Universidad de las Américas

Facultad de Ingeniería de Sistemas

Principios Básicos y Herramientas para la

Administración de Redes

Trabajo de titulación presentado en conformidad a los requisitos para obtener el título de:

INGENIERO DE EJECUCION EN COMPUTACION E INFORMATICA

Director del Trabajo: Ing. David Ramirez

Autor: Marlon Fabricio Molina P.

1999

Resumen

Muchas organizaciones hoy en día están moviéndose dentro de la arquitectura cliente/servidor dentro de sus ambientes computacionales. Haciendo que este movimiento pueda eliminar muchos de los problemas encontrados en un ambiente centralizado. Las organizaciones no pueden estar sujetas a los ciclos de desarrollo de sistemas o la lentitud de respuesta de datos de los mainframes. Sin embargo no están restringidos a un rápido crecimiento de sus redes LAN para de esta forma tener sus datos en una forma distribuida para que el usuario final pueda lograr una rápida respuesta a sus requerimientos de información y de esta forma lograr una mejor calidad en el servicio.

La administración de estas redes cliente/servidor a incrementado la complejidad de las redes empresariales dependiendo de la ubicación geográfica así como la incorporación de sistemas y software de una variedad de proveedores. Administrar una red distribuida requiere de una variedad de conocimientos sobre diferentes plataformas. Entonces la solución ha este problema debe ser direccionada mediante la ayuda de una base de conocimientos orientada a objetos diseñada específicamente para un desarrollo de aplicaciones de administración de redes que sean seguras, heterogéneas y sobre todo escalables. Muchas aplicaciones para administrar recursos en sistemas distribuidos (ejm. Usuarios, impresoras, sistemas de archivos) y operaciones (ejm. Seguridad, monitoreo de eventos y distribución de software) están ahora disponibles.

Para completar la transición hacia redes cliente/servidor, las organizaciones deben convertir las aplicaciones críticas desde un mainframe o ambientes de tiempos compartidos hacia un ambiente de red. Solo una distribución total de las aplicaciones en la red harán posible que las organizaciones aprovechen al máximo la arquitectura cliente/servidor.

Las aplicaciones cliente servidor complejas pueden crear un nuevo conjunto de problemas de administración, sin embrago las aplicaciones pueden ser particionadas en sistemas heterogéneos, grandes sistemas pueden encontrarse en una variedad de locaciones geográficas y los usuarios pueden estar distribuidos alrededor de un país o incluso del mundo.

Monitorear el estatus de cada aplicación o solo mantener un enlace de donde la aplicación fue desarrollada es muy difícil. Se ha incrementado la popularidad de herramientas cliente servidor que son pequeñas y a la vez tienen sucesivas revisiones. Esto hace que sea más frecuente continuas actualizaciones de software a través de la red para todas las computadoras que corren dicha aplicación.

Es por esto, que a pesar de contar con eficientes herramientas para la administración es fundamental que la organización cuente con principios y políticas bien definidas para la administración de redes.

Summary

Many organizations today are moving to client/server architectures in their computing environments. Making this move can eliminate many of the problems encountered in a strictly mainframe or strictly desktop computing environment. Organizations are no longer subject to lengthy application development cycles and slow data response times caused by mainframe computing. They are no longer restricted by the lack of scalability common in PC local area networks (LANs). With client/server computing, data can be distributed among several systems to provide substantially quicker response time and easier accessibility, giving end-users higher quality service.

Client/server management becomes increasingly complex as enterprise-wide networks span broad geographic locations and incorporate systems and software from a variety of vendors. Managing a distributed network requires a different set of skills than those needed for managing mainframe environments. Then the solution has addressed this problem with a distributed, object-oriented framework designed specifically for developing secure, heterogenous, and scalable Systems Management applications. Several applications for managing distributed system resources (for example, users, printers, and file systems) and operations (for example, security, event monitoring, and software distribution) are now available.

It is not enough, however, to manage only the system resources that comprise a distributed computing environment. To complete the transition to client/server networks, organizations must convert their mission-critical applications from mainframe or time-sharing environments into the networked environment. Only as fully distributed applications become available on the network can organizations fully realize the benefit of client/server architectures.

Complex client/server applications can create a whole new set of management and administration problems, however. Applications may be partitioned on several heterogenous systems; large systems may encompass a variety of geographical locations; and end-users may be distributed around the country, or even the world. Monitoring the status of such applications, or even just keeping track of where the application is deployed, can be difficult. The growing popularity of client/server development tools has shortened the time between successive revisions of an application. This results in more frequent software updates that need to be distributed to the client and server machines that run the application.

Indice

Introducción

Siendo esta la era de la computación distribuida y de los entornos multi-marca, en las empresas existen muchos sistemas conectados en red a través distintas ubicaciones geográficas. Como consecuencia, comienzan a producirse pesadillas administrativas, pues la administración de estas redes ha comenzado a ser más compleja y más costosa. Generalmente, los administradores de sistemas utilizan distintos esquemas de administración para cada plataforma de hardware que está conectada a la red, para lo cual deben invertir una cantidad considerable de tiempo y dinero para ganar experiencia sobre los múltiples sabores de herramientas administrativas.

Las organizaciones del mundo entero han incrementado su dependencia en el ambiente de computación en red. Esta es la razón por la cual se han ido integrando las operaciones de negocios y la administración de estas redes ha comenzado a ser muy crítica.

Con negocios críticos y con las aplicaciones y recursos que se están expandiéndose en todo sentido desde un mainframe hasta equipos de escritorio de redes privadas, una adecuada administración de estas redes se va tornando de suma importancia.

La administración de las redes puede ir estableciendo la diferencia, entre las empresas productivas y eficientes ya que grandes plataformas en ambientes escalables requieren de soluciones de administración prácticas, estas soluciones también deben satisfacer las necesidades de administración de ambientes con diferentes tipos de plataformas, para lo cual se necesita de herramientas de software que las integren.

Por esto es imprescindible con herramientas de administración de redes.

Una herramienta de administración debe proveer una vista común y simple de los recursos de la red así como también debería facilitar la integración de los diferentes ambientes de sistemas.

Disciplinas de administración o aplicaciones de administración deben operar de una forma transparente a través de diferentes ambientes operativos para permitir al usuario ejecutar cualquier actividad de administración u operación sobre múltiples plataformas con un solo comando consistente.

Un estudio profundo sobre costo-beneficio del uso de herramientas de administración de redes llegó a la conclusión que empresas que aplicaron sistemas de administración

incrementaron su productividad hasta en un 32.5% versus un 13.6% con soluciones parcialmente integradas y un 10.4% con soluciones no integradas.

La estrategia de un sistema de administración se debe basar en la integración total de los ambientes, integrando desde una base común de conocimientos hasta herramientas de gestión propias y de terceros, permitiendo incorporar soluciones para disciplinas específicas.

Por otro lado al disponerse de un entorno homogéneo de administración, no son necesarios especialistas en cada disciplina para cada entorno, y la incorporación de nuevas tecnologías no se ve limitada por cuestiones de la Administración de Sistemas. El hecho que se trabaje en base a una única interfaz de administración hace que los ciclos de capacitación y aprendizaje disminuyan drásticamente.

El sistema de Administración debe estar compuesto por diversos módulos que son tratados en este documento. Dado que cada módulo trabaja en base a una base común de conocimientos, la incorporación de cualquier módulo adicional potencia el desempeño y la funcionalidad de los demás módulos.

