next
Find All

Figure 116. Select the Profiles for Enterprise Risk Management

4. To create a new profile, select **Create -> Profile**, as shown in Figure 117.

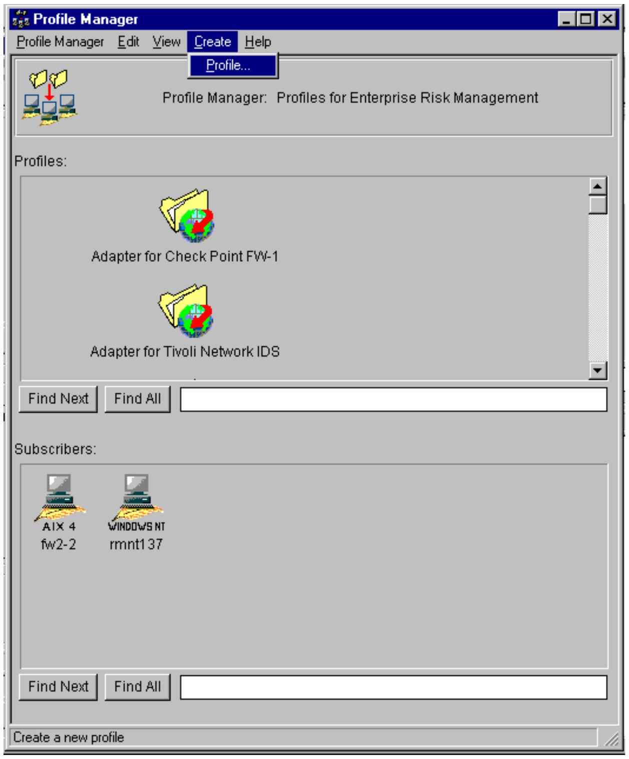
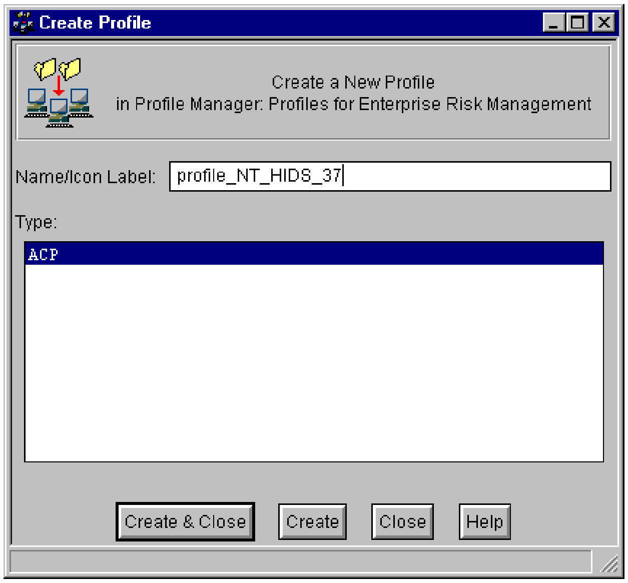

Profile Manager
Profile Manager Edit View Create Help
Profile...
Profile Manager: Profiles for Enterprise Risk Management
Profiles:
Adapter for Check Point FW-1
Adapter for Tivoli Network IDS
Find Next
Find All
Subscribers:
AIX 4
fw2-2
WINDOWS NT
rmnt137
Find Next
Find All
Create a new profile

Figure 117. Create a new profile for Host IDS

5. Create a new profile in the profile manager panels, as shown in Figure 118. Enter profile_NT_HIDS_37 as the new profile name and select ACP as the profile type. Finalize the creation by clicking on Create and Close.



Create a New Profile
in Profile Manager: Profiles for Enterprise Risk Management

Name/Icon Label: profile_NT_HIDS_37

Type:
ACP

Figure 118. Create profile

6. The new profile will appear in the Profile Manager view, as shown in Figure 119 on page 198.

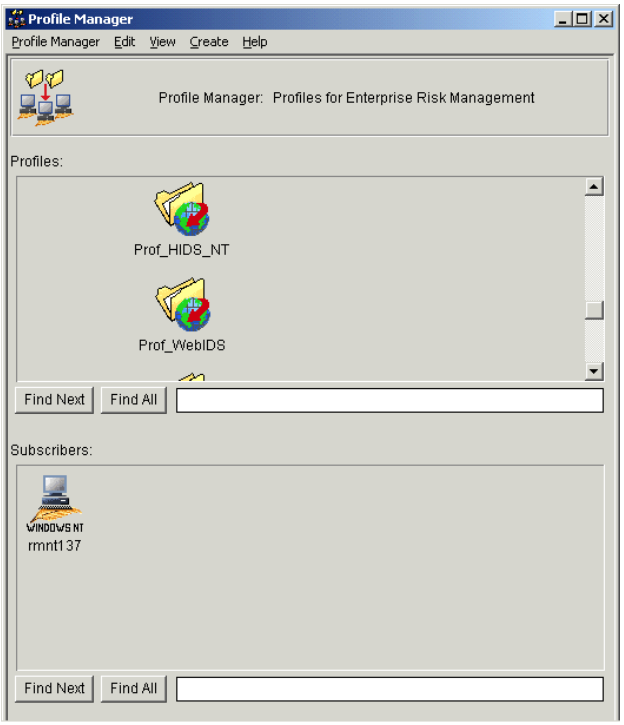
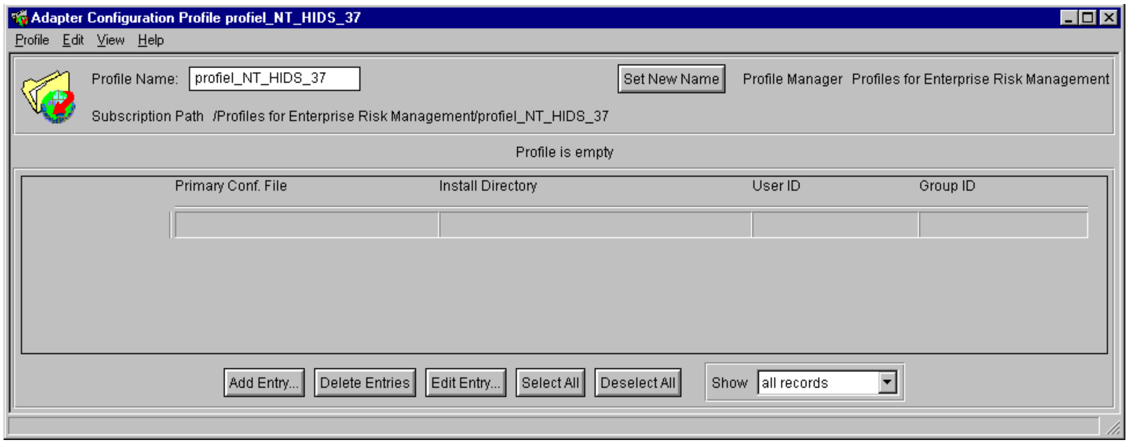


Figure 119. Select the new profile

7. Select the profile to install and double-click on it. The Adapter Configuration Profile dialog will appear, as shown in Figure 120 on page 199. Click on the Add entry button.



Adapter Configuration Profile profiel_NT_HIDS_37

Profile Name: profiel_NT_HIDS_37

Subscription Path /Profiles for Enterprise Risk Management/profiel_NT_HIDS_37

Profile Manager Profiles for Enterprise Risk Management

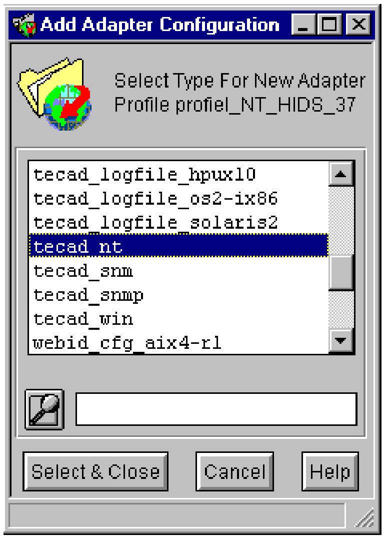
Profile is empty

Primary Conf. File	Install Directory	User ID	Group ID

Show all records

Figure 120. Add entry to new profile

8. Select the tecad_nt entry in the list shown in Figure 121 as the type for the new adapter profile. Click the Select & Close button.



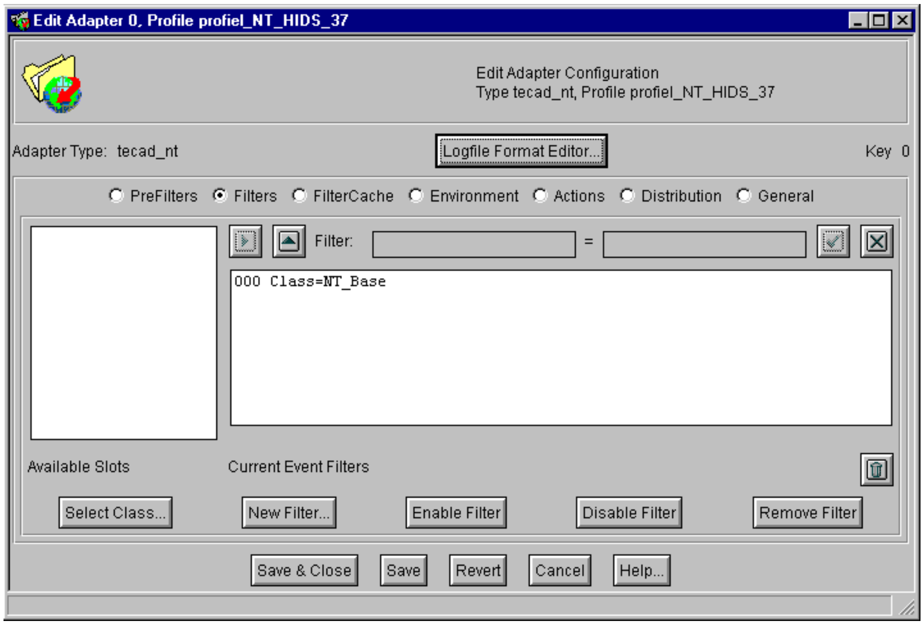
Add Adapter Configuration

Select Type For New Adapter Profile profiel_NT_HIDS_37

```
tecad_logfile_hpux10
tecad_logfile_os2-ix86
tecad_logfile_solaris2
tecad_nt
tecad_snm
tecad_snmp
tecad_win
webid_cfg_aix4-r1
```

Figure 121. Select the profile type

9. In the next dialog, shown in Figure 122 on page 200, you can edit the adapter configuration details for what type of operating systems events should be forwarded to the TEC server.



Edit Adapter 0, Profile profiel_NT_HIDS_37

Edit Adapter Configuration
Type tecad_nt, Profile profiel_NT_HIDS_37

Adapter Type: tecad_nt

Key 0

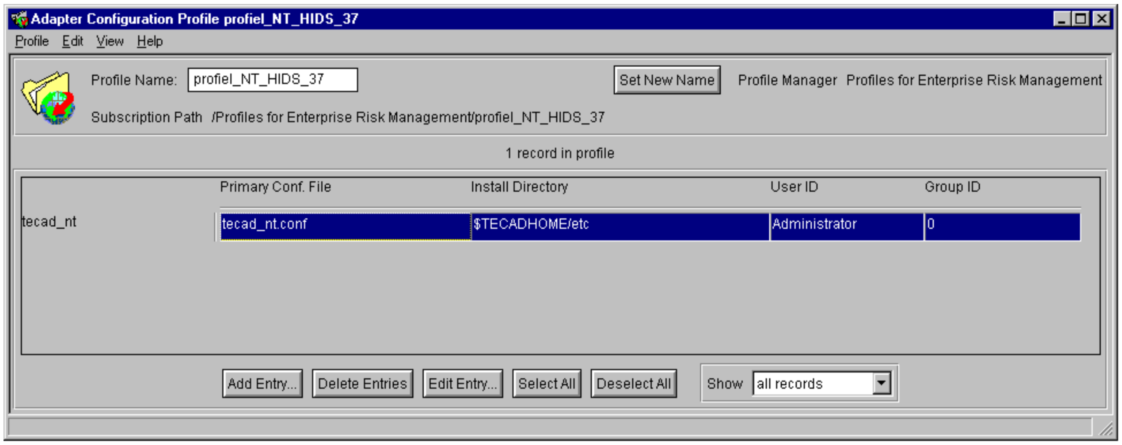
○ PreFilters ● Filters ○ FilterCache ○ Environment ○ Actions ○ Distribution ○ General

Filter: =

```
000 Class=NT_Base
```

Figure 122. Edit Adapter for new profile

10. Finally, you need to distribute the new profile to your target hosts, as shown in Figure 123.



Adapter Configuration Profile profiel_NT_HIDS_37

Profile Name: profiel_NT_HIDS_37

Profile Manager Profiles for Enterprise Risk Management

Subscription Path /Profiles for Enterprise Risk Management/profiel_NT_HIDS_37

1 record in profile

	Primary Conf. File	Install Directory	User ID	Group ID
tecad_nt	tecad_nt.conf	$TECADHOME/etc	Administrator	0

Show all records

Figure 123. Distribute the new profile

5.6.2.3 Configure the Host IDS sensor

In order to configure the Host IDS sensor on the Windows NT system realsecure, as shown in Figure 112 on page 191, you have to follow the next steps:

1. Set the Environment Path:

   DLL file path: x:\tivoli\lcf\bin\w320ix86\mrt\

2. Make a backup of the files:

   a. x:\tivoli\lcf\bin\w32-ix86\tme\tec\adapters\etc\c\tecad_nt.fmt

   b. x:\tivoli\lcf\bin\w32-ix86\tme\tec\adapters\etc\tecad_nt.cds

3. Copy the content of the file x:\hostids\riskmgr\acf_rep\os_nt.fmt to the end of the file x:\tivoli\lcf\bin\w32-ix86\tme\tec\adapters\etc\c\tecad_nt.fmt.

4. Execute the following command and make sure that everything is entered on one line:

   ```
   x:\tivoli\lcf\dat\1\cache\bin\w32-ix86\tme\tec\adapters\bin\nt_gencds
   x:\tivoli\lcf\bin\w32-ix86\tme\tec\adapters\etc\c\tecad_nt.fmt
   x:\tivoli\lcf\bin\e32-ix86\tme\tec\adapters\etc\tecad_nt.cds
   ```

5. Stop the TEC service and restart it using the following services.

   Open a command prompt and change the directory to the path x:\tivoli\lcf\bin\w32-ix86\tme\tec\adapters\bin, and enter:

   ```
   net stop End Point service
   net start End Point Service
   ```

6. We need to explicitly enable auditing of security events for the Windows NT system rm137nt using the User Manager. The details are described in bullet number 6. on page 192.

5.6.2.4 Risk Manager and Host IDS verification

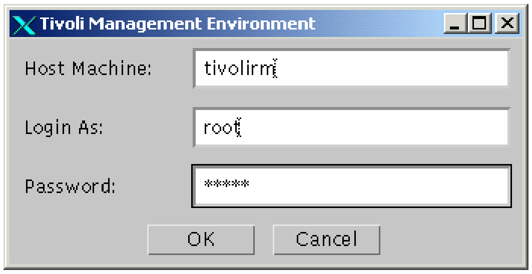
After doing the above steps, we need to verify that the configuration setup is working correctly. The test that is going to be done below is a simple login failure.

1. First login to the local host three times and enter a wrong password each time.

2. On the Risk Manager Server, start up the Tivoli Enterprise Console by issuing the command:

   ```
   # tec_console &
   ```

3. The logon dialog, as shown in Figure 124 on page 202, will be shown. Enter your user ID and password.



Host Machine: tivolirm

Login As: root

Password: ******

Figure 124. TEC Console login

4. After entering the password, the main TEC Console panel will appear, as shown in Figure 125.

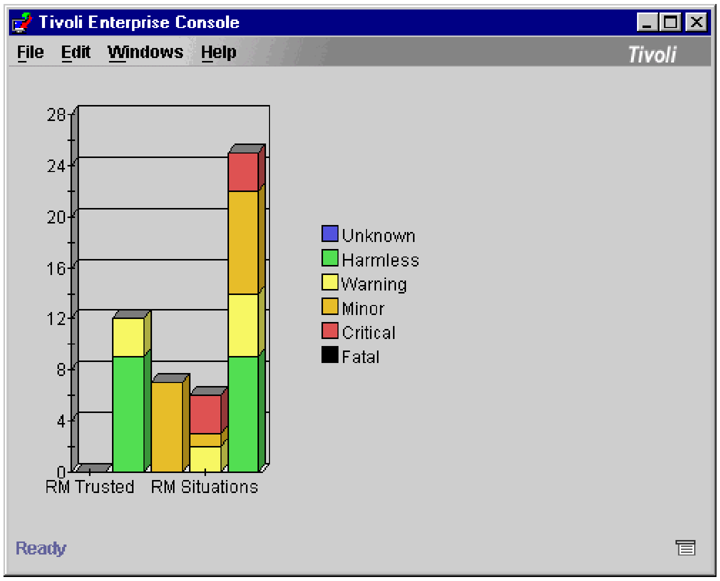
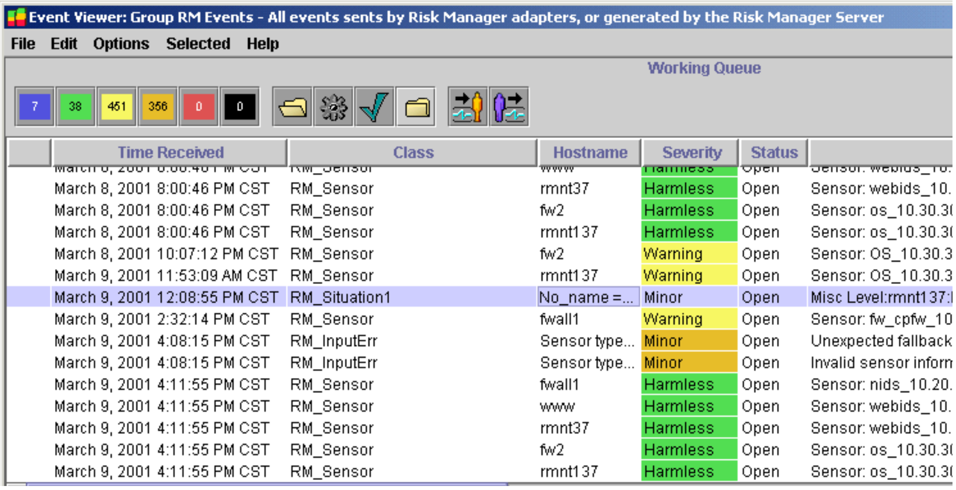


Figure 125. Tivoli Enterprise Console initial panel

5. Click on any portion on the bar chart and the Tivoli Event Viewer, depicted in Figure 126 on page 203, will appear. You should see some events with the Host IDS sensor name on it. Although it is not clear in the picture, some Host IDS events are shown on the panel which represent our failed login approach.



Event Viewer: Group RM Events - All events sents by Risk Manager adapters, or generated by the Risk Manager Server

	Time Received	Class	Hostname	Severity	Status	
	March 8, 2001 8:00:46 PM CST	RM_Sensor	www	Harmless	Open	Sensor: webids_10.
	March 8, 2001 8:00:46 PM CST	RM_Sensor	rmnt37	Harmless	Open	Sensor: webids_10.
	March 8, 2001 8:00:46 PM CST	RM_Sensor	fw2	Harmless	Open	Sensor: os_10.30.3
	March 8, 2001 8:00:46 PM CST	RM_Sensor	rmnt137	Harmless	Open	Sensor: os_10.30.3
	March 8, 2001 10:07:12 PM CST	RM_Sensor	fw2	Warning	Open	Sensor: OS_10.30.3
	March 9, 2001 11:53:09 AM CST	RM_Sensor	rmnt137	Warning	Open	Sensor: OS_10.30.3
	March 9, 2001 12:08:55 PM CST	RM_Situation1	No_name =...	Minor	Open	Misc Level:rmnt137:
	March 9, 2001 2:32:14 PM CST	RM_Sensor	fwall1	Warning	Open	Sensor: fw_cpfw_10
	March 9, 2001 4:08:15 PM CST	RM_InputErr	Sensor type...	Minor	Open	Unexpected fallback
	March 9, 2001 4:08:15 PM CST	RM_InputErr	Sensor type...	Minor	Open	Invalid sensor inforn
	March 9, 2001 4:11:55 PM CST	RM_Sensor	fwall1	Harmless	Open	Sensor: nids_10.20.
	March 9, 2001 4:11:55 PM CST	RM_Sensor	www	Harmless	Open	Sensor: webids_10.
	March 9, 2001 4:11:55 PM CST	RM_Sensor	rmnt37	Harmless	Open	Sensor: webids_10.
	March 9, 2001 4:11:55 PM CST	RM_Sensor	fw2	Harmless	Open	Sensor: os_10.30.3
	March 9, 2001 4:11:55 PM CST	RM_Sensor	rmnt137	Harmless	Open	Sensor: os_10.30.3

Figure 126. Tivoli Event Viewer

After all these configuration steps are followed, you should get a working Host Intrusion Detector Sensor.

Chapter 6. Intrusion detection

“Intrusion detection is the process of detecting unauthorized use of, or attack upon, a computer or network. Intrusion Detection Systems (IDS) are software or hardware systems that detect such misuse. IDSs can detect attempts to compromise the confidentiality, integrity, and availability of a computer or network. The attacks can come from attackers on the Internet, authorized insiders who misuse the privileges given them, and unauthorized insiders who attempt to gain unauthorized privileges.”[1]

After introducing important terms and concepts of intrusion detection, we give a brief insight into reconnaissance techniques used by prospective intruders.

A discussion of Tivoli Risk Manager and several of its intrusion detection sensors (such as network, host, Web and firewall IDS) follows, as well as their integration into Risk Manager.

We conclude with an excursion into the capabilities of Tivoli Decision Support concerning long term intrusion detection. Finally, a real world example will address some common pitfalls in a complex environment

6.1 Terms and concepts

Before going into greater detail, we define some of the terms associated with intrusion detection.

The first redbook on Risk Manager (see Appendix F.1, “IBM Redbooks” on page 359) also discusses threats, attacks, and hackers.

6.1.1 Threats

In order to prepare defense against intruders, it seems appropriate to reflect briefly on the damage an attack can result in:

- Disclosure of confidential data
- Tampering with data
- Erasing data
- Denial of service (DoS)
- Unauthorized use of resources (mail relaying, for example)
- Launching attacks to other sites

[1] Definition of intrusion detection in ITL Bulletin November 1999 (`http://www.nist.gov/itl/lab/bulletns/nov99.htm`)

All of these categories eventually result in a financial loss for your company, either, for example, directly, by interrupting production, or indirectly, by damaging your reputation.

An important part of a company's security concept is balancing the potential dangers versus the effort to protect your assets.

6.1.2 Offenders

"Know your enemy" is also an important concept when armouring your systems. Understanding who might want to intrude and what motivations drive them can be an invaluable source.

Some possible intruders and their motives are:

- Crackers and script kids

  While this group might still regard breaking into systems as an academic challenge, most security breaches in the DMZ, predominantly Web servers, are perpetrated by inexperienced kids fiddling with easy-to-use scripts readily available on the Internet.

- Employees

  We are not only considering disgruntled current or former employees, but also those misusing computers, be it due to negligence, ignorance, or a false sense of needing to be up-to-date with the latest tools, screen savers, and so on, which happen to be non-conformant with company standards.

- Competitors and spies

  If you are targeted by this kind of intruder, they are probably the most dangerous: they commonly have abundant resources, are determined to break your system, and probably use a combination of crackers and internals.

6.1.3 Attack versus misuse

Certain activities, although not in compliance with company policy, do not necessarily constitute an attack. Besides, uneducated users often cause disruptions unwittingly. We will distinguish between *attacks* and *misuse*.

6.1.3.1 Attacks

Attacks are activity patterns indicating that someone may be engaged in malicious, unauthorized, or otherwise undesirable activity involving the systems and/or data on your network. Examples of these include Denial of Service attacks (WinNuke, SYN Flood, and LAND), unauthorized access attempts (such as Back Orifice access and Brute Force login), pre-attack probes (such as SATAN scans, stealth scans, and connection attempts to non-existent services), suspicious activity (such as TFTP traffic), attempts to install backdoor programs (such as rootkit or BackOrifice2000), attempts to modify data or Web content, and attempts to stop services or kill programs.

6.1.3.2 Misuse

Misuse is non-attack activity that violates stated security or appropriate use policy. Examples of these include abuse of administrator privilege (installation of inappropriate services), HTTP activity (who is surfing the net and where they are going), analysis of access to Windows shares (for example, connections from engineering to accounting), and e-mail session decoding.

6.1.4 Potential targets

The targets an intruder chooses depend on his objectives; the DMZ may be just a stepping stone into your internal network. Servers with more important services should only run that service and should always have a Host IDS running.

These are the more popular targets that definitely need to be secured:

- Demilitarized Zone

  Web server, database, DNS, and application gateways (mail, web, and so on)

- Intranet

  Mailserver, databases, file servers, and certain PCs (at least management's)

- Internet

  SoHo PCs and laptops (remote access, even when via VPN)

The last item, company laptops, might be a bit surprising at first. They are, however, a prime target for intruders, since a VPN only protects the connection between the remote computer and the company network itself (by authenticating each other and encrypting traffic). On the other hand, remember that an unprotected Internet connection is used, leaving the remote system itself very vulnerable to attacks. Once it is compromised, the internal network is wide open.

Administrators should therefore deploy personal firewalls on systems remotely accessing the company network; Host IDS might be an even smarter addition.

6.1.5 External versus internal intrusion

Intruders coming from the Internet usually precede their efforts with reconnaissance activities, which can serve as a warning in advance. Within that span of time, administrators still have a chance to prevent damage.

An internal intruder, for example, company employees or contractors, have no need for most of the external's preparations and reconnaissance, since they are already quite familiar with the infrastructure. Therefore, they are less detectable and subsequently to be considered quite dangerous.

Physical intrusion

Always keep in mind, security must not be seen only from a technical point of view - an intruder will not bother to circumvent your firewall if he can gain physical access to your network easily. A laptop with all the tools available out there, plugged into a network outlet anywhere on your company premises, will not be seen by your Internet firewall or the intrusion detection tools in your DMZ. This is also true for any VPNs you might maintain with your branches or even business partners - the weakest part in such a scenario sets the level of security for all participants.

Internal offenders also include the playful sort of people who have ”read this, downloaded that” and figure their employers network is just the right environment to try out their latest tool from hacker sites. While usually not very successful in breaking into your more important systems, these activities still pose a rather serious threat to the availability of vital services. They also might compromise other users' accounts and can thereby cause any sort of hassle.

6.1.6 False alarms

Some of the internal intrusion attempts will be false alarms, such as employees mistyping passwords or lacking skill in applications they use.[2]

While these attempts cannot be neglected from an administrative point of view, in terms of security, these attempts should be discarded as noise that will distract your attention from the real thing.

A more sophisticated approach is *event flooding*, used to distract administrators from actual attacks. An experienced intruder, presuming you have deployed IDS, will try to disguise his proceedings by producing a lot of

[2] Misbehaving or poorly configured applications also contribute to such alarms. For example, using `xhost` instead of `xauth` for X11 authentication will produce a number of “AUTH X11 - Connection failed” events on Risk Manager.

noise, including faked source addresses and different targets than the one he is really attacking.

6.1.7 Host versus network intrusion detection

There is not really a decision between the two methods of gathering data to detect intrusions. Both are mandatory components, with network intrusion detection being the base, while host based sensors protect sensitive systems, such as Web servers, databases, or even firewalls.

While Network IDS provides early warning of attacks, Host IDS confirms the actual success or failure of intrusion attempts and collects further data, such as user or file names.

Furthermore, local users with access to a console who try passwords, attempt unauthorized access to files, or install hacker tools will only be noticed by an IDS implemented on that very host.

False sense of security

Do not let the implementation of an intrusion detection toolkit lure your into a false sense of security. It is important to apply patches and fixes relevant to the security of systems, both at operating system and application software level.

Be sure to review *How To Eliminate The Ten Most Critical Internet Security Threats* at:

`http://www.sans.org/topten.htm`.

Remember: false security can be worse than no security at all.

However, network sensors are usually what you will start off with, adding host based sensors as required.

6.1.8 Real-time versus long-time analysis

Another ongoing dispute exists over whether to use so-called real-time IDS versus long-term analysis. Again, both methods are mandatory in order to catch all occurrences of suspicious traffic.

While real-time IDS will catch unwary or brute-force attacks as well as actual break-ins and immediately alert administrators, it basically focuses on a short period of time in its analysis. The primary purpose of long-term IDS is to discover more advanced intrusion techniques, such as very slow scans or attacks over a prolonged period of time.

Due to the enormous amount of data, sufficient computing power is mandatory, especially for long-term analysis and correlation.

Tivoli Decision Support (refer to Chapter 7, “Reporting using TDS for Enterprise Risk Management” on page 255) is used for long-term analysis.

6.1.9 Location of sensors

Intrusion detection can serve two purposes: detecting attacks and detecting intrusions. As a rule of thumb, outside the firewall is attack detection, and inside is intrusion detection; therefore, an objective needs to be defined first. Attack detection basically requires an additional network intrusion detection system *outside* (preferably not on) your outer firewall.

With some sensors, like WebIDS and Firewall IDS, it is quite evident where to place them. Others, like Host IDS, might not be as obvious. As outlined in Section 6.1.4, “Potential targets” on page 207, Host IDS should be deployed on each one of the systems identified there. It is equally important to add Host IDS also on servers that already run some other form of IDS. An attacker only targeting for operating system flaws of a Web server or a firewall will not be seen by specialized IDS (although Network IDS will catch some of the probes). All of your Network IDS sensors also need to be secured by Host IDS.

If all important systems cannot be equipped with a sensor, either due to budget restraints, lack of time, or enough skilled intrusion detection specialists, be sure to move sensors around in variable intervals.

Be aware that Network IDS might turn out to be unable to catch all traffic if the machine is too slow and drops packets. Either invest in a faster system or consider further subnetting the network concerned.

In switched or very fast networks, it might even make sense to equip crucial systems with Network IDS in non-promiscuous mode, watching network traffic for just that very host.

6.2 Reconnaissance

Besides denial of service assaults, the goal of attacking a system is to gain access with administrative rights. The steps to achieve this are usually reconnaissance, selecting a worthwhile target, probing it for vulnerabilities, and exploiting vulnerabilities.

Some distinction should be made regarding external versus internal attackers. Although basically the same methods and tools are used, an internal attack will not require as much reconnaissance (as explained in Section 6.2.5, “External versus internal offenders” on page 218)

6.2.1 Basics

Attackers either try to find vulnerable systems to use as stepping stones for further intrusions or they direct their efforts at deliberately chosen sites. In the latter case, a great deal of information can be gathered from various sources.

The company home page almost always gives you information about the locations (see notice below) and sometimes employees.

Bigger companies have their own range of IP addresses, which can be looked up using the Whois-database at their respective Regional Internet Registries (RIR).[3]

[3] There are three Internet Registries in the world: one for Europe (RIPE NCC, `http://www.ripe.net`), one for the Americas (ARIN, `http://www.arin.net`), and one for Asia-Pacific (APNIC, `http://www.apnic.net`).

An example of the Whois-database output follows:

```
Whois Server Version 1.3

Domain names in the .com, .net, and .org domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: IBM.COM
   Registrar: NETWORK SOLUTIONS, INC.
   Whois Server: whois.networksolutions.com
   Referral URL: www.networksolutions.com
   Name Server: INTERNET-SERVER.ZURICH.IBM.COM
   Name Server: NS.WATSON.IBM.COM
   Name Server: NS.ERS.IBM.COM
   Name Server: NS.ALMADEN.IBM.COM
   Name Server: NS.AUSTIN.IBM.COM
   Updated Date: 02-sep-2000


>>> Last update of whois database: Thu, 15 Feb 2001 07:11:44 EST <<<
The Registry database contains ONLY .COM, .NET, .ORG, .EDU domains and Registrars.
```

Whois also provides further information on the registrant:

```
Registrant:
IBM Corporation (IBM-DOM)
   Old Orchard Rd
   Armonk, NY 10504
   US

   Domain Name: IBM.COM

   Administrative Contact, Technical Contact, Billing Contact:
      Trio, Nicholas R  (NRT1)  nrt@WATSON.IBM.COM
      IBM T.J. Watson Reserach Center
      PO Box 218
      Yorktown Heights, NY 10598
      (914) 945-1850

   Record last updated on 02-Sep-2000.
   Record expires on 20-Mar-2001.
   Record created on 19-Mar-1986.
   Database last updated on 15-Feb-2001 02:07:04 EST.

   Domain servers in listed order:
   NS.WATSON.IBM.COM 198.81.209.2
NS.ALMADEN.IBM.COM 198.4.83.35
NS.AUSTIN.IBM.COM 192.35.232.34
NS.ERS.IBM.COM 204.146.173.35
```

Remember, all of this information was gathered without having probed your network yet!

6.2.2 Probing your network

From now on, potential intruders leave traces of their intelligence gathering on your system. However, only some of these intrusions are automatically collected in system logs, usually only the more apparent ones (like unsuccessful attempts at guessing passwords). It is the administrators responsibility to enable further logging by using the respective tools, which we will cover in the next section.

We will now look at some tools that will be utilized against your network. Unfortunately, many of them are legitimately used by administrators for normal maintenance work; to tell the difference between that and an actual attack is one of Risk Manager's primary goals (by correlating all these normal occurrences).

6.2.2.1 nslookup

`nslookup` is used to look up domain name information about your external network. It also gives you information about some public services you offer, such as DNS and mail. Invoke `nslookup` in interactive mode (by not supplying any arguments on the command line), enter the domain name you want information about, varying the types by using the `set type=` command (interesting types are MX and NS, for example).

```
C:\>nslookup
Default Server:  ns.itsc.austin.ibm.com
Address:  10.1.1.1

> ibm.com
Server:  ns.itsc.austin.ibm.com
Address: 10.1.1.1

Non-authoritative answer:
Name:    ibm.com
Addresses:  129.42.19.99, 129.42.16.99, 129.42.17.99, 129.42.18.99

> set type=MX
> ibm.com
Server: ns.itsc.austin.ibm.com
Address:  10.1.1.1

Non-authoritative answer:
ibm.com MX preference = 0, mail exchanger = ns.watson.ibm.com

ns.watson.ibm.com internet address = 198.81.209.2

> set type=NS
> ibm.com
Server:  ns.itsc.austin.ibm.com
Address:  10.1.1.1

Non-authoritative answer:
ibm.com nameserver = NS.ERS.ibm.com
ibm.com nameserver = NS.AUSTIN.ibm.com
ibm.com nameserver = NS.WATSON.ibm.com

NS.ERS.ibm.com   internet address = 204.146.173.35
NS.AUSTIN.ibm.com  internet address = 192.35.232.34
NS.WATSON.ibm.com  internet address = 198.81.209.2
```

The `ls` command within `nslookup` requests a zone transfer, commonly used by secondary name servers for refreshing their database. Name servers are configured to give out this information just to these secondaries, because it also contains valuable information (that is, all your official hosts).

6.2.2.2 finger

Although only a few organizations still provide finger service, it often provides interesting details about accounts. For example, let us see when root was logged in last:

```
$ finger -l root@www.itsorisc.com
Login: root Name: System Administrator
Directory: root Shell: /bin/sh
Last login Fri Feb 16 17:07 (CET) on ttyp5 from fw.itsorisc.com
No plan.
$
```

Finger is also a nice tool to find non-root user accounts which usually are more easily compromised.

6.2.2.3 ping

Pinging the broadcast address of a subnet can be a neat way of discovering all the hosts on a subnet (and also for carrying out denial of service attacks). However, this will only work if pings to broadcast addresses are not blocked, usually at the router, which is strongly recommended.

6.2.2.4 traceroute

`traceroute` is a rather powerful tool for discovering details on network topology. Since it is widely used for network maintenance, administrators of target sites will not consider traceroute-related network traffic (UDP or ICMP) hostile.

traceroute through firewalls

Enterprises maintaining their Web servers in their own DMZ also tend to provide domain name service for their Internet hosts. Therefore, DNS is one of the few incoming UDP-based traffic allowed through firewalls, at least into the DMZ. At the same time, firewalls will block all other UDP or ICMP traffic originating from the “outside.”

By preventing `traceroute` from incrementing the port numbers as described in “Firewalking” at:

`http://www.packetfactory.net/Projects/Firewalk/firewalk-final.html`

traceroute can even bypass this firewall!

6.2.2.5 telnet

`telnet` has a nice feature allowing you to contact a lot more than just the login service by simply adding the corresponding port number. For some of them, like ftp or http, you can also use the respective clients. The client software restricts an intruder to the “normal” commands and procedures, however.

Let us try it:

```
$ telnet www.itsorisc.com
Trying...
Connected to www.itsorisc.com.
Escape character is '^]'.

AIX Version 4
(C) Copyrights by IBM and by others 1982, 1996.
login:


$ telnet www.itsorisc.com 25

220 www ESMTP Sendmail AIX4.3/8.9.3/8.9.3; Thu, 22 Feb 2001 10:35:55 -0600


$ telnet www.itsorisc.com 110
Trying...
telnet: connect: A remote host refused an attempted connect operation.
```

We used login, SMTP, DNS and IMAP, and gained a lot of information: it is an AIX version 4 box with telnet, DNS and SMTP (Sendmail version 8.9.3) running, but no IMAP server (“connection refused”).

The version of the most widely used name server, BIND, may also be determined by using `nslookup`:

```
$ nslookup -q=txt class=CHAOS version.bind. www.itsorisc.com
Server: ns.itsorisc.com
Address: 192.35.232.34

VERSION.BIND text = “8.2.3-REL”
$
```

For FTP, you might use the command line client, but HTTP via telnet is fun:

```
$ ftp www2.itsorisc.com
Connected to www2.itsorisc.com.
220 ntpd1 Microsoft FTP Service (Version 3.0).
Name (www2.itsorisc.com:peter):

$ telnet www2.itsorisc.com 80
BLA
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/4.0
Date: Thu, 22 Feb 2001 19:11:28 GMT
Content-Type: text/html
Content-Length: 87

$
```

A typical HTTP command would be `GET /index.html`; we used a non-existent command (`BLA`), causing the Web server to produce an error message along with a banner. It appears that Microsoft IIS is one of the few HTTP servers where the server itself produces a Server: banner, but most other servers will print their version in their standard HTML error page. You can (and should) change that configuration.

The banners of the different services usually state the name and version number of the daemon used. Such information facilitates determining which exploit on what operating system is to be deployed.

6.2.3 Advanced techniques

While all the tools we have mentioned so far provide some basic understanding of the network structure, we usually do not know much about the operating systems used and all the services provided (often a lot more than needed). Since exploiting known vulnerabilities is the way to compromise a system, scanning the targets will be our next step.

The tools used for scanning leave lots of information in our log files, so it makes sense to look at two of the more popular ones. Scanning a network is like trying the door knobs in a street. You’re not breaking in, but some administrators still will not like the fact, just like the people in your neighborhood. (That is, if they bother to log such occurrences and actually analyze the logs, anyway.)

6.2.3.1 nmap

This is one of the most powerful network scanners available; it also serves as a basis for other tools, such as nessus. nmap features several sophisticated scanning techniques, such as TCP, UDP, ICMP, and RPC, some of them with stealth characteristics. The remote operating system fingerprinting is also very handy; its ability to delay the progression of the scan and to fake source IP-addresses makes detecting the origin of the scan rather difficult.

6.2.3.2 nessus

nessus includes a vulnerability database that is continuously kept up-to-date; you can even enhance it with your own security test using plug-ins. Its reporting mechanism will not only tell you about the problems found, their severity and how crackers might exploit them, but it also provides hints on how on fixing these problems.

6.2.4 Social engineering

Another rather successful, although non-technical approach is called *social engineering*. It depicts using common sense, taking into account the fact that many users and administrators does not apply common sense as soon as they are in front of a keyboard and a monitor.

Turning keyboards to find a note with passwords on it can be rewarding, especially if the company has a strict “change password every three months, don’t recycle old passwords and use at least one non-alphanumeric” policy. Forgetting the fact that many users have 3-5 accounts on average, this policy often turns out to be quite harmful (which is easily verified by flipping keyboards in your favorite department - if users bother to hide their password list at all).

User help desks and system administrators are also a valuable, although involuntary, aid for attackers, especially if their management failed to strengthen their back on security related issues. This includes adequate training as well as the ability to enforce security policies. Not only might administrators be jeopardized by *social hacks* (phone calls like “I forgot my password, could you reset it to ...”), but also by managers ordering them to knowingly violate security policies due to some urgent security demand.

6.2.5 External versus internal offenders

While discussing the reconnaissance techniques in this chapter, you probably spotted one of the major differences between external and internal offenders. An internal offender is considered someone already familiar with your company, especially your network and your security procedures. Obviously, he already obtained more information than an external attacker probably ever will (in terms of background knowledge, that is).

Therefore, internal attackers are less likely to be discovered before they actually compromise systems, since less intelligence gathering also leaves fewer traces. This is another excellent reason for having host-based IDS on important servers, by the way (refer to the discussion in Section 6.1.7, “Host versus network intrusion detection” on page 209).