El objetivo de este trabajo es brindar una plataforma completa en materia de administración de dispositivos de redes, servidores, desktops, sistemas operativos, bases de datos, y aplicaciones de negocio manejando los conceptos de:

- Visión global del entorno informático.
- Alta escalabilidad del entorno y la herramienta de administración.
- Innovación tecnológica.
- Integración total.
- Protección de la inversión.

Dado el carácter integrado del Sistema de Administración, y de la capacidad de la base de conocimientos común de manejar cada elemento como un todo.

El objetivo de una correcta administración de la red es ayudar a las empresas a reducir los costos y la complejidad de manejar la computación distribuida, y haciendo esto, crear una ventaja competitiva.

El objetivo es proveer un entorno de administración flexible e integrado. La arquitectura debe forzar políticas de comportamiento común entre todas las aplicaciones de administración. Se suscribirán a un paradigma común de administración tal como se describe a continuación:

- Las aplicaciones de administración pueden ser vistas en una consola común
- Las guías operativas y las políticas corporativas pueden ser implementadas en el software de Administración y ser forzadas a toda la red
- Las tareas de administración pueden ser delegadas en forma segura y consistente
- Los recursos de la red pueden ser agrupados lógicamente para reducir la complejidad de administrar miles de recursos distribuidos
- Los cambios, modificaciones y actualizaciones pueden ocurrir a través de toda la empresa independientemente del tipo de máquina y modelo

El sistema de administración de la red será la infraestructura crítica que mejorará la confiabilidad de los sistemas a través de una implementación consistente de procesos de administración de calidad, permitiendo que los gerentes puedan construir una infraestructura informática que podrá crecer y cambiar con el negocio.

CAPITITULO I

Conceptos Generales.

Debido a que se trata de lograr administrar recursos de redes heterogéneas de una forma transparente para el usuario administrador de debe partir de una base de conocimientos común o Framework, la cual debe estar basada en una arquitectura abierta y orientada a objetos para aprovechar de esta forma las ventajas que dicha arquitectura ofrece como por ejemplo las herencias.

La naturaleza de un entorno distribuido, requiere reducir la complejidad de los sistemas utilizando las herramientas de una plataforma abierta que sea capaz de:

- Adaptarse a las "multi-marcas" de hardware y software.
- Permitir la expansión no anticipada, en cuanto a tamaño de red, cambios en aplicaciones, sistemas, etc.
- Administrar tanto los recursos lógicos del entorno (ej. bases de datos y aplicaciones) como también hardware y sistemas operativos.
- Disminuir la curva de aprendizaje y aumentar la productividad de los administradores junior.
- Integrar herramientas de administración existentes a otras que provengan de distintas fuentes en el futuro.

La plataforma de administración de sistemas distribuidos debe cumplir con todos estos requerimientos. El Framework debe utilizar una tecnología orientada a objetos para reducir la complejidad de los sistemas y sus diferencias, y asegurar escalabilidad y fácil customización. El

Framework, debe representar como una colección de objetos, permitiendo diseñar el modelo del entorno que se quiere administrar.

Los usuarios, computadoras cliente/servidor, grupos de usuarios, servicios, dispositivos, y otros recursos físicos y lógicos de la red, deben estar representadas como objetos que se autodescriben.

Toda la información necesaria para administrar los recursos de la red, también debe ser encapsulada como objetos, en lugar de programas y archivos difíciles de manejar y acceder.

Gracias a que los objetos residen en una única base de datos con la información para administrarlos, los administradores autorizados podrán acceder a ellos desde cualquier parte de la red. Estos objetos se interrelacionan para compartir información de administración y para representar la manera en que se asocian entre sí en el mundo real.

Portabilidad

El uso de una tecnología orientada a objetos permite a los desarrolladores tomar los servicios de un tipo o clase de objeto y aplicar técnicas idénticas sobre tipos de objetos similares o totalmente distintos. Esto le permite al programador escribir código para una clase de objeto y, eventualmente, desarrollar una "biblioteca" de rutinas para manipular los objetos.

Mantenimiento

Utilizando los conceptos de portabilidad descritos anteriormente, queda claro que el mantenimiento de código orientado a objetos se reduce muchísimo si se compara con una tecnología que no está orientada a objetos. Por ejemplo, si se escribe una rutina que haga un "sort" según un tipo de objeto, es muy simple utilizar esa misma funcionalidad sobre distintos tipos de objetos.

Escalabilidad

Para responder a necesidades de crecimiento, el sistema de administración de la red debe ser enfocado con sus aplicaciones a la escalabilidad. Una instalación puede dividirse lógicamente en

múltiples regiones conectadas entre sí, cada una con su propio servidor para administrar sus clientes locales. Esto permite coordinar las actividades a través de la red y administrar sitios remotos (por ejemplo, sucursales), eliminando así, los cuellos de botella de las estructuras con un único servidor.

Integración transparente

Utilizando todos los conceptos vistos hasta ahora, y combinando las herramientas de desarrollo se debe proporcionar una verdadera y transparente integración de aplicaciones, tanto propias como de terceros.

Fácil Personalización

Los objetos cuentan con la característica de "herencia". De esta forma se puede modificar las estructuras reusables según crea conveniente sin destruir las configuraciones originales. Por ejemplo, si se quiere que todas las passwords tengan una longitud de 15 caracteres, es posible efectivizar esta política a través de la función de "customización de políticas".

Un entorno de administración de sistemas basado en objetos no necesariamente reemplaza los mecanismos de administración presentes en el sistema operativo. Por el contrario, proporciona el fácil uso de objetos escondiendo los detalles y complejidades de las tareas de administración.

El objetivo principal de un sistema de administración de red debe ser el proveer una plataforma de administración capaz de simplificar la administración de cientos o miles de computadoras, principalmente desktops, en un entorno heterogéneo. El Framework utiliza mecanismos de autenticación, autorización, encriptado e integridad de datos.

CAPITULO II

Componentes del Sistema de Administración.

BASE DE CONOCIMIENTOS COMUNES. (FRAMEWORK)

Una red cliente/servidor esta compuesta por millones de piezas en movimiento. El Framework posee la particular habilidad de simplificar la administración modelando todos los elementos administrados y sus dependencias como objetos. Todas las aplicaciones utilizan los servicios del Framework. Esto implica que cuando se introducen mejoras a una función, por ejemplo el Calendario, todas las demás aplicaciones "heredan" las mejoras. Además el Framework funciona como un único punto de integración para todas las aplicaciones, brindando la capacidad de que todos los productos se integren mediante el Framework y tomen ventaja de sus capacidades. Ya no es el cliente el que se ve forzado a realizar la tarea de integrador.

Reducción de complejidad

Con el Framework cada recurso (hardware, sistema operativo, base de datos, etc.) es capturado y convertido en un objeto, brindando a las aplicaciones un modelo de sistema que es dinámicamente actualizable y esta basado en la realidad. Este acercamiento único es el que permite que los administradores de sistemas puedan manejar sistemas complejos exitosamente.

Servicios Comunes

Existe una gran cantidad de funciones que deben estar presentes en cualquier aplicación de administración. En lugar de tomar el modelo monolítico, duplicando funcionalidad en cada aplicación por separado, el Framework debe incluir servicios universales como Calendarizacion, movimiento de datos y administración de tareas dentro de si mismo. De esta manera cuando el

Framework es actualizado, todas las aplicaciones pueden aprovechar las mejoras de inmediato. La idea es no estar constantemente reinventando la rueda, todos los esfuerzos de desarrollo pueden ser dirigidos a lograr que un servicio específico sea el mejor de su clase.