As soon as an external attacker is successful in invading one of your internal hosts (usually by compromising a unprivileged user account first and then gaining access with administrative rights on that machine), he will adapt a strategy similar to the internal offender. Installing a rootkit and planting network sniffers is standard procedure - and also the reason for becoming root, a prerequisite for turning network interface cards to promiscuous mode.

6.3 Tivoli Risk Manager

Risk Manager is basically a Tivoli front end for intrusion detection. Its core consists of a correlation engine generating situations after analyzing the events received from a variety of sensors.

For further information on Risk Manager’s architecture, please see Chapter 3, “Risk Manager architecture”, in the redbook *Tivoli SecureWay Risk Manager:Correlating Enterprise Risk Management*, SG24-6021 and Chapter 3, “Risk Manager topology and infrastructure” on page 19.

6.3.1 Correlation

The purpose of correlating events using artificial intelligence algorithms is to help system administrators in large environments focus on critical situations, rather than being distracted by noise and less important activities on the network.

The correlation algorithms have been discussed in great detail in Chapter 4 of the redbook *Tivoli SecureWay Risk Manager: Correlating Enterprise Risk Management*, SG24-6021.

6.3.2 Description of Risk Manager and sensor events and classes

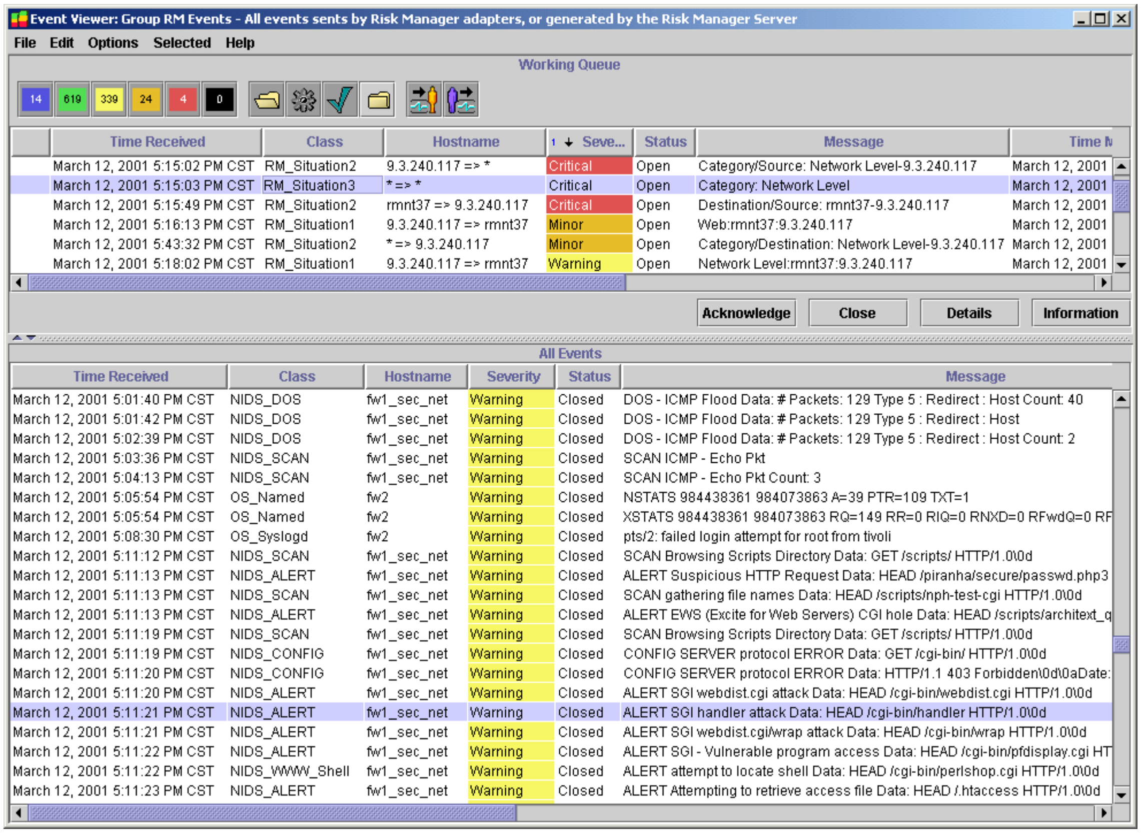
Currently, there is no extensive description of the events sent by the sensors and their classification. Information gathered from hands-on experience is compiled in the respective sections of this chapter.

In order to obtain a current listing of the classes implemented on your system, issue `wlsrbclass RM37RB` on the TEC Server. Some of the classes may be a super-class of others, explaining why you will not see them on the TEC console.

In some instances (like Host IDS; see Section 6.5.3.1, “Host IDS UNIX event classes” on page 236), it seems the number of existing classes exceeds the ones actually implemented.

6.3.3 Work flow

As Risk Manager is integrated into the TEC console (see Figure 127), the work flow is quite similar to standard TEC usage.

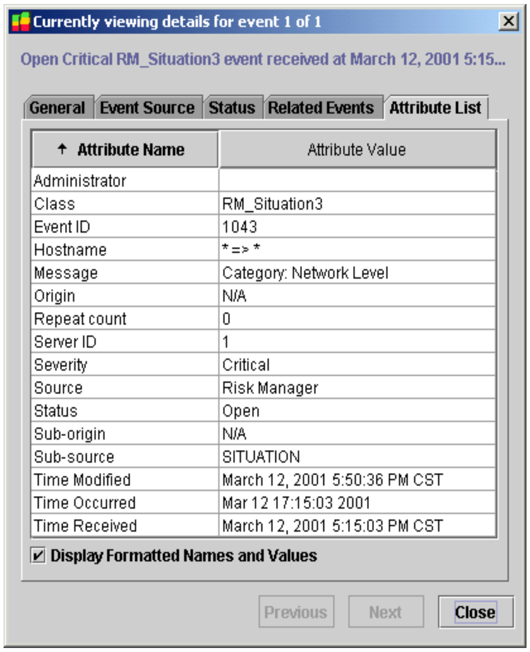

Event Viewer: Group RM Events - All events sents by Risk Manager adapters, or generated by the Risk Manager Server
File
Edit
Options
Selected
Help
Working Queue
14
619
339
24
4
0
Acknowledge
Close
Details
Information
All Events

	Time Received	Class	Hostname	1 ↓ Seve...	Status	Message	Time N
	March 12, 2001 5:15:02 PM CST	RM_Situation2	9.3.240.117 => *	Critical	Open	Category/Source: Network Level-9.3.240.117	March 12, 2001
	March 12, 2001 5:15:03 PM CST	RM_Situation3	* => *	Critical	Open	Category: Network Level	March 12, 2001
	March 12, 2001 5:15:49 PM CST	RM_Situation2	rmnt37 => 9.3.240.117	Critical	Open	Destination/Source: rmnt37-9.3.240.117	March 12, 2001
	March 12, 2001 5:16:13 PM CST	RM_Situation1	9.3.240.117 => rmnt37	Minor	Open	Web:rmnt37:9.3.240.117	March 12, 2001
	March 12, 2001 5:43:32 PM CST	RM_Situation2	* => 9.3.240.117	Minor	Open	Category/Destination: Network Level-9.3.240.117	March 12, 2001
	March 12, 2001 5:18:02 PM CST	RM_Situation1	9.3.240.117 => rmnt37	Warning	Open	Network Level:rmnt37:9.3.240.117	March 12, 2001

Time Received	Class	Hostname	Severity	Status	Message
March 12, 2001 5:01:40 PM CST	NIDS_DOS	fw1_sec_net	Warning	Closed	DOS - ICMP Flood Data: # Packets: 129 Type 5 : Redirect : Host Count: 40
March 12, 2001 5:01:42 PM CST	NIDS_DOS	fw1_sec_net	Warning	Closed	DOS - ICMP Flood Data: # Packets: 129 Type 5 : Redirect : Host
March 12, 2001 5:02:39 PM CST	NIDS_DOS	fw1_sec_net	Warning	Closed	DOS - ICMP Flood Data: # Packets: 129 Type 5 : Redirect : Host Count: 2
March 12, 2001 5:03:36 PM CST	NIDS_SCAN	fw1_sec_net	Warning	Closed	SCAN ICMP - Echo Pkt
March 12, 2001 5:04:13 PM CST	NIDS_SCAN	fw1_sec_net	Warning	Closed	SCAN ICMP - Echo Pkt Count: 3
March 12, 2001 5:05:54 PM CST	OS_Named	fw2	Warning	Closed	NSTATS 984438361 984073863 A=39 PTR=109 TXT=1
March 12, 2001 5:05:54 PM CST	OS_Named	fw2	Warning	Closed	XSTATS 984438361 984073863 RQ=149 RR=0 RIQ=0 RNXD=0 RFwdQ=0 RF
March 12, 2001 5:08:30 PM CST	OS_Syslogd	fw2	Warning	Closed	pts/2: failed login attempt for root from tivoli
March 12, 2001 5:11:12 PM CST	NIDS_SCAN	fw1_sec_net	Warning	Closed	SCAN Browsing Scripts Directory Data: GET /scripts/ HTTP/1.0\0d
March 12, 2001 5:11:13 PM CST	NIDS_ALERT	fw1_sec_net	Warning	Closed	ALERT Suspicious HTTP Request Data: HEAD /piranha/secure/passwd.php3
March 12, 2001 5:11:13 PM CST	NIDS_SCAN	fw1_sec_net	Warning	Closed	SCAN gathering file names Data: HEAD /scripts/nph-test-cgi HTTP/1.0\0d
March 12, 2001 5:11:13 PM CST	NIDS_ALERT	fw1_sec_net	Warning	Closed	ALERT EWS (Excite for Web Servers) CGI hole Data: HEAD /scripts/architext_q
March 12, 2001 5:11:19 PM CST	NIDS_SCAN	fw1_sec_net	Warning	Closed	SCAN Browsing Scripts Directory Data: GET /scripts/ HTTP/1.0\0d
March 12, 2001 5:11:19 PM CST	NIDS_CONFIG	fw1_sec_net	Warning	Closed	CONFIG SERVER protocol ERROR Data: GET /cgi-bin/ HTTP/1.0\0d
March 12, 2001 5:11:20 PM CST	NIDS_CONFIG	fw1_sec_net	Warning	Closed	CONFIG SERVER protocol ERROR Data: HTTP/1.1 403 Forbidden\0d\0aDate:
March 12, 2001 5:11:20 PM CST	NIDS_ALERT	fw1_sec_net	Warning	Closed	ALERT SGI webdist.cgi attack Data: HEAD /cgi-bin/webdist.cgi HTTP/1.0\0d
March 12, 2001 5:11:21 PM CST	NIDS_ALERT	fw1_sec_net	Warning	Closed	ALERT SGI handler attack Data: HEAD /cgi-bin/handler HTTP/1.0\0d
March 12, 2001 5:11:21 PM CST	NIDS_ALERT	fw1_sec_net	Warning	Closed	ALERT SGI webdist.cgi/wrap attack Data: HEAD /cgi-bin/wrap HTTP/1.0\0d
March 12, 2001 5:11:22 PM CST	NIDS_ALERT	fw1_sec_net	Warning	Closed	ALERT SGI - Vulnerable program access Data: HEAD /cgi-bin/pfdisplay.cgi HT
March 12, 2001 5:11:22 PM CST	NIDS_WWW_Shell	fw1_sec_net	Warning	Closed	ALERT attempt to locate shell Data: HEAD /cgi-bin/perlshop.cgi HTTP/1.0\0d
March 12, 2001 5:11:23 PM CST	NIDS_ALERT	fw1_sec_net	Warning	Closed	ALERT Attempting to retrieve access file Data: HEAD /.htaccess HTTP/1.0\0d

Figure 127. TEC Console with Risk Manager situations and events

Whenever a RM_Situation is raised, administrators will investigate the events that caused this situation by first examining the details of the situation itself (as seen in Figure 128 on page 221).



Open Critical RM_Situation3 event received at March 12, 2001 5:15...

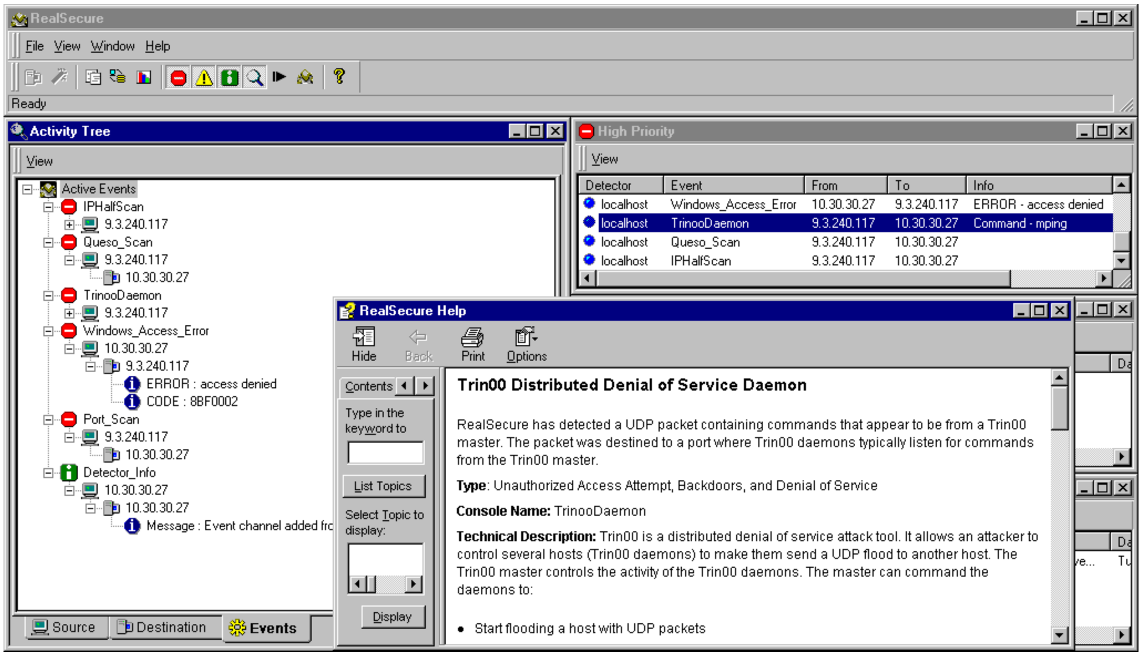
Attribute Name	Attribute Value
Administrator	
Class	RM_Situation3
Event ID	1043
Hostname	* => *
Message	Category: Network Level
Origin	N/A
Repeat count	0
Server ID	1
Severity	Critical
Source	Risk Manager
Status	Open
Sub-origin	N/A
Sub-source	SITUATION
Time Modified	March 12, 2001 5:50:36 PM CST
Time Occurred	Mar 12 17:15:03 2001
Time Received	March 12, 2001 5:15:03 PM CST

☑ Display Formatted Names and Values

Figure 128. Details of a Risk Manager situation

Next, the corresponding events provide further details on why the situation was raised.

In case events originated from non-Tivoli software, such as Checkpoint Firewall-1 or ISS Real Secure (see Figure 129 on page 222 for an example), consulting the respective consoles and log viewers is recommended.



Detector	Event	From	To	Info
localhost	Windows_Access_Error	10.30.30.27	9.3.240.117	ERROR - access denied
localhost	TrinooDaemon	9.3.240.117	10.30.30.27	Command - mping
localhost	Queso_Scan	9.3.240.117	10.30.30.27	
localhost	IPHalfScan	9.3.240.117	10.30.30.27	

Trin00 Distributed Denial of Service Daemon

RealSecure has detected a UDP packet containing commands that appear to be from a Trin00 master. The packet was destined to a port where Trin00 daemons typically listen for commands from the Trin00 master.

Type: Unauthorized Access Attempt, Backdoors, and Denial of Service

Console Name: TrinooDaemon

Technical Description: Trin00 is a distributed denial of service attack tool. It allows an attacker to control several hosts (Trin00 daemons) to make them send a UDP flood to another host. The Trin00 master controls the activity of the Trin00 daemons. The master can command the daemons to:

- Start flooding a host with UDP packets

Figure 129. ISS Real Secure

In the following sections, we describe the situations and events relevant to the most important Tivoli sensors.

6.4 Network intrusion detection

Intrusion detection at the network level is the foundation for any corporate level IDS. A network intrusion detection system watches traffic to and between all hosts in a subnet, yet covering only the respective subnet installed in.

Remember, a sensor behind a firewall is only seeing intrusion attempts, since the “noise” that accompanies an attack (network scans, host probes) are filtered. See the discussion in Section 6.1.9, “Location of sensors” on page 210.

6.4.1 Attack tools

6.4.1.1 Active: Scan and probe

A variety of tools exist besides those discussed in Section 6.2.3, “Advanced techniques” on page 217 for scanning networks and probing hosts for vulnerabilities. Some of these tools are equipped with stealth technology, trying to avoid detection by IDS.

6.4.1.2 Passive: Sniff

Sniffers like dsniff or ethereal are watching network traffic (just like the NIDS itself!), looking for interesting data, such as connection establishments with passwords in the clear (telnet, rsh, ftp, and so on).

Detecting sniffers

Sniffers are usually not detected by network intrusion systems, since they do not generate any network traffic.

There are tools, however, which try to find hosts in promiscuous mode in your network, by taking advantage of slightly different responses from IP-stacks when in promiscuous mode.

More information and the tools can be found at:

`http://www.linuxsecurity.com/resource_files/network_security/sniffing-faq.html`

and

`http://www.securiteam.com/unixfocus/Detecting_sniffers_on_your_network.html`

6.4.2 HAXOR

The Tivoli Network Intrusion Detection Option (NIDO), also known as *HAXOR*, monitors network activity and matches it to known network intrusion signatures in real time. HAXOR also passively verifies configurations of hosts.

6.4.2.1 What is HAXOR?

HAXOR is basically an intelligent packet filter. This is accomplished by watching the traffic on the network and making determinations at both the low (TCP/IP) and high (SMB/WWW and so on) protocol levels. Most packet filters will look at the header of packets and apply the filter rules to that. HAXOR will decode and piece together many of the low and high level protocols and apply its rules to those. For example, if your site has a policy forbidding wild-cards in the .rhosts file (effectively allowing anyone on the network access to that machine) and a user adds a wild-card to their .rhosts file over NFS, then HAXOR would detect that NFS protocol request, decode it, apply the 'no wild-card in .rhosts' rule, and issue an alert.

6.4.2.2 Supported protocols and attack categories

HAXOR supports the following protocols: FRAME, ARP, TCP, UDP, ICMP, RPC, DNS, NetBios, X11 and WWW (RIP and IPX are forthcoming).

See Table 8 for details on the respective attack signatures available for the supported protocols.

Table 8. Protocols supported

Protocol	Attack categories
ARP	Access control for changes in IP address/interface addresses
TCP	Access control (USER/TIME/Host/network based) Denial of Service Authentication failures (bad logins) Bad/Weak/default/Non existent passwords Time base ACL Service scans (depth and width) Content (signatures in streams of telnet/ftp/sendmail/ WWW/r-services) or any user defined service Session logging (ASCII, RAW, and TCPDUMP) Backdoor/rootkit checks Anti IDS Subversion code
UDP	Access control (user/TIME/Host/network based) Denial of Service Time base ACL Service scans (depth and width) Content (signatures in streams of tftp / ftp) or any user defined service ICMP access control (TIME/Host/network based) Stealth channel communications Different triggers Payload signatures Denial of service
RPC	Access control (USER/TIME/Host/network based) Denial of Service Time base ACL Content (nfs/mount/stat/yp*/portmapper/rusers, and so on.)
DNS	Access control (TIME/Host/network based) Denial of Service Time base ACL Spoofing Stealth channel communications Content

Protocol	Attack categories
NetBIOS	Access control (USER/TIME/Host/network based) Time base ACL Content/configuration Authentication
X11	Access control (TIME/Host/network based) Authentication Denial of Service Time base ACL Content
WWW	Access control (TIME/Host/network based) Authentication Denial of Service Time base ACL Content Selective filtering based on content

6.4.2.3 Platforms and network interfaces supported

HAXOR supports Ethernet, Token Ring, FDDI, SLIP, PPP, RAWIP and ATM. See Table 9 for details on which network interfaces are supported on which platforms.

Table 9. Platforms and network interfaces supported

Platform	Network interfaces
AIX 4.x on RS/6000	Ethernet, TR, FDDI, and SLIP
Solaris 2.5 on x86	Ethernet, TR, and FDDI
Solaris Sparc	Ethernet, TR, and FDDI
Linux 2.0.0	Ethernet, TR, FDDI, SLIP, and PPP

6.4.3 Tivoli Network Intrusion Detection System

Tivoli’s Network IDS (NIDS) is a very comprehensive sensor, providing not only raw events but also event classes (see Section 6.4.3.2, “Built-In and signature-based alerts” on page 226).

6.4.3.1 Event classes

The event classes listed in Table 10 show the more common types of network-based intrusions as defined by Risk Manager. There are five categories for NIDS: network, email, service, Web server, and host / user.

Table 10. Common types of network intrusions as defined by Risk Manager

NIDS class	Description
NIDS_ALERT	General alerts
NIDS_AUTH	Authentication errors, like failed logins
NIDS_BACKDOOR	Trojans
NIDS_CONFIG	Weak configuration leading to security holes
NIDS_DOS	Denial of Service
NIDS_SCAN	Network probes
NIDS_STEALTH	Stealth scans
NIDS_GOPHER	Abuse of gopher (rare)
NIDS_Loki	
NIDS_TFTP_PW_File	Download of /etc/passwd via tftp
NIDS_WWW_Shell	
NIDS_IntelBuffOverflow	Buffer overflows
NIDS_RS6KBuffOverflow	
NIDS_SparcBuffOverflow	
NIDS_SendMailPipeBug1	Sendmail bugs
NIDS_SendMailPipeBug2	
NIDS_SendMailPipeBug3	
NIDS_DefaultUserLogin	Attempt to login as default user, for example, “guest”

6.4.3.2 Built-In and signature-based alerts

Simple pattern matching in sessions or packet data has turned out to be insufficient to detect suspicious situations, requiring more sophisticated approaches.

The *built-in* alerts within Tivoli’s NIDS, found in the ids.msg file, are raised through analysis of stateful interaction within a protocol or analysis across multiple sessions. This is the reserved part of the token collection, which are not to be modified (except for their severity level).

In *signature-based* alerts, Network IDS looks for specified patterns in the packet or session data stream in a given protocol level. The patterns, along with the alert priority and the output message, are specified in the file ids.rules.

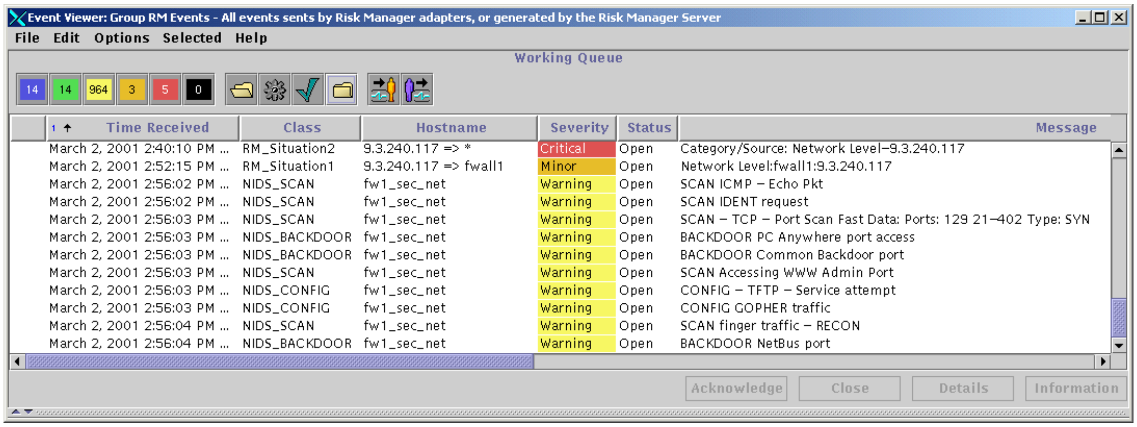
Please refer to Appendix B, “Attack Signatures”, of the *Tivoli Risk Manager Network Intrusion Detection Option User’s Guide Version 3.7* for descriptions and levels of the alert IDs

6.4.4 Analysis of common traces

In this section we discuss a number of common traces that will pop up on your event console. These were taken in a lab environment, so expect much more “noise” between the related events in the real world.

6.4.4.1 Network scan

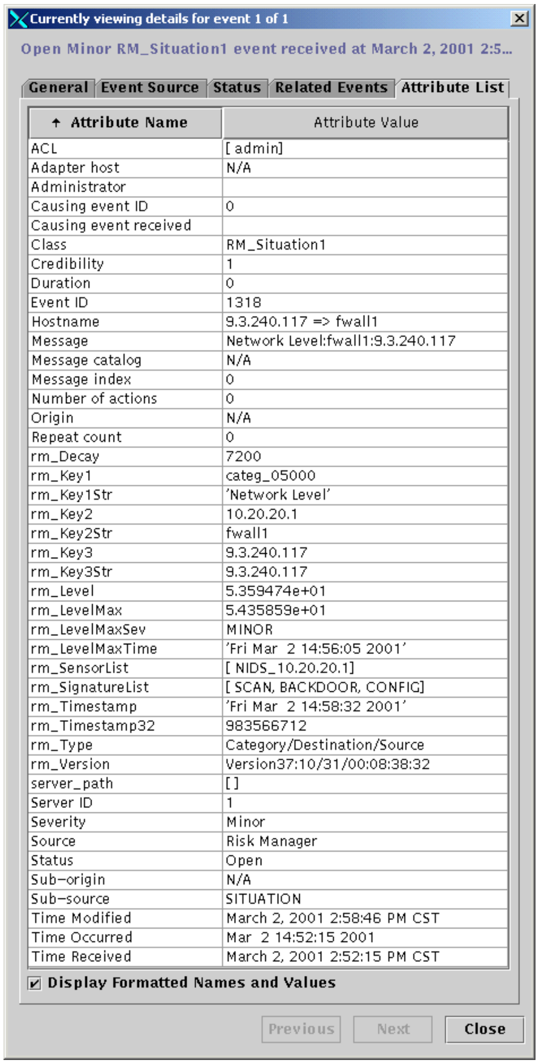
As we can see in Figure 130, a minor *Situation1* was raised by Risk Manager, and there are several NIDS warnings concerning scans.


Event Viewer: Group RM Events - All events sents by Risk Manager adapters, or generated by the Risk Manager Server
File
Edit
Options
Selected
Help
Working Queue
14
14
964
3
5
0
Acknowledge
Close
Details
Information

Time Received	Class	Hostname	Severity	Status	Message
March 2, 2001 2:40:10 PM ...	RM_Situation2	9.3.240.117 => *	Critical	Open	Category/Source: Network Level–9.3.240.117
March 2, 2001 2:52:15 PM ...	RM_Situation1	9.3.240.117 => fwall1	Minor	Open	Network Level:fwall1:9.3.240.117
March 2, 2001 2:56:02 PM ...	NIDS_SCAN	fw1_sec_net	Warning	Open	SCAN ICMP – Echo Pkt
March 2, 2001 2:56:02 PM ...	NIDS_SCAN	fw1_sec_net	Warning	Open	SCAN IDENT request
March 2, 2001 2:56:03 PM ...	NIDS_SCAN	fw1_sec_net	Warning	Open	SCAN – TCP – Port Scan Fast Data: Ports: 129 21–402 Type: SYN
March 2, 2001 2:56:03 PM ...	NIDS_BACKDOOR	fw1_sec_net	Warning	Open	BACKDOOR PC Anywhere port access
March 2, 2001 2:56:03 PM ...	NIDS_BACKDOOR	fw1_sec_net	Warning	Open	BACKDOOR Common Backdoor port
March 2, 2001 2:56:03 PM ...	NIDS_SCAN	fw1_sec_net	Warning	Open	SCAN Accessing WWW Admin Port
March 2, 2001 2:56:03 PM ...	NIDS_CONFIG	fw1_sec_net	Warning	Open	CONFIG – TFTP – Service attempt
March 2, 2001 2:56:03 PM ...	NIDS_CONFIG	fw1_sec_net	Warning	Open	CONFIG GOPHER traffic
March 2, 2001 2:56:04 PM ...	NIDS_SCAN	fw1_sec_net	Warning	Open	SCAN finger traffic – RECON
March 2, 2001 2:56:04 PM ...	NIDS_BACKDOOR	fw1_sec_net	Warning	Open	BACKDOOR NetBus port

Figure 130. Network scan - situation and events

A first step is to examine the situation itself, especially the attribute list (see Figure 131 on page 228). Here you find the address of the offender (rm_Key3, 9.3.240.117) as well as of the target (rm_Key2, 10.20.20.1) and also the signatures matched (SCAN, BACKDOOR, and CONFIG).



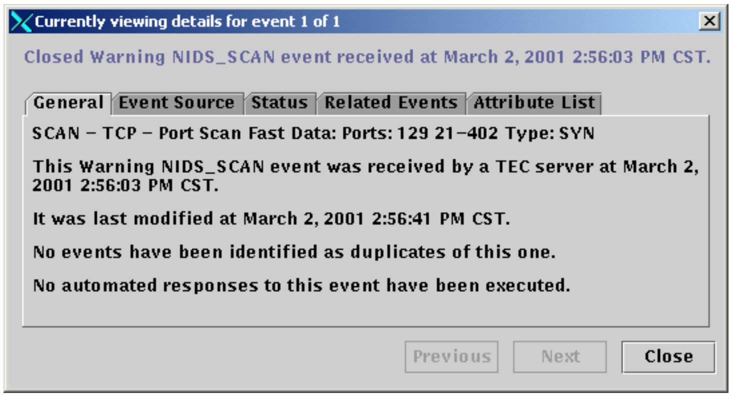
Open Minor RM_Situation1 event received at March 2, 2001 2:5...

Attribute Name	Attribute Value
ACL	[admin]
Adapter host	N/A
Administrator	
Causing event ID	0
Causing event received	
Class	RM_Situation1
Credibility	1
Duration	0
Event ID	1318
Hostname	9.3.240.117 => fwall1
Message	Network Level:fwall1:9.3.240.117
Message catalog	N/A
Message index	0
Number of actions	0
Origin	N/A
Repeat count	0
rm_Decay	7200
rm_Key1	categ_05000
rm_Key1Str	'Network Level'
rm_Key2	10.20.20.1
rm_Key2Str	fwall1
rm_Key3	9.3.240.117
rm_Key3Str	9.3.240.117
rm_Level	5.359474e+01
rm_LevelMax	5.435859e+01
rm_LevelMaxSev	MINOR
rm_LevelMaxTime	'Fri Mar 2 14:56:05 2001'
rm_SensorList	[NIDS_10.20.20.1]
rm_SignatureList	[SCAN, BACKDOOR, CONFIG]
rm_Timestamp	'Fri Mar 2 14:58:32 2001'
rm_Timestamp32	983566712
rm_Type	Category/Destination/Source
rm_Version	Version37:10/31/00:08:38:32
server_path	[ ]
Server ID	1
Severity	Minor
Source	Risk Manager
Status	Open
Sub–origin	N/A
Sub–source	SITUATION
Time Modified	March 2, 2001 2:58:46 PM CST
Time Occurred	Mar 2 14:52:15 2001
Time Received	March 2, 2001 2:52:15 PM CST

☑ Display Formatted Names and Values

Figure 131. Details of Situation1 of a network scan

Therefore, NIDS_BACKDOOR and NIDS_CONFIG were part of this situation and thus the attack. Further investigation of the related events (as seen in Figure 132 on page 229) can give us some more insight on the nature of the attack.



Closed Warning NIDS_SCAN event received at March 2, 2001 2:56:03 PM CST.

SCAN – TCP – Port Scan Fast Data: Ports: 129 21–402 Type: SYN

This Warning NIDS_SCAN event was received by a TEC server at March 2, 2001 2:56:03 PM CST.

It was last modified at March 2, 2001 2:56:41 PM CST.

No events have been identified as duplicates of this one.

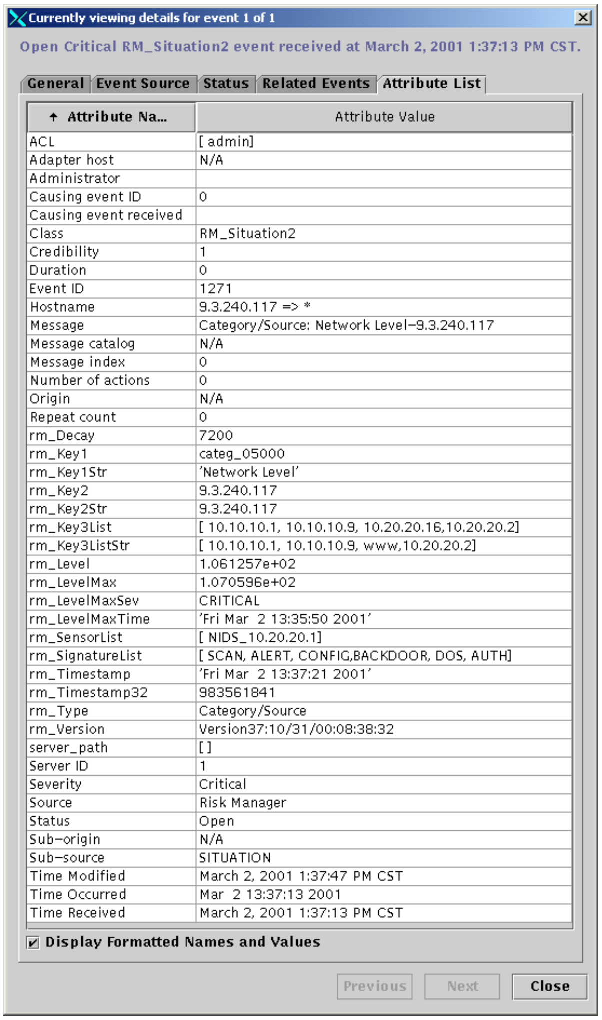
No automated responses to this event have been executed.

Figure 132. Details of a port scan

Please note that Risk Manager cannot (yet) give you further information on a number of situations. The one we just examined was caused by a simple `nmap 10.20.20.1` from 9.3.240.117.

6.4.4.2 Host probe

When further investigating a network scan, host probes are the next point of interest. The details in Figure 133 on page 230 show several hosts being targeted.



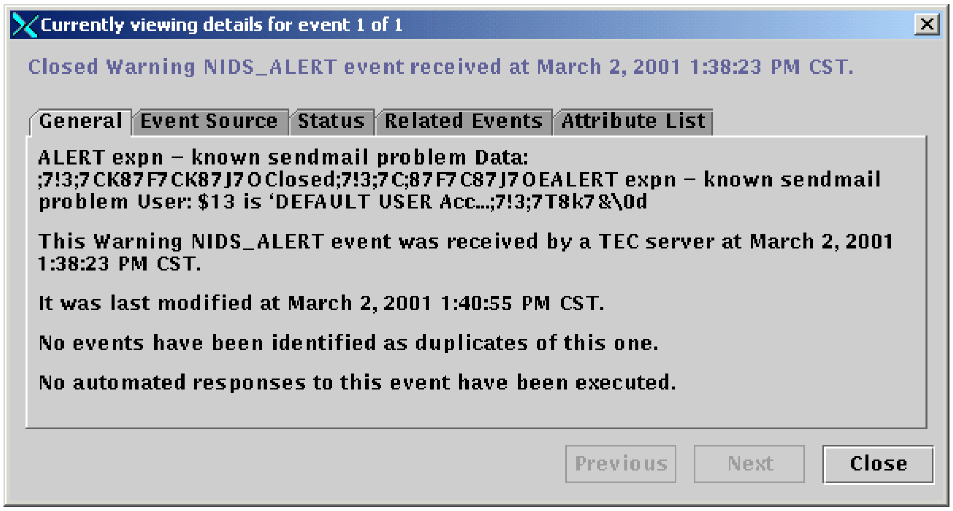
Open Critical RM_Situation2 event received at March 2, 2001 1:37:13 PM CST.

Attribute Na...	Attribute Value
ACL	[admin]
Adapter host	N/A
Administrator	
Causing event ID	0
Causing event received	
Class	RM_Situation2
Credibility	1
Duration	0
Event ID	1271
Hostname	9.3.240.117 => *
Message	Category/Source: Network Level–9.3.240.117
Message catalog	N/A
Message index	0
Number of actions	0
Origin	N/A
Repeat count	0
rm_Decay	7200
rm_Key1	categ_05000
rm_Key1Str	'Network Level'
rm_Key2	9.3.240.117
rm_Key2Str	9.3.240.117
rm_Key3List	[10.10.10.1, 10.10.10.9, 10.20.20.16,10.20.20.2]
rm_Key3ListStr	[10.10.10.1, 10.10.10.9, www,10.20.20.2]
rm_Level	1.061257e+02
rm_LevelMax	1.070596e+02
rm_LevelMaxSev	CRITICAL
rm_LevelMaxTime	'Fri Mar 2 13:35:50 2001'
rm_SensorList	[NIDS_10.20.20.1]
rm_SignatureList	[SCAN, ALERT, CONFIG,BACKDOOR, DOS, AUTH]
rm_Timestamp	'Fri Mar 2 13:37:21 2001'
rm_Timestamp32	983561841
rm_Type	Category/Source
rm_Version	Version37:10/31/00:08:38:32
server_path	[ ]
Server ID	1
Severity	Critical
Source	Risk Manager
Status	Open
Sub–origin	N/A
Sub–source	SITUATION
Time Modified	March 2, 2001 1:37:47 PM CST
Time Occurred	Mar 2 13:37:13 2001
Time Received	March 2, 2001 1:37:13 PM CST

☑ Display Formatted Names and Values

Figure 133. Situation raised due to network scans

Picking one of the targets listed, examine some of the events by viewing the corresponding details (Figure 134 on page 231).



Closed Warning NIDS_ALERT event received at March 2, 2001 1:38:23 PM CST.

ALERT expn – known sendmail problem Data: ;7!3;7CK87F7CK87J7OClosed;7!3;7C;87F7C87J7OEALERT expn – known sendmail problem User: $13 is ‘DEFAULT USER Acc...;7!3;7T8k7&\0d

This Warning NIDS_ALERT event was received by a TEC server at March 2, 2001 1:38:23 PM CST.

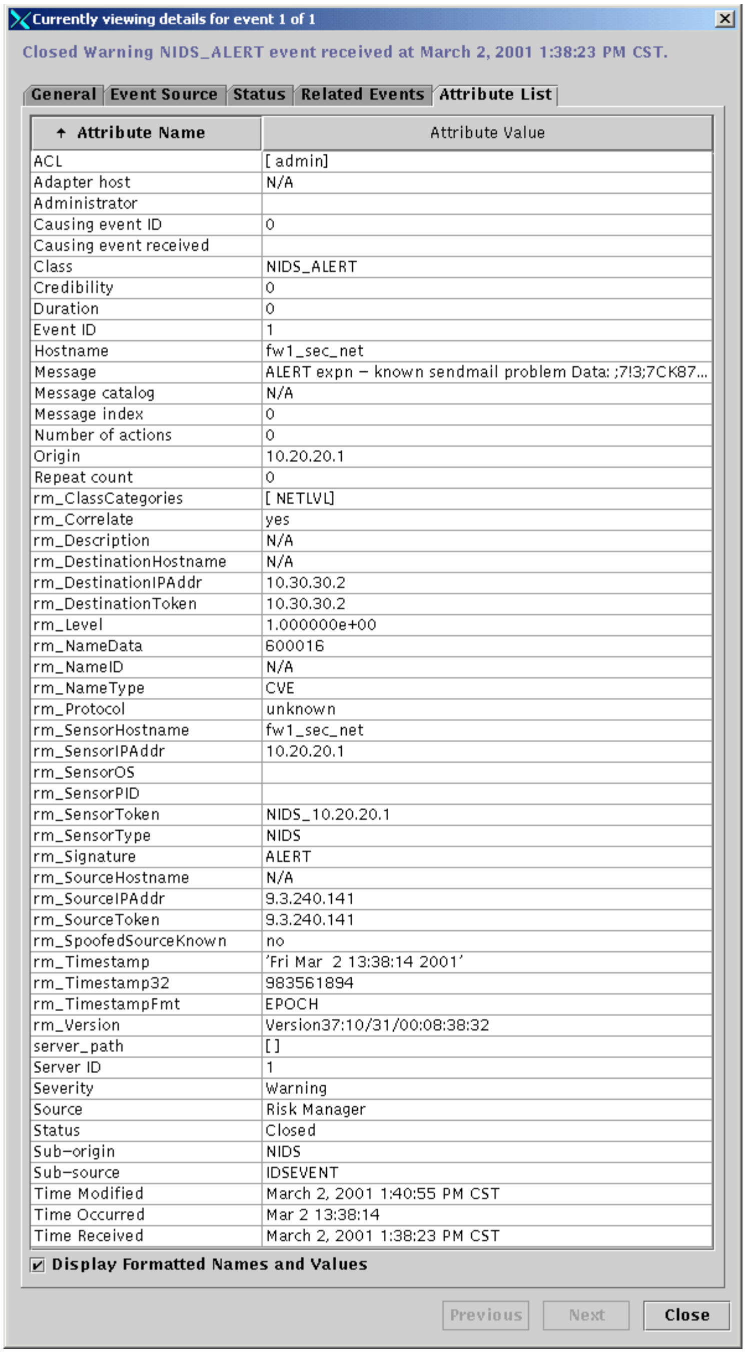
It was last modified at March 2, 2001 1:40:55 PM CST.

No events have been identified as duplicates of this one.

No automated responses to this event have been executed.

Figure 134. Sendmail probe seen by NIDS, caused by a host scan

The attribute list (see Figure 135 on page 232) reveals details of this sendmail probe.



Closed Warning NIDS_ALERT event received at March 2, 2001 1:38:23 PM CST.

↑ Attribute Name	Attribute Value
ACL	[admin]
Adapter host	N/A
Administrator	
Causing event ID	0
Causing event received	
Class	NIDS_ALERT
Credibility	0
Duration	0
Event ID	1
Hostname	fw1_sec_net
Message	ALERT expn – known sendmail problem Data: ;7!3;7CK87...
Message catalog	N/A
Message index	0
Number of actions	0
Origin	10.20.20.1
Repeat count	0
rm_ClassCategories	[NETLVL]
rm_Correlate	yes
rm_Description	N/A
rm_DestinationHostname	N/A
rm_DestinationIPAddr	10.30.30.2
rm_DestinationToken	10.30.30.2
rm_Level	1.000000e+00
rm_NameData	600016
rm_NameID	N/A
rm_NameType	CVE
rm_Protocol	unknown
rm_SensorHostname	fw1_sec_net
rm_SensorIPAddr	10.20.20.1
rm_SensorOS	
rm_SensorPID	
rm_SensorToken	NIDS_10.20.20.1
rm_SensorType	NIDS
rm_Signature	ALERT
rm_SourceHostname	N/A
rm_SourceIPAddr	9.3.240.141
rm_SourceToken	9.3.240.141
rm_SpoofedSourceKnown	no
rm_Timestamp	'Fri Mar 2 13:38:14 2001'
rm_Timestamp32	983561894
rm_TimestampFmt	EPOCH
rm_Version	Version37:10/31/00:08:38:32
server_path	[ ]
Server ID	1
Severity	Warning
Source	Risk Manager
Status	Closed
Sub-origin	NIDS
Sub-source	IDSEVENT
Time Modified	March 2, 2001 1:40:55 PM CST
Time Occurred	Mar 2 13:38:14
Time Received	March 2, 2001 1:38:23 PM CST

☑ Display Formatted Names and Values

Figure 135. Details of sendmail probe

Evaluating the attacks helps determine what tools intruders use and how much skill they put forth.

6.4.5 Adding your own signatures

Additional signatures can also be implemented by adding the rule and message in the appropriate files.

Consider the infamous phf bug as an example. In the file ids.rules, you would add the WWW service (if nonexistent):

```
#
# begin  ids.rules entry
#
PORTS 80
PTYPE TCP DST
SIG SRC   "bin/phf"    5055   7 "WWW - PHF attempt"
END
#
# end  ids.rules entry
#
```

The ids.rules entry says in effect:

Watch the network and all traffic going to port 80 and look for the signature "bin/phf." When that string is found in the data stream, issue alert #5055. Alert # 5055, which has an alert level of '7' and the text "WWW - PHF attempt," as well as the original string in which the signature was detected, will be issued.

However, such signature updates are usually provided by Tivoli. Extending the capabilities of NIDS is advisable for situations peculiar to your environment only, such as logins to certain accounts or extensive activity at uncommon times.

6.4.6 Other Network Intrusion Detection Systems

Adapters for a number of other NIDS exist, such as:

- ISS Real Secure
- Cisco Secure IDS (NetRanger)

Depending on the information provided by these IDS, Risk Manager receives rather detailed events. It is common practice to also view the event log on that respective IDS, as mentioned in Section 6.3.3, “Work flow” on page 220.

6.5 Host Intrusion Detection

Host IDS covers events generated from unusual results of standard operating system services. Examples are unsuccessful attempts to use daemons such as telnet, ftp or sendmail, but also uncommon load or memory shortage (which might indicate denial of service).

6.5.1 Tivoli Host IDS

The current Tivoli host intrusion detection is a passive approach where Tivoli provides an adapter to the system log (syslog on UNIX or EventLog on NT). Only events logged by the operating system will be passed on to Risk Manager.

It is important to keep in mind that only services that are running (and have enabled logging!) will generate system log events. Therefore, Tivoli Host IDS will not see probes for non-responding ports (another good reason for deploying NIDS in every subnet).

Whenever a system with Host IDS deployed is mentioned in a situation, the *OS_* events of that host should be inspected.

6.5.2 Windows

The Windows NT Host IDS focuses on login and account events, but also standard process and object events are taken into account.

6.5.2.1 Host IDS Windows NT event classes

In Table 11, events commonly encountered on Windows NT have been compiled. For a complete list of NT event classes, see Appendix B.1.6.2, “Windows NT” on page 328.

Table 11. Common NT Host ID Event Classes

Class	Description
OS_NT_Login	Successful login
OS_NT_Logoff	Logout of a user
OS_NT_LogonFailure	Failed login attempt
OS_NT_AccountDisabled	Account disabled, for example, due to too many failed login attempts
OS_NT_AccountDeleted	

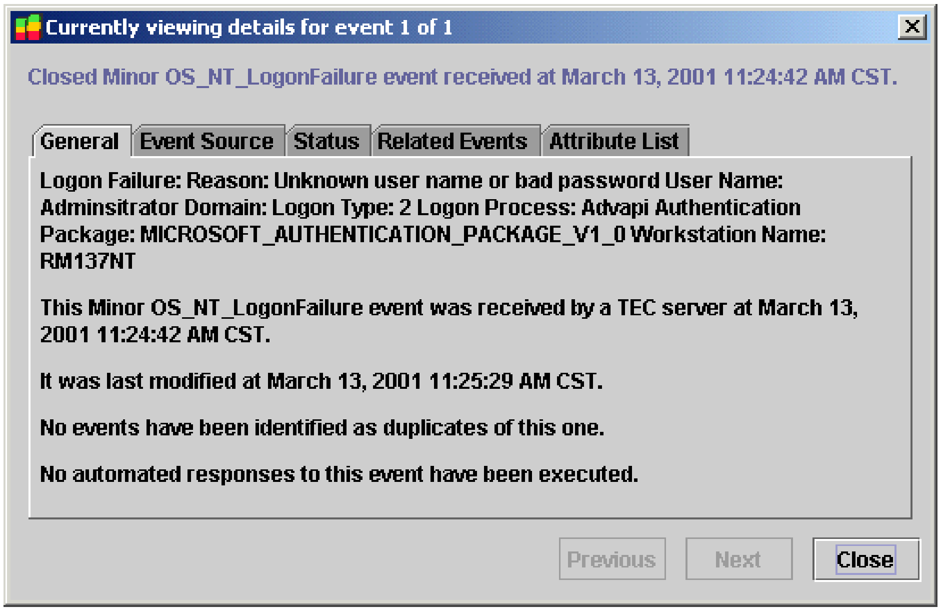
Class	Description
OS_NT_UserAccountChanged	Change of access rights, audit configuration
OS_NT_GlobalGroupMemberRemoved	
OS_NT_PriviledgedServiceCalled	
OS_NT_PriviledgedServiceFail	
OS_NT_TrustedLogonProcessRegistered	
OS_NT_SpecialPriviledesAssigned	
OS_NT_ProcessCreated	
OS_NT_ProcessExited	
OS_NT_ObjectOpen	
OS_NT_ObjectDeleted	
OS_NT_HandleClosed	

Windows NT Risk Manager events forwarded to the TEC Server are also providing information that is only marginally relevant for intrusion detection. Those include the ones not commented in Table 11 on page 234, such as OS_NT_ProcessCreated and OS_NT_ProcessExited.

More experienced users might find it useful to edit the os_nt.fmt file in order to avoid some of the events considered superfluous.

6.5.2.2 Sample event

One of the most prevalent events host probes will create are failed logins, as seen in Figure 136 on page 236.



Closed Minor OS_NT_LogonFailure event received at March 13, 2001 11:24:42 AM CST.

Logon Failure: Reason: Unknown user name or bad password User Name: Adminsitrator Domain: Logon Type: 2 Logon Process: Advapi Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Workstation Name: RM137NT

This Minor OS_NT_LogonFailure event was received by a TEC server at March 13, 2001 11:24:42 AM CST.

It was last modified at March 13, 2001 11:25:29 AM CST.

No events have been identified as duplicates of this one.

No automated responses to this event have been executed.

Figure 136. Windows NT login failed

6.5.3 UNIX

There are two host intrusion adapters available for UNIX: AIX and Solaris. In this redbook, we will only cover the AIX adapter.

6.5.3.1 Host IDS UNIX event classes

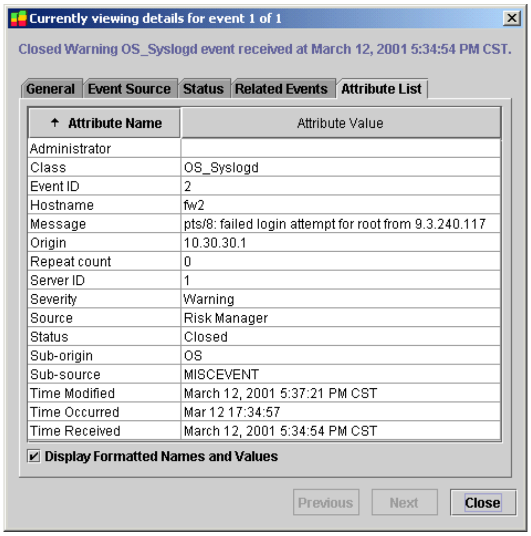
Table 12 lists the UNIX events usually occurring. Again, the complete list is to be found in Appendix B.1.6.1, “UNIX” on page 325. For reference, we also included Table 13 on page 238 with messages generated by this sensor.

Table 12. Common UNIX event classes

Class	Description
OS_Snmpd	SNMP-related attacks, such as “PUBLIC” password
OS_Sendmail	
OS_Syslogd	Failed login attempts
OS_Named	
OS_Inetd	
OS_Xntpd	

6.5.3.2 Sample events

Unsuprisingly, failed logins (as in Figure 137) are among the most common events on UNIX.



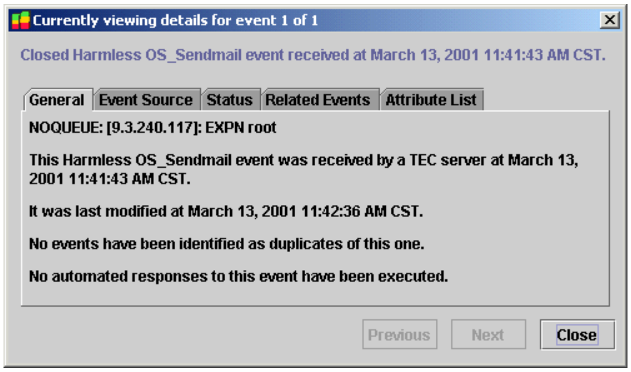
Closed Warning OS_Syslogd event received at March 12, 2001 5:34:54 PM CST.

↑ Attribute Name	Attribute Value
Administrator	
Class	OS_Syslogd
Event ID	2
Hostname	fw2
Message	pts/8: failed login attempt for root from 9.3.240.117
Origin	10.30.30.1
Repeat count	0
Server ID	1
Severity	Warning
Source	Risk Manager
Status	Closed
Sub-origin	OS
Sub-source	MISCEVENT
Time Modified	March 12, 2001 5:37:21 PM CST
Time Occurred	Mar 12 17:34:57
Time Received	March 12, 2001 5:34:54 PM CST

☑ Display Formatted Names and Values

Figure 137. UNIX login failure

As a matter of fact, many flavors of UNIX come with a lot of unnecessary services enabled by default. A probe to one of them results in events like the one in Figure 138.



Closed Harmless OS_Sendmail event received at March 13, 2001 11:41:43 AM CST.

NOQUEUE: [9.3.240.117]: EXPN root

This Harmless OS_Sendmail event was received by a TEC server at March 13, 2001 11:41:43 AM CST.

It was last modified at March 13, 2001 11:42:36 AM CST.

No events have been identified as duplicates of this one.

No automated responses to this event have been executed.

Figure 138. Sendmail EXPN probe

Use Auditing!

The use of auditing tools like the Trusted Computing Base (TCB) on AIX or Tripwire cannot be emphasized enough.

Any time Host IDS alarms you of a potential compromise, verifying the integrity of your systems against a known-to-be-good status is the only alternative to reinstalling all machines deemed affected. Missing only one affected system, containing a root kit, for example, can be considered fatal.

Table 13. Host IDS Events on AIX

Category	Message
Date	date set by os_User clock reset (step) os_step
Syslog	syslogd: os_logfile: No space left on device
OS	bad signal stack pid = rm_SensorPID os_silo silo overflow host name rebooted by os_by
Root	root login os_on_tty root login from os_on_tty root login refused on os_on_tty root login from host rm_SourceHostname refused
SU	su success: os_fromUser -> os_toUser su failure: os_fromUser -> os_toUser
Login	repeated login failure on os_on_tty repeated login failure from host rm_SourceHostname, user User
File System	os_file_system file system
Mount	os_file_system mounted on os_mount_point os_file_system unmounted from os_mount_point
NFS	NFS server rm_SensorHostname not responding NFS server rm_SensorHostname ok NFS: remote file system on host os_file_system_host full
Socks	sockd: connection from os_from to os_to sockd: connection from os_from to os_to terminated sockd: transfer between os_from and os_to

6.6 Web intrusion

Breaking into a Web server is basically motivated by three objectives:

1. Causing a denial of service.
2. Defacing the Web site.[4]
3. Using the Web server as a stepping stone for further attacks, either to other servers in the DMZ (such as a database) or into the company's internal network. This is usually made possible by the fact that sometimes connections from the DMZ to the internal network are permitted, such as database accesses or backup data streams.

The third objective is true for other systems in your DMZ as well. However, most often the Web server is granted some sort of access to your internal network, rendering it a rewarding target.

6.6.1 Tools for probing

Before attacking, an intruder will gather such information, such as what Web server type and version is running. The other services the system offers are also of interest; why bother with a secured Web server when there is an old and unpatched wu-ftp running?

Whisker and the CGI-library of Nessus are popular tools to probe your Web servers for commonly known vulnerabilities, such as preinstalled demo scripts with flaws.

6.6.2 Compromising Web servers

Placing a corporate Web server behind a firewall should be common practice by now, so attackers will take that into account and concentrate on the Web service itself.

There are various ways to gain access to the computer running the server software by exploiting flaws either directly in that software or the applications, such as CGI-scripts the users added. Not all of them are as neat as the infamous Microsoft IIS Unicode flaw, but it is possible to become root by abusing faulty CGI-scripts or even complex Web applications.

[4] Archives of defaced sites are maintained at `http://rootshell.com/hacked_sites/` and `http://www.attrition.org/mirror/attrition/`. Attrition also has interesting statistics, including defacements per server software and operating system.

Microsoft Unicode flaw

Web Server Folder Traversal Vulnerability

Microsoft's Internet Information Server (IIS) versions 4 and 5 are vulnerable to a malformed URL attack using `../` encoded in unicode to traverse beyond the Web servers document root folder. For example, `http://127.0.0.1/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\` executes the `dir` command; replace this with `ftp` and you can easily download neat hacking tools (say, netcat) to this machine.

For details, visit:

`http://packetstorm.securify.com/0010-exploits/iis-unicode.txt`

6.6.3 Tivoli Web Intrusion Detection

The Tivoli Web Intrusion Detection facility (Web IDS) is a log file adapter written in Perl. It can analyze several log file formats, matching entries with its built-in signatures (in the sig.nefarious file) and classes.

6.6.3.1 Platforms

Tivoli Web IDS runs on several Web servers on the AIX, Solaris, and Windows NT platforms (see Table 14).

Table 14. Web IDS Web servers and Platforms

Web server	Platforms	Log file format
Apache	AIX, Solaris, and NT	CLF (Common Log Format)
iPlanet (Netscape)	AIX, Solaris, and NT	CLF and Netscape
Microsoft IIS	NT	CLF, NCSA, IIS, IIS-ASCII, and ODBC
Lotus Domino	AIX, Solaris, and NT	CLF
IBM HTTPD (Websphere)	AIX, Solaris, and NT	CLF
Webseal (Policy Director)	AIX, Solaris, and NT	CLF

The events detected on these Web servers are quite similar; despite the varying log formats, they basically provide the same information to Risk Manager.

6.6.3.2 Event classes

Special attention should be paid to *suspicious*, *insecure* and *invalid* messages (shown in Table 15).

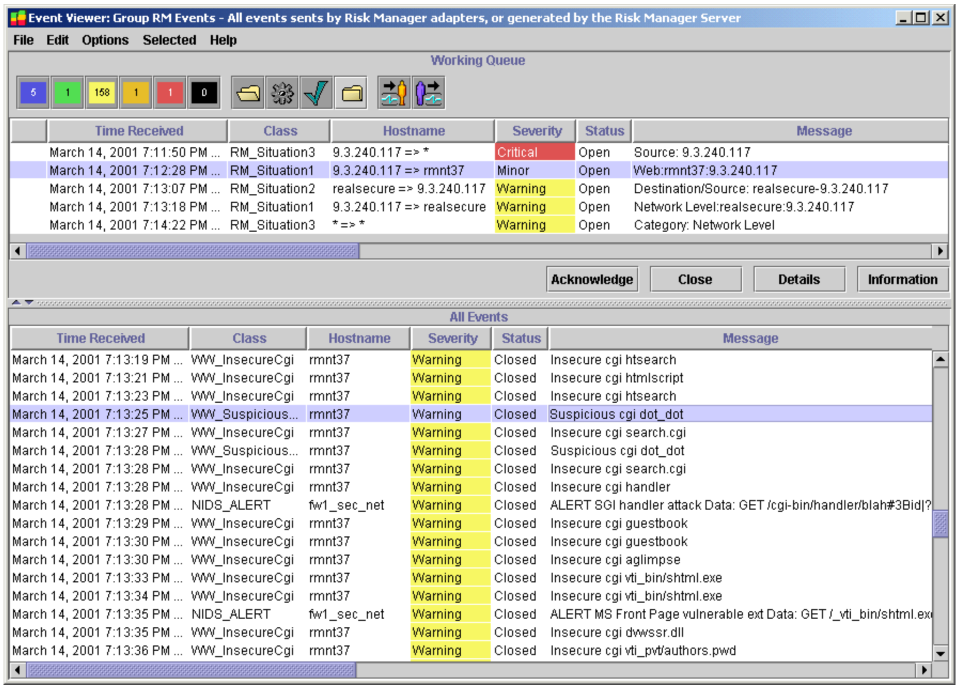
Table 15. Web IDS event classes

Class	Message
WW_Catchall	
WW_InvalidLogEntry	Unsupported log format
WW_WrongUrl	
WW_EmptyUrl	
WW_AuthenticationError	Invalid credentials provided for http access control
WW_SuspiciousHexCodes	Use of Unicode, for example %2E%2E
WW_SuspiciousHexCodesQuery	
WW_SuspiciousHexCodesUrl	
WW_InvalidHexCodesQuery	
WW_InvalidHexCodesUrl	
WW_AllowedMethods	Allowed methods: OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, and CONNECT
WW_Directory	Directory paths like /../ or /bin/
WW_SuspiciousCgi	Use of uncommon parameters for a CGI, such as search=test; rm -rf *
WW_InsecureCgi	Access to known vulnerable CGIs
WW_ClientError	Malformed request
WW_Success	Successful access to insecure / suspicious CGI; check host for intrusion
WW_Decision	

6.6.4 Analysis of common traces

The scope of any Web intrusion detection is usually limited to discovering suspicious activity (see event classes in Table 15 on page 241). Besides probes to your Web servers, Web IDS will also see legitimate traffic. That traffic nevertheless can be dangerous simply due to the fact that a number of widely used CGIs still have vast security holes. In such cases, check whether the CGIs are actually needed, and if so, try to install updated versions.

In Figure 139, a critical situation exists, regarding network traffic from host name 9.3.240.117 (which happens to be a Web server).

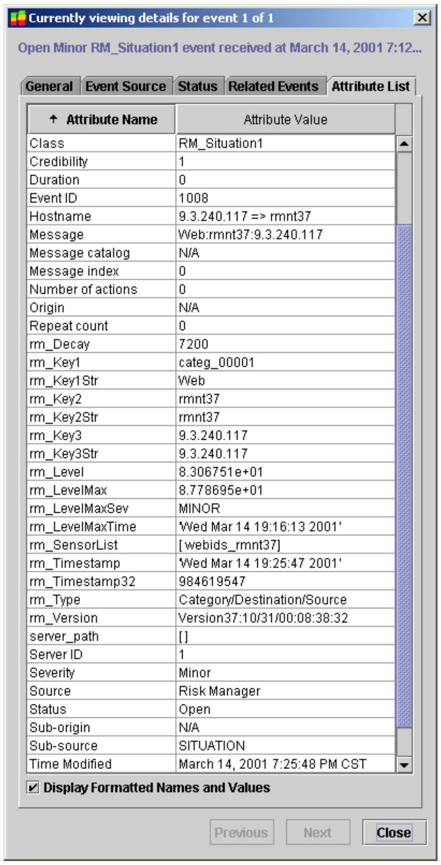

Event Viewer: Group RM Events - All events sents by Risk Manager adapters, or generated by the Risk Manager Server
File
Edit
Options
Selected
Help
Working Queue
5
1
158
1
1
0
Acknowledge
Close
Details
Information
All Events

Time Received	Class	Hostname	Severity	Status	Message
March 14, 2001 7:11:50 PM ...	RM_Situation3	9.3.240.117 => *	Critical	Open	Source: 9.3.240.117
March 14, 2001 7:12:28 PM ...	RM_Situation1	9.3.240.117 => rmnt37	Minor	Open	Web:rmnt37:9.3.240.117
March 14, 2001 7:13:07 PM ...	RM_Situation2	realsecure => 9.3.240.117	Warning	Open	Destination/Source: realsecure-9.3.240.117
March 14, 2001 7:13:18 PM ...	RM_Situation1	9.3.240.117 => realsecure	Warning	Open	Network Level:realsecure:9.3.240.117
March 14, 2001 7:14:22 PM ...	RM_Situation3	* => *	Warning	Open	Category: Network Level

Time Received	Class	Hostname	Severity	Status	Message
March 14, 2001 7:13:19 PM ...	WW_InsecureCgi	rmnt37	Warning	Closed	Insecure cgi htsearch
March 14, 2001 7:13:21 PM ...	WW_InsecureCgi	rmnt37	Warning	Closed	Insecure cgi htmlscript
March 14, 2001 7:13:23 PM ...	WW_InsecureCgi	rmnt37	Warning	Closed	Insecure cgi htsearch
March 14, 2001 7:13:25 PM ...	WW_Suspicious...	rmnt37	Warning	Closed	Suspicious cgi dot_dot
March 14, 2001 7:13:27 PM ...	WW_InsecureCgi	rmnt37	Warning	Closed	Insecure cgi search.cgi
March 14, 2001 7:13:28 PM ...	WW_Suspicious...	rmnt37	Warning	Closed	Suspicious cgi dot_dot
March 14, 2001 7:13:28 PM ...	WW_InsecureCgi	rmnt37	Warning	Closed	Insecure cgi search.cgi
March 14, 2001 7:13:28 PM ...	WW_InsecureCgi	rmnt37	Warning	Closed	Insecure cgi handler
March 14, 2001 7:13:28 PM ...	NIDS_ALERT	fw1_sec_net	Warning	Closed	ALERT SGI handler attack Data: GET /cgi-bin/handler/blah#3Bid|?
March 14, 2001 7:13:29 PM ...	WW_InsecureCgi	rmnt37	Warning	Closed	Insecure cgi guestbook
March 14, 2001 7:13:30 PM ...	WW_InsecureCgi	rmnt37	Warning	Closed	Insecure cgi guestbook
March 14, 2001 7:13:30 PM ...	WW_InsecureCgi	rmnt37	Warning	Closed	Insecure cgi aglimpse
March 14, 2001 7:13:33 PM ...	WW_InsecureCgi	rmnt37	Warning	Closed	Insecure cgi vti_bin/shtml.exe
March 14, 2001 7:13:34 PM ...	WW_InsecureCgi	rmnt37	Warning	Closed	Insecure cgi vti_bin/shtml.exe
March 14, 2001 7:13:35 PM ...	NIDS_ALERT	fw1_sec_net	Warning	Closed	ALERT MS Front Page vulnerable ext Data: GET /_vti_bin/shtml.ex
March 14, 2001 7:13:35 PM ...	WW_InsecureCgi	rmnt37	Warning	Closed	Insecure cgi dvwssr.dll
March 14, 2001 7:13:36 PM ...	WW_InsecureCgi	rmnt37	Warning	Closed	Insecure cgi vti_pvt/authors.pwd

Figure 139. Web IDS events on Tivoli console

Upon further examination, the details of this situation provide useful information, as shown in Figure 140 on page 243:



Open Minor RM_Situation1 event received at March 14, 2001 7:12...

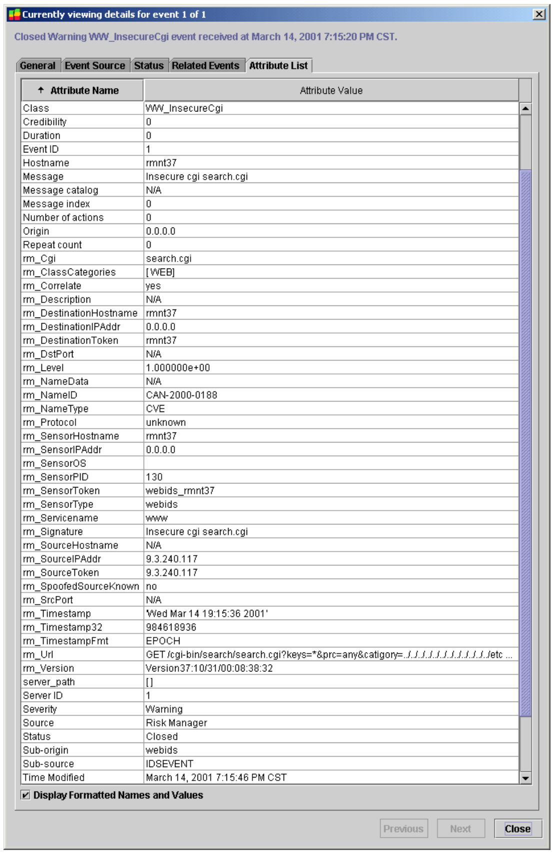
Attribute Name	Attribute Value
Class	RM_Situation1
Credibility	1
Duration	0
Event ID	1008
Hostname	9.3.240.117 => rmnt37
Message	Web:rmnt37:9.3.240.117
Message catalog	N/A
Message index	0
Number of actions	0
Origin	N/A
Repeat count	0
rm_Decay	7200
rm_Key1	categ_00001
rm_Key1Str	Web
rm_Key2	rmnt37
rm_Key2Str	rmnt37
rm_Key3	9.3.240.117
rm_Key3Str	9.3.240.117
rm_Level	8.306751e+01
rm_LevelMax	8.778695e+01
rm_LevelMaxSev	MINOR
rm_LevelMaxTime	'Wed Mar 14 19:16:13 2001'
rm_SensorList	[webids_rmnt37]
rm_Timestamp	'Wed Mar 14 19:25:47 2001'
rm_Timestamp32	984619547
rm_Type	Category/Destination/Source
rm_Version	Version37:10/31/00:08:38:32
server_path	[]
Server ID	1
Severity	Minor
Source	Risk Manager
Status	Open
Sub-origin	N/A
Sub-source	SITUATION
Time Modified	March 14, 2001 7:25:48 PM CST

☑ Display Formatted Names and Values

Figure 140. A critical Web IDS situation

- The *source address* is 9.3.240.117.
- *Destination* is our Web server, rmnt37.
- The *sensor list* also includes a NIDS installed on the same network, which also sees these attacks.

The events are visible in the lower part of the Tivoli console most of them are WW_InsecureCGI, so someone was probably trying to find a vulnerable CGI script.



Closed Warning WW_InsecureCgi event received at March 14, 2001 7:15:20 PM CST.

↑ Attribute Name	Attribute Value
Class	WW_InsecureCgi
Credibility	0
Duration	0
Event ID	1
Hostname	rmnt37
Message	Insecure cgi search.cgi
Message catalog	N/A
Message index	0
Number of actions	0
Origin	0.0.0.0
Repeat count	0
rm_Cgi	search.cgi
rm_ClassCategories	[WEB]
rm_Correlate	yes
rm_Description	N/A
rm_DestinationHostname	rmnt37
rm_DestinationIPAddr	0.0.0.0
rm_DestinationToken	rmnt37
rm_DstPort	N/A
rm_Level	1.000000e+00
rm_NameData	N/A
rm_NameID	CAN-2000-0188
rm_NameType	CVE
rm_Protocol	unknown
rm_SensorHostname	rmnt37
rm_SensorIPAddr	0.0.0.0
rm_SensorOS	
rm_SensorPID	130
rm_SensorToken	webids_rmnt37
rm_SensorType	webids
rm_Servicename	www
rm_Signature	Insecure cgi search.cgi
rm_SourceHostname	N/A
rm_SourceIPAddr	9.3.240.117
rm_SourceToken	9.3.240.117
rm_SpoofedSourceKnown	no
rm_SrcPort	N/A
rm_Timestamp	'Wed Mar 14 19:15:36 2001'
rm_Timestamp32	984618936
rm_TimestampFmt	EPOCH
rm_Url	GET /cgi-bin/search/search.cgi?keys=*&prc=any&catigory=../../../../../../../../../../../../etc ...
rm_Version	Version37:10/31/00:08:38:32
server_path	[]
Server ID	1
Severity	Warning
Source	Risk Manager
Status	Closed
Sub-origin	webids
Sub-source	IDSEVENT
Time Modified	March 14, 2001 7:15:46 PM CST

☑ Display Formatted Names and Values

Figure 141. Details of a WW_InsecureCGI event

The attributes shown in Figure 141 again unveil some interesting details:

- The script probed (rm_CGI) was script.cgi.
- The URL itself is quite long:

```
GET
/cgi-bin/search/search.cgi?keys=*&prc=any&category=../../../../../../..
/../../../../../etc
```

- The NameID, CAN-2000-0188, is a reference to a CANdidate for the Common Vulnerabilities and Exposures (CVE).[5]

This example was generated by the *CGI abuses* plug-in of Nessus.

[5] A CVE vulnerability search engine can be found at `http://icat.nist.gov`. For our example (CAN-2000-0188), a search returns the following explanation: “EZShopper 3.0 search.cgi CGI script allows remote attackers to read arbitrary files via a .. (dot dot) attack or execute commands via shell metacharacters.”

The traces you gather and their relevance greatly depend on the services and Web applications you are running in your own DMZ.

When NIDS and Host IDS are deployed, Web IDS events always correlate with those from network and host intrusion sensors. While Web IDS only alerts you about suspicious activity, network and host IDS will usually provide you with far more hints on the ongoing attack.

6.7 Firewall intrusion detection

Firewalls basically keep all the noise from your DMZ and internal networks. If deploying an additional NIDS (as described in Section 6.1.9, “Location of sensors” on page 210) is not an option, Firewall IDS can give a basic idea on what is bouncing off a network.

Standard firewall configuration includes logging only denied packets, due to the fast fill-up of disk space. The traffic permitted is considered legitimate anyway, so logging for certain ports or hosts will only be turned on occasionally.

6.7.1 CheckPoint Firewall-1

The adapter for CheckPoint Firewall-1 merely delivers alarms to the TEC server.

6.7.1.1 Event classes

The events (see list in Appendix B.1.5, “Firewall and Router IDS” on page 320) are categorized as follows:

- Service
- ICMP
- Auth
- Control

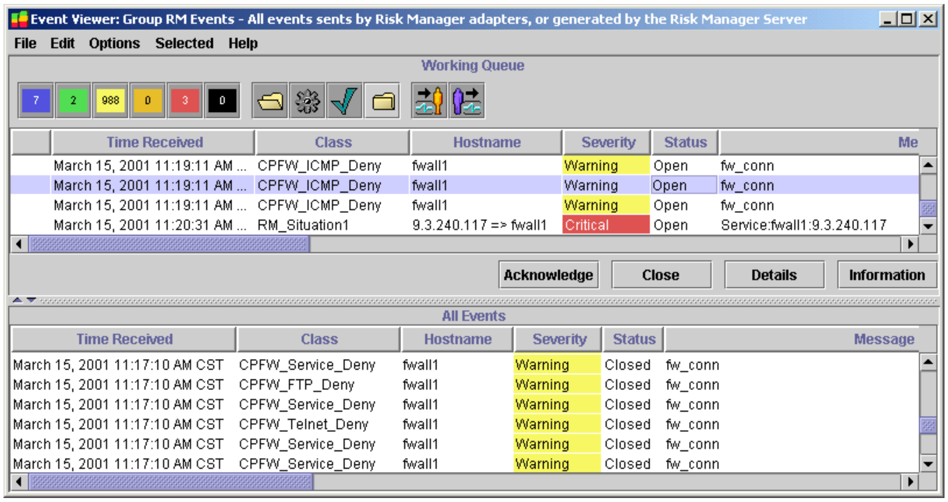
Services explicitly specified comprise:

- FTP
- HTTP
- Telnet
- Login

Both *permit* and *deny* instances of these exist.

6.7.1.2 Analysis of common traces

Risk Manager situations will arise when too many denials occur pertaining to particular hosts, as in Figure 142.


Event Viewer: Group RM Events - All events sents by Risk Manager adapters, or generated by the Risk Manager Server
File
Edit
Options
Selected
Help
Working Queue
7
2
988
0
3
0
Acknowledge
Close
Details
Information
All Events

Working Queue

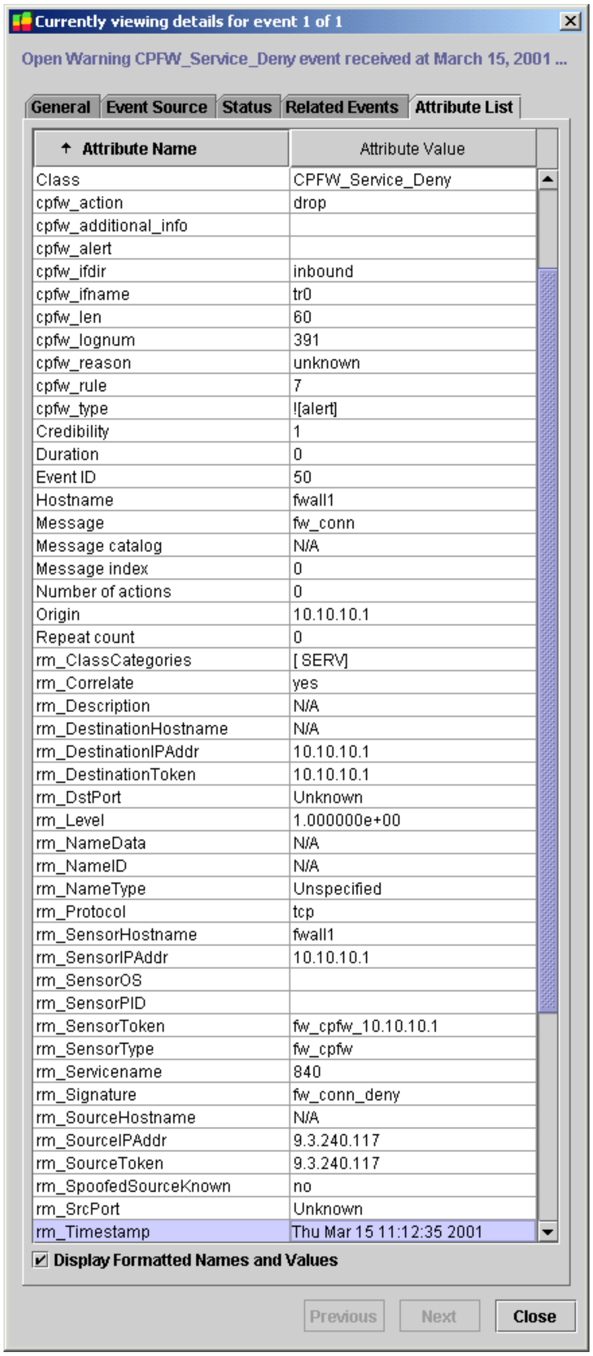
	Time Received	Class	Hostname	Severity	Status	Me
	March 15, 2001 11:19:11 AM ...	CPFW_ICMP_Deny	fwall1	Warning	Open	fw_conn
	March 15, 2001 11:19:11 AM ...	CPFW_ICMP_Deny	fwall1	Warning	Open	fw_conn
	March 15, 2001 11:19:11 AM ...	CPFW_ICMP_Deny	fwall1	Warning	Open	fw_conn
	March 15, 2001 11:20:31 AM ...	RM_Situation1	9.3.240.117 => fwall1	Critical	Open	Service:fwall1:9.3.240.117

All Events

Time Received	Class	Hostname	Severity	Status	Message
March 15, 2001 11:17:10 AM CST	CPFW_Service_Deny	fwall1	Warning	Closed	fw_conn
March 15, 2001 11:17:10 AM CST	CPFW_FTP_Deny	fwall1	Warning	Closed	fw_conn
March 15, 2001 11:17:10 AM CST	CPFW_Service_Deny	fwall1	Warning	Closed	fw_conn
March 15, 2001 11:17:10 AM CST	CPFW_Telnet_Deny	fwall1	Warning	Closed	fw_conn
March 15, 2001 11:17:10 AM CST	CPFW_Service_Deny	fwall1	Warning	Closed	fw_conn
March 15, 2001 11:17:10 AM CST	CPFW_Service_Deny	fwall1	Warning	Closed	fw_conn

Figure 142. Events from Firewall-1 in the Tivoli console

The situation details (Figure 143 on page 247) show a number of denied service requests originating from a single host (9.3.240.117).



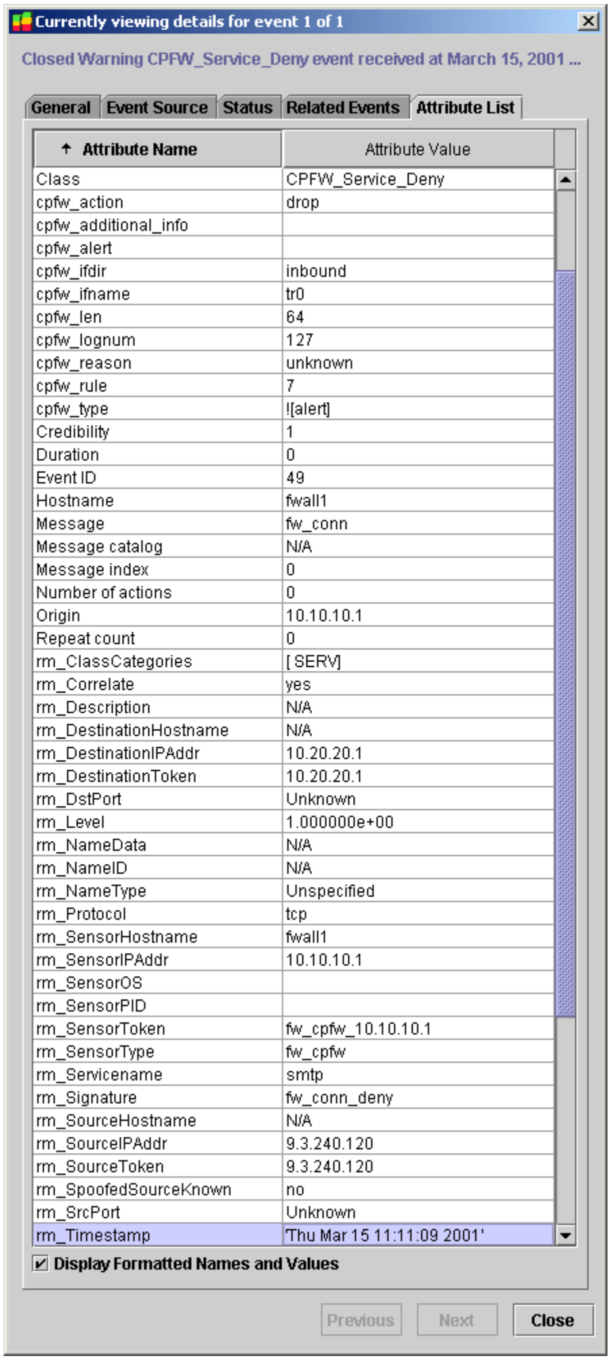
Open Warning CPFW_Service_Deny event received at March 15, 2001 ...