Servicio de Calendario

Framework debe incluir un servicio de calendarizacion apto para todas las tareas de administración que se deban ejecutar, opciones de reintentos, time-outs, fechas y horarios permitidos, etc, lo cual libra a administradores de tareas de mantenimiento repetitivas, ya que estas pueden ser encapsuladas por un administrador "senior" como una Tarea dentro del framework y posteriormente ser ejecutadas por otros administradores previamente autorizados sin la necesidad de que el administrador senior se encuentre presente para lograr el nivel de autorización requerido en los diversos sistemas operativos.

Todos los servicios comunes provistos por el Framework son parte integral de las aplicaciones de administración. Los fundamentos de administración mediante Políticas, Consistencia (transparencia entre plataformas), Administración por Suscripción, Delegación Segura de Autoridad, y Escalabilidad, derivan de atributos del Framework.

Simplificación de Integración

Se requiere de una gran gama de aplicaciones para administrar cualquier empresa compleja. Sin embargo, la cantidad de herramientas necesarias en un entorno distribuido puede hacer que la complejidad de integración salga fuera de control. Al querer hacer que todos los productos de administración funcionen juntos, usted mismo se ve forzado a integrar cada producto con todos los anteriores, una tarea cuya complejidad tiene crecimiento exponencial. Sin embargo, con una infraestructura sólida, probada y abierta, el trabajo de integración se reduce drásticamente ya que la única tarea de integración es la de la aplicación con el Framework. La integración es una

facilidad inherente a las aplicaciones de administración basadas en el Framework. Integración simplificada significa que las aplicaciones de administración trabajan juntas, y con el poder del Framework es simple tenerlas trabajando con una gran gama de las mejores aplicaciones de terceros.

Roles de un Administrador

Las acciones disponibles para un administrador dependen de los *roles* de autorización que se le hayan asignado. Los roles disponibles dependen de los módulos que se encuentren instalados. Los roles provistos por el Framework permiten dividir el control en funciones tales como backup, restore, instalación de productos. Existen otros roles con un alcance más amplio como ser *super, senior, admin y user*, cada uno de los cuales proporciona diferentes capacidades en el entorno de administración. Cabe aclarar que estos roles no son jerárquicos. Es decir, que si un administrador tiene el rol *senior* no necesariamente podría realizar *backup* de la base de datos. Esto evita la necesidad de tener múltiples super usuarios.

Los roles pueden asignarse a nivel MR (regiones de administración) o a nivel recurso. Si se aplica un rol a nivel recurso, el administrador tendrá el mismo rol para todos los recursos que estén dentro de ese recurso, salvo que se especifique un rol diferente en los distintos niveles jerárquicos.

Hay tres pasos importantes que determinan los roles de un administrador:

1. Determinar qué acciones necesitará tomar el administrador y sobre qué tipo de recursos.
2. Identificar el rol de recurso o de MR requerido para posibilitar esas acciones.
3. Asignar los roles de recurso y/o de MR al administrador.

Una vez definido un administrador, se determina que es lo que aparecerá en su "desktop".

Logins de los Administradores

Cada administrador tendrá un registro conteniendo un *user login name* y uno o más *set login names:*

User login name. Es el nombre del administrador. Identifica los roles asignados al administrador y el Desktop que se va a utilizar para este administrador.

Set login name. El administrador se conecta al sistema con su login específico del sistema y luego inicia el Desktop. *Set login name* es una tabla (una para cada administrador) que contiene los login de sistema que el administrador puede utilizar. Es posible limitar desde que nodo puede usarse dicho login.

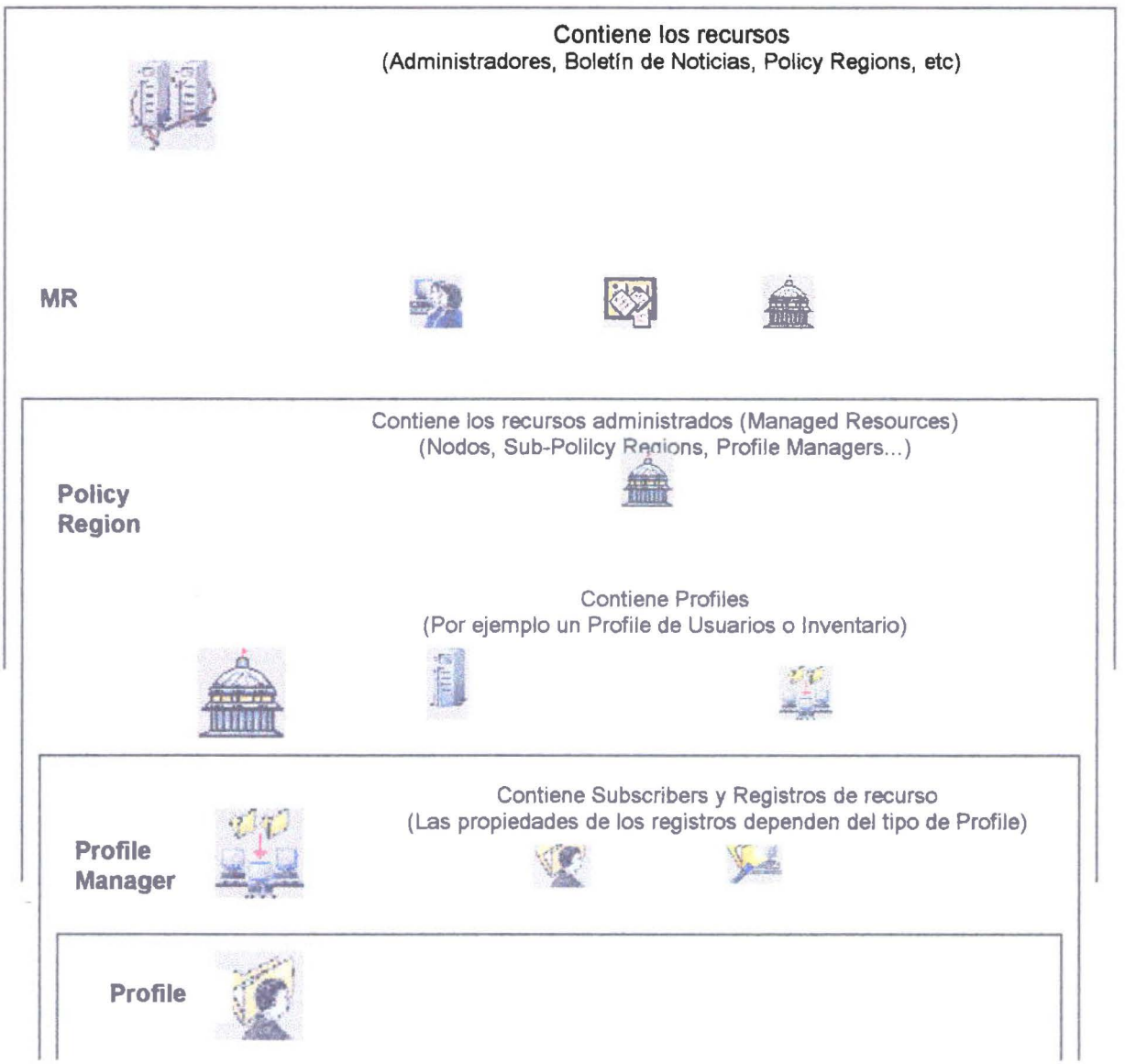
Ids de Usuario utilizados por el Framework

Una vez que un administrador tiene un icono disponible para ejecutar una acción, entonces el administrador debe tener el rol requerido en la Policy region del sistema destino. La mayoría de las aplicaciones permiten definir el ID del sistema a utilizar para realizar una acción sobre los nodos. Esta cuenta debe existir en el nodo destino, y debe tener los permisos necesarios para completar la operación.