↑ Attribute Name	Attribute Value
Class	CPFW_Service_Deny
cpfw_action	drop
cpfw_additional_info	
cpfw_alert	
cpfw_ifdir	inbound
cpfw_ifname	tr0
cpfw_len	60
cpfw_lognum	391
cpfw_reason	unknown
cpfw_rule	7
cpfw_type	![alert]
Credibility	1
Duration	0
Event ID	50
Hostname	fwall1
Message	fw_conn
Message catalog	N/A
Message index	0
Number of actions	0
Origin	10.10.10.1
Repeat count	0
rm_ClassCategories	[SERV]
rm_Correlate	yes
rm_Description	N/A
rm_DestinationHostname	N/A
rm_DestinationIPAddr	10.10.10.1
rm_DestinationToken	10.10.10.1
rm_DstPort	Unknown
rm_Level	1.000000e+00
rm_NameData	N/A
rm_NameID	N/A
rm_NameType	Unspecified
rm_Protocol	tcp
rm_SensorHostname	fwall1
rm_SensorIPAddr	10.10.10.1
rm_SensorOS	
rm_SensorPID	
rm_SensorToken	fw_cpfw_10.10.10.1
rm_SensorType	fw_cpfw
rm_Servicename	840
rm_Signature	fw_conn_deny
rm_SourceHostname	N/A
rm_SourceIPAddr	9.3.240.117
rm_SourceToken	9.3.240.117
rm_SpoofedSourceKnown	no
rm_SrcPort	Unknown
rm_Timestamp	Thu Mar 15 11:12:35 2001

☑ Display Formatted Names and Values

Figure 143. A situation resulting from a network scan denied by the firewall

Viewing the attribute list in the event detail panel reveals further information: an inbound (cpfw_ifdir) connection attempt for port 840 (rm_Servicename) was dropped (cpfw_action). Names are only provided for a few services; usually rm_Servicename just states port numbers.



Closed Warning CPFW_Service_Deny event received at March 15, 2001 ...

Attribute Name	Attribute Value
Class	CPFW_Service_Deny
cpfw_action	drop
cpfw_additional_info	
cpfw_alert	
cpfw_ifdir	inbound
cpfw_ifname	tr0
cpfw_len	64
cpfw_lognum	127
cpfw_reason	unknown
cpfw_rule	7
cpfw_type	![alert]
Credibility	1
Duration	0
Event ID	49
Hostname	fwall1
Message	fw_conn
Message catalog	N/A
Message index	0
Number of actions	0
Origin	10.10.10.1
Repeat count	0
rm_ClassCategories	[SERV]
rm_Correlate	yes
rm_Description	N/A
rm_DestinationHostname	N/A
rm_DestinationIPAddr	10.20.20.1
rm_DestinationToken	10.20.20.1
rm_DstPort	Unknown
rm_Level	1.000000e+00
rm_NameData	N/A
rm_NameID	N/A
rm_NameType	Unspecified
rm_Protocol	tcp
rm_SensorHostname	fwall1
rm_SensorIPAddr	10.10.10.1
rm_SensorOS	
rm_SensorPID	
rm_SensorToken	fw_cpfw_10.10.10.1
rm_SensorType	fw_cpfw
rm_Servicename	smtp
rm_Signature	fw_conn_deny
rm_SourceHostname	N/A
rm_SourceIPAddr	9.3.240.120
rm_SourceToken	9.3.240.120
rm_SpoofedSourceKnown	no
rm_SrcPort	Unknown
rm_Timestamp	'Thu Mar 15 11:11:09 2001'

☑ Display Formatted Names and Values

Figure 144. Details of a Service_Deny event

6.7.2 Other firewalls

The second firewall Risk Manager supports is *Cisco PIX*, providing some greater detail through its log adapter because of the more specific log entries Cisco generates.

Another adapter exists for *Cisco Router*s, whose contribution to intrusion detection is their ACL-capability, so it seems appropriate to list them here as well.

6.8 Experience Risk Manager

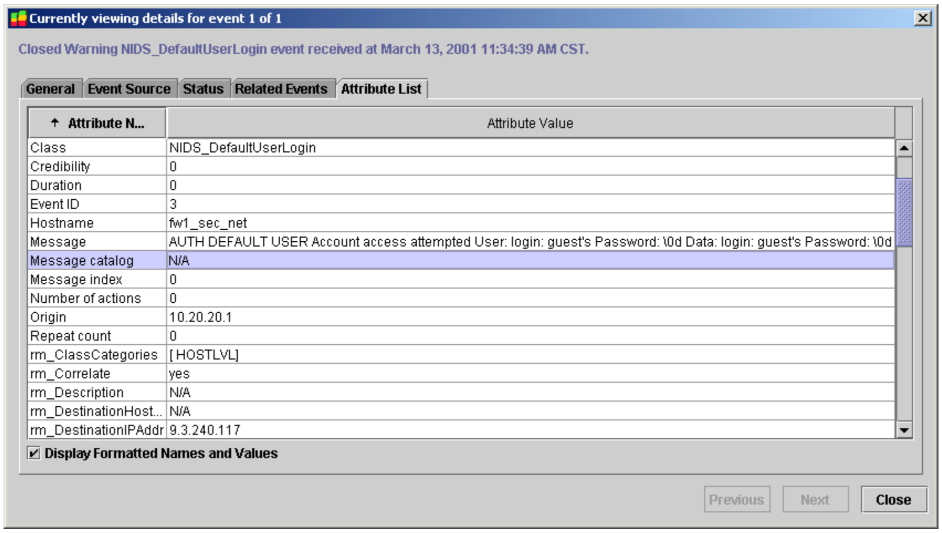
In this concluding section, some of the experiences and difficulties encountered with Risk Manager 3.7 have been compiled.

6.8.1 Real world examples

Intrusion detection systems usually present attacks in several ways, due to the various input the different types of sensors receive.

6.8.1.1 Failed guest login

Attempts to login using an alleged guest account fail repeatedly. Both Network IDS and Host IDS send alarms, albeit from different perspectives.



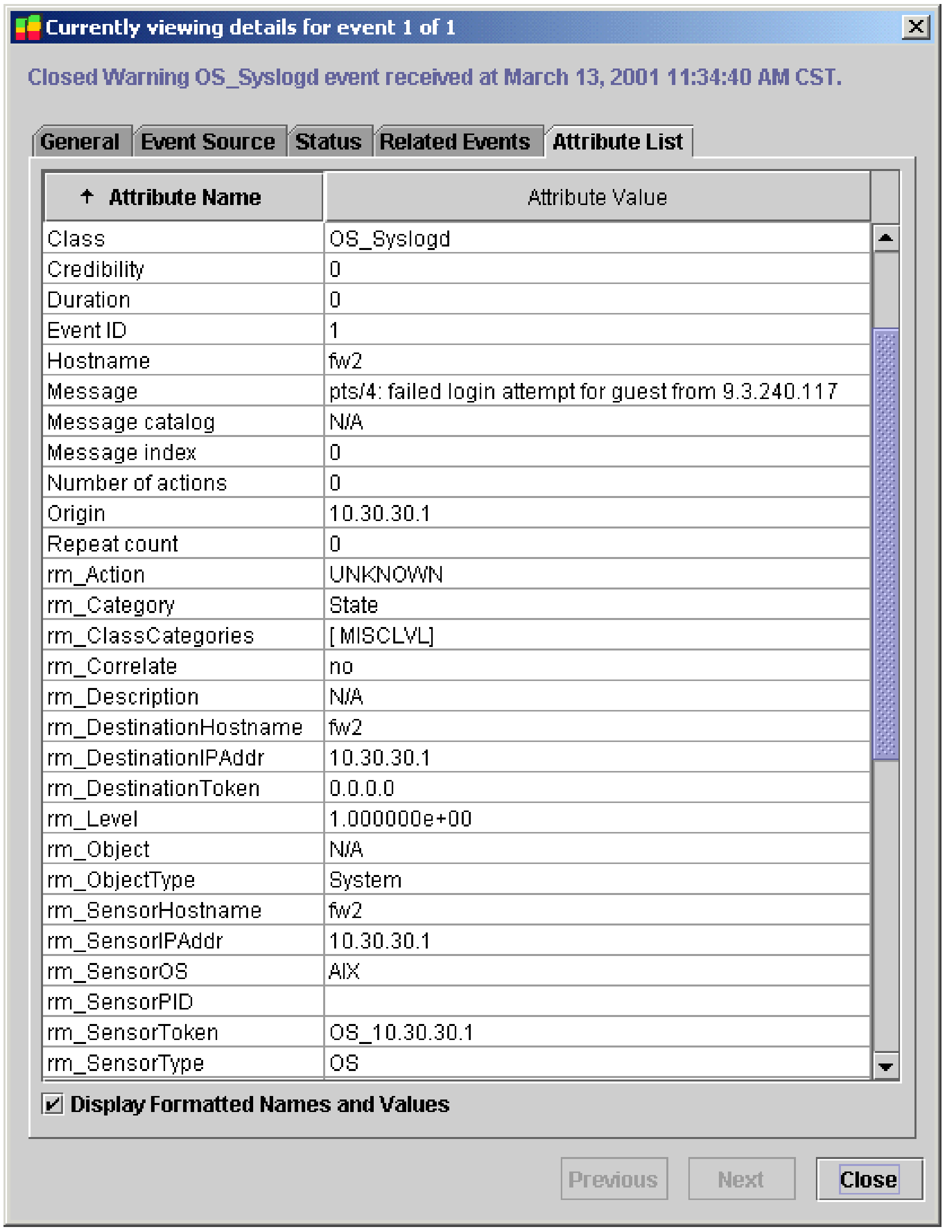
Closed Warning NIDS_DefaultUserLogin event received at March 13, 2001 11:34:39 AM CST.

↑ Attribute N...	Attribute Value
Class	NIDS_DefaultUserLogin
Credibility	0
Duration	0
Event ID	3
Hostname	fw1_sec_net
Message	AUTH DEFAULT USER Account access attempted User: login: guest's Password: \0d Data: login: guest's Password: \0d
Message catalog	N/A
Message index	0
Number of actions	0
Origin	10.20.20.1
Repeat count	0
rm_ClassCategories	[HOSTLVL]
rm_Correlate	yes
rm_Description	N/A
rm_DestinationHost...	N/A
rm_DestinationIPAddr	9.3.240.117

☑ Display Formatted Names and Values

Figure 145. Failed guest login seen by NIDS

While NIDS also provides further input information (Figure 145), Host IDS merely reports the unsuccessful attempt itself (Figure 146 on page 251).



Closed Warning OS_Syslogd event received at March 13, 2001 11:34:40 AM CST.

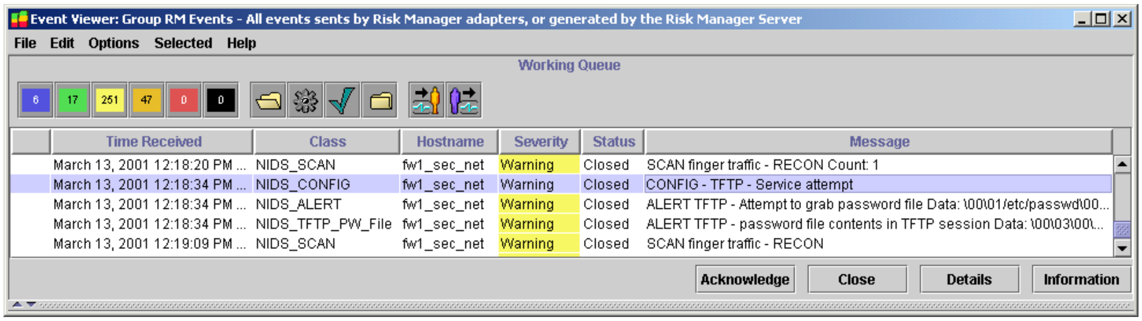
Attribute Name	Attribute Value
Class	OS_Syslogd
Credibility	0
Duration	0
Event ID	1
Hostname	fw2
Message	pts/4: failed login attempt for guest from 9.3.240.117
Message catalog	N/A
Message index	0
Number of actions	0
Origin	10.30.30.1
Repeat count	0
rm_Action	UNKNOWN
rm_Category	State
rm_ClassCategories	[MISCLVL]
rm_Correlate	no
rm_Description	N/A
rm_DestinationHostname	fw2
rm_DestinationIPAddr	10.30.30.1
rm_DestinationToken	0.0.0.0
rm_Level	1.000000e+00
rm_Object	N/A
rm_ObjectType	System
rm_SensorHostname	fw2
rm_SensorIPAddr	10.30.30.1
rm_SensorOS	AIX
rm_SensorPID	
rm_SensorToken	OS_10.30.30.1
rm_SensorType	OS

☑ Display Formatted Names and Values

Figure 146. Failed guest login seen by Host IDS

6.8.1.2 TFTP download of /etc/passwd

Three different NIDS events (see Figure 147 on page 252) report the successful download of the password file residing in /etc/passwd.


Event Viewer: Group RM Events - All events sents by Risk Manager adapters, or generated by the Risk Manager Server
File
Edit
Options
Selected
Help
Working Queue
6
17
251
47
0
0
Acknowledge
Close
Details
Information

Time Received	Class	Hostname	Severity	Status	Message
March 13, 2001 12:18:20 PM ...	NIDS_SCAN	fw1_sec_net	Warning	Closed	SCAN finger traffic - RECON Count: 1
March 13, 2001 12:18:34 PM ...	NIDS_CONFIG	fw1_sec_net	Warning	Closed	CONFIG - TFTP - Service attempt
March 13, 2001 12:18:34 PM ...	NIDS_ALERT	fw1_sec_net	Warning	Closed	ALERT TFTP - Attempt to grab password file Data: \00\01/etc/passwd\00...
March 13, 2001 12:18:34 PM ...	NIDS_TFTP_PW_File	fw1_sec_net	Warning	Closed	ALERT TFTP - password file contents in TFTP session Data: \00\03\00\...
March 13, 2001 12:19:09 PM ...	NIDS_SCAN	fw1_sec_net	Warning	Closed	SCAN finger traffic - RECON

Figure 147. NIDS reports download of /etc/passwd using TFTP

Although Host IDS was also installed on the system, it did not recognize this attack!

6.8.2 Common problems

In our test environment, we encountered some small problems with the current Risk Manager version and the Tivoli Framework environment. These situations are described in the following sections.

6.8.2.1 No more events from a sensor

Sensors and adapters still tend to terminate relatively often in our environment. Be aware that this occurs without any warning to administrators, so if you have not received events from one of your adapters lately, it is usually not because the bad guys gave up. Tivoli development has been increasing availability and reliability of all sensors and adapters.

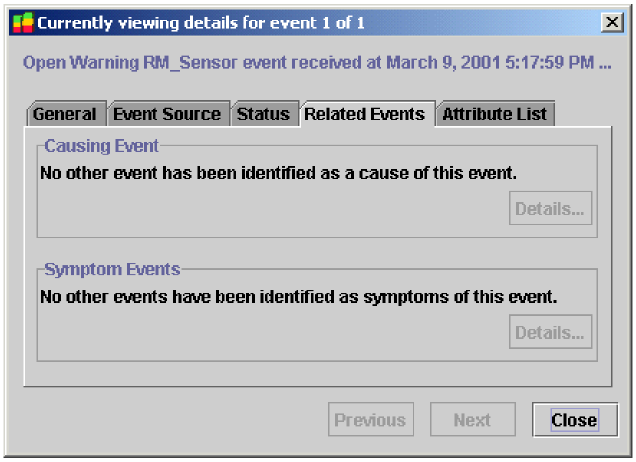
The same problem exists when your DB2 database on the TEC server is full, then extended to all sensors immediately. This situation can be avoided by defining an alert on the DB2 machine to inform the administrator about this shortage, so he can increase the database size before it comes to a halt.

6.8.2.2 some.host.org

Don’t get confused by some.host.org in the rm_KeyList; this seems to be a left over from debugging Risk Manager. (For the skeptic, try `nslookup`; a domain host.org does not even exist.)

6.8.2.3 No related events

Besides very rare exceptions, there will be no related events shown on the Related Events panel of the Currently viewing details panel (see Figure 148 on page 253).



Currently viewing details for event 1 of 1

Open Warning RM_Sensor event received at March 9, 2001 5:17:59 PM ...

Causing Event

No other event has been identified as a cause of this event.

Symptom Events

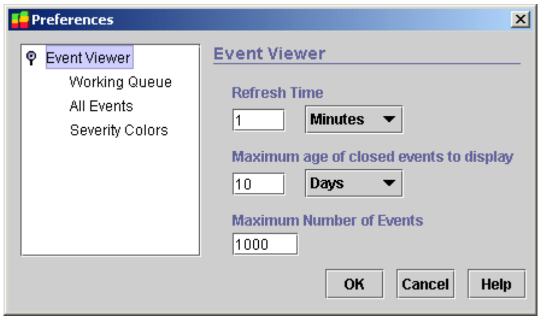
No other events have been identified as symptoms of this event.

Figure 148. Details panel: no related events

This is true for almost all situations, which, by definition, have events related to them. This shortcoming is due to a restriction in TEC and it will be solved with the next Risk Manager release.

6.8.2.4 Only open events in event viewer

The Tivoli event viewer, with its maximum age (see Figure 149) set to zero, will still show open events of the present day, but not the closed ones. Simply increase the number of days; ten should be reasonable.



Preferences

Event Viewer

Refresh Time: 1 Minutes

Maximum age of closed events to display: 10 Days

Maximum Number of Events: 1000

Figure 149. Tivoli configuration panel for days shown

This concludes our problems with using Risk Manager in a real world environment. Most of functions delivered splendid results and they will save time for the security officers or administrators in the field.

Chapter 7. Reporting using TDS for Enterprise Risk Management

If you have Tivoli Decision Support (TDS) installed and configured, you may use the Tivoli Decision Support for Enterprise Risk Management Guide V 1.0 (referred to as the ERM Guide hereafter) to provide vendor-neutral risk assessment, intrusion detection, firewall management and virus management decision support capabilities.

TDS relies on data collected in relational database(s). The ERM Guide depends on the data collected by endpoints supported by Tivoli Risk Manager 3.7. It also supports new data retrieved by endpoints which comply with IDEF specs. All such data is stored in the Tivoli Event Console (TEC) database managed by the TEC Server in a Tivoli Managed Region (TMR). The guide reads Risk Manager events from the Tivoli Event Console (TEC) database, which is implemented on several RDBMS platforms. Risk Manager events are those TEC event records in which the SOURCE attribute has the value, RISKMGR.

This data is accessed directly using Crystal Reports or collected using queries for creation of a multidimensional cube that is used by Cognos PowerPlay reports.

After populating the database, you can use TDS to obtain views and reports provided by the ERM Guide.

Note

Since the ERM Guide uses the TEC database, it is a good idea to install the TDS for Event Management Guide in addition to the ERM Guide. TDS for Event Management Guide helps you to analyze the TEC events. We will not cover the implementation of the TDS for Event Management Guide in this chapter. A good source that you can refer for the TDS for Event Management Guide is the redbook *Early Experiences with Tivoli Enterprise Console 3.7,* SG24-6015.

7.1 Implementing the TDS for Enterprise Risk Management Guide

To use the ERM Guide, you should first install TDS in a stand-alone or network mode. You may refer to the IBM Redbook *Using Tivoli Decision Support Guides*, SG24-5506, for more information about the Tivoli Decision Support product.

There are three main steps required to install and configure the ERM Guide:

1. Install the ERM Guide.
2. Set up an ODBC connection.
3. Customize TDS:
   a. Import the ERM Guide.
   b. Add the data source.
   c. Assign the data source.
   d. Build the cubes.
   e. Automate the build process.

We will explain these steps in the following sections.

Note

If TDS is installed in standalone mode, the TDS file server and Tivoli Discovery Administrator reside on the same machine. If TDS is installed in network mode, these components are on different machines. In our environment, we used the standalone mode.

7.1.1 Prerequisite software

The following software products are required to use the ERM Guide:

- Windows NT 4.0 with Service Pack 4 or Windows 98.

Note

We recommend you to use Windows NT 4.0 as your TDS platform to be able to use the TDS Process Scheduler and security features of NT.

- Tivoli Decision Support V 2.1 with the following patches:
  - Patch 2.1-TDS-0001
  - Patch 2.1-TDS-0004
  - Patch 2.1-TDS-0005
- The database client for the ERM Guide database and the corresponding 32-bit ODBC database client driver.

The ERM Guide uses a RDBMS to access the data. The following databases are currently supported by the ERM Guide:

- DB2 5.2 and 6.1
- Oracle 7.3.4, 8.0.5 and 8.1.5

Please consult to the Tivoli Decision Support for Enterprise Risk Management Release Notes for the odbc driver requirements.

7.1.2 Prerequisite hardware

The following minimum PC AT compatible hardware is required for running the TDS and the ERM Guide:

- 128 MB RAM
- Adequate free space on the hard drive, which depends on the size of installation. But a good rule of thumb is that you need at least 500 MB of free space on the TDS server.

Since TDS (especially at the cube building stage) is a very CPU intensive program, we recommend you get the fastest CPU you can afford for the server. You may refer to *Tivoli Decision Support Release Notes 2.1,* GI10-9852 for more information about TDS hardware requirement considerations.

7.1.3 Installing the ERM Guide

The Tivoli Decision Support for Enterprise Risk Management Guide is shipped on the Risk Manager 3.7 installation CD-ROM. The CD-ROM includes the standard TDS installer and the Guide will be installed using this installer. To install the ERM Guide, you must perform the following steps:

1. On the TDS file server (which would be the same machine as the Tivoli Discovery Interface machine, if you choose the standalone mode TDS installation as opposed to the network mode installation), select **Start -> Run**.
2. In the Run dialog box, type the following command, where drive is the drive containing the ERM Guide CD-ROM:

   ```
   drive:\Rm_tds\setup.exe
   ```

3. Choose Finish to complete the installation of TDS for Enterprise Risk Management 1.00.0000.

Note

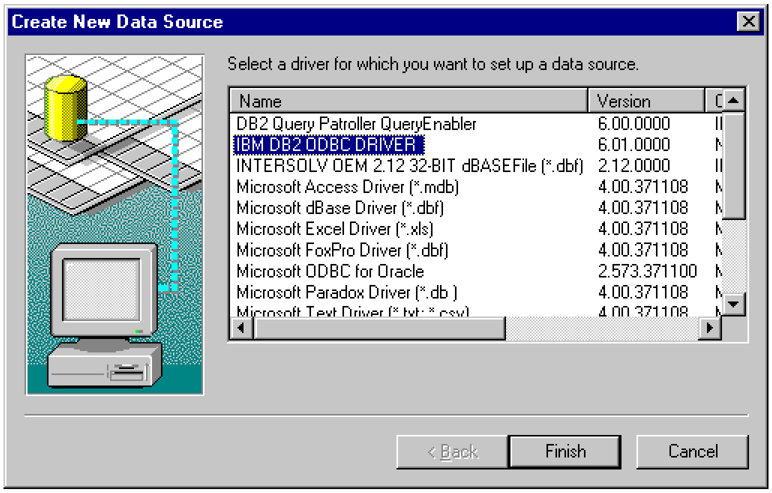
The ERM Guide does not prompt for an installation path; instead, it uses the NetPath entry in the registry file. This entry is normally assigned during the installation of the TDS file server. But you may change it later from the Tivoli Discovery Interface by selecting **View->Options ->Source Path**.

7.1.4 Setting up an ODBC connection

To use the ERM Guide, you have to set up an ODBC driver. Since our database was DB2, we used the DB2 native ODBC device driver that was installed with DB2 V 6.1. If the database you will be using is Oracle, you have to use the ODBC driver that is specified in the Tivoli Decision Support for Enterprise Risk Management Release Notes.

We performed the following steps in order to configure the ODBC connection in our environment:

1. Select **Start->Settings->Control Panel** to open the Windows Control Panel.
2. Choose the ODBC icon from the Windows Control Panel.
3. Select System DSN and choose Add.
4. From the Create New Data Source dialog box, choose IBM DB2 ODBC Driver, as shown in Figure 150 on page 259, and click Finish.

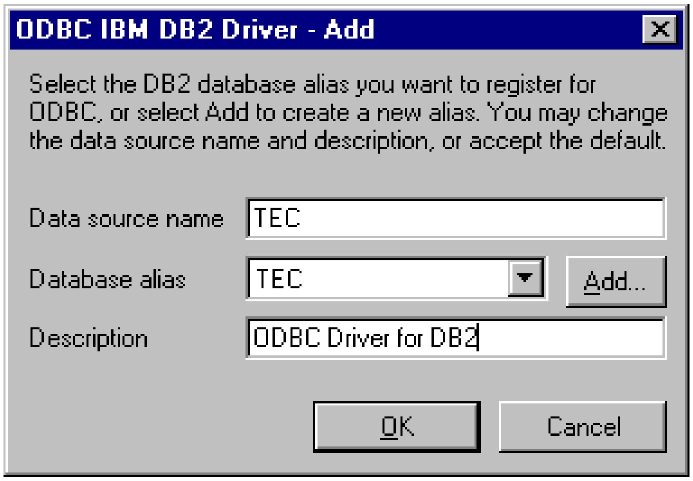


Select a driver for which you want to set up a data source.

Name	Version	C
DB2 Query Patroller QueryEnabler	6.00.0000	II
IBM DB2 ODBC DRIVER	6.01.0000	N
INTERSOLV OEM 2.12 32-BIT dBASEFile (*.dbf)	2.12.0000	II
Microsoft Access Driver (*.mdb)	4.00.371108	N
Microsoft dBase Driver (*.dbf)	4.00.371108	N
Microsoft Excel Driver (*.xls)	4.00.371108	N
Microsoft FoxPro Driver (*.dbf)	4.00.371108	N
Microsoft ODBC for Oracle	2.573.371100	N
Microsoft Paradox Driver (*.db)	4.00.371108	N
Microsoft Text Driver (*.txt; *.csv)	4.00.371108	N

Figure 150. Create New Data Source dialog

5. In the ODBC setup panel, fill in the Data Source Name and the Database Alias, as shown in Figure 151, and click OK.



Select the DB2 database alias you want to register for ODBC, or select Add to create a new alias. You may change the data source name and description, or accept the default.

Data source name: TEC

Database alias: TEC

Description: ODBC Driver for DB2

Figure 151. DB2 ODBC setup

To use the ERM Guide, you need to customize TDS by doing the following:

1. Import the ERM Guide.
2. Establish from which source the guide will find the data and create a link to that source.

The following sections explain each step in detail.

7.1.5 Importing the ERM Guide

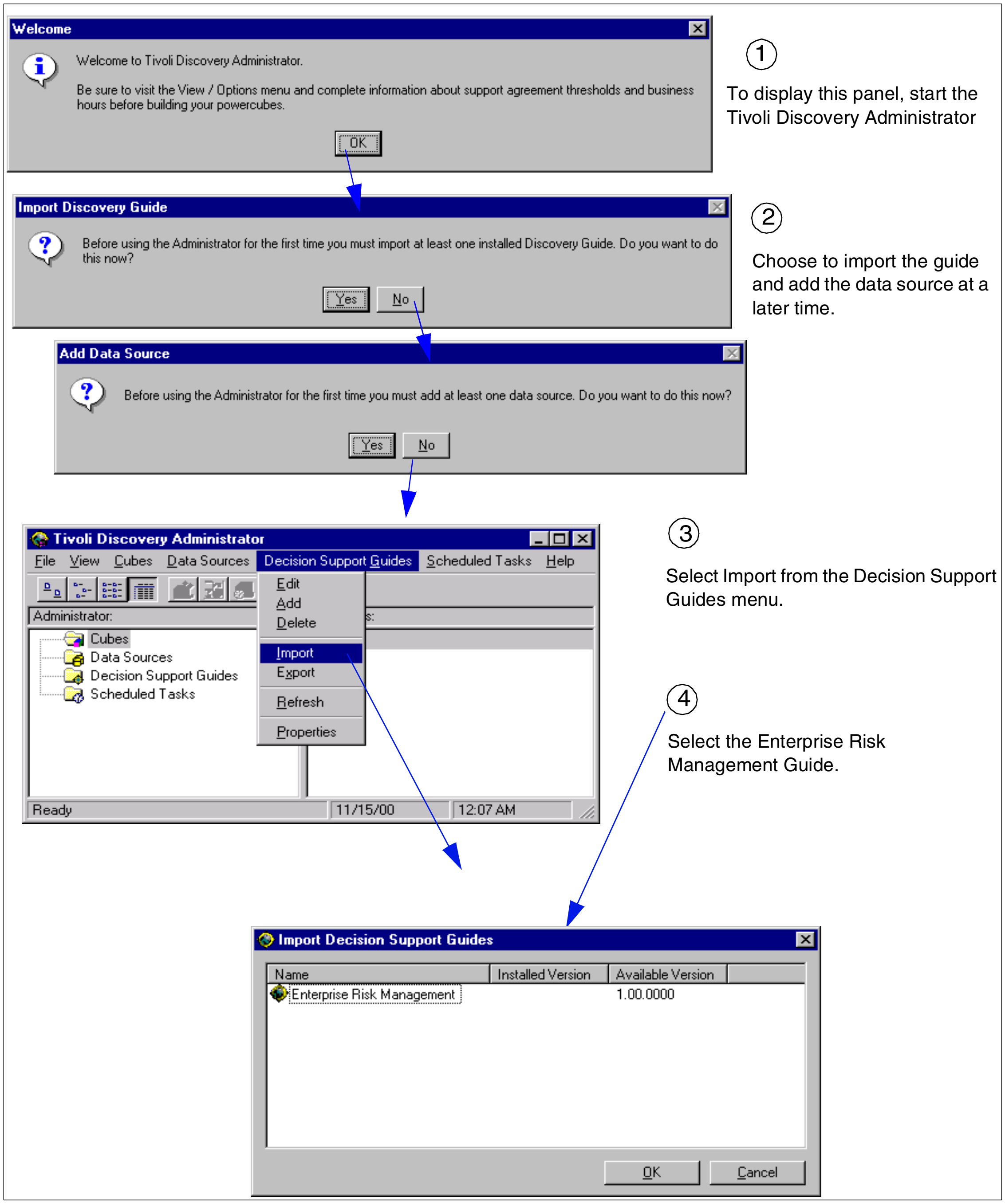
To import the ERM Guide to TDS, you need to do the following, as shown in Figure 152 on page 261:

1. Select **Start->Programs->Tivoli Decision Support->Tivoli Discovery Administrator**. If you start the TDS Discovery Administrator for the first time, the Welcome box appears; otherwise, go to step 5.
2. Enter OK, and the Import Discovery Guide box will appear.
3. To import the guide at a later time, enter No. The Add Data Source box appears.
4. To add the data source at a later time, enter No.
5. Select Import from the Decision Support Guides menu bar. In the new panel, click on Enterprise Risk Management 1.0 and then OK.

   The result is that the ERM Guide is imported, and the following cubes can be seen on the TDS Discovery Administrator panel:

   a. Risk Manager AntiVirus Status

   b. Risk Manager Archived Events



Welcome

Welcome to Tivoli Discovery Administrator.

Be sure to visit the View / Options menu and complete information about support agreement thresholds and business hours before building your powercubes.

1 To display this panel, start the Tivoli Discovery Administrator

Import Discovery Guide

Before using the Administrator for the first time you must import at least one installed Discovery Guide. Do you want to do this now?

2 Choose to import the guide and add the data source at a later time.

Add Data Source

Before using the Administrator for the first time you must add at least one data source. Do you want to do this now?

3 Select Import from the Decision Support Guides menu.

4 Select the Enterprise Risk Management Guide.

Import Decision Support Guides

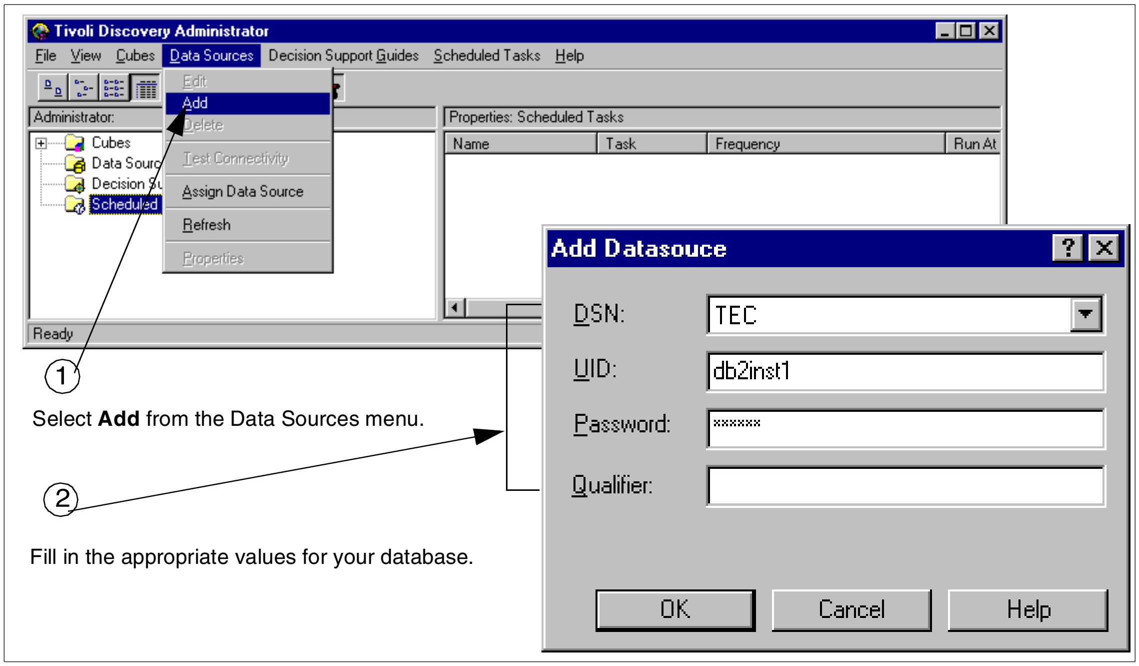
Name	Installed Version	Available Version
Enterprise Risk Management		1.00.0000

Figure 152. Importing the ERM Guide

7.1.6 Adding the data source

The next step is to add the data source from which the guide will extract data. From the TDS Discovery Administrator panel, perform the following steps as shown in Figure 153:

1. From the **Data Sources** menu bar, select the **Add** option. As a result, the Add Datasource panel appears.
2. Fill in the Data Source Name (DSN), the user ID (UID), and Password to access the data in this database, and the Qualifier. For DB2, we used the user ID *db2inst1* and password *tivoli*. You do not need to enter a Qualifier for DB2. Press OK to finish adding the TEC datasource.



DSN: TEC

UID: db2inst1

Password: ******

Qualifier:

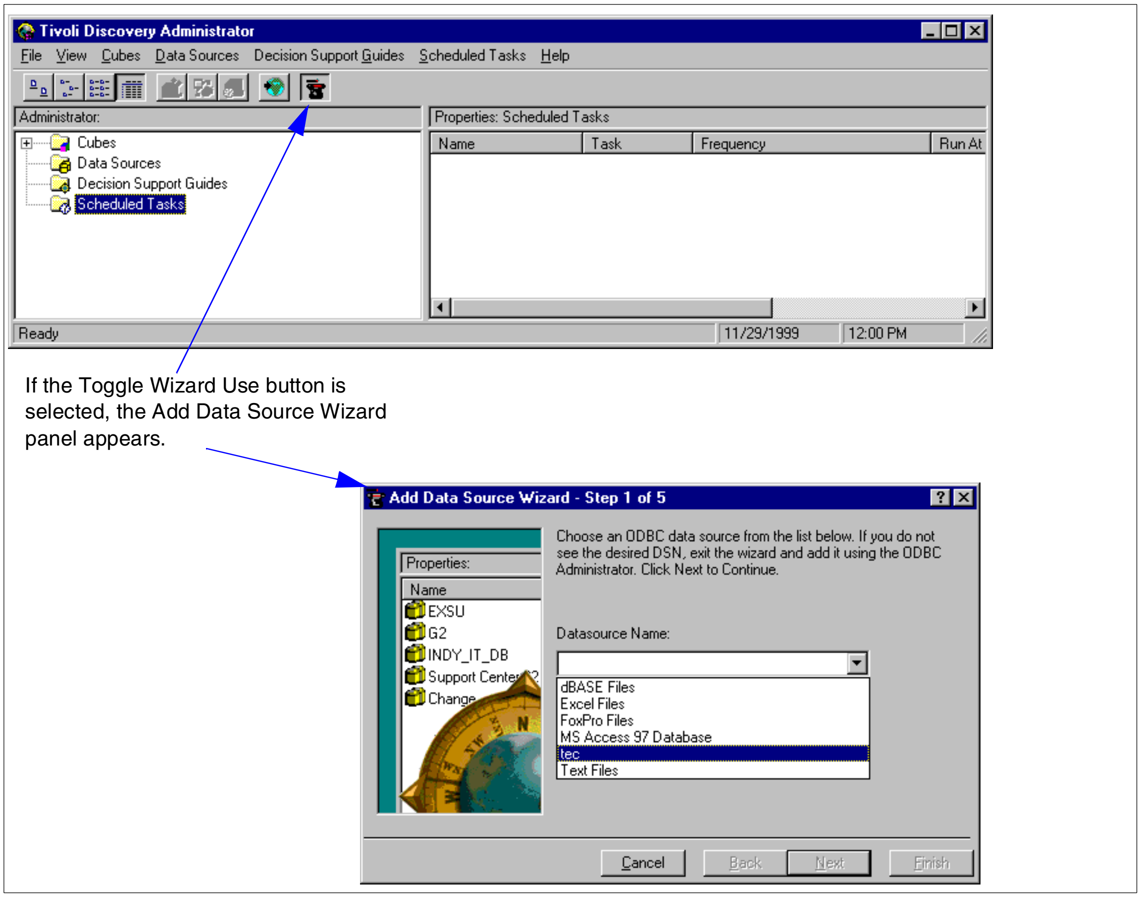
1. Select **Add** from the Data Sources menu.

2. Fill in the appropriate values for your database.

Figure 153. Adding a data source

Note

If the Toggle Wizard Use button is pressed on the Tivoli Discovery Administrator panel (see Figure 154 on page 263), you get the Add Data Source Wizard instead of the Add Datasource panel. Both panels accomplish the same function (adding a datasource), but the Wizard prompts you with the parameters in several panels



Choose an ODBC data source from the list below. If you do not see the desired DSN, exit the wizard and add it using the ODBC Administrator. Click Next to Continue.

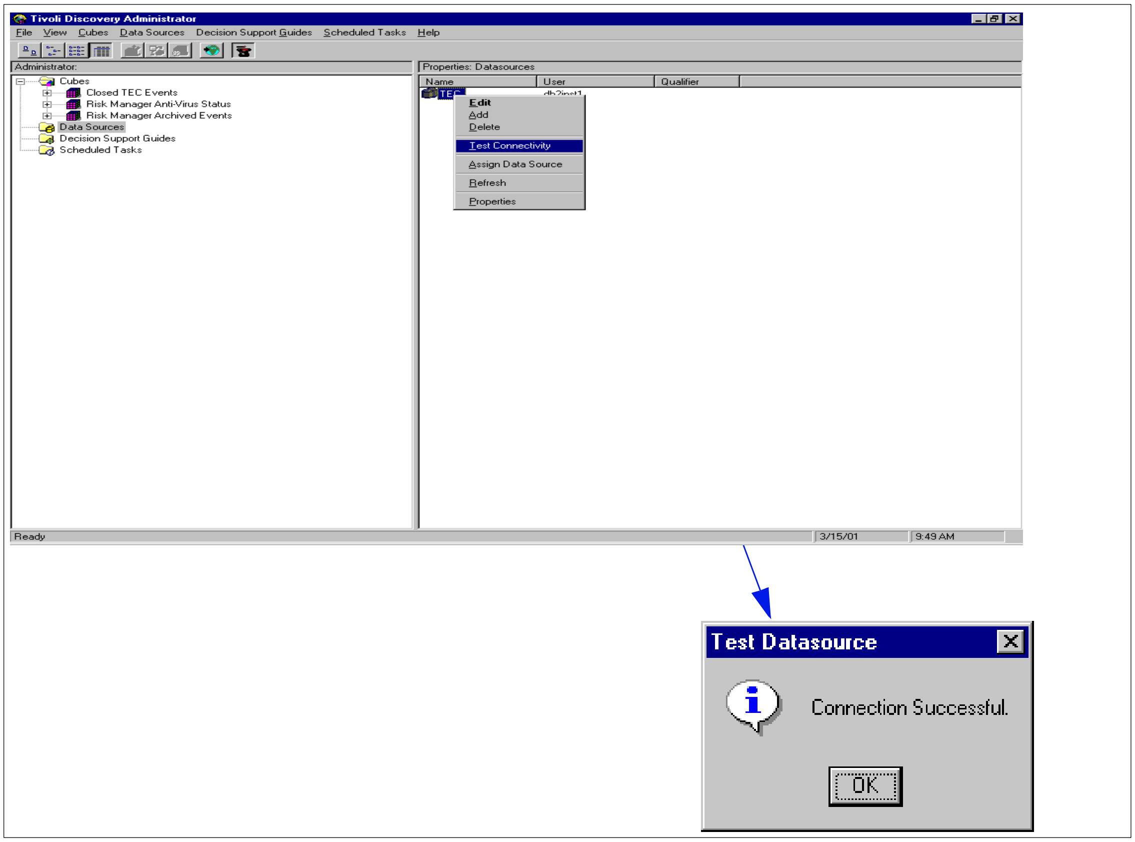
Datasource Name:

dBASE Files
Excel Files
FoxPro Files
MS Access 97 Database
tec
Text Files

If the Toggle Wizard Use button is selected, the Add Data Source Wizard panel appears.

Figure 154. Toggle Wizard Use button

3. After adding a new data source, it is possible to test its connection. To test the connection to the TEC database, right-click the data source TEC from the Tivoli Discovery Administrator Properties panel.
4. From the next panel, choose Test Connectivity, as shown in Figure 155 on page 264; the Connection Successful box should appear.



Connection Successful.

Figure 155. Testing the connection to the TEC database

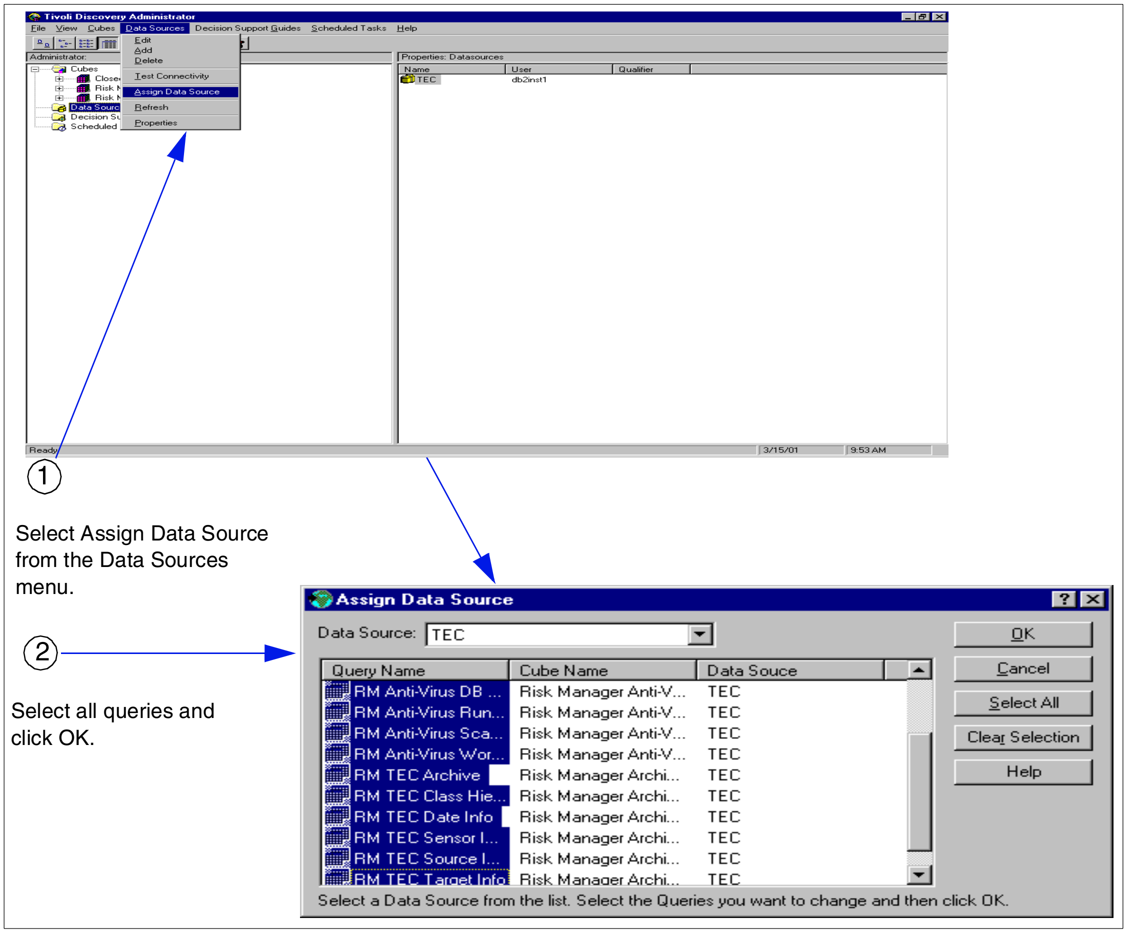
Important

The Test Connectivity function tests whether your odbc datasource can successfully connect to the database client or not. It does not guarantee that you have a a successful end to end database connection from the client to the server. The test may even be successful if your database server is down. You have to test your database client to server connectivity with native database tools.

7.1.7 Assigning the data sources

Assigning the data sources means creating a link between the queries from the ERM Guide and the database(s) used as source(s) of data. To assign the data source, you should perform the following steps, as shown in Figure 156:

1. From the Data Sources menu bar, select the **Assign Data Source** option; the Assign Data Source panel appears.
2. Select TEC as the Data Source, assign to it all the queries used by the ERM Guide to build the cubes, and press OK. As a result, the selected data source is assigned to the selected queries, and the Tivoli Discovery Administrator panel appears again.



Select Assign Data Source from the Data Sources menu.

Select all queries and click OK.

Data Source: TEC

Query Name	Cube Name	Data Souce
RM Anti-Virus DB ...	Risk Manager Anti-V...	TEC
RM Anti-Virus Run...	Risk Manager Anti-V...	TEC
RM Anti-Virus Sca...	Risk Manager Anti-V...	TEC
RM Anti-Virus Wor...	Risk Manager Anti-V...	TEC
RM TEC Archive	Risk Manager Archi...	TEC
RM TEC Class Hie...	Risk Manager Archi...	TEC
RM TEC Date Info	Risk Manager Archi...	TEC
RM TEC Sensor I...	Risk Manager Archi...	TEC
RM TEC Source I...	Risk Manager Archi...	TEC
RM TEC Target Info	Risk Manager Archi...	TEC

Select a Data Source from the list. Select the Queries you want to change and then click OK.

Figure 156. Assigning a data source

Note

You may use the Ctrl key to select more than one query at the same time.

7.1.8 Building the ERM Guide cubes

Once you have imported the ERM Guide, established that the guide will find the data in the Inventory and MDist2 databases, and created links with these databases, you can build the following cubes that belong to the ERM Guide:

- Risk Manager AntiVirus Status
- Risk Manager Archived Events

There are two way to build the cubes; manually and automatically. The next section describes both methods.

7.1.8.1 Manual build process

From the Tivoli Discovery Administrator interface, you must perform the following steps:

1. In the Administrator panel of the Tivoli Discovery Administrator, click on the Cubes folder.
2. Right click on the Risk Manager Archived Events cube, and select **Build**, as shown in Figure 157 on page 267.

Note

Unlike some other guides, cube build order is not important in the ERM Guide.

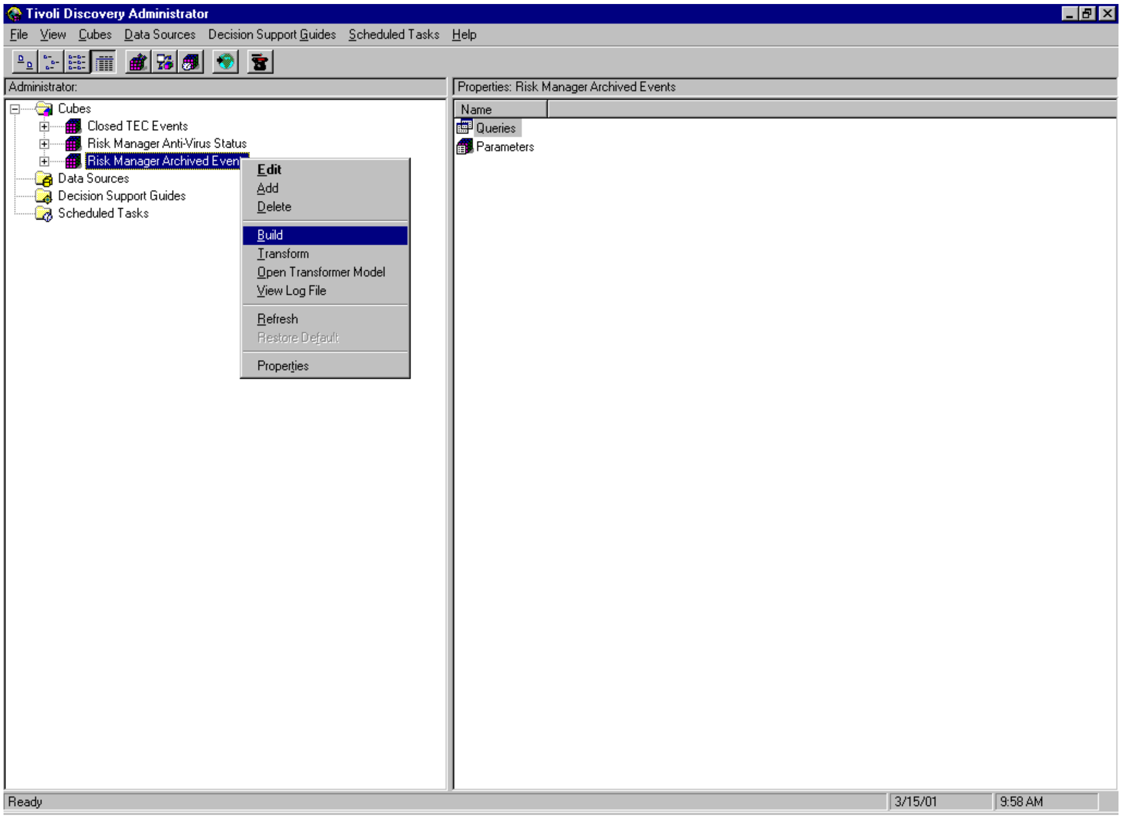
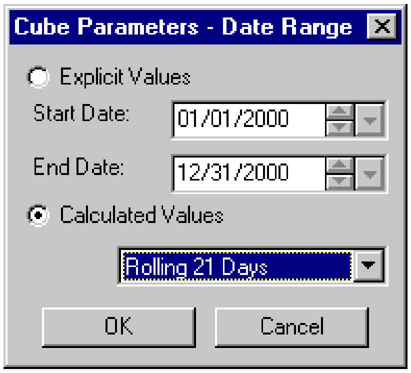


Figure 157. Building the cube

Note

You can use the data range parameter to specify the time period of the data to be included in the cube. If you do not set this parameter, the ERM Guide cubes are built with the last seven days of data. To specify a different time interval (for example, rolling 21 days):

1. Double-click on the cube you want to build; the cube properties will appear.
2. Double-click the Parameters option.
3. Set the Date Range parameters to the appropriate value by double clicking Date Range, as shown in Figure 158 on page 268.



Cube Parameters - Date Range

○ Explicit Values

Start Date: 01/01/2000

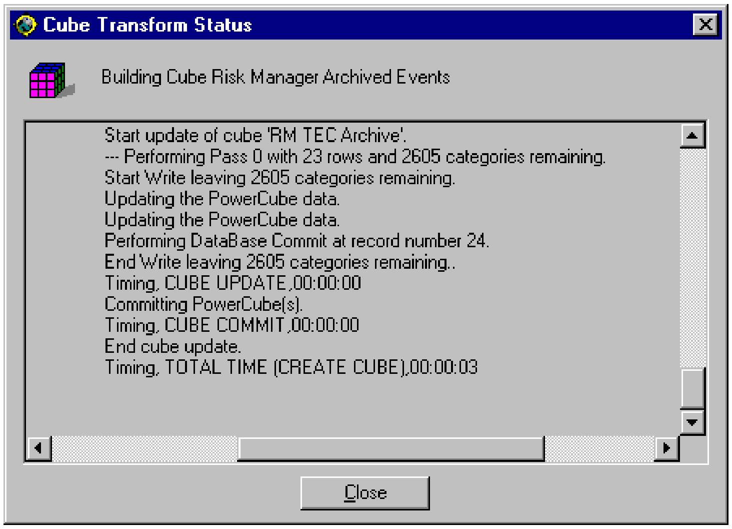
End Date: 12/31/2000

● Calculated Values

Rolling 21 Days

Figure 158. Cube Parameters Data Range

4. In the Confirm Build Cube panel, press Yes if you want to build the cube with the specified parameters. The Cube Transformation Status panel will appear as shown in Figure 159. From this panel, you can check whether the cubes are built correctly.



Cube Transform Status

Building Cube Risk Manager Archived Events

```
Start update of cube 'RM TEC Archive'.
--- Performing Pass 0 with 23 rows and 2605 categories remaining.
Start Write leaving 2605 categories remaining.
Updating the PowerCube data.
Updating the PowerCube data.
Performing DataBase Commit at record number 24.
End Write leaving 2605 categories remaining..
Timing, CUBE UPDATE,00:00:00
Committing PowerCube(s).
Timing, CUBE COMMIT,00:00:00
End cube update.
Timing, TOTAL TIME (CREATE CUBE),00:00:03
```

Figure 159. Cube Transformation Status panel

5. Perform the same step for the other cube, namely the Risk Manager AntiVirus Status.

Important

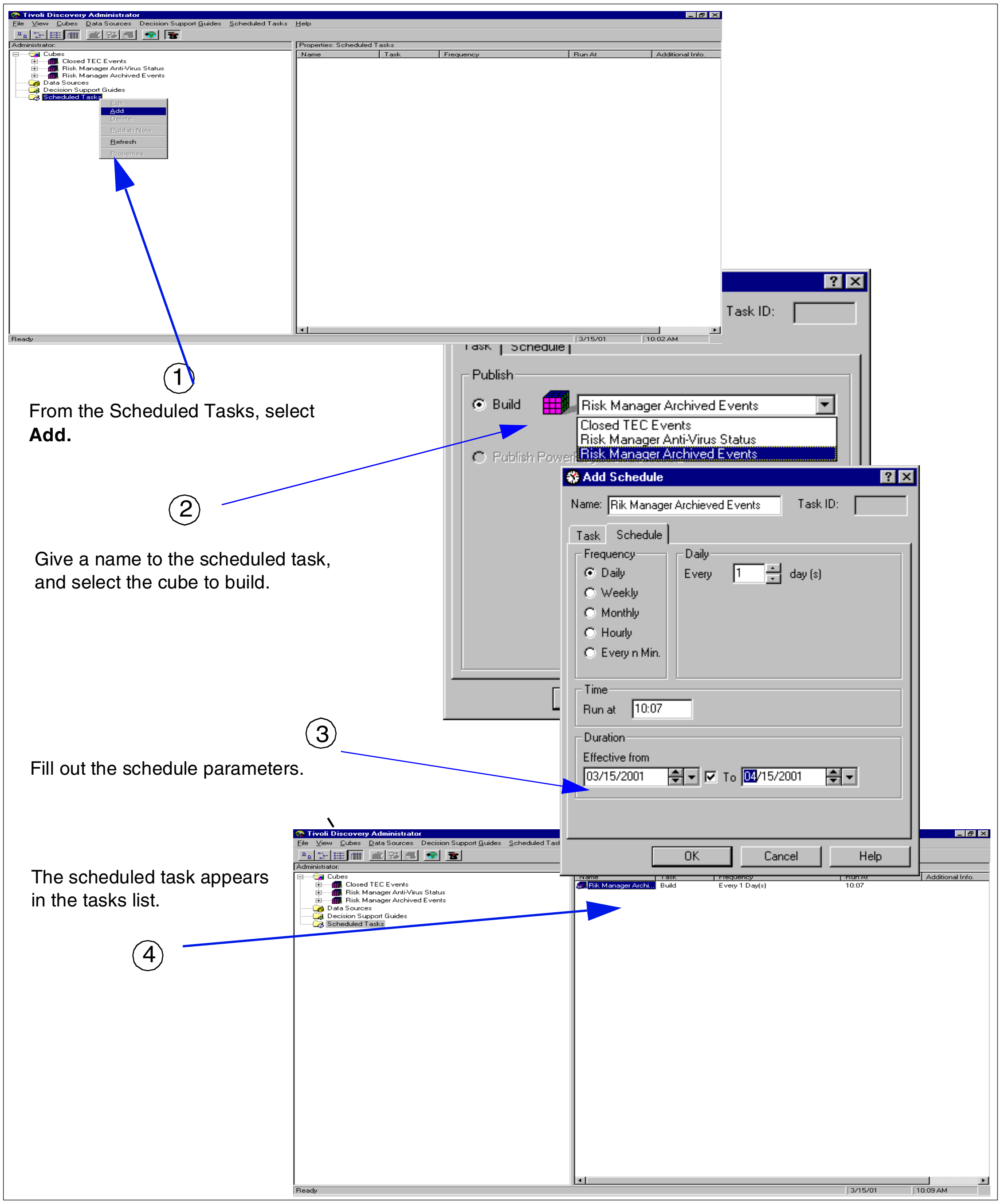
You may have noticed a Transform function in the menu besides the Build, when you right-click on the cube name. It is important to understand the difference between Build and Transform. By selecting Build you are telling TDS to first to run the queries associated with the cube and then to create the cube using Cognos Transform. On the other hand if you select Transform, TDS will begin the cube building immediately *without* first running the queries. For troubleshooting purposes, you may first want to run the queries first (by right clicking on the query name and selecting Export) to see if the problem is in running the queries or creating the cube.

7.1.8.2 Automated build process

Instead of building the cubes manually, you may want to automate the cube building process. By choosing this option, the cube can be built during off-hours when the system is free, and you ensure that the cubes are kept up-to-date. For scheduled cube building, refer to *Using Tivoli Decision Support Guides,* SG24-5506.

To schedule the building of a cube, perform the following steps, as shown in Figure 160 on page 270:

1. On the Scheduled Task menu, right-click and select **Add**.
2. On the Add Schedule panel, type the name of the scheduled task, such as ERM Guide Cube Build, and select ERM2.0_analysis1cube.
3. Click the schedule button, and type the appropriate values.
4. Press OK to finish adding the scheduled task. As a result, you may see the scheduled task from the Tivoli Discovery Administrator interface.



1. From the Scheduled Tasks, select **Add.**

2. Give a name to the scheduled task, and select the cube to build.

3. Fill out the schedule parameters.

4. The scheduled task appears in the tasks list.

Build: Risk Manager Archived Events

Name: Rik Manager Archieved Events

Task ID:

Frequency: ● Daily ○ Weekly ○ Monthly ○ Hourly ○ Every n Min.

Daily: Every 1 day (s)

Time: Run at 10:07

Duration: Effective from 03/15/2001 ☑ To 04/15/2001

Name	Task	Frequency	Run At	Additional Info.
Rik Manager Archi...	Build	Every 1 Day(s)	10:07	

Figure 160. Scheduling the building of a cube

7.1.9 View the data with the Tivoli Discovery Interface

To view the collected data, start the Tivoli Discovery Interface:

1. Select **Start->Programs->Tivoli Decision Support->Tivoli Discovery Interface**.
2. Click on Guides, and select Enterprise Risk Management from the installed guides, as shown in Figure 161.

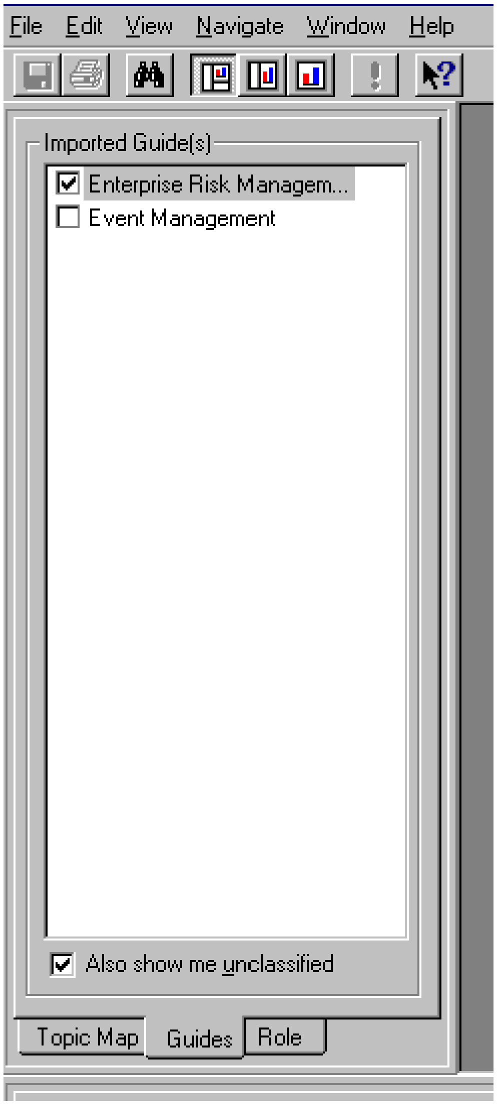
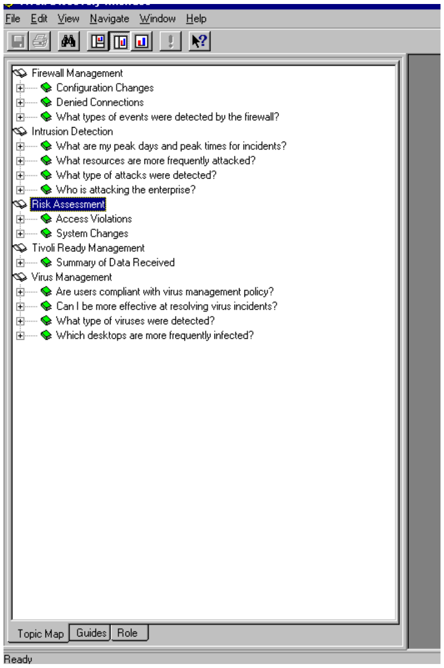

File Edit View Navigate Window Help
Imported Guide(s)
☑ Enterprise Risk Managem...
□ Event Management
☑ Also show me unclassified
Topic Map
Guides
Role

Figure 161. Tivoli Discovery Interface

3. Turn to the Topic Map, and double-click on the Enterprise Risk Management icon. You will see the topic map shown in Figure 162.



- Firewall Management
  - Configuration Changes
  - Denied Connections
  - What types of events were detected by the firewall?
- Intrusion Detection
  - What are my peak days and peak times for incidents?
  - What resources are more frequently attacked?
  - What type of attacks were detected?
  - Who is attacking the enterprise?
- Risk Assessment
  - Access Violations
  - System Changes
- Tivoli Ready Management
  - Summary of Data Received
- Virus Management
  - Are users compliant with virus management policy?
  - Can I be more effective at resolving virus incidents?
  - What type of viruses were detected?
  - Which desktops are more frequently infected?

Figure 162. Enterprise Risk Management Guide topics

7.1.10 Sample views

In this section, we will go through some of the views of the ERM Guide. This section is also intended to show you some TDS techniques for analyzing your data, especially if you are unfamiliar with the Tivoli Discovery Interface.

1. Double click on the Attack Rate by Destination Network Address view under the Intrusion Detection topic.
2. Select **View->Split Screen** to get a full panel graph.
3. You should see the Attack Rate by Destination Network Address view, as seen in Figure 163 on page 273

Note

If you do not see the dimension line under the top menu bar, you can activate it by selecting **View->Dimension Line** from the top menu bar.

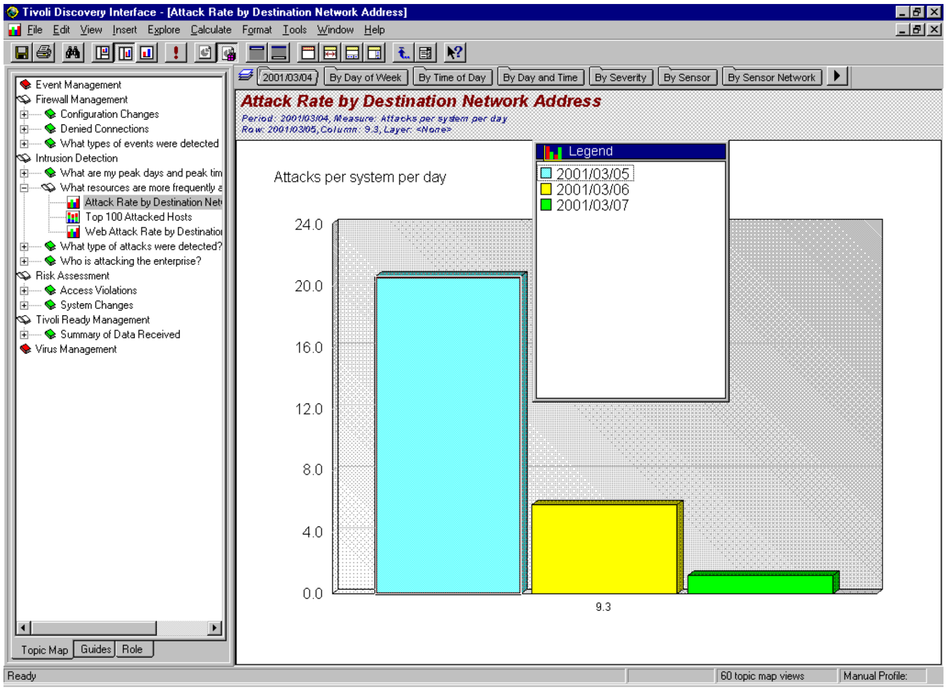

Tivoli Discovery Interface - [Attack Rate by Destination Network Address]
File Edit View Insert Explore Calculate Format Tools Window Help
Event Management
Firewall Management
Configuration Changes
Denied Connections
What types of events were detected
Intrusion Detection
What are my peak days and peak tim
What resources are more frequently a
Attack Rate by Destination Net
Top 100 Attacked Hosts
Web Attack Rate by Destinatio
What type of attacks were detected?
Who is attacking the enterprise?
Risk Assessment
Access Violations
System Changes
Tivoli Ready Management
Summary of Data Received
Virus Management
Topic Map
Guides
Role
2001/03/04
By Day of Week
By Time of Day
By Day and Time
By Severity
By Sensor
By Sensor Network
Attack Rate by Destination Network Address
Period: 2001/03/04, Measure: Attacks per system per day
Row: 2001/03/05, Column: 9.3, Layer: <None>
Attacks per system per day
24.0
20.0
16.0
12.0
8.0
4.0
0.0
9.3
Legend
🟦 2001/03/05
🟨 2001/03/06
🟩 2001/03/07
Ready
60 topic map views
Manual Profile:

Figure 163. Attack Rate by Destination Network Address graph

4. To see the attack rate by time of day, drag and drop the By Time of Day dimension from the Dimension Line on the Legend. This view is shown in Figure 164 on page 274.

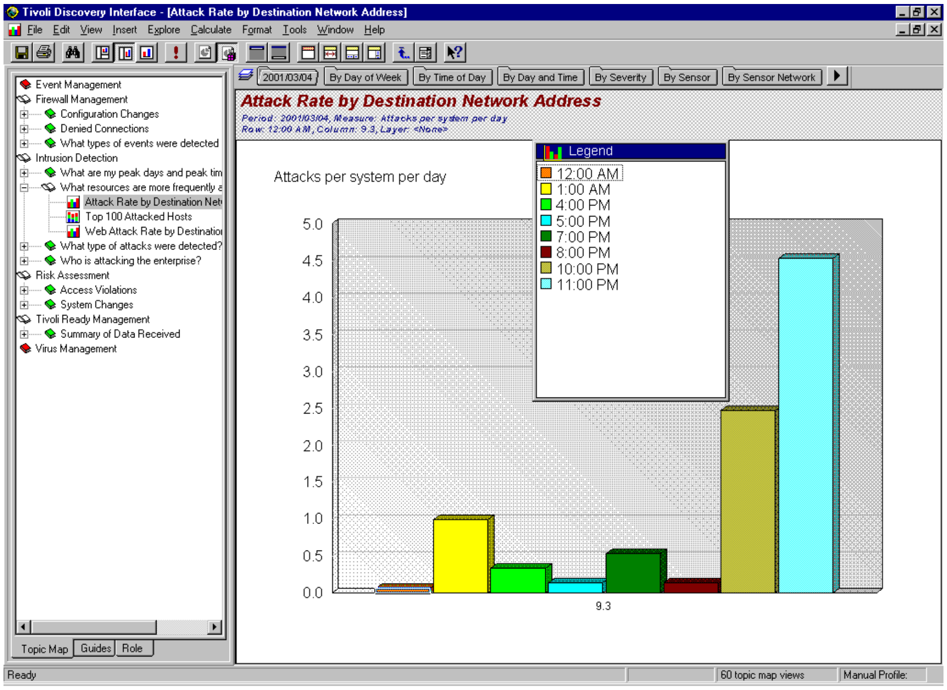

Tivoli Discovery Interface - [Attack Rate by Destination Network Address]
File Edit View Insert Explore Calculate Format Tools Window Help
2001/03/04
By Day of Week
By Time of Day
By Day and Time
By Severity
By Sensor
By Sensor Network
Event Management
Firewall Management
Configuration Changes
Denied Connections
What types of events were detected
Intrusion Detection
What are my peak days and peak tim
What resources are more frequently a
Attack Rate by Destination Net
Top 100 Attacked Hosts
Web Attack Rate by Destinatio
What type of attacks were detected?
Who is attacking the enterprise?
Risk Assessment
Access Violations
System Changes
Tivoli Ready Management
Summary of Data Received
Virus Management
Topic Map
Guides
Role
Attack Rate by Destination Network Address
Period: 2001/03/04, Measure: Attacks per system per day
Row: 12:00 AM, Column: 9.3, Layer: <None>
Attacks per system per day
Legend
12:00 AM
1:00 AM
4:00 PM
5:00 PM
7:00 PM
8:00 PM
10:00 PM
11:00 PM
5.0
4.5
4.0
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
9.3
Ready
60 topic map views
Manual Profile:

Figure 164. Attack Rate by Destination view sliced according to By Time of Day

Note

This operation is called *slicing and dicing* in TDS terms. It is done by applying different dimensions to the data. It is one of the most robust techniques for analyzing the data.

5. You may want to use the ranking feature of TDS in order to rank the graph output. Select **Explore->Rank** and accept the defaults to rank in descending order in the panel that opens.

Note

This operation is called *ranking* in TDS terms. You can rank all items as well as a specific number of items, such as Top 5.

6. After you finish the ranking operation, you can see that the resulting graph, shown in Figure 165, is ranked in descending order with 11:00 PM taking the highest share in terms of number of attacks.

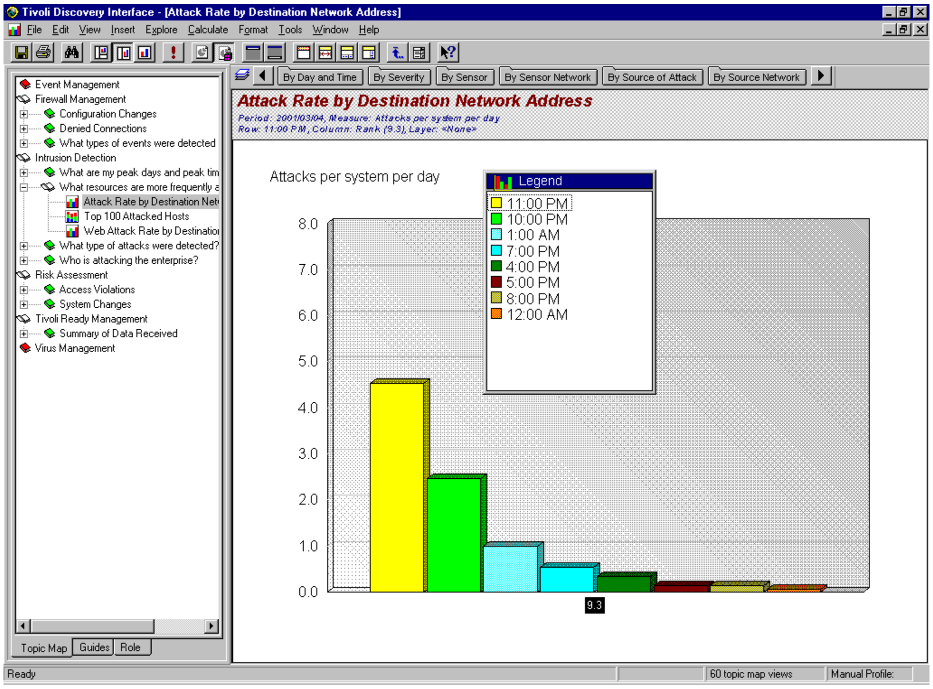

Tivoli Discovery Interface - [Attack Rate by Destination Network Address]
File Edit View Insert Explore Calculate Format Tools Window Help
Event Management
Firewall Management
Configuration Changes
Denied Connections
What types of events were detected
Intrusion Detection
What are my peak days and peak tim
What resources are more frequently a
Attack Rate by Destination Netv
Top 100 Attacked Hosts
Web Attack Rate by Destinatio
What type of attacks were detected?
Who is attacking the enterprise?
Risk Assessment
Access Violations
System Changes
Tivoli Ready Management
Summary of Data Received
Virus Management
Topic Map
Guides
Role
By Day and Time
By Severity
By Sensor
By Sensor Network
By Source of Attack
By Source Network
Attack Rate by Destination Network Address
Period: 2001/03/04, Measure: Attacks per system per day
Row: 11:00 PM, Column: Rank (9.3), Layer: <None>
Attacks per system per day
8.0
7.0
6.0
5.0
4.0
3.0
2.0
1.0
0.0
9.3
Legend
11:00 PM
10:00 PM
1:00 AM
7:00 PM
4:00 PM
5:00 PM
8:00 PM
12:00 AM
Ready
60 topic map views
Manual Profile:

Figure 165. Ranked graph

7. Double-click on the 11:00 PM bar (which is the time slot with the highest number of attacks) in the Legend to get the details of that range, as seen in Figure 166 on page 276.

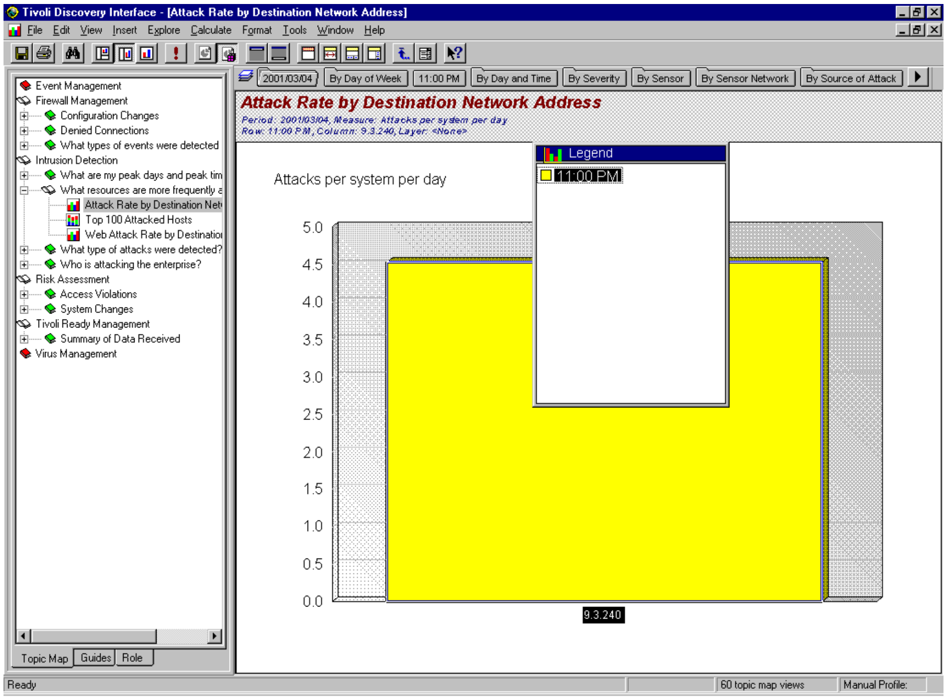

Tivoli Discovery Interface - [Attack Rate by Destination Network Address]
File Edit View Insert Explore Calculate Format Tools Window Help
2001/03/04
By Day of Week
11:00 PM
By Day and Time
By Severity
By Sensor
By Sensor Network
By Source of Attack
Event Management
Firewall Management
Configuration Changes
Denied Connections
What types of events were detected
Intrusion Detection
What are my peak days and peak tim
What resources are more frequently a
Attack Rate by Destination Net
Top 100 Attacked Hosts
Web Attack Rate by Destinatio
What type of attacks were detected?
Who is attacking the enterprise?
Risk Assessment
Access Violations
System Changes
Tivoli Ready Management
Summary of Data Received
Virus Management
Topic Map
Guides
Role
Attack Rate by Destination Network Address
Period: 2001/03/04, Measure: Attacks per system per day
Row: 11:00 PM, Column: 9.3.240, Layer: <None>
Attacks per system per day
Legend
11:00 PM
5.0
4.5
4.0
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
9.3.240
Ready
60 topic map views
Manual Profile:

Figure 166. Drill down on 11:00 PM bar

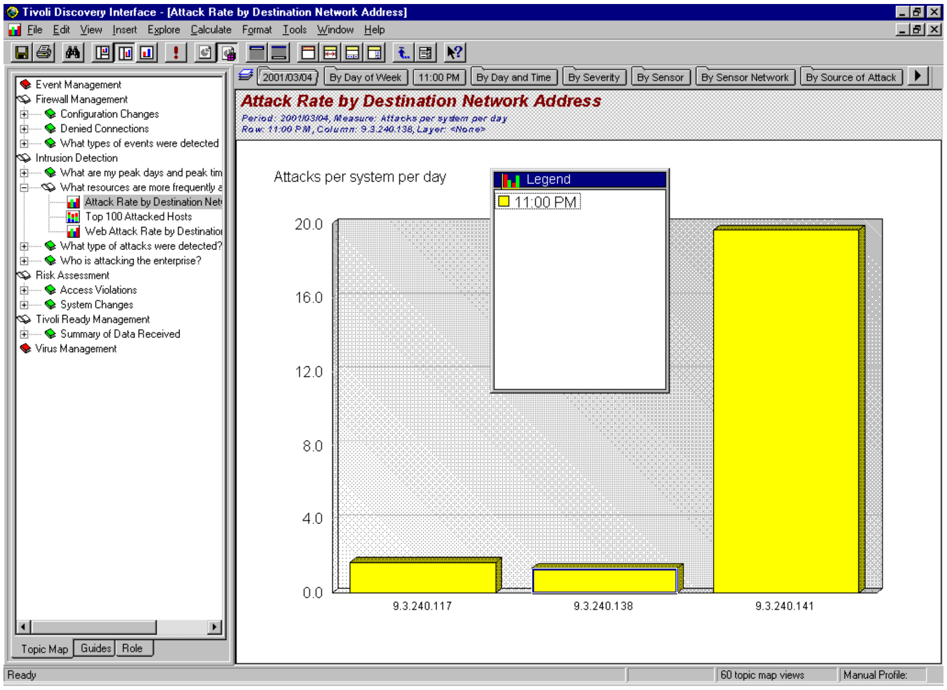
Note

This operation is called *drill-down* in TDS terms and is used to access more detailed data, for example, YEAR->MONTH->DAY. The drill down paths depend on the models of the cubes. *Drill-up* is the opposite of drill-down, that is, you access a more aggregated view from a detailed view.

8. If you are interested in all the attacks that occurred against the network address 10.30.30.3, double-click on the 10.30.30.3 network address item in the Legend to get the graph shown in Figure 167 on page 277. You could have done the same thing by first selecting the network address10.30.30.3 from the Legend and then selecting **Format->Hide->Unselected Categories** from the top menu bar.

Note

This operation is called *filtering* in TDS terms, and is used to analyze a subset of the data shown on the graph.



Attack Rate by Destination Network Address

Period: 2001/03/04, Measure: Attacks per system per day
Row: 11:00 PM, Column: 9.3.240.138, Layer: <None>

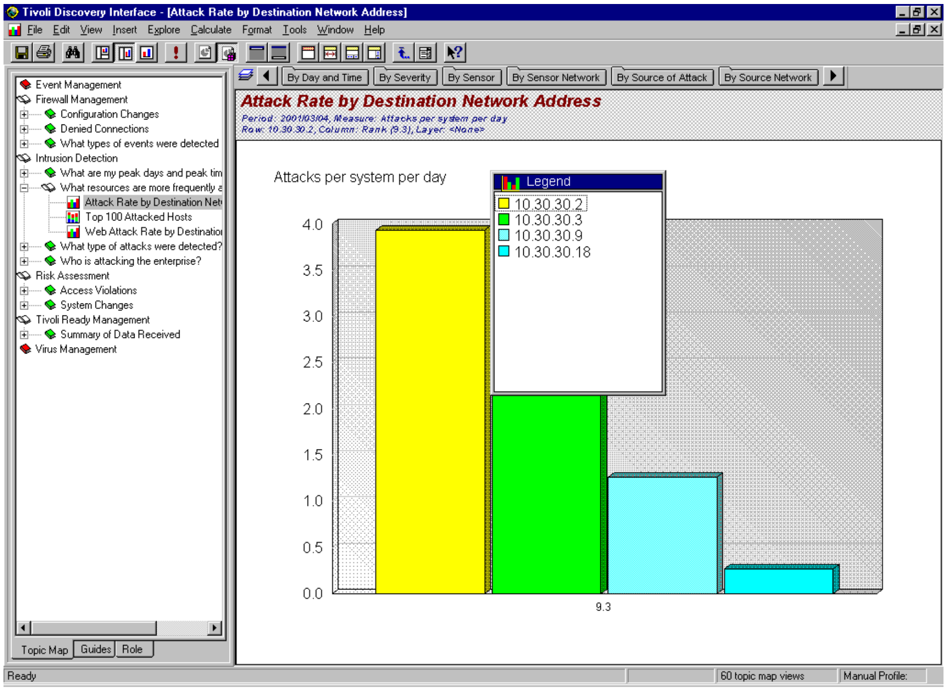
Figure 167. Analyzing attacks to the network address 10.30.30.3

9. Press Ctrl-z twice to get the graph shown in Figure 168 on page 278.

Note

It is possible for you to lose your way when browsing through the different views. Ctrl-z is a convenient way to undo the last operation. You can also select **Edit->Undo Drag/Drop Categories** from the Tivoli Discovery Interface to do the same thing.