En un entorno Unix, el Framework utiliza el ID *nobody* para realizar ciertas operaciones en un nodo administrado. Si esta cuenta no existe, entonces el Framework crea la cuenta MErsrvd.

En entornos NT, el Framework agrega una cuenta denominada *MErsrvd,* sin privilegios y que pertenece al grupo *Domain Users.*

La figura demuestra la jerarquía de la administración de los recursos.



Jerarquía de la Administración de Recursos

Políticas y Policy Regions

A medida que los recursos del sistema y de la red a administrar crecen, se torna más importante la posibilidad de tener una manera de dividir las funciones de administración en un modelo lógico. El

sistema de administración debe hacer esto a través de políticas de administración. Una política especifica reglas de administración para los recursos de un tipo en particular. Por ejemplo, se puede implementar una política para determinar que ciertas tareas solo pueden ejecutarse en ciertas máquinas, donde las tareas y las máquinas (nodos) son recursos administrados. Los recursos que pueden administrarse dependen de las aplicaciones de administración que estén instaladas. Un recurso administrado representa un recurso del sistema o de la red que se quiere administrar.

Las políticas se implementan de manera escalable a través del uso de *Policy Regions.* Los recursos a administrar tales como nodos y los propios del entorno se asignan a una Policy Region. Las actividades de administración sobre ese recurso van a estar sujetas a políticas *default* y políticas de *validación.* Una política default define un conjunto de valores (propiedades) predeterminados que se asignan a un recurso al crearse el mismo. Estos valores pueden ser de tres tipos: ninguno, una constante o el resultado de un script.

Una política de validación determina si todos los recursos de una Policy Region deben *obedecer* la política establecida en la Region. Al habilitar las políticas de validación se previene que los administradores creen o modifiquen los recursos de manera tal que no cumplan con las políticas establecidas dentro de la Region. Es posible diseñar las políticas de forma tan granular como se quiera. Cada Policy Region puede contener tanto nodos a administrar como otras Policy Regions (subregiones).

Noticias

Un punto importante a considerar cuando se establece una política de seguridad, es el seguimiento de las actividades de los administradores. El sistema de administración debe poseer una función de notificación que informa sobre las operaciones de administración de sistemas detallando el

administrador que llevó a cabo las mismas. Se puede implementar esta función a través del uso de *noticias* y *grupos de noticias:*

Noticia	Un mensaje que tiene que ver con alguna operación o cambio en el sistema distribuido.
Grupo de Noticia	Una colección de Noticias específicas de una aplicación u operación. A los administradores se los suscribe a los grupos de noticias correspondientes a su rol, para que reciban los mensajes en el desktop de administración .

Servicios del Framework

Task Library

El recurso *Task Library* (biblioteca de tareas) permite al administrador crear *tasks* y *jobs*. Una *task* es una operación o conjunto de operaciones que se necesitan ejecutar de manera rutinaria en el entorno. Un *job* es una tarea que se ejecuta sobre recursos administrados específicos.

Tasks

Una tarea se define y se almacena dentro de una task library y, por lo tanto puede volver a utilizarse sin tener que redefinirla. Es de gran utilidad definir tareas para delegar autoridad a administradores que realizan ciertas funciones de alto nivel sin darles acceso de alto nivel al sistema en sí. Cuando se crean tareas se definen los siguientes aspectos (Ver Figura):

- ✓ Programas a ejecutar según la plataforma
- ✓ Rol del administrador requerido

- ✓ User ID y grupo del usuario bajo el cual se ejecutará la tarea

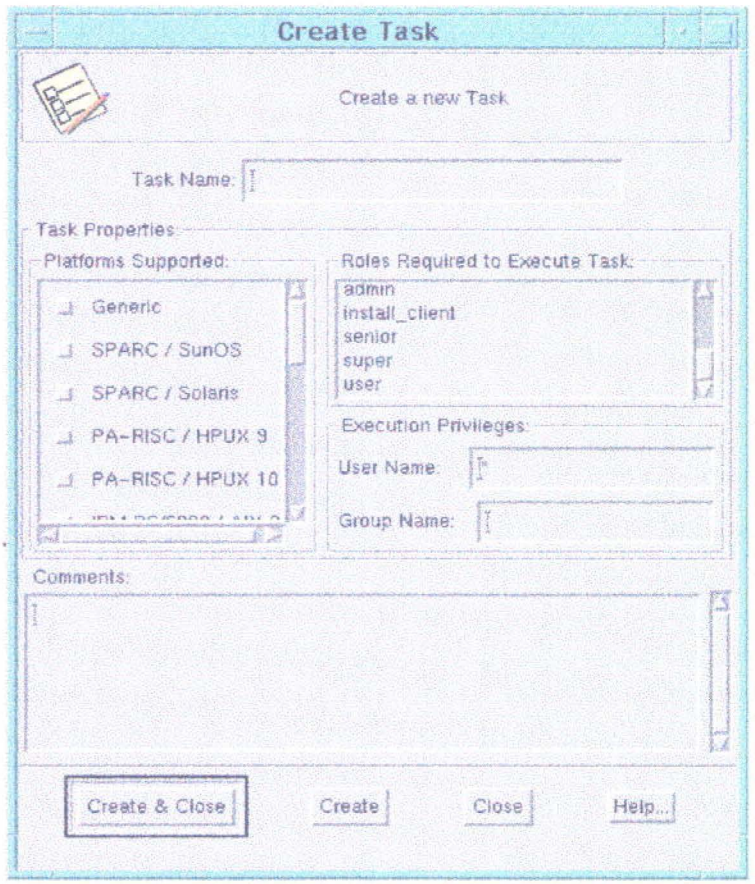


Figura . Ventana para Crear Tasks

Para ejecutar la tarea una sola vez sin crear un *job*, se define lo siguiente:

- ✓ Endpoints de la tarea: la máquina sobre la cual se ejecutará la tarea
- ✓ Formato y destino de la salida
- ✓ Parámetros de ejecución (ej: valor de time-out)
- ✓ Modo de ejecución (serial o paralelo)

Jobs

Un job es una tarea que se ejecuta sobre un conjunto específico de recursos administrados. La tarea debe existir antes de crear el job. Se pueden crear varios jobs que ejecuten la misma tarea, pero con distintos conjuntos de recursos administrados como endpoints de la tarea. Cuando se define un job se especifica lo siguiente:

- ✓ Endpoints de la tarea: la máquina sobre la cual se ejecutará la tarea
- ✓ Formato y destino de la salida
- ✓ Parámetros de ejecución (ej: valor de time-out)
- ✓ Modo de ejecución (serial o paralelo)

Scheduler

El *Scheduler* es un servicio del entorno que permite realizar una sola vez o periódicamente, *jobs* definidos por el usuario y otras funciones tales como la distribución de un perfil. En el entorno, permitirá realizar tareas que deben llevarse a cabo regularmente o en los horarios que los administradores no están disponibles para arrancar esas funciones. Por ejemplo, se puede programar que todos los viernes a la misma hora se haga un shutdown de un servidor por razones de mantenimiento, y, si esta acción falla, reintentar cinco veces durante una hora. La Figura muestra la ventana que permite programar jobs.

Cuando se programa un job, se especifica los siguiente:

- ✓ Fecha y hora de inicio
- ✓ Si el job debe repetirse, indicar de qué manera

- ✓ Avisos que deben realizarse una vez finalizado el job
- ✓ Condiciones para cancelar el job
- ✓ Reintentos en caso de falla del job

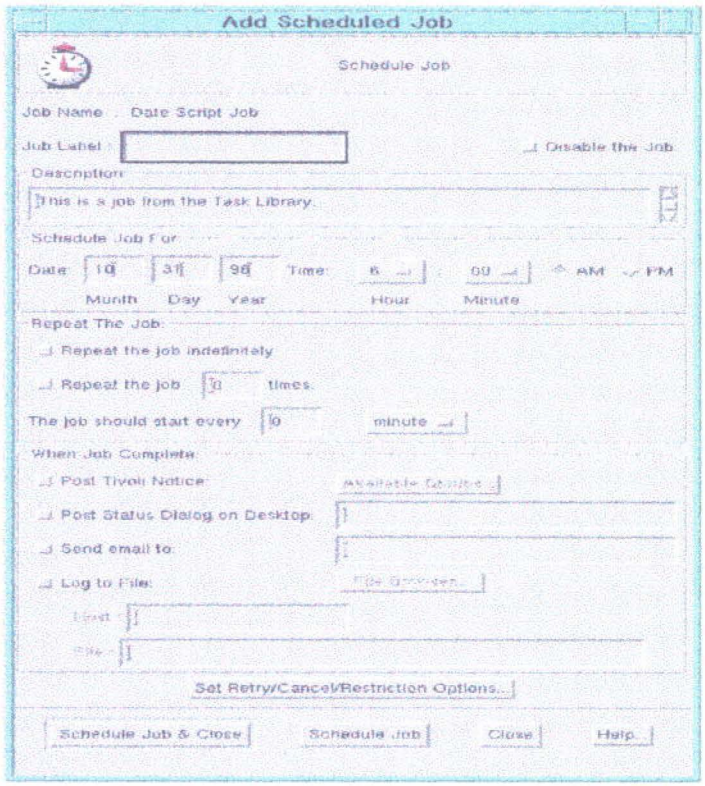


Figura. Ventana para crear un Job

CAPITULO III

ADMINISTRACIÓN DE USUARIOS.

Los administradores de sistemas pasan una considerable cantidad de tiempo administrando usuarios y grupos en un entorno distribuido. Constantemente la empresa necesita generar y borrar cuentas de usuarios en diferentes entornos y, adicionalmente, a medida que las necesidades de los usuarios cambian, estas cuentas deben actualizarse.

Tradicionalmente, los administradores de sistemas tenían que manejar usuarios en una sola arquitectura o sistema operativo. En la actualidad la mayoría de los entornos distribuidos tienen usuarios que necesitan cuentas en varios sistemas operativos.

Cada sistema operativo, Unix, Windows NT y Netware, tiene su propio grupo de archivos o base de datos de configuración que describen la cuenta del usuario para ese sistema. También cada tipo de Unix tiene su propio grupo de archivos de configuración.

Además para poder manejarse con las cuentas de usuarios de los distintos sistemas operativos, es inevitable que existan variaciones en las políticas de administración de usuarios a lo largo de toda la empresa.

El administrador de usuarios debe ofrecer las herramientas para manejar los usuarios en los entornos más comunes, así como también en los Unix más populares.

Debe tener las siguientes características:

- Interface gráfica única para manejar cuentas de usuarios Unix, Windows NT y Netware
- Modelos que permiten armar un registro completo, ingresando la mínima información.
- Posee una facilidad de ubicación centralizada, para una rápida localización del registro de un usuario específico dentro de todo el entorno.

- Permite la administración de información general, así como también información de cuentas Unix, Windows NT y Netware en un solo registro
- No es necesario realizar una carga manual de la información de usuarios, el modulo de administración de usuarios debe permitir tomar la información de usuarios ya creados en cualquier nodo administrado.

Para poder recibir esta información los nodos administrados se suscriben a los perfiles.

La relación entre perfiles, profile managers y nodos administrados se muestra en la Figura

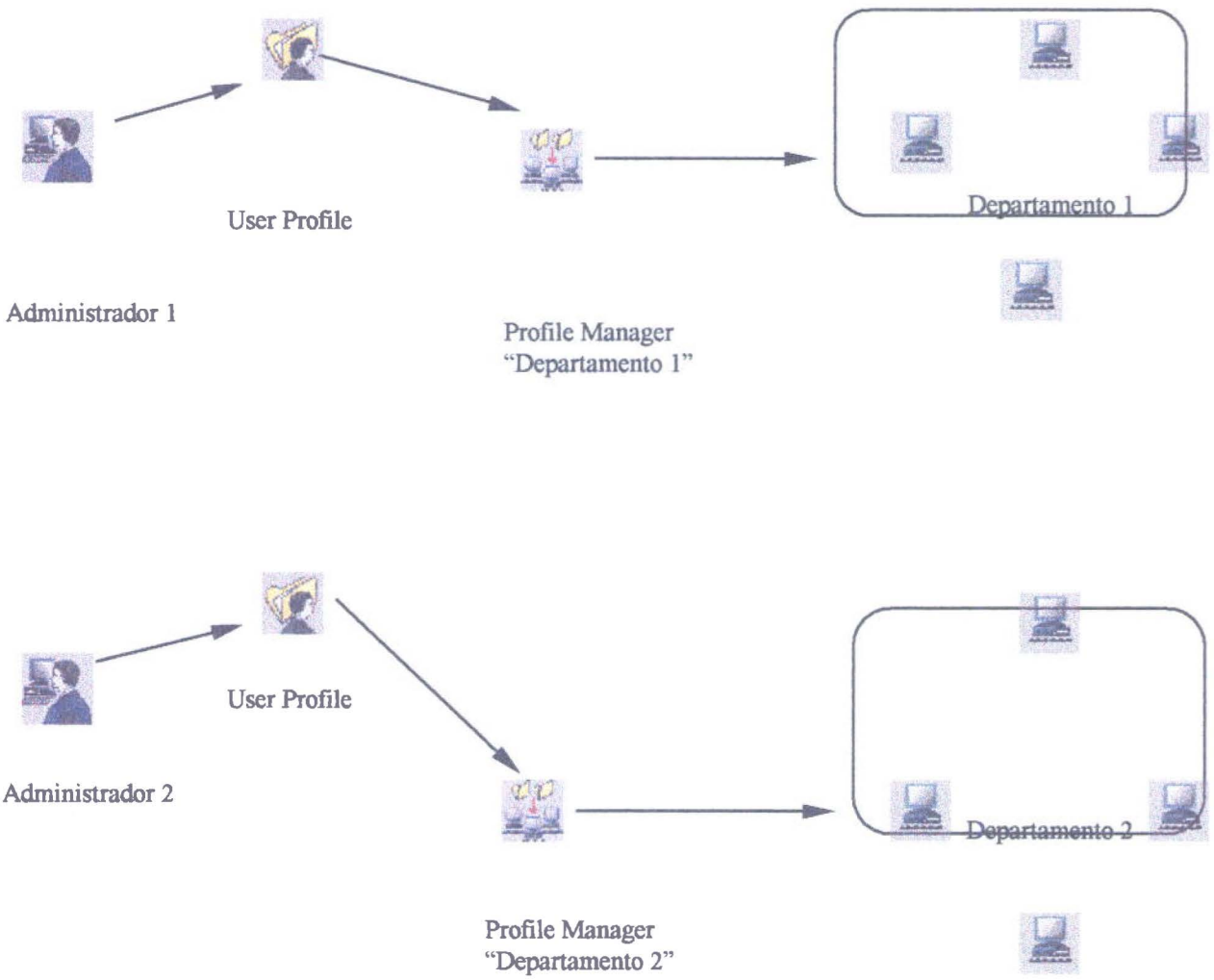


Figura. Relaciones entre usuarios

Inicialmente, se importan los registros de los profiles utilizando la función *populate*, esto permite obtener la información de los archivos de configuración desde los distintos nodos administrados.