10. To see the source of attacks, regardless of the time frame or network address, you can drag and drop the By Source of Attack dimension on the Legend. The result is seen in Figure 165 on page 275.



Attack Rate by Destination Network Address

Period: 2001/03/04, Measure: Attacks per system per day
Row: 10.30.30.2, Column: Rank (9.3), Layer: <None>

Figure 168. Attack sources

11. You can further analyze the attack sources data by applying a dimension (such as Time of Day) to it.

7.2 Summary

In this chapter, we have seen how to use the Tivoli Decision Support for Enterprise Risk Management Guide. We have gone through some examples that may help you understand some of the data analyzing techniques while using the ERM Guide. Using TDS with the ERM Guide provides you vendor-neutral risk assessment, intrusion detection, firewall management and virus management decision support capabilities. For more information on TDS, you may refer to *Using Tivoli Decision Support Guides,* SG24-5506.

Appendix A. Risk Manager classes

As a reference, we have collected and documented all the Risk Manager classes in this appendix, which gives a listing of all classes and class attributes along with brief descriptions. Each subsection starts with a list of classes shown in tree form.

Some of the classes may be a super-class of others, especially in Section B.1.6, “Host IDS” on page 325.

A.1 Correlation classes (riskmgr.baroc)

The following gives a listing of the more important attributes defined in each class along the chain from the top level EVENT class to the final class RM_User. For each attribute the following information is given:

Attribute Name of the attribute.

Type Type and default value, if any.

Used in correlation Indicates if the attribute is used in the correlation process.

Set Typical method used to set the value (BAROC, Adapter, or either). Attributes can either be set from data coming from an adapter or as defaults in the BAROC file.

Description Brief description of what the attribute represents, including any issues that should be considered when setting the attribute's value.

Figure 169 on page 280 gives an overview of the basic RM_Event class hierarchy.

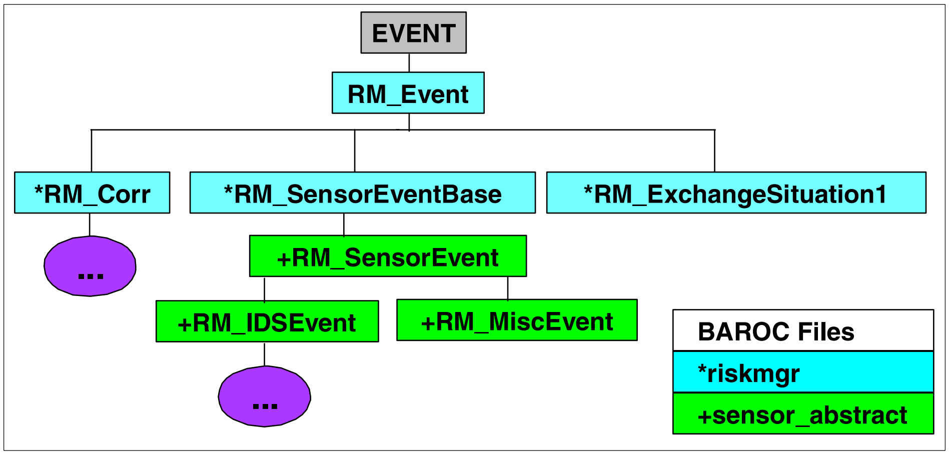


Figure 169. RM_Event class hierarchy

A.1.1 Attributes from the class EVENT

These are attributes defined in the top level TEC class EVENT. They are always available for every event and some have special importance because they are used as display strings in various fields on the TEC Console. These are not all the attributes defined in EVENT.

Attribute severity

Type Enumeration SEVERITY, default=WARNING

Used in correlation No

Set BAROC

Description This should be one of (in increasing levels of severity) HARMLESS, MINOR, WARNING, or CRITICAL. This will be displayed on the TEC Console in the first field. The events will have a status of CLOSED unless there is a problem in processing the event, in which case the status will remain OPEN.

Attribute date

Type String

Used in correlation No

Set Adapter

Description Typically a timestamp for when the event was generated in a human readable format, such as "04

Jul 2000 12:30:44." TEC fills this in from date_reception if it is not set by the adapter.

Attribute hostname

Type String, default='N/A'

Used in correlation No

Set Adapter

Description The name of the host on which the sensor is running. Risk Manager fills this in with information from rm_SensorHostname. This will be displayed on the TEC Console in the "Hostname" field.

Attribute msg

Type String

Used in correlation No

Set Adapter

Description A brief description of the event. Setting this attribute is quite important because the value is displayed on the TEC Console in the "Message" field. If the adapter has not set this value, then it will be set from rm_Signature, if available.

A.1.2 RM_Event

This is the base class for all Risk Manager events. It is used to set default values for various attributes of the class EVENT and define attributes common to all Risk Manager classes.

Attributes modified:

source	default='RISKMGR';
sub_source	default='N/A';
origin	default='N/A';
sub_origin	default='N/A';
hostname	default='N/A';
adapter_host	default='N/A';
msg	default='N/A';
msg_catalog	default='N/A';
msg_index	default=0;
repeat_count	default=0;

Attributes defined:

rm_Version	STRING,default='Version37:10/31/00:08:38:32';
rm_Timestamp	STRING,default='N/A';
rm_Timestamp32	INT32,default=0;

A.1.3 RM_Corr

RM_Corr is the base class for correlation related events (see Figure 170).

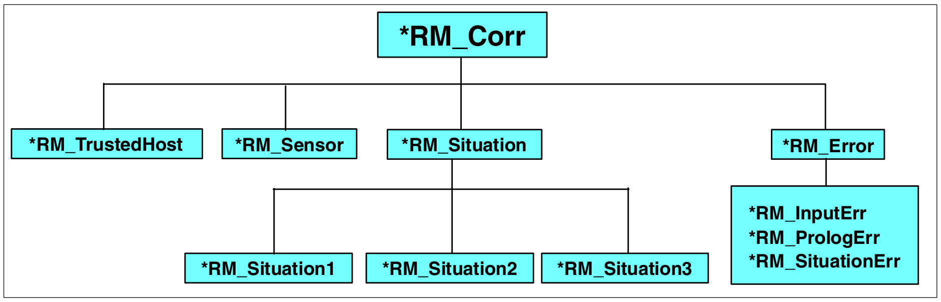


Figure 170. RM_Corr Class Hierarchy

Attributes modified:

sub_source	default='CORR';

Attributes defined:

None

A.1.3.1 RM_TrustedHost

This is activity detected from a host which is considered trusted. Do not raise an alert for activity from this host, but do maintain a list of destination hosts related to this source host.

Attributes modified:

sub_source	default='TRUSTEDHOST';

Attributes defined:

rm_HostToken	STRING, default='0.0.0.0';
rm_Hostname	STRING, default='N/A';
rm_HostIPAddr	STRING, default='N/A';
rm_SensorList	LIST_OF STRING, default=[];
rm_SignatureList	LIST_OF STRING, default=[];
rm_DestinationTokenList:	LIST_OF STRING, default=[];

rm_DestinationHostnameList	LIST_OF STRING, default=[];
rm_DestinationHostIPAddrList	LIST_OF STRING, default=[];

A.1.3.2 RM_Sensor

This represents identification information for a sensor instance.

Attributes modified:

sub_source	default='SENSOR';
severity	default='HARMLESS';

Attributes defined:

rm_SensorType	STRING, default='N/A';
rm_SensorHostname	STRING, default='N/A';
rm_SensorIPAddr	STRING, default='0.0.0.0';
rm_SensorPID	STRING, default='N/A';

A.1.3.3 RM_Situation

This is the base class for situation events. Situation events are the result of the aggregation and correlation process. The aggregation and correlation process can also result in the modification of existing situation events.

Attributes modified:

sub_source	default='SITUATION';

Attributes defined:

rm_SensorList	LIST_OF STRING;	
rm_SignatureList	LIST_OF STRING;	
rm_Level	REAL	default=1.0;
rm_LevelMax	REAL	default=0.0;
rm_LevelMaxTime	STRING	default='N/A';
rm_Decay	INTEGER;	
rm_Type	STRING	default='';
rm_Key1	STRING	default='';
rm_Key1Str	STRING	default='';
rm_Timestamp32	INT32	default=0;

RM_Situation1

This is the Situation 1 event. rm_Type = Category/Source/Destination

No aggregation is being performed, and all three keys are specified:

- Key1 = Category
- Key2 = Source
- Key3 = Destination

Attributes modified:

rm_Type	default='Category/Destination/Source';
rm_Key1	default='0';

Attributes defined:

rm_Key2	STRING	default='0.0.0.0';
rm_Key2Str	STRING;	
rm_Key3	STRING	default='0.0.0.0';
rm_Key3Str	STRING;	

RM_Situation2
This is the Situation 2 event.

Aggregation is over one key. Two other keys are specified:

- Situation 2-1 rm_Type = Destination/Source
  - Key1 = Destination
  - Key2 = Source
  - Key3 = List of categories
- Situation 2-2 rm_Type = Category/Destination
  - Key1 = Category
  - Key2 = Destination
  - Key3 = List of sources
- Situation 2-3 rm_Type = Category/Source
  - Key1 = Category
  - Key2 = Source
  - Key3 = List of destinations

Attributes modified:

rm_Type	default='Category/Destination';

Attributes defined:

rm_Key2	STRING;	
rm_Key2Str	STRING;	
rm_Key3List	LIST_OF STRING	default=[];
rm_Key3ListStr	LIST_OF STRING	default=[];

RM_Situation3

This is the Situation 3 event.

Aggregation is over two keys. One key is specified:

- Situation 3-1 rm_Type = Source
  - Key1 = Source
  - Key2 = List of categories
  - Key3 = List of destinations
- Situation 2-2 rm_Type = Destination
  - Key1 = Destination
  - Key2 = List of categories
  - Key3 = List of sources
- Situation 2-3 rm_Type = Category
  - Key1 = Category
  - Key2 = List of destinations
  - Key3 = List of sources

Attributes modified:

rm_Type	default='Category';

Attributes defined:

rm_Key2List	LIST_OF STRING	default=[];
rm_Key2ListStr	LIST_OF STRING	default=[];
rm_Key3List	LIST_OF STRING	default=[];
rm_Key3ListStr	LIST_OF STRING	default=[];

A.1.3.4 RM_Error

This is the base class for errors. The file name and line number reference information (when available) is generated using CMVC keywords: %W% for file information and %C% for line number. Additional information is provided in the rm_ErrMethod attribute, which contains the method name and (when available) the arguments passed.

Attributes modified:

sub_source	default='ERROR';
severity	default='CRITICAL';

Attributes defined:

rm_ErrFile	STRING	default='unknown';
rm_ErrLine	STRING	default='unknown';
rm_ErrMethod	STRING	default='unknown';

RM_InputErr

This class represents problems processing input data, such as data within an event (timestamps, host information, sensor information) and the various configuration settings (such as set_host, set_sensor, set_trusted_host, set_threshold, etc.).

Attributes modified:

None

Attributes defined:

None

RM_PrologErr

General Prolog errors.

Attributes modified:

None

Attributes defined:

None

RM_SituationErr

This class represents problems encountered when generating situation events or processing raw information used to update or create situation facts and events.

Attributes modified:

None

Attributes defined:

rm_SituationName	STRING;
rm_SituationType	STRING;
rm_Key1	STRING;
rm_Key1Str	STRING;
rm_Key2	STRING;
rm_Key2Str	STRING;
rm_Key3	STRING;
rm_Key3Str	STRING;
rm_SensorToken	STRING;
rm_SensorTokenStr	STRING;
rm_Signature	STRING;

A.1.4 RM_SensorEventBase

This is the base class for RM_SensorEvent. Used to set default values for various attributes of the class EVENT. Also used to extend the EVENT class by adding several attributes which are used for correlation.

Attributes modified:

severity	default='WARNING';

Attributes defined:

rm_SensorToken	STRING	default='N/A_0.0.0.0';
rm_DestinationToken	STRING	default='0.0.0.0';
rm_SourceToken	STRING	default='0.0.0.0';

A.1.5 RM_ExchangeSituation1

This is the class provided for encapsulating situation 1 facts so that they may be sent to another TEC Server.

Attributes modified:

sub_source	default='EXCHANGE';

Attributes defined:

rm_ClassToken	STRING;	
rm_TargetToken	STRING;	
rm_TargetHostname	STRING	default='none';
rm_TargetIPAddr	STRING	default='0.0.0.0';
rm_SourceToken	STRING;	
rm_SourceHostname	STRING	default='none';

rm_SourceIPAddr	STRING	default='0.0.0.0';
rm_SensorTokenList	LIST_OF STRING;	
rm_TimeUpdated	INT32;	
rm_SignatureList	LIST_OF STRING;	
rm_DecayList	LIST_OF STRING;	

A.2 RM_SensorEvent classes (sensor_abstract.baroc)

Comments and descriptions from various sources have been collected here. The label idwg-00: indicates that the information is from the IDWG draft 00 document.

Each section begins with the class name in bold and one or more class names in parentheses. The class names in parentheses are the previous Zurich class names. More than one class name in parentheses indicates that the classes were merged into the new class.

```
RM_Event ISA EVENT
 RM_SensorEventBase ISA RM_SensorEvent
     RM_SensorEvent ISA RM_SensorEventBase(sensor_abstract.baroc)
           RM_MiscEvent ISA RM_SensorEvent(sensor_abstract.baroc)
           RM_IDSEvent ISA RM_SensorEvent(sensor_abstract.baroc)
           | RM_IDSNetwork ISA RM_IDSEvent(sensor_abstract.baroc)
           | | RM_Scan ISA RM_IDSNetwork(sensor_abstract.baroc)
           | | RM_Flood ISA RM_IDSNetwork(sensor_abstract.baroc)
           | | RM_ICMP ISA RM_IDSNetwork(sensor_abstract.baroc)
           | | RM_IP ISA RM_IDSNetwork(sensor_abstract.baroc)
           | | RM_Tool ISA RM_IDSNetwork(sensor_abstract.baroc)
           | | RM_Service ISA RM_IDSNetwork(sensor_abstract.baroc)
           | | | RM_StringMatch ISA RM_Service(sensor_abstract.baroc)
           | | | RM_Trojan ISA RM_Service(sensor_abstract.baroc)
           | | | RM_RIP ISA RM_Service(sensor_abstract.baroc)
           | | | RM_FileAccess ISA RM_Service(sensor_abstract.baroc)
           | | | RM_ThirdHost ISA RM_Service(sensor_abstract.baroc)
           | | | RM_Command ISA RM_Service(sensor_abstract.baroc)
           | | | RM_User ISA RM_Service(sensor_abstract.baroc)
           | | | RM_DNS ISA RM_Service(sensor_abstract.baroc)
           | | | RM_SNMP ISA RM_Service(sensor_abstract.baroc)
           | | | RM_RemoteTool ISA RM_Service(sensor_abstract.baroc)
           | | | RM_Email ISA RM_Service(sensor_abstract.baroc)
           | | | RM_WebServer ISA RM_Service(sensor_abstract.baroc)
           | | | | RM_InsecureCgi ISA RM_WebServer (sensor_abstract.baroc)
          | | | | RM_PrivilegedCmd ISA RM_WebServer (sensor_abstract.baroc)
           | RM_IDSInternal ISA RM_IDSEvent(sensor_abstract.baroc)
           | RM_IDSHost ISA RM_IDSEvent(sensor_abstract.baroc)
           | RM_HostResource ISA RM_IDSHost (sensor_abstract.baroc)
           | RM_HostUser ISA RM_IDSHost(sensor_abstract.baroc)
           | | RM_TargetAccount ISA RM_HostUser (sensor_abstract.baroc)
           | | | RM_HUTUser ISA RM_TargetAccount (sensor_abstract.baroc)
           | | RM_TargetFile ISA RM_HostUser(sensor_abstract.baroc)
           | | RM_TargetProcess ISA RM_HostUser (sensor_abstract.baroc)
           | | RM_AuditPolicy ISA RM_HostUser (sensor_abstract.baroc)
```

A.2.1 RM_SensorEvent

This is the base class for events generated by a sensor.

Attributes modified:

sub_source	default='SENSOREVENT';

Attributes defined:

rm_SensorType	STRING	default='N/A';
rm_SensorHostname	STRING	default='N/A';
rm_SensorIPAddr	STRING	default='0.0.0.0';
rm_SensorPID	STRING	default='';
rm_SensorOS	STRING	default='';
rm_DestinationHostname	STRING	default='N/A';
rm_DestinationIPAddr	STRING	default='0.0.0.0';
rm_SourceHostname	STRING	default='N/A';
rm_SourceIPAddr	STRING	default='0.0.0.0';
rm_SpoofedSourceKnown	STRING	default='no';
rm_Signature	STRING	default='N/A';
rm_Description	STRING	default='N/A';
rm_Level	REAL	default=1.0;
rm_TimestampFmt	STRING	default='N/A';
rm_Correlate	STRING	default='no';
rm_ClassCategories	LIST_OF STRING	default=[];

Attribute rm_SensorType

Type String, default='N/A'

Used in correlation Yes

Set Adapter or BAROC

Description Name of the sensor type, for example, Web IDS, realsecure, and so on. This may be set at the adapter and sent along with the event or it may be set as a default in each new class entry in the BAROC file. The advantage of setting it at the adapter level (for example, via an FMT or CDS file) is that you only need to set it in one place, and not as a default in many class definitions. The disadvantage of setting it at the adapter is that it generates some additional network traffic, because the data is being sent along with the event.

Attribute rm_SensorIPAddr or rm_SensorHostname

Type String, default='0.0.0.0' or 'N/A'

Used in correlation Yes

Set Adapter

Description Host identification information for the sensor instance. Either an IP address or a host name (preferably the fully qualified name) is required to identify the sensor instance. This is the machine on which the sensor is running. If both are available, then provide both. If only one is available and you have a choice, then provide the IP address. This is used to identify the sensor, so it should be unique. If the host name is being used without being fully qualified, then uniqueness may be a concern. For example, sensors running on machine1.sub1.com and machine1.sub2.com may both report themselves as running on machine1. In this case, the events from the two sensors would be grouped together during correlation.

Attribute rm_SensorPID

Type String, default=''

Used in correlation No

Set Adapter

Description Process ID for the sensor. Set this if available and if useful.

Attribute rm_SensorOS

Type String, default=''

Used in correlation No

Set Adapter

Description Operating system on which the sensor is running. Set this if available and if useful.

Attribute rm_Timestamp

Type String, default='N/A'

Used in correlation Yes

Set Adapter

Description rm_Timestamp should be set to the timestamp associated with occurrence of the suspicious activity. The preferred format is epoch time, the time in seconds since 01 Jan 1970 00:00:00. A convenient way of converting to this format (if it is available) is via the UNIX C library routine mktime. The general idea is to get a timestamp as close as possible to the occurrence of the activity. The attribute rm_TimestampFmt may be used to specify an alternate format. If no timestamp is available, the attribute rm_TimestampFmt should be set to 'NONE'. In this case, the date_reception value is used. date_reception is the time at which the event arrived at the TEC Event Server. If there is an error processing the timestamp information, the date_reception value is used and an RM_InputErr error event is generated.

Attribute rm_TimestampFmt

Type String, default='N/A'

Used in correlation Yes

Set BAROC or Adapter

Description This determines the format being used in setting rm_Timestamp. Possible values are shown in Table 16.

Table 16. Values for rm_TimestampFmt

	Description	**Used by**
N/A	This is the default value. The date_reception will be used and an RM_InputErr error event will be generated.	
NONE	The timestamp information is unavailable; use date_reception.	CISCO Router via SNMP adapter

	Description	Used by
EPOCH	The timestamp is the number of seconds since 1 Jan 1970 00:00:00.	NetRanger via C adapter to TEC Logfile Adapter Web IDS via integrated adpater to TEC Logfile Adapter Realsecure via Java adapter to TEC Logfile Adapter Checkpoint Firewall via direct CAT
TIME1	The timestamp is in the format Aug 10 2000 13:49:21	CISCO PIX Firewall via TEC Logfile Adapter
TIME2	The timestamp is in the format Apr 6 09:48:21	Standard TEC Logfile Adapter OS Unix via TEC Logfile Adapter
TIME3	The timestamp is in the format Thursday, August 10, 2000 11:20:37	Realsecure via TEC SNMP Adapter
TIME4	The timestamp is in the format Sep 07 12:28:44 2000	OS NT via TEC NT Logfile Adapter Norton Antivirus via TEC NT Logfile Adapter

Attribute rm_Signature

Type String, default='N/A'

Used in correlation No

Set Adapter

Description A string giving a brief description of the suspicious activity. A more detailed (but still relatively brief) description can be placed in rm_Description. Note that although this attribute is not currently used for correlation, it may be used for correlation in the future. To support this, an effort should be made to keep signatures consistent within a product type (product type=firewall, router, network-based IDS, host-based IDS, and so on). The amount of variable information in the signature should be minimized. The variable information in a signature should be useful from a correlation point of view. The type of variable information that would go into a signature would depend on the type of event. For example, suspicious Web activity involving a CGI script might include the name of the CGI script, but not the source and destination information.

Attribute rm_Description

Type String, default=''

Used in correlation No

Set Adapter

Description A string giving a brief description of the suspicious activity. Generally this is considered less important than setting rm_Signature. Note that TEC has a limit of 255 characters for the STRING type.

Attribute rm_Level

Type Integer, default=1.0

Used in correlation Yes

Set BAROC

Description Used to set a numerical value for the severity level of the event. This attribute should be included with a default value in all classes in your BAROC file so that a user may easily tune Risk Manager by modifying the default value. This attribute can be used to tune RM by increasing or decreasing it to give an event type (that is, an event of the given class) a higher or lower severity (or weighting or importance) relative to other event types. A value of 1.0 is considered nominal. The general guideline is to use LOW=0.5, MEDIUM=1.0, and HIGH=2.0.

This value is related to the threshold settings defined in riskmgr_thresholds.pro. For example, for rm_Level=1.0 and a setting of threshold('situation1',_,5,20,100, 200,_,_,_), then a Situation 1 event of severity WARNING would be generated when approximately 20 events were received. Note that since a time decay function is being used, it will probably require slightly more than 20 events (and the events must be received close together in time). Also, note that this example assumes that there is not already a dominating Situation 2 or Situation 3 event being displayed. Finally, note that the example assumes that only the raw severity levels of the individual events (the rm_Level values) went into determining the situation event severity level. The severity level for a situation event can be significantly increased above the accumulated raw values when the correlation process determines that a sequence of events are related and an increase in severity level is warranted.

Attribute rm_DestinationIPAddr or rm_DestinationHostname

Type String, default='0.0.0.0' or 'N/A'

Used in correlation Yes

Set Adapter

Description Host identification information for the destination host. The IP address or host name (preferably the fully qualified name) of the host which is the target or destination of the activity. If both are available, then provide both. If only one is available and you have a choice, then provide the IP address. For a host-based type IDS sensor, this would typically be the host on which the sensor is running. This is used to identify the host for correlation, so it should be unique. If the host name is being used without being fully qualified, then uniqueness may be a concern. For example, hosts machine1.sub1.com and machine1.sub2.com may both be reported as machine1. In this case, events related to the two hosts would be grouped together during correlation. This is one of the keys used for aggregation (leading to the various types of situations).

Attribute rm_SourceIPAddr or rm_SourceHostname

Type String, default='0.0.0.0' or 'N/A'

Used in correlation Yes

Set Adapter

Description Host identification information for the source host. The IP address or host name (preferably the fully qualified name) of the host that is the source of the activity. If both are available, then provide both. If only one is available and you have a choice, then provide the IP address. For a host-based type IDS sensor, this would typically not be relevant. This is used to identify the host for correlation, so it should be unique. If the host name is being used without being fully qualified, then uniqueness may be a concern. For example, hosts machine1.sub1.com and machine1.sub2.com may both be reported as machine1. In this case, events related to the two hosts would be grouped together during correlation. This is one of the keys used for aggregation (leading to the various types of situations). Do not forget that attacks often involve spoofed (that is, forged) source host information.

Attribute rm_SpoofedSourceKnown

Type String, default='no'

Used in correlation Yes

Set Adapter

Description A value of 'yes' indicates that the sensor has been able to detect that the source information has been spoofed or forged. Note that a value of 'no' does not indicate that the source information has not been forged.

Attribute rm_Correlate

Type String, default varies by class

Used in correlation Yes

Set Adapter or BAROC

Description A value of 'yes' indicates that the event will be correlated. A value of 'no' indicates that no aggregation or correlation processing is to be done. This is for events whose information will primarily be used in data mining activities. The sensor identification information and destination host identification information is still processed and used to fill in origin, sub_origin and host name.

Attribute rm_ClassCategories

Description The list of class categories (by short names) to which an event of this class belongs.

A.2.2 RM_MiscEvent

This is the base class for Non-IDS related events, such as router re-config, device restarted, user added, and so on.

Attributes:

rm_Category Used to group different categories of miscellaneous# events, for data-mining purposes. Where appropriate, it's recommended that the following string values before creating new values:

Configuration	Configuration has changed
State	State of object has changed
AccountAdmin	User, Group, ACL changes
Access	Access decision made
Policy	E.G. security policy change
Installation	Object has been (un)installed
Error	Error has occurred
Misc	Uncategorized change
Unknown	Unknown category

rm_ObjectType Used to identify the nature of the object, for data-mining purposes. Where appropriate, it's recommended that the following string values be used before creating new values, such as User, Group, ACL, System, File, Address, Router, Application, Domain, Misc, or Drive.

rm_Object Name of the object (e.g. user name, hostname, application, device name, etc.)

rm_Action An enumeration of actions. Select the value that best describes the event.

Attributes modified:

sub_source	default='MISCEVENT';
rm_Correlate	default='no';

Attributes defined:

rm_Category	STRING	default='N/A';
rm_ObjectType	STRING	default='N/A';

rm_Object	STRING	default='N/A';
rm_Action	rm_misc_actionE	default='NONE';

A.2.3 RM_IDSEvent

This is the base class for events representing IDS type activity (see Figure 171). Activity that is most likely not related to an intrusion attempt should go under the RM_MiscEvent part of the class hierarchy. Non-IDS activity might be something like users being added to a system or a firewall being reconfigured.

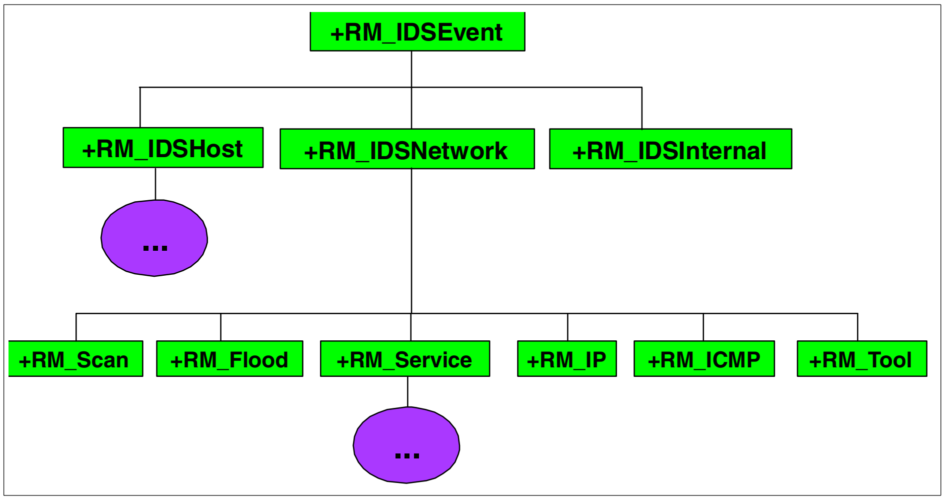


Figure 171. RM_IDSEvent Class Hierarchy

Attributes modified:

sub_source	default='IDSEVENT';
rm_Level	default=1.0;
rm_Correlate	default='yes';

Attributes defined:

rm_NameType	STRING	default='Unspecified';
rm_NameID	STRING	default='N/A';
rm_NameData	STRINGdefault='N/A';	

Attributes	rm_NameType, rm_NameID, rm_NameData
Type	String

Used in correlation No

Set Adapter

Description These provide for identifying vulnerabilities and exposures using a standard system (such as BugTraq or CVE).

rm_NameType	STRING	default = "Unspecified";#Type of ID
rm_NameID	STRING	default = ""; #String containing ID
rm_Namedata	STRING	default = ""; #String containing additional info

The attribute rm_NameType should take on one of the values found in Table 17.

Table 17. rm_NameType values

Value	Meaning
CVE	CVE identifier
BugTraq	BugTraq identifier
Vendor	Vendor defined identifier
Unspecified	[Default]

A.2.3.1 RM_IDSNetwork (ES_RealOrigin, ES_SpoofedOrigin)

This is the base class (see Figure 172) for network type activity (that is, when both a source and a destination host are involved). Either network-based or host-based IDS products may report this type of information. The majority of events classified here are expected to be from network-based IDS products.

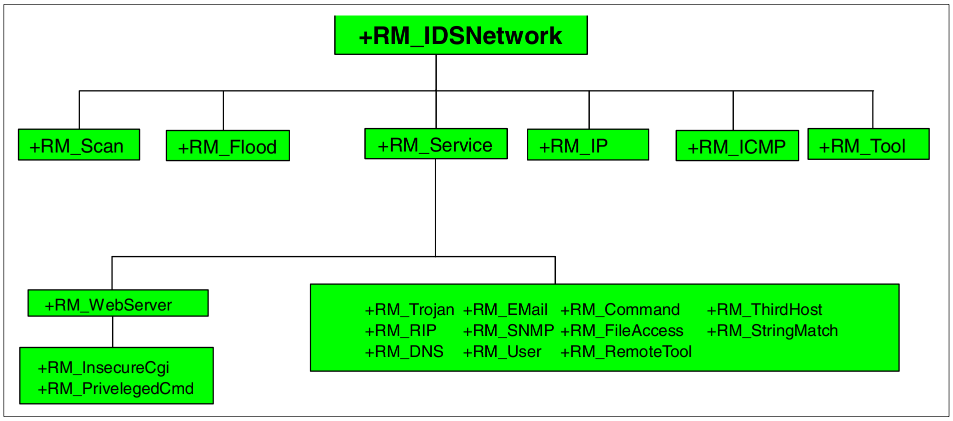

+RM_IDSNetwork
+RM_Scan
+RM_Flood
+RM_Service
+RM_IP
+RM_ICMP
+RM_Tool
+RM_WebServer
+RM_InsecureCgi
+RM_PrivelegedCmd
+RM_Trojan +RM_EMail +RM_Command +RM_ThirdHost
+RM_RIP +RM_SNMP +RM_FileAccess +RM_StringMatch
+RM_DNS +RM_User +RM_RemoteTool

Figure 172. RM_IDSNetwork Class Hierarchy

idwg-00: (ES_RealOrigin)

This class contains alerts for when there is no way to differentiate between a spoofed origin and the real source of the alert. This does not mean that the intrusion-detection sensor makes any guarantee that the source given in the alert is the one that actually carried out the alert.

idwg-00: (ES_SpoofedOrigin)

Some attacks require spoofing the origin of the packet. This set of subclasses contains alerts for which we are certain that the source address is not the origin of the alert. A typical example of this class of alerts is the land attack, when source and destination addresses are the same. When it is not possible to determine if the address is false, then the AS_REALORIGIN subclass hierarchy is used (even though the address may still be wrong).

Attributes defined:

rm_Protocol	STRING	default= 'unknown';

Attribute	rm_Protocol
Type	String, default='unknown'
Used in correlation	No
Set	Adapter or BAROC
Description	Protocol. Set this if available and if important.

RM_Scan

Attributes defined:

rm_PortCount	INTEGER	default=0;

RM_Flood

Attributes defined: none

RM_ICMP (ESR_ICMP)

Suspicious activity related to ICMP traffic. Although this might cover such things as ping floods (or other kinds of ICMP floods), the RM_Flood class is probably a more suitable place.

This indicates ICMP type attacks, such as floods.

idwg-00: (ESR_ICMP)

This class groups attacks related to ICMP traffic. The typical attacks covered by this class are ping floods (or other kinds of ICMP floods), but also BGP, EGP, and other low-level protocols. ARP/RARP is also a candidate here.

Attributes defined:

rm_ICMPCode	STRING	# ICMP code
rm_ICMPType	STRING	# ICMP type

RM_IP (ESR_IP)

This class deals with unknown IP activity

Attributes defined:

rm_Reason	STRING	default= 'unknown';

RM_Tool (ESR_Tool)

This class gives tool names.

idwg-00: (ESR_Tool)

This class groups information concerning the detection of tool activity, such as SATAN, ISS, or others.

Attributes defined:

rm_Toolname	STRING	default=";

RM_Service (ESR_SingleService)

idwg-00: (ESR_SingleService)

This class covers all intrusion-detection alerts that contain the triplet (destination, source, service). As such, most intrusion detection alerts will be mapped onto subclasses of this class.

Attributes defined:

rm_SrcPort	STRING	default = 'N/A'; # Service name or pointer
rm_DstPort	STRING	default = 'N/A';
rm_Servicename	STRING	default = 'N/A';

Attribute	rm_DestinationPort
Type	String, default='N/A'
Used in correlation	No

Set Adapter or BAROC

Description Destination port as a string. Set this if available and if important.

Attribute rm_SourcePort

Type String, default='N/A'

Used in correlation No

Set Adapter or BAROC

Description Source port as a string. Set this if available and if important.

Attribute rm_ServiceName

Type String, default='N/A'

Used in correlation No

Set Adapter or BAROC

Description Name of the service. Set this if available and if important.

- RM_Command (ESRS_CmdDecode, ESRSC_UserInfo)

  idwg-00: (ESRS_CmdDecode)

  This class covers alerts describing commands that are passed by users and are related to suspicious activity.

  idwg-00: (ESRSC_UserInfo)

  The suspicious command is associated with a user and password.

  Attributes defined:

rm_Command	STRING;	command line
rm_User	STRING	default = 'N/A';
rm_Password	STRING	default = 'N/A';

- RM_DNS (ESRS_DnsCommand)

  idwg-00: (ESRS_DnsCommand)

  This class covers DNS-related alerts. The number of DNS-related alerts generated by intrusion-detection sensors has prompted the creation of this class.

  Attributes defined:

rm_Domain	STRING;	domain name

- RM_Email (ESRS_EMail)

  This class covers email-related events. For example, the suspicious activity could be something which involves sendmail or SMTP.

  Attributes defined:

rm_Address	STRING;	email address

- RM_FileAccess (ESRS_FileAccess)

  idwg-00: (ESRS_FileAccess)

  This class covers alerts related to file accesses.

  Attributes defined:

rm_File	STRING;	file accessed (for example transferred)

- RM_ThirdHost (ESRS_ThirdHost, ESRST_UserInfo)

  idwg-00: (ESRS_ThirdHost)

  Certain alerts report attacks that involve three hosts. An example of such attack is ftp bounce. This class reports the identity of the machine used in the bounce.

  idwg-00: (ESRST_UserInfo)

  In addition to the third host involved, the user triggering the alert is reported.

  Attributes defined:

rm_ThirdHost	STRING;	Third ip address involved in attack
rm_ThirdPort	INTEGER;	Third port involved

- RM_StringMatch (ESRS_StringMatch)

  idwg-00: (ESRS_StringMatch)

  This class covers alerts produced by an intrusion detection sensor matching a given pattern with an input stream (described in the service). One example of this is the decoding of text protocols by certain intrusion detection sensors, which then generate an alert when a given string matches in the flow.

  Attributes defined:

rm_Content	STRING;	String as detected by sensor

- RM_RIP (ESRS_RIP)

  idwg-00: (ESRS_RIP)

  This class covers routing related alerts.[1]

  Attributes defined:

rm_Metric	INTEGER;	route metric
rm_Route	STRING;	IP of new hop in route

- RM_RemoteTool (ESRS_RemoteTools)

  Contains attributes for a local user and a remote user.

  Attributes defined:

rm_LocalUser	STRING;
rm_RemoteUser	STRING;

- RM_SNMP (ESRS_SNMP, ESRSS_Activity)

  idwg-00: (ESRS_SNMP)

  This class covers SNMP-related alerts.[2] The number of SNMP-related alerts generated by intrusion-detection sensors has prompted the creation of this class.

  idwg-00: (ESRSS_Activity)

  This class covers SNMP-related alerts when the intrusion detection sensor provides the entire PDU in addition to the Community and object requested.

  Attributes defined:

rm_Community	STRING;	community name
rm_OID	STRING;	object identifier
rm_Command	STRING;	this is the command issued (GET,GETNEXT, ...)

- RM_Trojan (ESRS_Trojan)

  idwg-00: (ESRS_Trojan)

  This class covers Trojan detection alerts. Alerts, such as detection of Back Orifice, NetBus, and other well-known trojans are expected to go there.

[1] G. Malkin, *Rip Version 2*, Request For Comments (Standards track) 2453, Internet Engineering Task Force, November 1998

[2] J. Case, R. Mundy, D. Partain and B. Stewart, *Introduction to Version 3 of the Internet-Standard Network Management Framework*, Request For Comments (Informational) 2570, Internet Engineering Task Force, April 1999

Attributes defined:

rm_Trojan	STRING;	Trojan name
rm_Command	STRING;	Trojan command executed
rm_Args	STRING;	Args given to the command

- RM_User (ESRS_UserDecode, ESRSU_Passwd, ESRS_PassDecode)

  idwg-00: (ESRS_UserDecode)

  This class covers user-related alerts. Examples of such alerts include logins (telnet, ftp, login, and ssh) or r-services.

  idwg-00: (ESRSU_Passwd)

  Extends ESRS_UserDecode by adding an attribute for the password.

  idwg-00: (ESRS_PassDecode)

  This class covers alerts reporting passwords, only when they cannot be attached to the associated account or user information directly. The service in this case is expected to be an authenticated service, such as telnet or ftp.

  Attributes defined:

rm_User	STRING;	user name as seen in packets
rm_Password	STRING	default = 'N/A';

Attribute	rm_User
Type	String, no default
Used in correlation	No
Set	Adapter or BAROC
Description	Name of the user.

Attribute	rm_Password
Type	String, default='N/A'
Used in correlation	No
Set	Adapter or BAROC
Description	Password. Set this if available and if important.

- RM_WebServer (ESRS_WebServer)

  This class and its subclasses group activity are related to Web server attacks. As web servers are prominent targets of attack, it is normal that we should put a lot of effort in these classes, as we expect tools to use them a lot.

idwg-00: (ESRS_WebServer)

This class covers alerts related to the web service. This includes all web-related traffic, most of the html documentation servers in UNIX environments running on port 8888 or port 8080. There are many alerts generated by this service, therefore it has been specialized in the class hierarchy.

Attributes defined:

rm_Url	STRING;	URL accessed

- RM_InsecureCgi (ESRSW_InsecureCgi)

  idwg-00: (ESRSW_InsecureCgi)

  This class covers alerts that report attempts to use well known vulnerable cgi programs. For example, the requests for well known php and asp vulnerabilities are reported by alerts of this class.

  Attributes defined:

rm_Cgi	STRING;	cgi script name

- RM_PrivilegedCmd (ESRSW_PrivilegedCmd)

  idwg-00: (ESRSW_PrivelegedCmd)

  This class covers alerts reporting attempted or successful shell or interpreter accesses through the Web server (that is, bat, sh, csh, perl).

  Attributes defined:

rm_Command	STRING;	command being tried

A.2.3.2 RM_IDSInternal (E_Weird or E_Internal)

Class provided for reporting internal IDS sensor anomalies. This class could be used for reporting IDS sensor exceptions or events that might represent an attack against the IDS sensor.

Attributes defined:

rm_Description	default='';	Description of the anomaly

RM_IDSHost (ES_Application)

This is the base class (Figure 173 on page 306) for single host type activity (that is, when the suspicious activity is local to the host being monitored). Although either network-based or host-based IDS products may report this type of information, it is anticipated that a majority of events classified here will be from host-based type IDS products. In this case, the destination host should be interpreted as the local host that is being monitored.