CAPITULO IV

ADMINISTRACIÓN DE SEGURIDAD.

El modulo de administración de seguridad debe permitir realizar la administración de seguridad en formar consistente y eficiente a lo largo de toda la empresa. Provee una administración de acceso de los usuarios a los recursos basada en roles, implementación de políticas de seguridad y auditoria.

Administrar la seguridad de los recursos de IT (Information Technology) en Mainframes, Servers y Workstations es crítico para la productividad de una empresa. Esta compleja y cara tarea requiere un conocimiento detallado de los sistemas de seguridad, una amplia variedad de conocimientos y una importante estructura de soporte. Esto es magnificado, cuando existe una gran cantidad de sistemas heterogéneos y distribuidos en toda la empresa. Los resultados de una ausencia de una administración de seguridad son generalmente, seguridad inefectiva, altos costos administrativos, servicio pobre y retrasos en la implementación de nuevas aplicaciones por problemas de seguridad.

El modulo de administración de seguridad junto con el modulo de administración de usuarios debe proveer la solución más completa a este problema, debe proveer una interface única de administración de seguridad. La administración basada en roles simplifica y automatiza la administración de cambios de acceso a los recursos. La instauración de políticas de seguridad se realiza en forma sencilla aunque la implementación de las mismas en cada sistema de seguridad sea diferente. También debe proveer control central de las políticas de auditoría y reglas para el análisis de auditoría. El modulo de administración de seguridad debe mantener un log de auditoría único que para todos los administradores, esto simplifica enormemente el análisis de las acciones de los administradores. El control de la seguridad puede mantenerse de forma centralizada

mientras la administración de seguridad se realiza de manera descentralizada, manteniendo eficazmente los controles de seguridad de la instalación.

El módulo de administración de seguridad proporciona una administración de seguridad centralizada basada en roles, además de integrar los mejores aspectos y funcionalidades.

El modulo de administración de seguridad establece un nivel de seguridad consistente a través de las diversas plataformas de la empresa. Estas capacidades permiten implementar las políticas de seguridad que requieren los negocios críticos.

El objetivo de una política de seguridad es proteger los capitales de una empresa, como los activos, el equipamiento, la seguridad de los empleados y la información.

La información es un capital muy importante dado que la pérdida o alteración de la misma puede provocar situaciones críticas y riesgosas

El modulo de administración de seguridad permite implementar las políticas de seguridad que la empresa considere necesarias y que hayan sido evaluadas y definidas:

- *Estándares:* controles de acceso fisicos (CPUs, LANs, dispositivos de almacenamiento) y lógicos (archivos, bases de datos, programas)
- *Reglas:* control de auditoría, políticas de login, passwords y recursos
- *Procesos:* implementación de estándares
- *Roles* relevantes: Proveedor de servicios (quienes procesan la información), dueño de los datos, auditor, administrador de seguridad, usuario de los datos, etc.
- *Responsabilidades:* asociadas a los distintos roles

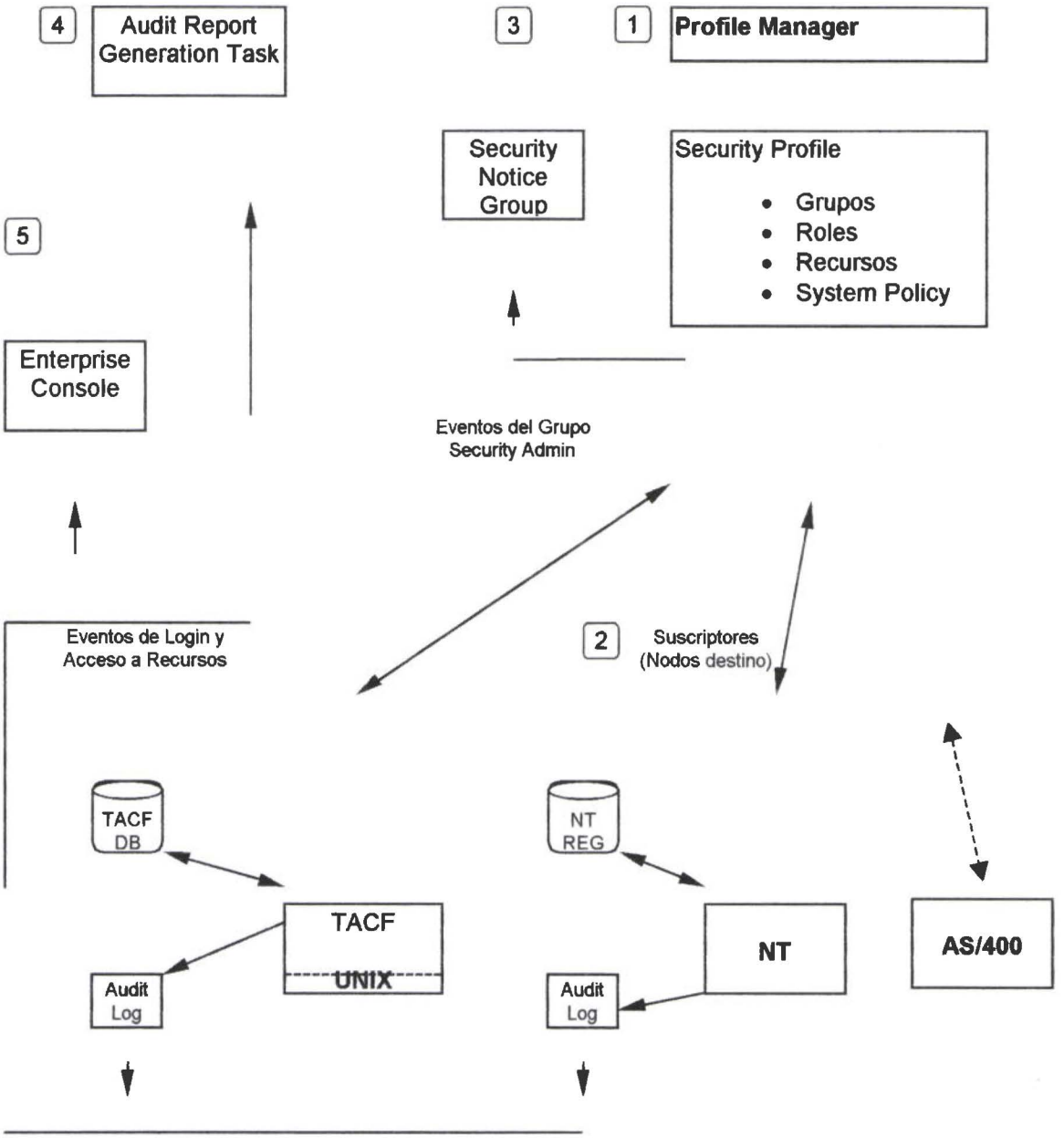
Con el modulo de administración de seguridades se puede:

- Establecer una política de auditoría consistente para sus sistemas

- Controlar todas las operaciones relacionadas con las tareas de administración de seguridad (creación de nuevos perfiles de seguridad, definición de nuevos roles, grupos, recursos o nuevas políticas del sistema)
- Recolectar información relacionada con la seguridad proveniente de distintos puntos y luego generar reportes
- Generar un evento cuando se producen violaciones a la seguridad
- Recolectar los eventos y compararlos con los umbrales definidos y, si exceden los mismos, generar una alerta
- Definir Roles relacionados con las tareas de los usuarios (tipo de acceso a los recursos)
- Definir los Grupos de usuarios que tienen responsabilidades similares dentro de la organización.
- Asociar los usuarios con los grupos y los grupos con los roles

El modulo de administración de seguridad es una aplicación basada en perfiles, por lo tanto, utiliza las características básicas del Framework: *profile managers, suscriptores, distribución, boletines de información, biblioteca de tareas* (Ver Glosario al final de este documento).

La Figura de la página siguiente ilustra la arquitectura y la relación entre los componentes mencionados anteriormente:



Los números de la figura anterior indican, además, las tareas relacionadas con la configuración del entorno de seguridad en la aplicación:

1. Se crean los perfiles de seguridad en el Profile Manager correspondiente.

2. Se suscriben al Profile Manager los nodos a administrar de las redes de la empresa.

- El enlace bidireccional entre el profile manager y los suscriptores indica que los datos fluyen hacia ambas direcciones. Se crean registros dentro de los perfiles de seguridad (y se distribuyen a los nodos destino) y/o los datos se toman (populate) de los nodos destino para llenar los registros de seguridad
- Cada uno de los nodos destino tiene su propio sistema de seguridad (por ejemplo: NT registry y TACF en Unix), en el cual se direcciona la información de seguridad a partir de los perfiles

3. El grupo de Noticias de Seguridad almacena toda la información relacionada con los eventos de seguridad, y los administradores autorizados se informan de la creación o modificación de los registros de seguridad y la distribución de los perfiles.
4. Se ejecutan tareas y jobs (utilizando los servicios de "scheduler" del Framework) sobre nodos destino específicos o sobre los suscriptores (a través del profile manager).
5. Se monitorean eventos específicos provenientes de los log de auditoría de cada nodo destino. Los detalles de estos eventos se rutean a la consola empresarial, donde se toman las acciones correspondientes o se alerta a los operadores cuando se trata de un posible problema de seguridad.

Administración de Acceso a los Recursos basada en Roles

El modelo de administración que utiliza, eleva la administración de acceso a los recursos al nivel de la organización del negocio de la empresa.

El modulo de seguridad enfoca la administración centralizada al acceso seguro, de uno o más usuarios, a los recursos de los sistemas y aplicaciones, donde un usuario puede ser un individuo (grupo que contiene un solo miembro) o un grupo de individuos.

De esta manera se administra grupos (colecciones de usuarios), roles (definen las capacidades necesarias para realizar una función dada) y recursos (a los cuales se proveen derechos de acceso específicos a través de los roles).

Recursos

Los recursos son programas, archivos, sistemas o cualquier otro objeto de la empresa que requiere una protección de acceso común. La definición de un único recurso puede contener uno o más recursos a nivel sistema del mismo tipo (por ejemplo, todos los archivos). Esto permite asignarle un grupo de accesos a través de un rol en lugar de hacerlo con cada recurso en particular.

Roles

La administración de seguridad basada en roles es la clave y proporciona un poderoso y sofisticado mecanismo que facilita, en gran medida, las tareas de administración requeridas para manejar de manera segura el acceso de los usuarios a los recursos de la empresa.Un rol define un conjunto de capacidades requeridas para llevar a cabo una función dada. Una vez que la empresa sigue el modelo de grupos y roles, donde cada grupo tiene capacidades específicas para acceder a uno o más recursos del sistema basado en los roles que se le asignan, la administración de la seguridad puede realizarse casi exclusivamente al nivel de la organización. Los administradores ya no necesitan asignar privilegios de acceso a los recursos para los UserIDs de empleados nuevos dependiendo de las necesidades de sus funciones. Simplemente, se asignan los nuevos empleados a uno o más grupos de la organización definidos previamente.

Grupos

Los grupos son una colección de usuarios en una organización, tales como divisiones, departamentos, equipos de proyectos, etc. Para permitir a los administradores acercarse aún más

al modelo jerárquico de la organización, los grupos contienen otros grupos (por ejemplo, las divisiones contienen departamentos, los departamentos contienen equipos de proyectos, etc.).

El modulo de administración de seguridad se provee a los grupos de las capacidades necesarias asignándoles uno o más roles.

Políticas del Sistema

El modulo de administración de seguridad provee un avanzado mecanismo de administración para las políticas de seguridad de la empresa. Para los servicios de seguridad de los sistemas y aplicaciones, los administradores autorizados especifican las políticas de seguridad para passwords, auditoría, logins, y accesos por *default* a los recursos. Se definen una sola vez, se distribuyen a todos los sistemas y se aplican consistentemente a todos los usuarios. La Figura proporciona una visión conceptual de la relación entre la definición de las políticas, independientemente de los sistemas y, la distribución de esas políticas a los distintos tipos de nodos destino (que tienen sistemas de seguridad propios).

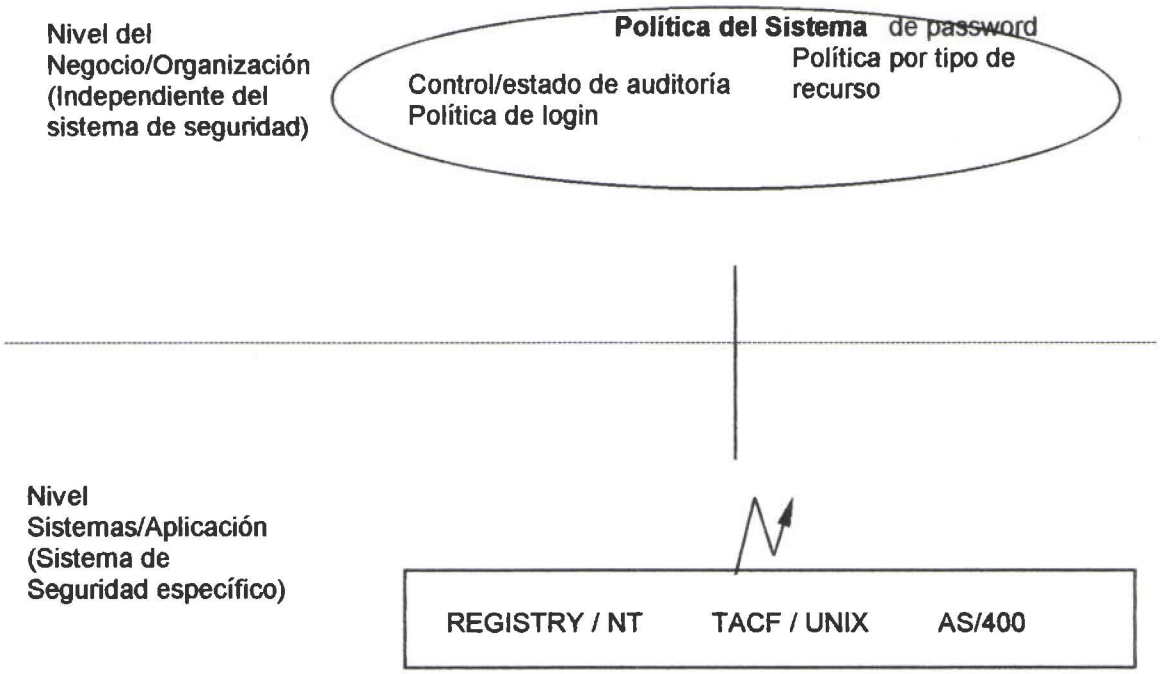


Figura. Visión conceptual de la Administración de Políticas del Sistema

Roles de Autorización.

Toda la administración se basa en la **delegación de autoridad**, para lo cual agrega nuevos roles a la administracíon del entorno que son específicos para la administración de seguridad. Esto permite mayor granularidad al entorno ya que ningún otro Rol del entorno podrá administrar la seguridad de la organización.