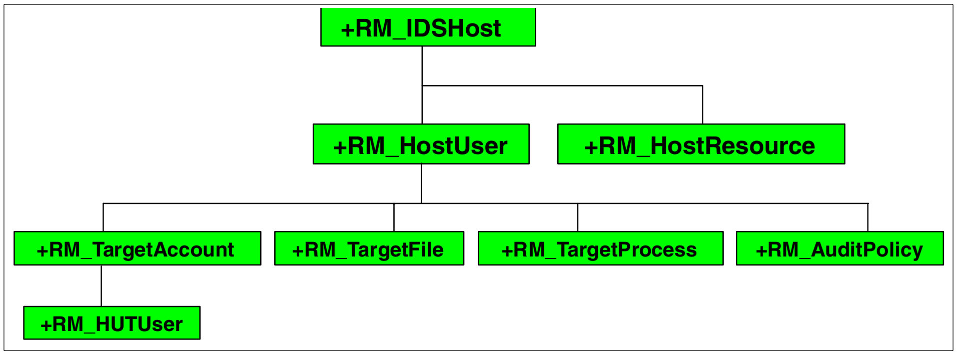


Figure 173. RM_IDSHost Class hierarchy

idwg-00: (ES_Application)

This class represents alerts that are happening on the local machine. In most cases, this means that the attack is being run locally. Examples of such alerts include reading passwords on a Windows 95 box, the SUN loadmodule, and certain symlink vulnerabilities. An alert of this class means that the attack/anomaly is carried out locally. It does not mean that the attacker/perpetrator is local to the device. For example, the loadmodule attack would be reported by the same alert, irrespective of the fact that the user is logged in on the console (physical presence) or remotely connected via telnet. To report the second case completely, two such alerts have to be generated: one for the connection and one for the local action.

Attributes defined:

rm_PtyInfo	STRING	default = 'N/A';
rm_SrcPort	STRING	default = 'N/A';
rm_DstPort	STRING	default = 'N/A';
rm_Servicename	STRING	default = 'N/A';
rm_PID	INTEGER;	

RM_HostResource

Host based IDS type activity related to a one or more resources, such as a file system reaching full capacity or a process using excessive memory.

Attributes defined:

rm_Name	STRING	default = 'N/A';
rm_State	STRING	default = '';

RM_HostUser

Attributes defined:

rm_HUsername	STRING	default = 'N/A';
rm_HUserID	STRING;	
rm_HUserDomain	STRING;	
rm_HUPurpose	STRING;	
rm_HUAdditional	STRING;	actually used only as a privelege field

- RM_TargetAccount

  Attributes defined:

rm_HUTAccountname	STRING	default = 'N/A';
rm_HUTAccountID	STRING;	
rm_HUTAccountDomain	STRING;	
rm_HUTPurpose	STRING;	
rm_HUTAdditional	STRING;	actually used only as a privelege field

  - RM_HUTUser

    Attributes defined:

rm_HUTUAccountname	STRING	default = 'N/A';
rm_HUTUAccountID	STRING;	
rm_HUTUAccountDomain	STRING;	
rm_HUTUPurpose	STRING;	
rm_HUTUAdditional	STRING;	actually used only as a privelege field or domain field for account policy changed

- RM_TargetFile

  Attributes defined:

rm_HUTFilename	STRING	default = 'N/A'; name of file (with path)
rm_HUTAccessFlags	STRING;	

- RM_TargetProcess

  Attributes defined:

rm_HUTProcessID	STRING	default = 'N/A';
rm_HUTProcessname	STRING;	

- RM_AuditPolicy

  #Actually only for NT audit

  Attributes defined:

rm_SystemSuccess	STRING;
rm_SystemFailure	STRING;
rm_LogonSuccess	STRING;
rm_LogonFailure	STRING;
rm_ObjectAccessS	STRING;
rm_ObjectAccessF	STRING;
rm_PrivilegeUseS	STRING;
rm_PrivilegeUseF	STRING;
rm_DetailedTrackingS	STRING;
rm_DetailedTrackingF	STRING;
rm_PolicyChangeS	STRING;
rm_PolicyChangeF	STRING;
rm_AccountMgmtS	STRING;
rm_AccountMgmtF	STRING;

A.3 Generic Classes (sensor_generic.baroc)

The following lines are the contents of the sensor_generic.baroc file:

```
RM_Event ISA EVENT
  RM_SensorEventBase ISA RM_SensorEvent
     RM_SensorEvent ISA RM_SensorEventBase
```

```
RM_MiscEvent ISA RM_SensorEvent
  | RM_GenericMisc ISA RM_MiscEvent(sensor_generic.baroc)
  RM_IDSEvent ISA RM_SensorEvent
  | RM_GenericIDS ISA RM_IDSEvent(sensor_generic.baroc)
  | RM_IDSNetwork ISA RM_IDSEvent
  | | RM_GenericIDSNetwork ISA RM_IDSNetwork (sensor_generic.baroc)
  | RM_IDSHost ISA RM_IDSEvent
  | | RM_GenericIDSHost ISA RM_IDSHost(sensor_generic.baroc)
```

A.3.1 RM_MiscEvent

A.3.1.1 RM_GenericMisc

A general purpose class for reporting an event of type RM_MiscEvent. Designed to facilitate rapid development of an adapter. An adapter developer could use this class initially before developing a BAROC class file specifically for the sensor.

Attributes modified:

rm_SensorType	default='generic';
rm_Level	default=1.0;
rm_TimestampFmt	default='NONE';

Attributes defined: none

A.3.2 RM_IDSEvent

A.3.2.1 RM_GenericIDS

A general purpose class for reporting an event of type RM_IDSEvent. Designed to facilitate rapid development of an adapter. An adapter developer could use this class initially before developing a BAROC class file specifically for the sensor.

Attributes modified:

rm_SensorType	default='generic';
rm_Level	default=1.0;
rm_TimestampFmt	default='NONE';

Attributes defined: none

A.3.2.2 RM_GenericIDSNetwork

A general purpose class for reporting an event of type RM_IDSNetwork. Designed to facilitate rapid development of an adapter. An adapter developer could use this class initially before developing a BAROC class file specifically for the sensor.

Attributes modified:

rm_SensorType	default='generic';
rm_Level	default=1.0;
rm_TimestampFmt	default='NONE';

Attributes defined: none

A.3.2.3 RM_GenericIDSHost

A general purpose class for reporting an event of type RM_IDSHost. Designed to facilitate rapid development of an adapter. An adapter developer could use this class initially before developing a BAROC class file specifically for the sensor.

Attributes modified:

rm_SensorType	default='generic';
rm_Level	default=1.0;
rm_TimestampFmt	default='NONE';

Attributes defined: none

Appendix B. Risk Manager classes and files

This appendix lists all the Risk Manager classes and files.

B.1 Class lists

This section will list the following different Risk Manager classes:

- Base classes
- Network IDS classes
- Web IDS classes
- Firewall and Router IDS classes
- Host IDS

B.1.1 Risk Manager classes

This is the detailed list of Risk Manager base classes:

- RM_Event
- RM_Corr
- RM_TrustedHost
- RM_Sensor
- RM_Situation
- RM_Situation1
- RM_Situation2
- RM_Situation3
- RM_Error
- RM_SituationErr
- RM_PrologErr
- RM_InputErr
- RM_SensorEventBase
- RM_ExchangeSituation1
- RM_SensorEvent
- RM_MiscEvent
- RM_IDSEvent
- RM_IDSInternal
- RM_IDSHost
- RM_HostResource
- RM_HostUser
- RM_TargetAccount
- RM_TargetFile
- RM_TargetProcess

- RM_AuditPolicy
- RM_HUTUser
- RM_IDSNetwork
- RM_Scan
- RM_Flood
- RM_ICMP
- RM_IP
- RM_Tool
- RM_Service
- RM_StringMatch
- RM_Trojan
- RM_RIP
- RM_FileAccess
- RM_ThirdHost
- RM_Command
- RM_User
- RM_DNS
- RM_SNMP
- RM_RemoteTool
- RM_Email
- RM_WebServer
- RM_InsecureCgi
- RM_PrivilegedCmd
- RM_GenericMisc
- RM_GenericIDS
- RM_GenericIDSHost
- RM_GenericIDSNetwork

B.1.2 Klaxxon

This is the detailed list of the Klaxxon classes:

- Klaxon_Catchall
- Klaxon_Probe
- Klaxon_Probe_NoPort

B.1.3 Network IDS

This section is divided into the different types of supported NIDS:

- ISS Real Secure
- Cisco Secure IDS
- Tivoli Network Intrusion Detection System Option

B.1.3.1 Real Secure

This is the detailed list of ISS Real Secure classes:

- RS_Catchall
- RS_Catchall_DS
- RS_Catchall_DSP
- RS_Catchall_UDA
- RS_HTTP_DotDot
- RS_HTTP_RobotsTxt
- RS_HTTP_NCSA_Buffer_Overflow
- RS_HTTP_NT8.3_Filename
- RS_HTTP_Netscape_SpaceView
- RS_HTTP_Netscape_PageServices
- RS_HTTP_IE3_URL
- RS_HTTP_IIS_DATA
- RS_HTTP_Phf
- RS_HTTP_Unix_Passwords
- RS_HTTP_IE_BAT
- RS_HTTP_NphTestCgi
- RS_HTTP_Shells
- RS_HTTP_TestCgi
- RS_HTTP_WebSite_Uploader
- RS_HTTP_Sgi_Handler
- RS_HTTP_WebSite_Sample
- RS_HTTP_IISExAir_DoS
- RS_HTTP_Campas
- RS_HTTP_FaxSurvey
- RS_HTTP_Cold_Fusion
- RS_HTTP_IIS3_Asp_Dot
- RS_HTTP_IIS3_Asp_2e
- RS_HTTP_WebFinger
- RS_HTTP_Cachemgr
- RS_HTTP_MachineInfo
- RS_HTTP_Count
- RS_HTTP_SiteCsc_Access
- RS_HTTP_Webgais
- RS_HTTP_FormMail
- RS_HTTP_Guestbook
- RS_HTTP_Websendmail
- RS_HTTP_Classifieds_Post
- RS_HTTP_Glimpse
- RS_HTTP_HTMLScript
- RS_HTTP_Novell_Convert

- RS_HTTP_Novell_Files
- RS_HTTP_PHP_Overflow
- RS_HTTP_Pfdisplay_Read
- RS_HTTP_Pfdisplay_Execute
- RS_HTTP_RegEcho
- RS_HTTP_RpcNLog
- RS_HTTP_SCO_View-Source
- RS_HTTP_SGI_Wrap
- RS_HTTP_SGI_Webdist
- RS_HTTP_Verity_Search
- RS_HTTP_Carbo_Server
- RS_HTTP_Info2WWW
- RS_HTTP_JJ
- RS_HTTP_Cdomain
- RS_PmapDump
- RS_Ip_HalfScan
- RS_Queso_Scan
- RS_Rlogin_Froot
- RS_Windows_Access_Error
- RS_Ftp_Syst
- RS_Ftp_Root
- RS_FSP_Detected
- RS_Finger_User
- RS_Port_Scan
- RS_UDP_Port_Scan
- RS_Kerberos_User_Snarf
- RS_DNS_Length_Overflow
- RS_Echo_Denial_of_Service
- RS_Generic_Intel_Overflow
- RS_MountdExport
- RS_MountdMnt
- RS_NfsMknod
- RS_Finger_Perl
- RS_Email_Expn
- RS_Email_Vrfy
- RS_Email_Vrfy_Overflow
- RS_Email_Helo_Overflow
- RS_Email_Ehlo
- RS_Email_Pipe
- RS_Email_Decode
- RS_Email_Debug
- RS_Email_Wiz
- RS_Email_Qmail_Length

- RS_Ident_Error
- RS_Snmp_Set
- RS_Sun_SNMP_Backdoor
- RS_HP_OpenView_SNMP_Backdoor
- RS_Imap_User
- RS_Imap_Password
- RS_Imap_Overflow
- RS_POP_Overflow
- RS_TearDrop
- RS_Land_UDP
- RS_Land
- RS_Ident_User
- RS_Finger_Bomb
- RS_FTP_Bounce
- RS_FTP_PrivilegedBounce
- RS_PingFlood
- RS_Smurf
- RS_Win_IGMP_DOS
- RS_Windows_OOB
- RS_PingOfDeath
- RS_SYNFlood
- RS_IPProtocolViolation
- RS_BackOrifice
- RS_TrinooDaemon
- RS_NetBus_Pro
- RS_IPUnknownProtocol
- RS_IPFrag
- RS_Satan
- RS_ISS
- RS_Login_S
- RS_Logout
- RS_Guest
- RS_UseOfUserRights
- RS_Password_change_F
- RS_Password_change_S
- RS_Login_F_Locked
- RS_Login_F_Bad
- RS_Login_F_Expired
- RS_Login_F_Disabled
- RS_Logon_Admin_Privileges
- RS_Global_group_user_added
- RS_Global_group_user_removed
- RS_Local_group_changed

- RS_Local_group_created
- RS_Local_group_deleted
- RS_Local_group_user_added
- RS_Local_group_user_removed
- RS_Account_policy_change
- RS_User_account_changed
- RS_User_account_created
- RS_User_account_deleted
- RS_User_right_granted
- RS_User_right_revoked
- RS_Audit_log_cleared
- RS_Audit_policy_change
- RS_User_added_to_local_admin_group
- RS_User_admin_right_granted
- RS_Important_programs
- RS_Privilege_service_called
- RS_Registry_autorun_changed
- RS_Program_started
- RS_Program_exited
- RS_Logon_process_registered
- RS_BF_login_attack
- RS_BF_login_attack_S
- RS_Change_password_attack
- RS_Change_password_attack_S
- RS_Registry_eventlog_settings_changed
- RS_Registry_NT_security_options_changed
- RS_Changes_to_important_files
- RS_Config-log_files_deleted
- RS_Suspect_portscan
- RS_Suspect_FTP
- RS_Suspect_IMAP
- RS_Suspect_Netstat
- RS_Suspect_POP3
- RS_Suspect_POP2
- RS_Suspect_SMTP
- RS_Suspect_Systat
- RS_Suspect_Telnet
- RS_Suspect_Whois
- RS_Suspect_WWW
- RS_Suspect_Finger
- RS_Suspect_Time
- RS_Suspect_SSH
- RS_Suspect_Sunrcp

- RS_Suspect_Netbus

B.1.3.2 Cisco Secure IDS (NetRanger)

This is the detailed list of Cisco Secure IDS classes:

- NR_Catchall
- NR_Catchall_DS
- NR_Catchall_DSP
- NR_IPO_Bad_Options
- NR_IPO_Record_Packet
- NR_IPO_TimeStamp
- NR_IPO_Provide
- NR_IPO_Source_Route
- NR_IPO_SATNET_ID
- NR_IPO_Strict_Route
- NR_ICMP_Sweep_Echo
- NR_ICMP_Sweep_Timestamp
- NR_ICMP_Sweep_Address
- NR_ICMP_Traffic
- NR_ICMP_Smurf
- NR_Loki
- NR_General_Loki
- NR_IP_Fragment_Attack
- NR_Impossible_IP_Packet
- NR_IP_Fragments_overlap
- NR_TCP_Connection
- NR_TCP_Port_Sweep
- NR_NetBios_OOB_Data
- NR_NetBIOS_Stat
- NR_NetBios_Session_Setup_Failure
- NR_Windows_Guest_Login
- NR_UDP_Packet
- NR_UDP_Port_Sweep
- NR_UDP_Bomb
- NR_TFTP_Passwd_File
- NR_Normal_SATAN_Probe
- NR_Heavy_SATAN_Probe
- NR_ypupdated_Attempt
- NR_Ident_Newline
- NR_Ident_Improper_Request
- NR_CrashPackets
- NR_ICMP
- NR_Large_ICMP_Traffic

- NR_ICMP_Flood
- NR_Smail_Attack
- NR_Sendmail_Invalid_Recipient
- NR_Sendmail_Invalid_Sender
- NR_Sendmail_Recon
- NR_Sendmail_Decode_Alias
- NR_CmdDecode
- NR_FTP_Remote_Command_Execution
- NR_FTP_SYST_Command_Attempt
- NR_FTP_CWD_root
- NR_FTP_Authorization_Failure
- NR_UserPassword
- NR_FTP_Improper_Address
- NR_FTP_Improper_Port
- NR_WWW_phf_Attack
- NR_WWW_General_cgi-bin_Attack
- NR_InsecureCGI
- NR_WWW_campas_Attack
- NR_WWW_glimpse_Attack
- NR_WWW_nph-test-cgi
- NR_WWW_test-cgi_Attack
- NR_WWW_php_View_File
- NR_WWW_sgi_wrap_Bug
- NR_WWW_url_File
- NR_WWW_lnk_File
- NR_WWW_bat_File
- NR_HTML_File_Has_url_Link
- NR_HTML_File_Has_lnk_Link
- NR_HTML_File_Has_bat_Link
- NR_WWW_IIS_View_Source_Bug
- NR_WWW_IIS_Hex_View_Source
- NR_IIS_DotDot_View_Bug
- NR_IIS_DotDot_Execute_Bug
- NR_IIS_DotDot_Denial_Bug
- NR_IIS_Long_URL_Crash
- NR_RemoteTools
- NR_DNS_Zone_Transfer
- NR_DNS_Zone_Transfer_High_Port
- NR_DNS_Request_For_All_Records
- NR_RPC_Dump
- NR_Ident_Buffer_Overflow
- NR_Telnet_Authorization_Failure
- NR_StringMatch

B.1.3.3 Tivoli NIDS option

This is the detailed list of Tivoli NIDS classes:

- NIDS_IDSNetworkBase
- NIDS_EMailBase
- NIDS_ServiceBase
- NIDS_WebServerBase
- NIDS_HostUserBase
- NIDS_ALERT
- NIDS_AUTH
- NIDS_BACKDOOR
- NIDS_CONFIG
- NIDS_DOS
- NIDS_SCAN
- NIDS_STEALTH
- NIDS_GOPHER
- NIDS_Loki
- NIDS_TFTP_PW_File
- NIDS_WWW_Shell
- NIDS_IntelBuffOverflow
- NIDS_RS6KBuffOverflow
- NIDS_SparcBuffOverflow
- NIDS_SendMailPipeBug1
- NIDS_SendMailPipeBug2
- NIDS_SendMailPipeBug3
- NIDS_DefaultUserLogin

B.1.4 Web IDS

This is the detailed list of Web IDS classes:

- WW_Catchall
- WW_InvalidLogEntry
- WW_WrongUrl
- WW_EmptyUrl
- WW_AuthenticationError
- WW_SuspiciousHexCodes
- WW_SuspiciousHexCodesQuery
- WW_InvalidHexCodesQuery
- WW_SuspiciousHexCodesUrl
- WW_InvalidHexCodesUrl
- WW_AllowedMethods
- WW_Directory
- WW_SuspiciousCgi

- WW_InsecureCgi
- WW_ClientError
- WW_Success
- WW_Decision

B.1.5 Firewall and Router IDS

This section is divided into the different types of supported firewalls and routers:

- CheckPoint FireWall-1
- Cisco PIX
- Cisco Router

B.1.5.1 CheckPoint Firewall-1 classes

This is the detailed list of CheckPoint FireWall-1 classes:

- CPFW_ServiceBase
- CPFW_Service
- CPFW_Service_Deny
- CPFW_Service_Permit
- CPFW_FTP_Deny
- CPFW_FTP_Permit
- CPFW_HTTP_Deny
- CPFW_HTTP_Permit
- CPFW_Telnet_Deny
- CPFW_Telnet_Permit
- CPFW_Login_Deny
- CPFW_Login_Permit
- CPFW_ICMPBase
- CPFW_ICMP_Deny
- CPFW_ICMP_Permit
- CPFW_AuthBase
- CPFW_Auth_Deny
- CPFW_Auth_Permit
- CPFW_ControlBase
- CPFW_Control
- CPFW_LogFile_Switch
- CPFW_LogFile_Eof

B.1.5.2 Cisco PIX Firewall classes

This is the detailed list of Cisco PIX Firewall classes:

- PIX_Catchall

- PIX_RM_MiscEvent
- PIX_Generic_Harmless
- PIX_Generic_Warning
- PIX_Generic_Minor
- PIX_Generic_Critical
- PIX_RM_Service
- PIX_RM_IDSNetwork
- PIX_start_firewall
- PIX_TCP_in_conn_denied
- PIX_list_out_conn_denied
- PIX_java_applet_conn_denied
- PIX_UDP_in_conn_denied
- PIX_in_UDP_DNS_conn_denied
- PIX_in_from_out_conn_denied
- PIX_in_xlate_same_denied
- PIX_IP_options_conn_denied
- PIX_in_ping_PAT_denied
- PIX_in_ping_denied
- PIX_nonSYN_noconn_denied
- PIX_in_spoof_denied
- PIX_out_icmp_denied
- PIX_access_group_denied
- PIX_teardrop_denied
- PIX_RIP_authent_failed
- PIX_modified_SMTP
- PIX_authent_start
- PIX_authent_server_connect_failed
- PIX_all_authent_server_connect_failed
- PIX_authent_succeeded
- PIX_authent_user_pw_failed
- PIX_authorize_succeeded
- PIX_authorize_failed
- PIX_authorize_failed_no_authent
- PIX_authent_failed_overload
- PIX_authent_started_session
- PIX_authent_cache_timeout
- PIX_route_lookup_failure
- PIX_arp_request_failed
- PIX_config_changing
- PIX_config_reset
- PIX_config_end_change
- PIX_config_changed
- PIX_user_login

- PIX_begin_config_read
- PIX_user_changing_config
- PIX_clear_finished
- PIX_firewall_reboot
- PIX_sending_pkt_too_big
- PIX_too_many_conns_for_xlate
- PIX_embryonic_limit_exceeded
- PIX_FTP_data_conn_failed
- PIX_RCMD_conn_failed
- PIX_UDP_conn_failed
- PIX_NAT_internal_embryonic
- PIX_ESP_error
- PIX_config_failed
- PIX_LU_internal_error
- PIX_LU_insufficient_resources
- PIX_LU_unknown_object
- PIX_LU_NAT_out_of_sync
- PIX_LU_NAT_no_xlate
- PIX_LU_UDP_conn_failed
- PIX_LU_no_PAT_port
- PIX_LU_NAT_xlate_failed
- PIX_LU_missing_packet
- PIX_SNMP_unable_to_open_channel
- PIX_SNMP_unable_to_open_trap_channel
- PIX_SNMP_internal_recv_error
- PIX_SNMP_internal_send_error
- PIX_SNMP_too_big
- PIX_PPTP_socket_io_error
- PIX_PPTP_hastable_error
- PIX_PPP_interface_error
- PIX_PPP_alloc_error
- PIX_built_TCP_permit
- PIX_teardown_TCP_permit
- PIX_built_H245_permit
- PIX_built_H323_permit
- PIX_built_UDP_permit
- PIX_teardown_UDP_permit
- PIX_rebuilt_TCP_permit
- PIX_conns_in_use
- PIX_URL_FTPSR_success
- PIX_URL_ACC_success
- PIX_URL_access_denied
- PIX_URL_server_timeout

- PIX_URL_request_failed
- PIX_URL_request_pending
- PIX_URL_not_responding
- PIX_URL_not_responding_allow
- PIX_PAT_xlate_built
- PIX_xlate_built
- PIX_xlate_teardown
- PIX_PAT_xlate_teardown
- PIX_no_xlate_for_protocol
- PIX_no_xlate_by_type
- PIX_xlate_orphan
- PIX_inside_telnet_denied
- PIX_telnet_permit
- PIX_telnet_pw_failures
- PIX_max_login_attempts
- PIX_NAT_addr_overlap
- PIX_Mgr_denied_inside_telnet
- PIX_Mgr_permitted_inside_telnet
- PIX_RIP_unexpected_msg
- PIX_cant_find_SPI
- PIX_cant_find_AHESP
- PIX_SA_id_no_match
- PIX_recv_not_encrypt
- PIX_PPTP_unexpected_xgre
- PIX_PPTP_bad_protocol_xgre
- PIX_PPP_mschap_needed
- PIX_PPP_radius_needed
- PIX_PPP_aaa_needed
- PIX_PPP_client_ip_needed
- PIX_PPTP_spoofed_pkt
- PIX_PPP_missing_key_attrib
- PIX_modified_activex
- PIX_modified_java
- PIX_bad_tcp_hdr_len
- PIX_invalid_transport
- PIX_PPTP_out_of_sequence
- PIX_aaa_authent_sent
- PIX_aaa_authent_recv
- PIX_PPTP_tunnel_created
- PIX_PPTP_tunnel_deleted
- PIX_need_to_frag_but_DF
- PIX_FO_Gen_Replication
- PIX_FO_Replication

- PIX_Config_Replication
- PIX_NAT_addr_overlap
- PIX_Mgr_denied_inside_telnet
- PIX_Mgr_permitted_inside_telnet
- PIX_RIP_unexpected_msg
- PIX_cant_find_SPI
- PIX_cant_find_AHESP
- PIX_SA_id_no_match
- PIX_recv_not_encrypt
- PIX_PPTP_unexpected_xgre
- PIX_PPTP_bad_protocol_xgre
- PIX_PPP_mschap_needed
- PIX_PPP_radius_needed
- PIX_PPP_aaa_needed
- PIX_PPP_client_ip_needed
- PIX_PPTP_spoofed_pkt
- PIX_PPP_missing_key_attrib
- PIX_modified_activex
- PIX_modified_java
- PIX_bad_tcp_hdr_len
- PIX_invalid_transport
- PIX_PPTP_out_of_sequence
- PIX_aaa_authent_sent
- PIX_aaa_authent_recv
- PIX_PPTP_tunnel_created
- PIX_PPTP_tunnel_deleted
- PIX_need_to_frag_but_DF
- PIX_FO_Gen_Replication
- PIX_FO_Replication
- PIX_Config_Replication

B.1.5.3 Cisco Router

This is the detailed list of Cisco Router classes:

- CR_ConfEvent
- CR_CfgManMIBNotnPrefix_CfgManEvent
- CR_CfgChanged
- CR_workgroup_sysCfgChangeTrap
- CR_entityMIBTraps_entCfgChange
- CR_EsCfg_EsStackCfgChange
- CR_RootChanged
- CR_dot1dBridge_newRoot
- CR_Cat2600TsDmnNewRoot

- CR_EsVLANs_EsVLANNewRoot
- CR_TopologyChanged
- CR_dot1dBridge_topologyChange
- CR_cat2600TsDmnTopologyChange
- CR_EsVLANs_EsVLANTopologyChange
- CR_AddrChanged
- CR_FastHubMIBObject_ipAddressChange
- CR_series2000_ipAddressChange
- CR_PortChanged
- CR_EsPort_EsPortStrNFwdEntry
- CR_Authentication_Failure_generic
- CR_Authentication_Failure_specific
- CR_FastHubMIBObjects_LogonIntruder
- CR_series2000_logonIntruder
- CR_series2000_broadcastStorm
- CR_SibuMgrsNotns_ciscoSibuMgrsConsoleLogonIntruder
- CR_Reload
- CR_TCP_Conn_Close
- CR_cipCsnaNotnPrefix_cipCsnaLlc2ConnLimitExceeded
- CR_NetRegMIBNotns_ciscoNetRegDNSQueueTooBig
- CR_StackNotnsPrefix_tokenRingSoftErrExceededTrap

B.1.6 Host IDS

This section is divided into the different types of supported operating systems:

- UNIX based
- Windows NT

B.1.6.1 UNIX

This is the detailed list of UNIX Host IDS classes:

- OS_MiscEvent
- OS_IDSEvent
- OS_User
- OS_TargetFile
- OS_ResourceEvent
- OS_AuditPolicy
- OS_MiscUser
- OS_Base
- OS_IDSBase
- OS_No_Resources
- OS_No_Permission

- OS_Server_No_Response
- OS_Server_OK
- OS_DateBase
- OS_Date
- OS_Date_Set
- OS_LoginBase
- OS_Login
- OS_Root_LoginBase
- OS_Root_Login
- OS_Root_Login_SuccessBase
- OS_Root_Login_Success
- OS_Root_Login_Success_From
- OS_Root_Login_FailureBase
- OS_Root_Login_Failure
- OS_Root_Login_Failure_From
- OS_Repeated_Login_Failure
- OS_Repeated_Login_Failure_From
- OS_Passwd
- OS_SuBase
- OS_Su
- OS_Su_Success
- OS_Su_Failure
- OS_YP
- OS_Ypchsh
- OS_Ypchfn
- OS_Yppasswd
- OS_Ypbind
- OS_NIS_No_Response
- OS_NIS_OK
- OS_AutomounterBase
- OS_Automounter
- OS_Automount
- OS_AmdBase
- OS_Amd
- OS_Amd_Mounted
- OS_Amd_Unmounted
- OS_Cron
- OS_Idi
- OS_Fsck
- OS_Getty
- OS_Comsat
- OS_Ftp
- OS_Ftpd

- OS_Snmpd
- OS_Rftp
- OS_Mosaic
- OS_Named
- OS_Nnrpd
- OS_Innd
- OS_Rlogind
- OS_Routed
- OS_Gated
- OS_Rshd
- OS_Rexecd
- OS_Rwhod
- OS_Talkd
- OS_Telnetd
- OS_Rtelnet
- OS_Tftpd
- OS_Inetd
- OS_Init
- OS_Mountd
- OS_Pcnfsd
- OS_Rarpd
- OS_Rquotad
- OS_Rstatd
- OS_SyslogdBase
- OS_Syslogd
- OS_Syslogd_NoSpaceBase
- OS_Syslogd_NoSpace
- OS_EbbackupdBase
- OS_Ebbackupd
- OS_Ebbackupd_Waiting
- OS_XntpdBase
- OS_Xntpd
- OS_Xntpd_Clock_Reset
- OS_Xntpd_Ntpdate
- OS_SendmailBase
- OS_Sendmail
- OS_Sendmail_No_Space
- OS_Sendmail_Loopback
- OS_Nfsd
- OS_KernelBase
- OS_Kernel
- OS_File_Write_ErrorBase
- OS_File_Write_Error

- OS_File_System_FullBase
- OS_File_System_Full
- OS_NFS_No_Response
- OS_NFS_OK
- OS_NFS_File_System_Full
- OS_NFS_Write_Error
- OS_LOCAL_File_System_Full
- OS_SWAP_File_System_Full
- OS_Silo_Overflow
- OS_Sendsig_Err
- OS_Kernel_Panic
- OS_SockdBase
- OS_Sockd
- OS_Sockd_Connected
- OS_Sockd_Terminated
- OS_Sockd_Transfer
- OS_Reboot

B.1.6.2 Windows NT

This is the detailed list of Windows NT Host IDS classes:

- OS_NT_MixinEvent
- OS_NT_MiscBase
- OS_NT_IDSEvent
- OS_NT_ResourceEvent
- OS_NT_DiskFull
- OS_NT_Internal_Error_In_The_DHCP_Server
- OS_NT_Capacity_Alert
- OS_NT_Trustee_Relationship_Failed
- OS_NT_Security_DatabaseBase
- OS_NT_Security_Database
- OS_NT_Security_Database_Error
- OS_NT_DHCP_Rejected_Allocation_Request
- OS_NT_Domain_Not_Contactable
- OS_NT_Trustee_Relationship
- OS_NT_Privileged_Service_Called
- OS_NT_Trusted_Process_Logon_Success
- OS_NT_AuditPolicy
- OS_NT_AccountManagementSuccessBase
- OS_NT_AccountManagementSuccess
- OS_NT_Group_Management_Change_SuccessBase
- OS_NT_Group_Management_Change_Success
- OS_NT_Global_Group_Changed

- OS_NT_Local_Group_Member_Removed
- OS_NT_Account_Password_Change_Success
- OS_NT_LogonFailureBase
- OS_NT_LogonFailure
- OS_NT_OutOfVirtualMemory
- OS_NT_TFTPDAccessDirInvalid
- OS_NT_ServerInvalidVirtualRoot
- OS_NT_StartingNamed
- OS_NT_SystemStarting
- OS_NT_SystemShuttingDown
- OS_NT_AuditMessagesDiscarded
- OS_NT_TrustedLogonProcessRegistered
- OS_NT_AuthenticationPackageAdded
- OS_NT_NotificationPackageAdded
- OS_NT_Log_Cleared
- OS_NT_LogonTimeRestrictionViolation
- OS_NT_AccountDisabled
- OS_NT_AccountExpired
- OS_NT_LogonNotAllowed
- OS_NT_LogonRequestDenied
- OS_NT_PasswordExpired
- OS_NT_LogonFailureNetlogonNotActive
- OS_NT_LogonFailureUnexpected
- OS_NT_Logoff
- OS_NT_LogonFailureAccountLockedOut
- OS_NT_ObjectOpen
- OS_NT_NoPermission
- OS_NT_HandleAllocated
- OS_NT_HandleClosed
- OS_NT_ObjectOpenedForDelete
- OS_NT_ObjectDeleted
- OS_NT_SpecialPrivilegesAssigned
- OS_NT_PrivilegedServiceCalled
- OS_NT_PrivilegedServiceFail
- OS_NT_ProcessCreated
- OS_NT_ProcessExited
- OS_NT_HandleDuplicated
- OS_NT_IndirectObjectAccessObtained
- OS_NT_UserRightsAssigned
- OS_NT_UserRightsRemoved
- OS_NT_NewTrustedDomain
- OS_NT_RemoveTrustedDomain
- OS_NT_AuditPolicyChange

- OS_NT_AccountCreated
- OS_NT_AccountTypeChanged
- OS_NT_AccountEnabled
- OS_NT_PasswordChangeAttempt
- OS_NT_PasswordChanged
- OS_NT_UserAccountDisabled
- OS_NT_AccountDeleted
- OS_NT_GlobalGroupAdded
- OS_NT_GlobalGroupMemberAdded
- OS_NT_GlobalGroupMemberRemoved
- OS_NT_GlobalGroupDeleted
- OS_NT_LocalGroupCreated
- OS_NT_LocalGroupMemberAdded
- OS_NT_LocalGroupMemberRemoved
- OS_NT_LocalGroupDeleted
- OS_NT_LocalGroupChanged
- OS_NT_GeneralAccountDatabaseChanged
- OS_NT_GlobalGroupChanged
- OS_NT_UserAccountChanged
- OS_NT_DomainPolicyChanged
- OS_NT_UserAccountLockedOut
- OS_NT_DriveMayBeCorrupt
- OS_NT_UnexpectedShellStop
- OS_NT_DHCPCardLeaseError
- OS_NT_EventLogStarted
- OS_NT_EventLogStopped
- OS_NT_UnexpectedSystemReboot
- OS_NT_SystemReboot
- OS_NT_NetlogonTerminatedWithError
- OS_NT_BrowserReceivedInvalidDatagram
- OS_NT_BrowserReceivedTooManyInvalidDatagrams
- OS_NT_NFSDInvalidExportPath
- OS_NT_LoginBase
- OS_NT_Login

B.1.7 RMV

This is the detailed list of RMV classes:

- RMV_EventBase
- RMV_Base
- RMV_Misc
- RMV_VirusFound
- RMV_FileOpenError

- RMV_AgentNotInstalled
- RMV_AgentInstalled
- RMV_AgentStarted
- RMV_AgentStopped
- RMV_VirusDBOutOfDate
- RMV_VirusDBUpdated
- RMV_VirusDBDownloaded
- RMV_ScanStarted
- RMV_ScanAborted
- RMV_ScanComplete
- RMV_ConfigurationChanged
- RMV_ForwardedToQuarantineServer

B.2 Files

The Risk Manager Server component lays down the following RMCC files in the following part of the directory tree:

- %BINDIR%\RISKMGR for Windows NT
- $BINDIR/RISKMGR for UNIX

The subdirectory $BINDIR/RISKMGR/corr contains the installation scripts and associated files, as shown in Table 18.

Table 18. Risk Manager installation scripts and files

File	Content
riskmgr_baroc.lst	List of BAROC files to be loaded
riskmgr_cfg.lst	List of Prolog configuration files
riskmgr_pro.lst	List of Prolog files (pre-compiled)
riskmgr_rules.lst	List of rule sets to be loaded
riskmgr_eventgroups.dat	TEC 3.7 Console event group definitions (for importing)
rmcorr_cfg	Wrapper script to call rmcorr_cfg.sh
rmcorr_cfg.sh	Main script for modifying and updating the rule base
rmt_corrstatus	Script for task - UNIX version
rmt_corruninstall	Script for task - UNIX version
rmt_corrupdate	Script for task - UNIX version
rmt_corrstatus.cmd	Script for task - NT version

File	Content
rmt_corruninstall.cmd	Script for task - NT version
rmt_corrupdate.cmd	Script for task - NT version

The subdirectory $BINDIR/RISKMGR/corr/tec contains the rules files, Prolog files, pre-compiled Prolog files, and BAROC files, as shown in Table 19.

Table 19. Risk Manager rules, Prolog and BAROC files

File	Content
boot.rls	Rules executed on TEC_Start: Load Prolog files, start timers, and so on.
normalization.rls	This rules file contains statements to normalize the information related to: • The intrusion detection system that sent the event. Intrusion detection systems talking to the event console must be identified in the configuration of the console. If a new intrusion detection system sends messages, a severe alert is raised. • The destination identified in the attack. • The source identified in the alert. New sources are expected to occur every time, and they are automatically generated without information being displayed.
sensorevent.rls	Rules for processing RM_SensorEvent events.
situation.rls	Rules for analyzing situation events.
timer.rls	Rules for executing timers: Refresh, Cleanup, and Forward.
riskmgr_categories.pro	Configuration file for Class Category definitions and associations: set_category_name, category_assign_super, and category_assign.
riskmgr_hosts.pro	Configuration file for host and sensor definitions: set_host, set_trusted_host, set_sensor, set_downgrade_sensor_creation, and set_ignore_sensor_creation.
riskmgr_links.pro	Configuration file for relationships between raw events: set_storm_events, set_linked_events, and set_duplicate_events.

File	Content
riskmgr_parameters.pro	Configuration file for general parameters: set_timestamp_jitter, set_situation_expiration, set_situation_cleanup_interval, set_interface_refresh, set_ratio_down, set_ratio_up, set_decay_value, drop_unsecure_events, forward_situations, set_forward_interval, and set_forward_tec.
riskmgr_thresholds.pro	Configuration file for thresholds: set_threshold.
parse_p.pro	Prolog code used when reading in configuration files.
parse_p.wic	Compiled Prolog file.
normalization_p.pro	Prolog code used during the normalization process.
normalization_p.wic	Compiled Prolog file.
situation_p.pro	Prolog code used during the processing of situation events and facts.
situation_p.wic	Compiled Prolog file.
templates_p.pro	Prolog utility routines.
templates_p.wic	Compiled Prolog file.
riskmgr.baroc	Class definitions for top level Risk Manager classes and all classes directly related to correlation (as opposed to sensor related classes), such as RM_Situation, RM_Error, and so on.
sensor_abstract.baroc	Class definitions for sensor related classes for Risk Manager. These are the abstract base classes from which adapter developers will derive when defining sensor specific classes.
sensor_generic.baroc	General purpose classes derived from abstract classes in the RM_SensorEvent tree (sensor_abstract.baroc). Their purpose is to facilitate rapid development of an adapter. An adapter developer might use these classes initially before developing a BAROC file specifically for the sensor type under consideration.
cpfw.baroc	Class definitions for Checkpoint Firewall.
crouter_snmp.baroc	Class definitions for Cisco Router.
klaxon.baroc	Class definitions for Klaxon.
netranger.baroc	Class definitions for Cisco IDS (formerly Netranger).

File	Content
nids.baroc	Class definitions for NIDS (Network IDS, as known as HAXOR).
os.baroc	Class definitions for HIDS (Host IDS).
pix.baroc	Class definitions for Pix Firewall.
realsecure.baroc	Class definitions for ISS Realsecure.
rmvirus.baroc	Class definitions for virus detectors (Norton AntiVirus).
webids.baroc	Class definitions for Web IDS (formerly WebWatcher).

Appendix C. Integrating new sensor types into Risk Manager

This appendix discusses issues related to the development of a new sensor type for Risk Manager (RM) Version 3.7. The issues covered are mainly related to the RM correlation component and the TEC Event Server, as opposed to issues related to the client or TEC Adapter side.

C.1 Introduction

The term *sensor* is used to describe the application or product that is the source of data that will generate the TEC events. The term *adapter* refers to the application that takes the data, formats it into an event, and sends the event to the TEC Event Server. The adapter assigns class names and fills in class attributes. If the sensor generates appropriate SNMP traps or syslog (or NT eventlog) entries, then the existing TEC Logfile Adapter or TEC SNMP Adapter may be used. If the Logfile Adapter is used, then an appropriate FMT file must be developed. If the SNMP Adapter is used, then an appropriate CDS file must be developed. A standalone adapter can be written using the Risk Manager Common Adapter Toolkit (CAT). If working directly with the sensor source code is an option, then building the adapter functionality into the sensor application using CAT is also a possibility.

For illustrative purposes, consider the task of integrating a sensor called ftp_watcher into Risk Manager. Furthermore, suppose that this new sensor detects ftp login failures (among other things) and you want the information from the ftp login failure events to be sent to Risk Manager (that is, the TEC Event Server with Risk Manager components installed).

C.2 General steps

Follow these steps to integrate the sensors:

1. Analyze event data and create a class hierarchy.
2. Implement the class hierarchy as a BAROC file.

TEC rules

Because of the way TEC 3.6 rules select incoming events, all incoming events must be instances of leaf classes. A leaf class is a class at the bottom of the hierarchy. If you have a class that is used as a base class for other classes, then the Risk Manager rules will not see any events that are instances of the base class.

3. Derive all new classes from a class in the tree described in sensor_abstract.baroc.
4. Put all class files for the new sensor in a single BAROC file.
5. Assign classes to class categories as desired.
6. Add any desired category assignments for specific classes into riskmgr_categories.pro using category_assign entries.
7. Place your BAROC file in the RM installation directory.
8. Add your BAROC file name to the end of the list of files contained in riskmgr_baroc.lst (located in the RM installation directory).
9. Make sure that the adapter sending TEC events for your new sensor type assigns class names and fills in class attributes appropriately.
10. If necessary, create an FMT or CDS file and install it at the adapter.
11. Update Risk Manager components at the TEC Event Server
12. Run:

```
rmcorr_cfg -update
```

13. If you have loaded the new BAROC file into your rule base by hand, all that is really necessary is to restart the TEC Event Server.

C.3 Example: FTP login failure

Suppose the ftp_watcher tool provides the following information for the FTP login failure:

- IP address of source
- Fully qualified host name of destination
- User name for user attempting to login
- Timestamp of attempt (as seconds since 1 Jan 1970 00:00:00)

C.3.1 Selecting a base class

This section describes the process used to select a base class for the event from within the sensor_abstract.baroc class hierarchy. The class hierarchies and class attributes are described in Appendix B.1, “Class lists” on page 311.

RM_SensorEvent Always start from here.

RM_IDSEvent The ftp login failure event would be considered IDS type activity.

RM_IDSNetwork There is a source and a destination, so this is network type activity.

RM_Service The event involves the ftp service.

RM_User There is a user involved.

The final selection for a base class is thus RM_User.

C.3.2 Mandatory attributes

The mandatory attributes are those used to identify the sensor. These are rm_SensorType and rm_SensorIPAddr (or rm_SensorHostname). If these are not set, then correlation processing will fail and the event severity will be set to UNKNOWN.

Additionally, for events that are instances of a class derived from RM_IDSEvent, then it is mandatory that host information for at least one of the source host and destination host be provided. The host information may be the IP address (rm_DestinationIPAddr or rm_SourceIPAddr) or the host name (rm_DestinationHostname or rm_SourceHostname). If no information is available for either the destination or the source host, then correlation processing will fail and the event severity will be set to UNKNOWN. Note that for a typical RM_IDSEvent, it is expected that both destination and source information will be available.

Note that although setting rm_Timestamp and rm_TimestampFmt is not mandatory, if the appropriate settings are not used, then RM_InputErr error events will be generated for incoming events. Note also that although the other attributes are not mandatory, the value of correlation and the usefulness of the information at the TEC Console (and in database mining with Tivoli Decision Support at a later time) can all be greatly reduced if they are not set appropriately.

It is also mandatory that the attributes source and sub_source not be set by the adapter. Additionally, the attributes origin, sub_origin, and host name will be filled in by Risk Manager, and so should not be set by the adapter. If they are set by the adapter, the values will be overwritten.

C.3.3 Setting Attributes

To determine the attributes for RM_User (including inherited attributes), as shown in Table 20 on page 338, the `wlsrbclass` command can be used on a TMR system that has the RM components installed:

```
wlsrbclass -d rulebasename RM_User
```

Table 20. RM_attributes

Class Name	**Attributes**
RM_User ISA	RM_Service
	server_handle
	date_reception
	event_handle
	source
	sub_source
	origin
	sub_origin
	hostname
	adapter_host
	date
	status
	administrator
	acl
	credibility
	severity
	msg
	msg_catalog
	msg_index
	duration
	num_actions
	repeat_count

Class Name	Attributes
	cause_date_reception
	cause_event_handle
	rm_Version
	rm_Timestamp
	rm_TimestampFmt
	rm_Timestamp32
	rm_SensorToken
	rm_DestinationToken
	rm_SourceToken
	rm_SensorType
	rm_SensorHostname
	rm_SensorIPAddr
	rm_SensorPID
	rm_SensorOS
	rm_DestinationHostname
	rm_DestinationIPAddr
	rm_SourceHostname
	rm_SourceIPAddr
	rm_SpoofedSourceKnown
	rm_Signature
	rm_Description
	rm_Level
	rm_Correlate
	rm_NameType
	rm_NameID
	rm_NameData
	rm_Protocol

Class Name	Attributes
	rm_SrcPort
	rm_DstPort
	rm_Servicename
	rm_User
	rm_Password

C.3.4 BAROC file entry

The entry in the BAROC file ftp_watcher.baroc should look similar to this:

```
#------------------------------------------------------------
TEC_CLASS:
  FW_FTPLoginFailure ISA RM_User
  DEFINES {
    rm_SensorType: default = 'ftp_watcher';
    rm_TimestampFmt: default = 'EPOCH';
    rm_Level : default=1.0;
    rm_Servicename : default = 'ftp';
    rm_User: default='N/A';
};
END
#------------------------------------------------------------
```

C.3.5 FMT file entry

If ftp_watcher is going to use the TEC Logfile Adapter or CAT via an fmt file, then an fmt file is needed. Suppose that the syslog entry generated by ftp_watcher for an ftp login failure looks like this:

```
"Aug 6 16:14:46 myhost ftp_watcher myhost.sub.com 933948886 john_doe
dest.host.com 1.2.3.4 ftp login failure"
```

The format file entry then might look like this:

```
//-----------------------------------------------------------
//"Aug 6 16:14:46 myhost ftp_watcher myhost.sub.com 933948886
// john_doe dest.host.com 1.2.3.4 ftp login failure"
FORMAT FW_FTPLoginFailure
%t %s ftp_watcher %s %s %s %s %s %s*
date $1
rm_Timestamp $4
rm_TimestampFmt EPOCH
rm_SensorHostname $3
```

```
rm_Signature $8
rm_DestinationHostname $6
rm_SourceIPAddr $7
rm_User $5
rm_SensorType ftp_watcher
END
//----------------------------------------------------------
```

Format files often have a base entry at the beginning and then use the FOLLOWS keyword to build on it. This mechanism can be used to set an attribute that is common for all the event classes for the sensor. For example, the attributes rm_SensorType and rm_TimestampFmt could be set in this way. The format file entries might then look like this:

```
//----------------------------------------------------------
// "Aug 6 16:14:46 myhost ftp_watcher myhost.sub.com 933948886
// john_doe dest.host.com 1.2.3.4 ftp login failure"
FORMAT FW_Base
%t %s ftp_watcher %s %s %s %s %s %s*
date $1
rm_Timestamp $4
rm_TimestampFmt EPOCH
rm_SensorHostname $3
rm_SensorType ftp_watcher
END
//----------------------------------------------------------
//----------------------------------------------------------
// "Aug 6 16:14:46 myhost ftp_watcher myhost.sub.com 933948886
// john_doe dest.host.com 1.2.3.4 ftp login failure"
FORMAT FW_FTPLoginFailure FOLLOWS FW_Base
%t %s ftp_watcher %s %s %s %s %s %s*
rm_Signature $8
rm_DestinationHostname $6
rm_SourceIPAddr $7
rm_User $5
END
//----------------------------------------------------------
```

The other mechanism for setting rm_SensorType is to set it as a default value for each new class you create associated with your new sensor. The advantage of using the fmt file (or another mechanism that sets it at the adapter level) is that you only need to set it in one place, and not as a default, in many class definitions. The disadvantage of using the fmt file is that it generates additional network traffic, because the data is being sent along with the event.

Note that the base entry has nothing to do with the class hierarchy. In fact, the fmt file has no knowledge of the inheritance aspects of the class hierarchy.

C.4 Important points to remember

- DO derive as far down in the sensor_abstract.baroc tree as is feasible. This gives Risk Manager as much specific information as possible about the type of the event.
- DO minimize the number of new attributes. Additional attributes may be created and may make sense for informational purposes, but note that the extra information will not be used by RM.
- DO derive only one level when deriving from the sensor_abstract.baroc tree. You can create a hierarchy of your own under the chosen sensor_abstract.baroc class (and sometimes this may make sense), but, as mentioned above for additional attributes, note that RM will not use this additional information.
- DO make your class names identifiable with your sensor type. For example, all ftp_watcher classes might begin with FW_ and the ftp login failure event might be called FW_FTPLoginFailure.
- DO make your attribute names identifiable with your sensor type. For example, all ftp_watcher attributes might begin with fw_.
- DO put all your classes in one BAROC file, for example, ftp_watcher.baroc.
- DO set the following attributes:
    - rm_Timestamp
        - Timestamp associated with occurrence of the suspicious activity.
        - Preferable format is epoch, seconds since 01 Jan 1970 00:00:00.
    - rm_TimestampFmt
        - Timestamp format being used. The default is 'N/A'.
    - rm_SensorType
        - Name of the sensor type, for example, "ftp_watcher".
        - This is used for ignore_sensor_creation and downgrade_sensor_creation (see riskmgr_hosts.pro) and is useful for later database searches.
        - This may be set at the adapter and sent along with the event or it may be set as a default in the BAROC file.

  - rm_SensorIPAddr or rm_SensorHostname
    - Host identification information for the sensor instance.
- DO NOT modify sensor_abstract.baroc or riskmgr.baroc.
- DO NOT set the source or sub_source attributes. Risk Manager sets appropriate defaults for these attributes. The defaults are used in data mining (Tivoli Decision Support).
- DO NOT set the origin, sub_origin, or host name attributes unless needed for other purposes (such as in an FMT file). Risk Manager sets these, overwriting anything set by the adapter.

Appendix D. Tivoli Management Framework 3.7.1 enhancements

Tivoli Framework 3.7.1 enhancements can be grouped into three broad categories:

- Endpoint Manager, Gateway and Endpoint enhancements
- Security enhancements
- Mobile client

We will only cover the security enhancements in Section D.1, “Security enhancements” on page 345, while the mobile client and the Endpoint Manager, Gateway and Endpoint enhancements will not be covered in this appendix because it is not relevant to the Risk Manager discussion.

D.1 Security enhancements

In today’s enterprise system management world, privacy and security should be implemented more carefully than ever. As many systems and networks are all interconnected, having a very secure communication media for management or application data transmission is one of the foremost design issues in enterprise management. Security is vital in the new system management and e-business world.

Therefore, it is one of the main targets of Tivoli to provide a very secure communication mechanism for the whole Tivoli product suite. Tivoli Framework 3.7.1 is now equipped with tools like SSL that you can use to create very secure communication channels.

D.1.1 Security terminology

First, we will define some of the terms that we will use:

Connection An autonomous, uniquely-identified, two-ended, bidirectional, stream-type data path that is established between two peers.

Channel An abstract data path between two peers. Multiple channels can exist for a single connection, and one channel can have multiple connections.

Client The consumer of a provided capability or resource, or the initiator of a network connection.

Server The provider of a capability or resource, or the listener or acceptor of a network connection request from a client.

Local A connection between peers on the same machine.

Remote A connection between peers on separate machines that uses externally-accessible network ports.

D.1.2 Network security in Framework 3.7.1

Security enhancements in 3.7.1 include:

- Provides privacy for network communications following an industry standard.
- Implements an enhanced scheme for traversing firewalls; no longer uses a port range.
- Retains 100 percent backward-compatibility with all Tivoli Enterprise products, including Application Development Environment extensions.

D.1.3 SSL components for Tivoli Enterprise products

Tivoli Framework 3.7.1 supports SSL protocol. We will cover this in detail in the following section.

D.1.3.1 Secure Socket Layer (SSL)

SSL is a protocol that provides data privacy via strong encryption and public key negotiation with possibility for authentication. This protocol is used by Web servers to provide security for connections between Web servers and Web browsers, by the Lightweight Directory Access Protocol (LDAP) to provide security for connections between LDAP clients and LDAP servers, and by Host-on-Demand V2 to provide security for connections between the client and the host system.

Additional applications based on this protocol are in development.

SSL provides security for the connection over which you can communicate. SSL was developed jointly by Netscape Communications and RSA Data Security.

Many companies worldwide have adopted SSL as their communication protocol of choice. In fact, many financial transactions on the Internet, including on-line banking, are now conducted using SSL. It also provides cryptographic functionality to applications.

D.1.3.2 How SSL works?

SSL is a protocol that provides privacy and integrity between two communicating applications using TCP/IP. The Hypertext Transfer Protocol (HTTP) for the World Wide Web uses SSL for secure communications.

Data privacy in SSL is maintained by using strong encryption and public key negotiation. The data going back and forth between client and server is encrypted using a symmetric algorithm such as DES or RC4. A public-key algorithm—usually RSA—is used for the exchange of the encryption keys and for digital signatures.

Versions 1 and 2 of the SSL protocol provide only server authentication. Version 3 adds client authentication, using both client and server digital certificates.

> **Note**
>
> Tivoli Framework 3.7.1 supports server authentication only.

For more information about SSL, please refer to:

`http://developer.netscape.com/docs/manuals/security.html`

D.1.3.3 SSL security layer structure for Tivoli products

Figure 174 on page 348 illustrates the security layer structure implemented with SSL for Tivoli products.

NetSec is an interface in the communications layer developed to support SSL.

GSKit is an IBM implementation of SSL, Version 3. The GSK-SSL NetSec module is implemented for 3.7.1. The GSKIT runtime package is on the 3.7.1 CD. Table 21 shows the GSKit version for different operating system types.

Table 21. GSKit versions

Operating system	GSKit version
AIX, NT, Solaris, OS/2	4.0.3
HP	3.01D

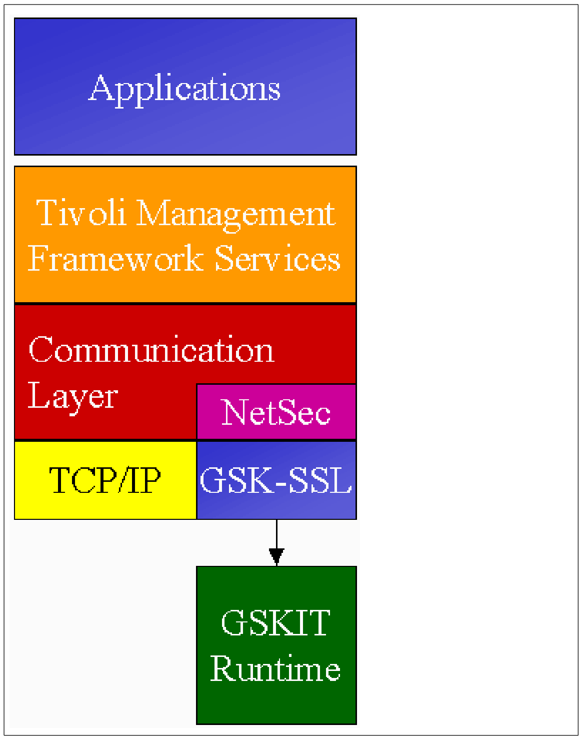


Figure 174. SSL security layer structure for Tivoli products

D.1.4 Enabling SSL

A generic SSL can be used for:

- Creation of RSA, DH, and DSA key parameters
- Creation of X.509 certificates, Certificate Signing Requests (CSRs), and Certification Revocation Lists (CRLs)
- Calculation of message digests
- Encryption and decryption with ciphers
- SSL/TLS client and server tests
- Handling of S/MIME signed or encrypted mail

Each Managed Node can be enabled individually. The Tivoli Management Region Server (TMR Server) must be SSL-capable before enabling any Managed Nodes. GSKit must be installed and loadable on each enabled Managed Node. Managed Node must be restarted for the changes to take effect after executing the `odadmin set_network_security` command.

SSL is configured using the odadmin command as follows:

```
odadmin set_network_security none | SSL | FORCE_SSL [od. | clients | all]
```

This command sets the network security level of a Managed Node. You can set the network security level on specified object dispatchers (od), all client object dispatchers (clients), or all object dispatchers (all).

SSL options are explained in Table 22.

Table 22. SSL options

Option name	Description
none	Specifies that Secure Socket Layer (SSL) is not used by the Managed Node, except when it is SSL-capable and is communicating with a FORCE_SSL Managed Node. This is the default setting.
SSL	Specifies that the Managed Node uses SSL when communicating with other SSL Managed Nodes. SSL is not used when communicating to a node with a setting of none.
FORCE_SSL	Specifies that the Managed Node only communicates using SSL. Non-SSL connections are not accepted by the Managed Node, so they will appear as broken communication attempts. It is not a good idea to set TMR Servers to FORCE_SSL.

D.1.5 Inter-ORB communication

Inter-ORB communication is the basic interaction mechanism between the different Object Request Brokers (ORBs, also known as oservs) in the installation. Another name for this is inter-dispatcher communication. It uses TCP connections. The communication takes place whenever requests from one Managed Node invoke a remote method on another Managed Node. The Inter-ORB communication also manages communications between a Managed Node and a TMR Server when a method request needs to be authorized and its implementation details resolved. This connectivity is also termed as the Object-Call or objcall channel. The ORB that initiates the connection acts as a TCP client, while the ORB that accepts the request is the TCP server. The roles of TCP client and TCP server are in the context of the request and do not necessarily have any relationship to the Tivoli roles of client and server.

In other words, an ORB that is a server to one remote ORB can also invoke TCP client requests on other remote ORBs. The ORB dispatchers that communicate over this connection have a sustained TCP connection over TCP port 94. These connections can only be disrupted due to network faults or if a dispatcher is restarted.

Figure 175 shows the ORB communication between SSL implemented Managed Nodes. There can be no communication between Node B and Node C.

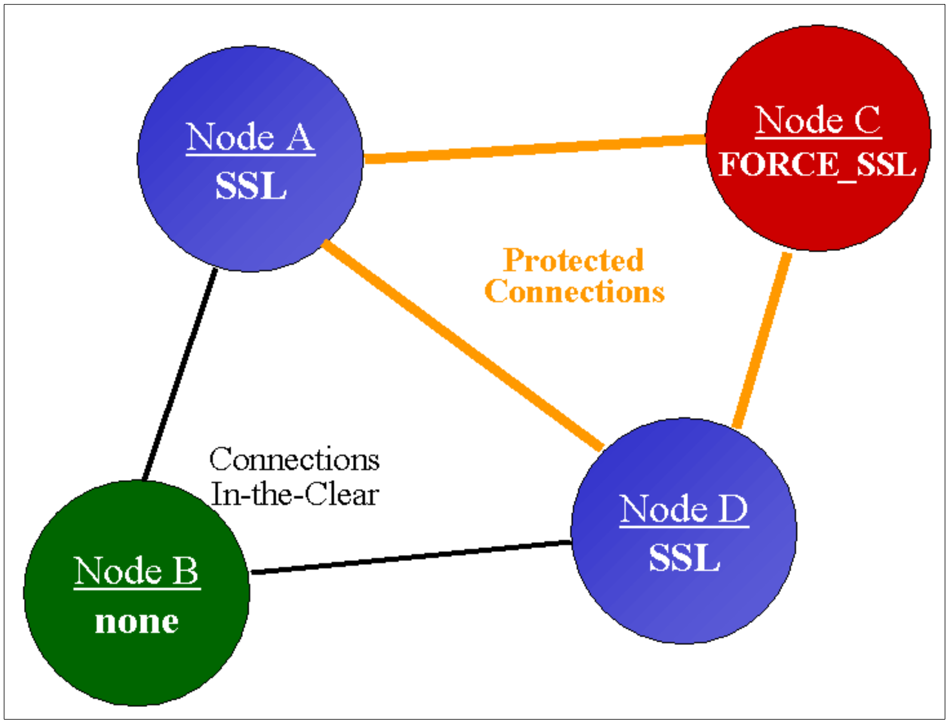


Figure 175. Inter-ORB communication implemented with SSL

Note that in multiple TMR environments, FORCE_SSL cannot be used by either TMR Server when establishing an InterRegion connection.

For more information about Inter-ORB communication, please refer to the redbook *Tivoli Enterprise Internals and Problem Determination*, SG24-2034.

D.1.6 Setting ciphers

Ciphers are the encryption, key, and hash methods used by SSL to protect the channel. GSK-SSL supports eight cipher settings, each of which is represented by a two-character code.

Specify the ciphers you want for each Managed Node individually using a command similar to:

```
odadmin set_ssl_ciphers "050A09" od#
odadmin set_ssl_ciphers default od#
```

The following ciphers are supported:

- RC4-128/40
- DES
- 3DES
- RC2-40
- SHA
- MD5

D.1.7 Public key, authentication, and KeyStores

SSL has built-in public key peer authentication. SSL support in Tivoli Management Framework, Version 3.7.1, is provided for data privacy, not for peer authentication. For peer authentication, however, you can manipulate the KeyStore contents manually on the Managed Nodes. If you have access to Tivoli support WEB site, the document under the following link will help you to customize iKeyman:

```
https://www.tivoli.com/secure/support/Prodman/manuals/AB/FRMWK/framework/
iKeyman.html
```

D.1.8 The BDT firewall problem

Bulk Data Transfer (BDT) is a technique used when large data transfers (typically greater than 16 KB) are required between objects on separate systems. Rather than have the data go from object on system A through oserv on system A to oserv on system B to object on system B, BDT utilizes a technique know as Inter-Object Messaging (IOM). IOM establishes a direct network connection between two methods (hence inter-object). This not only makes transferring large amounts of data more efficient, but there is also less work for an oserv. The terms BDT and IOM are often used interchangeably to mean the same thing. Strictly speaking, BDT is what we need to do, and IOM is how we do it.

BDT/IOM:

- Is used any time the data is being transferred is larger than 16 KB
- Does not use port 94 for transferring data
- Is not just used during multiplexed distributions

For transferring small bits of data (less than 16 KB) back and forth, the server and Managed Node use the already open ports (Managed Nodes) or re-open the known ports (6543 for PC Managed Nodes and usually 9494 for TMAs). Anytime there is a chance for large amounts of data to be sent, the TMR Server and Managed Node will attempt to open an IOM channel.

For more information about Inter-ORB communication, please refer to the redbook *Tivoli Enterprise Internals and Problem Determination*, SG24-2034

7.2.0.1 SSL support for BDT

SSL supports IOM and other large-scale data transfers. With single-port BDT disabled, IOM channels in Tivoli Management Framework work like they always have.

D.1.9 BDT channel implementation before Tivoli Framework 3.7.1

Figure 176 shows the communication setup between BDT channels across firewalls in previous versions of Tivoli Framework.

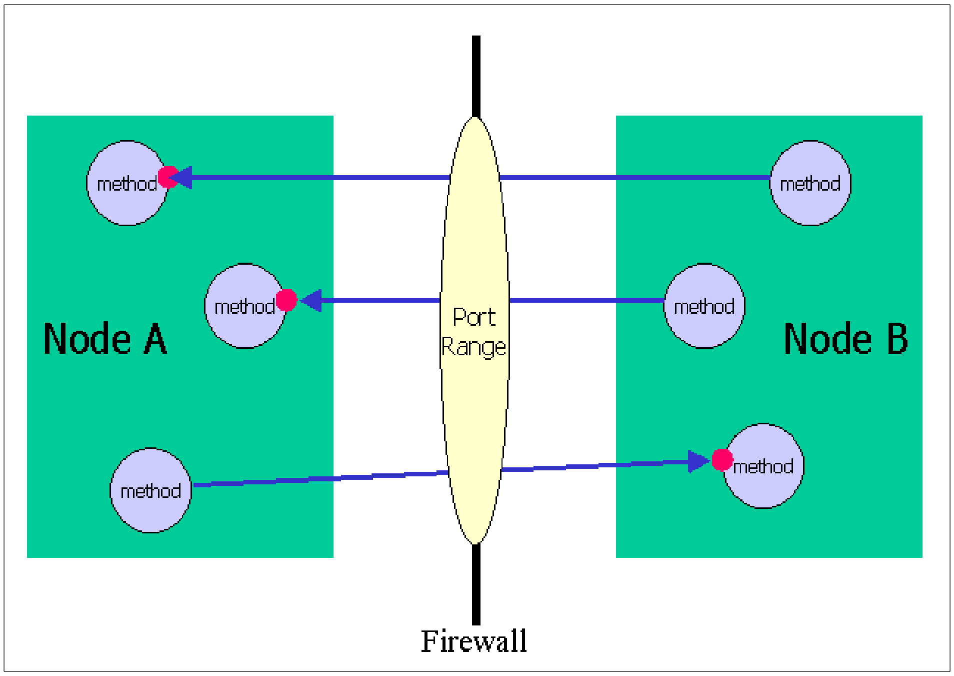


Figure 176. BDT channels between Managed Nodes

First, BDT-create opens a listener port, and then the method is called on the peer. Finally, BDT-collect opens the channel. In this scenario, the port range is recommended to allow up to three times the number of ports as there are Managed Nodes.

D.1.10 Single-port BDT

Figure 177 shows the communication setup between BDT channels across firewalls when single_port_bdt is set to TRUE.

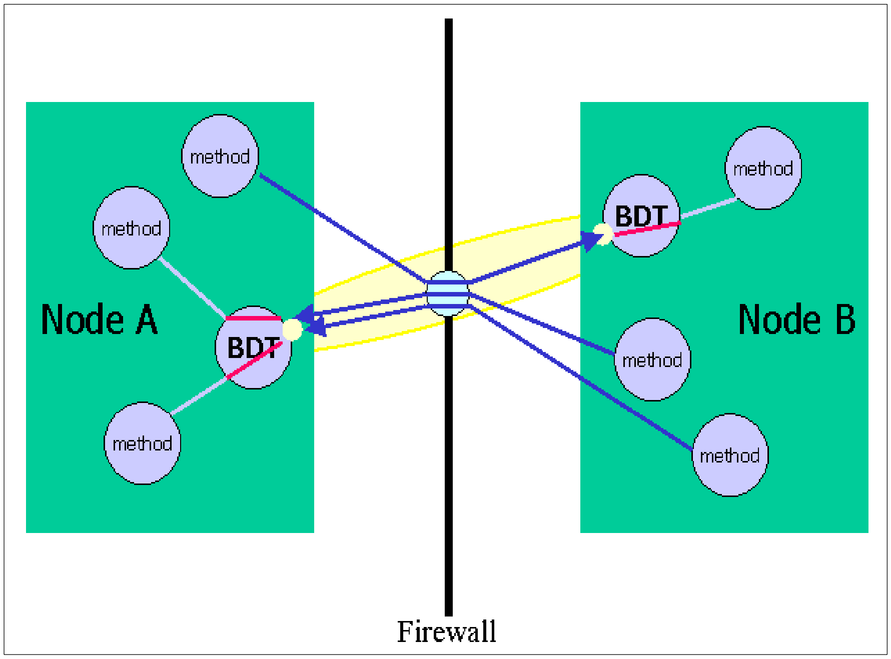


Figure 177. BDT channels between Managed Nodes (continued)

BDT-create registers with service. The related method is called on the peer, and then BDT-connect opens the channel. Finally, service forwards the data.

To enable single-port BDT, use:

```
odadmin single_port_bdt TRUE od#
```

Enabled Managed Nodes use a BDT service, or proxy, for created channels. Therefore, each Managed Node uses only one listener port. The BDT service bridges the data streams for the life of the channel.

All BDT traffic for each Managed Node uses a single service port. The port range is reduced to one configurable port value.

D.1.11 Configuration details of BDT for Managed Nodes

The port value is configurable for each Managed Node with the command:

```
odadmin set_bdt_port 9401 od#
```

Extended BDT clients are SSL capable. The BDT service is part of the MDist2 Repeater. MDist 2 channels do not use proxies, but they use a single port.

D.1.11.1 SSL for BDT

BDT channels are protected by SSL when both of the following conditions are met:

- The single port BDT mode is selected.
- SSL is enabled on both Managed Nodes.

Local channels are not SSL-protected for better performance. BDT channels are service-side authenticated in a manner similar to how Web servers work.

D.1.11.2 Performance

SSL and single-port BDT can reduce performance. The performance overhead depends on the cipher size (longer ciphers have more overhead), cryptographic algorithm, and hash algorithm that are used for secure communication. The type and number of operations, and the CPU and network workload also affect the performance. Providing real-world data about performance will help refine these new features.

D.1.11.3 Issues

There a number of issues when using the SSL and single-port BDT functions with Tivoli Framework. These are:

- FORCE_SSL is not always enforced.
- Creating a Gateway requires a subsequent `odadmin reexec`.
- Enabling BDT requires an `odadmin reexec`.
- HP-UX BDT is not SSL capable.

Appendix E. Special notices

This publication is intended to help IBM and Tivoli customers, Business Partners and professionals to understand, plan, and deploy the Tivoli Risk Manager product and infrastructure. The information in this publication is not intended as the specification of any programming interfaces that are provided by Tivoli Risk Manager. See the PUBLICATIONS section of the IBM Programming Announcement for Tivoli Risk Manager for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AIX
AS/400
CT
DB2
e (logo)®
IBM ®
Lotus
Netfinity
OS/2
Redbooks Logo
SP
Tivoli Enterprise Console
TME 10
XT
APPN
AT
Current
Domino
Early
IBM.COM
MQSeries
Notes
Redbooks
RS/6000
System/390
Tivoli Management Environment
WebSphere

The following terms are trademarks of other companies:

Tivoli, Manage. Anything. Anywhere.,The Power To Manage., Anything. Anywhere.,TME, NetView, Cross-Site, Tivoli Ready, Tivoli Certified, Planet Tivoli, and Tivoli Enterprise are trademarks or registered trademarks of Tivoli Systems Inc., an IBM company, in the United States, other countries, or both. In Denmark, Tivoli is a trademark licensed from Kjøbenhavns Sommer - Tivoli A/S.

C-bus is a trademark of Corollary, Inc. in the United States and/or other countries.

Cisco SecureIDS and NetRanger are trademarks of Cisco Systems, Inc.

ISS RealSecure is a trademark of Internet Security Systems, Inc.

Symantec and Norton AntiVirus are trademarks of Symantec Corporation.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

PC Direct is a trademark of Ziff Communications Company in the United States and/or other countries and is used by IBM Corporation under license.

ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States and/or other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

Appendix F. Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

F.1 IBM Redbooks

For information on ordering these publications see “How to get IBM Redbooks” on page 363.

- *CheckPoint VPN-1/Firewall-1 on AIX: A Cookbook for Stand-Alone and High Availability Solutions,* SG24-5492
- *Deploying a Public Key Infrastructure*, SG24-5512
- *Early Experiences with Tivoli Enterprise Console 3.7*, SG24-6015
- *A Secure Way to Protect Your Network: IBM SecureWay Firewall for AIX V4.1*, SG24-5855
- *IP Network Design Guide*, SG24-2580
- *LDAP Implementation Cookbook*, SG24-5110
- *Tivoli Enterprise Internals and Problem Determination*, SG24-2034
- *Tivoli SecureWay Policy Director: Centrally Managing e-business Security,* SG24-6008
- *Tivoli SecureWay Risk Manager: Correlating Enterprise Risk Management*, SG24-6021
- *Understanding IBM SecureWay FirstSecure*, SG24-5498
- *Understanding LDAP*, SG24-4986
- *Using Tivoli Decision Support Guides*, SG24-5506

F.2 IBM Redbooks collections

Redbooks are also available on the following CD-ROMs. Click the CD-ROMs button at **ibm.com**/redbooks for information about all the CD-ROMs offered, updates and formats.

CD-ROM Title	Collection Kit Number
IBM System/390 Redbooks Collection	SK2T-2177
IBM Networking Redbooks Collection	SK2T-6022
IBM Transaction Processing and Data Management Redbooks Collection	SK2T-8038
IBM Lotus Redbooks Collection	SK2T-8039

CD-ROM Title	Collection Kit Number
Tivoli Redbooks Collection	SK2T-8044
IBM AS/400 Redbooks Collection	SK2T-2849
IBM Netfinity Hardware and Software Redbooks Collection	SK2T-8046
IBM RS/6000 Redbooks Collection	SK2T-8043
IBM Application Development Redbooks Collection	SK2T-8037
IBM Enterprise Storage and Systems Management Solutions	SK3T-3694

F.3 Other resources

These publications are also relevant as further information sources:

- *Tivoli Decision Support for Enterprise Risk Management Release Notes* (only available with product)
- *Tivoli Decision Support Release Notes 2.1*, GI10-9852
- Crume, *Inside Internet Security: What Hackers Don't Want You to Know*, Addison Wesley Longman, Inc., 2000, ISBN 0201675161
- Goncalves, et al., *Check Point Firewalls: An Administration Guide*, The McGraw-Hill Companies, 1999, ISBN 007134229X
- Northcutt, *Network Intrusion Detection: An Analyst's Handbook Second Edition*, New Riders Publishing, 2000, ISBN 0735710082
- Scambray, et al., *Hacking Exposed: Network Security Secrets & Solutions Second Edition*, McGraw-Hill Professional Book Group, 2000, ISBN 0072127481
- Toxen, *Real World Linux Security: Intrusion Prevention, Detection and Recovery*, Prentice Hall PTR, 2000, ISBN 0130281875
- Wood, et al., *Intrusion Detection Message Exchange Requirements*, Internet Engineering Task Force, found at:

  `http://www.ietf.org/internet-drafts/draft-ietf-idwg-requirements-05.txt`

F.4 Referenced Web sites

These Web sites are also relevant as further information sources:

- `http://www.gocsi.com`
  Computer Security Institute
- `http://icat.nist.gov`
  ICAT Metabase, A Searchable Vulnerability Index

- `http://www.ietf.org/ids.by.wg/idwg.html`
  Internet Drafts on the Intrusion Detection Exchange Format from the Internet Engineering Task Force
- `http://www.sans.org`
  SANS (System Administration, Networking, and Security) Institute
- `http://www.tivoli.com/products/solutions/security/`
  Tivoli Security Management Solutions overview
- `http://www.cve.mitre.org`
  This is the CVE Web site, which holds information about CVE itself, the CVE list and a wealth of links to related information and activities.
- `http://www.apnic.net`
  Asia Pacific Network Information Centre
- `http://www.internic.net`
  The InterNIC Web site provides the public information regarding Internet domain name registration services.
- `http://www.itl.nist.gov`
  Information Technology Laboratory (ITL)
- `http://www.packetstormsecurity.org/`
  Packet Storm is an extremely large and current security tools resource that is for the community, by the community. Packet Storm is a non-profit organization kept alive for the sole purpose of helping secure the World's networks.
- `http://rootshell.com/beta/news.html`
  Rootshell is a site with detailed information about vulnerabilities.
- `http://www.attrition.org`
  Attrition.org is a computer security Web site dedicated to the collection, dissemination, and distribution of information about the industry for anyone interested in the subject. They maintain one of the largest catalogs of security advisories, cryptography, text files, and denial of service attack information.
- `http://www.linuxsecurity.com`
  The Linux center for security
- `http://developer.netscape.com/docs/manuals/security.html`
  Netscape security documentation
- `http://www.elink.ibmlink.ibm.com/pbl/pbl`
  IBM publications online catalog

F.5 Tools

The tools mentioned in this redbook, especially Chapter 6, “Intrusion detection” on page 205, are available on the Internet.

As some of these Web addresses will change in the future, there is an excellent list of tools at:

```
http://www.insecure.org/tools.html
```

How to get IBM Redbooks

This section explains how both customers and IBM employees can find out about IBM Redbooks, redpieces, and CD-ROMs. A form for ordering books and CD-ROMs by fax or e-mail is also provided.

- **Redbooks Web Site** **ibm.com**/redbooks

  Search for, view, download, or order hardcopy/CD-ROM Redbooks from the Redbooks Web site. Also read redpieces and download additional materials (code samples or diskette/CD-ROM images) from this Redbooks site.

  Redpieces are Redbooks in progress; not all Redbooks become redpieces and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

- **E-mail Orders**

  Send orders by e-mail including information from the IBM Redbooks fax order form to:

	e-mail address
In United States or Canada	pubscan@us.ibm.com
Outside North America	Contact information is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Telephone Orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	Country coordinator phone number is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Fax Orders**

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	Fax phone number is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

This information was current at the time of publication, but is continually subject to change. The latest information may be found at the Redbooks Web site.

IBM Intranet for Employees

IBM employees may register for information on workshops, residencies, and Redbooks by accessing the IBM Intranet Web site at http://w3.itso.ibm.com/ and clicking the ITSO Mailing List button. Look in the Materials repository for workshops, presentations, papers, and Web pages developed and written by the ITSO technical professionals; click the Additional Materials button. Employees may access MyNews at http://w3.ibm.com/ for redbook, residency, and workshop announcements.

IBM Redbooks fax order form

Please send me the following:

Title **Order Number** **Quantity**

First name Last name

Company

Address

City Postal code Country

Telephone number Telefax number VAT number

□ Invoice to customer number

□ Credit card number

Credit card expiration date Card issued to Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

Glossary

ACF	Adapter Configuration Facility.
AIM	Availability Intermediate Manager.
APAR	Authorized Program Analysis Report.
B2B	Business to Business.
B2C	Business to Consumer.
BAROC	Basic Recorder of Objects in C.
BID	Numbering scheme for vulnerabilities used by BUGTRAQ.
Buffer Overflow	A special type of vulnerability in software programs that allow a hacker to gain unauthorized access to parts of a system's memory.
BUGTRAQ	A mailing list based service that updates subscribers about new vulerabilities and security breaches.
CAT	Common Adapter Toolkit.
CERT	The CERT coordination center, which is the reporting center for Internet security problems. CERT is a registered service mark of Carnegie Mellon University (not an acronym).
CVE	Common Vulnerabilities and Exposures.
Directive	The configuration or control statement in an NSA control file.
DMZ	The demilitarized zone, which is part of the network infrastructure that separates the Internet from the enterprise's internal network(s).
DOS	Denial of service attack.
DDOS	Distributed denial of service attack.
EJB	Enterprise Java Beans.
ERS	IBM Emergency Response Service.
Event Adapter	A single module that transports events generated by supported IDS applications directly to the TEC server for processing.
FID	Finding identifier.
Findings	Any information gathered by a scan.
IDEF	Intrusion Detection Exchange Format.
IDS	Intrusion Detection System.
IDWG	Intrusion Detection Working Group.
IKE	Internet Key Exchange.
LEA	Log Export API.
libc	The name of the C compiler library package under Linux.

Logfile Adapter Collects events out of the NT event log or the UNIX syslog at certain intervals and sends them to the TEC server for processing.

man pages The online help library under UNIX.

MITRE The MITRE Corporation (`www.mitre.org`).

MSKB Microsoft Knowlege Base.

Network Scan An activity to gain information about a network and the systems attached to it.

NSA Network Services Auditor.

OPSEC CheckPoint Open Platform for Secure Enterprise Connectivity.

Perl A scripting language that is popular in UNIX circles.

PKCS Public Key Cryptography Standards.

PKI Public Key Infrastructure.

POP3 Post Office Protocol Version 3.

Pre-adapter Retrieves and formats event information from third party products, such as Cisco Secure IDS or ISS Realsecure, and stores this information in either a syslog format or NT event log format.

Red Hat A Linux distributor.

RIM RDBMS Interface Module.

RIR Regional Internet Registries.

RMEIF Risk Manager Event Integration Facility.

SAM Suspicious Activity Monitor.

SIS Software Installation Services.

SMTP Simple Mail Transfer Protocol.

SuSE A Linux distributor.

TEC Tivoli Enterprise Console.

TME Tivoli Management Environment.

TMR Tivoli Management Region.

vi A text editor, which is widely used under UNIX.

VPN Virtual Private Network.

XF An X-Force Vulnerability database service offered by ISS.

Index

IBM Redbooks review

Your feedback is valued by the Redbook authors. In particular we are interested in situations where a Redbook "made the difference" in a task or problem you encountered. Using one of the following methods, **please review the Redbook, addressing value, subject matter, structure, depth and quality as appropriate.**

- Use the online **Contact us** review redbook form found at ibm.com/redbooks
- Fax this form to: USA International Access Code + 1 845 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Document Number **Redbook Title**	SG24-6036-00 e-business Risk Management with Tivoli Risk Manager
Review	
What other subjects would you like to see IBM Redbooks address?	
Please rate your overall satisfaction:	O Very Good O Good O Average O Poor
Please identify yourself as belonging to one of the following groups:	O Customer O Business Partner O Solution Developer O IBM, Lotus or Tivoli Employee O None of the above
Your email address: The data you provide here may be used to provide you with information from IBM or our business partners about our products, services or activities.	 O Please do not use the information collected here for future marketing or promotional contacts or other communications beyond the scope of this transaction.
Questions about IBM's privacy policy?	The following link explains how we protect your personal information. ibm.com/privacy/yourprivacy/

e-business Risk Management
with Tivoli Risk Manager

e-business Risk Management

with Tivoli Risk Manager

A comprehensive validation of correlating intrusive events

Integrating a multitude of different sensor technologies

Integration with Tivoli Decision Support

Tivoli Risk Manager is an integrated e-business Risk Management solution that is based on Tivoli Framework. It enables customers to centrally monitor attacks, threats, and vulnerabilities by correlating security alerts across a diversity of security point product deployments. By correlating these security alerts across intrusion detectors, Web servers, firewalls, and routers, Risk Manager enables administrators to eliminate clutter (such as false positives), centrally correlate distributed attacks, identify real security threats with a high degree of integrity and confidence, and use adaptive event response using the Tivoli Enterprise Console.

This redbook explains Tivoli Risk Manager 3.7 solutions, outlines the planning steps, details installation and configuration tasks, and discusses various intrusion attacks and security breaches. It further describes the reporting integration with Tivoli Decision Support.

This book is a valuable resource for security administrators and architects who wish to understand and implement a centralized risk management solution.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-6036-00 ISBN 0738422452