Los roles de autorización para administrar componentes de seguridad del entorno son:

- *Security Admin*: asigna autoridad completa para administrar el acceso a los recursos de la organización.
- *Security Auditor*: asigna autoridad completa para auditar el uso de los recursos del sistema y controlar los eventos de seguridad del log de auditoría.
- *Security Operator*: asigna autoridad para listar los datos de los recursos de seguridad y realizar un seguimiento de administración de seguridad de los archivos.

Integración con la Consola Empresarial

El modulo de Administración de Seguridad envía eventos a la Consola Empresarial (ver descripción de este módulo más adelante). Algunos de los eventos del log de auditoría de seguridad que selecciona la Consola Empresarial se resumen a continuación:

- ✓ Logins, exitosos y no exitosos
- ✓ Accesos a archivos, exitosos y no exitosos
- ✓ Archivos que han sido modificados
- ✓ Programas que han sido modificados
- ✓ Conexiones/desconexiones a la red exitosas y no exitosas

Reglas de correlación de eventos:

- ✓ El modulo de administración de seguridad provee reglas de correlación a la Consola Empresarial para determinar relaciones entre eventos y qué acciones tomar.

Tareas del Modulo de Administración de Seguridad

El modulo de administración de seguridad provee una biblioteca de tareas que le permite al administrador ejecutar jobs de servicios de segurirdad sobre uno o múltiples sistemas de seguridad. El administrador puede modificar y personalizar las características de ejecución predeterminadas de cada tarea (output del job, sistema donde se ejecutará el job, si el job va a correr en modo serial en cada sistema, en paralelo en todos los sistemas, etc.). Entre las tareas provistas por la biblioteca se encuentran las siguientes:

- ✓ Configurar el archivo de Log de Auditoría

- ✓ Generar Reportes de Auditoría
- ✓ Generar Reportes del Log de Errores

Configuración del entorno de seguridad

En la definición y configuración del entorno de seguridad están involucrados los siguientes pasos:

1. Se crea el/los *profile managers* que van a contener los perfiles de seguridad (Ver. Figura).

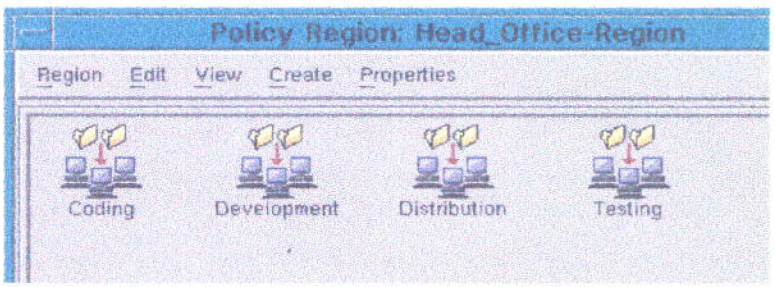


Figura . Profile Managers

2. Se crea el *perfil de seguridad* que va a contener las políticas generales del sistema, los recursos, los roles y los grupos (Ver Figura).

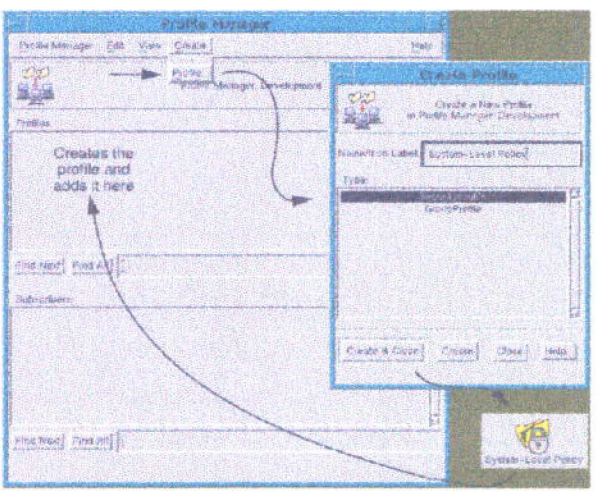


Figura. Perfil para políticas generales del sistema

3. Se definen las políticas generales del sistema en el grupo *"System Policy"* (Ver Figura)

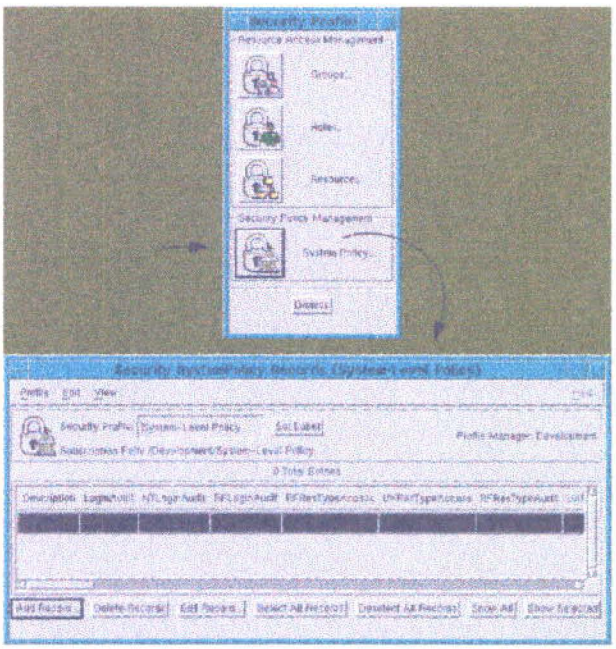
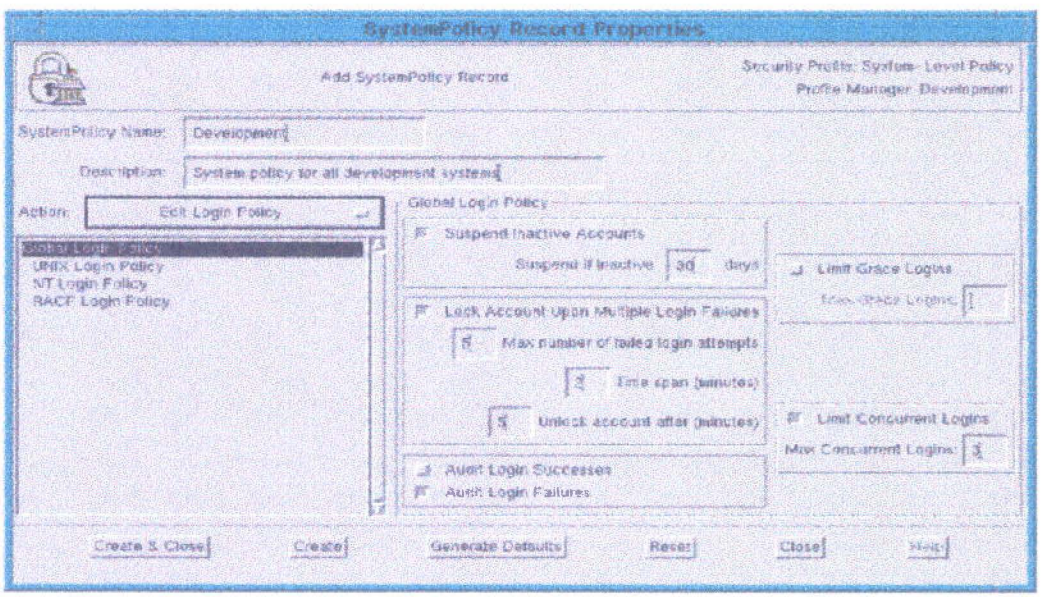
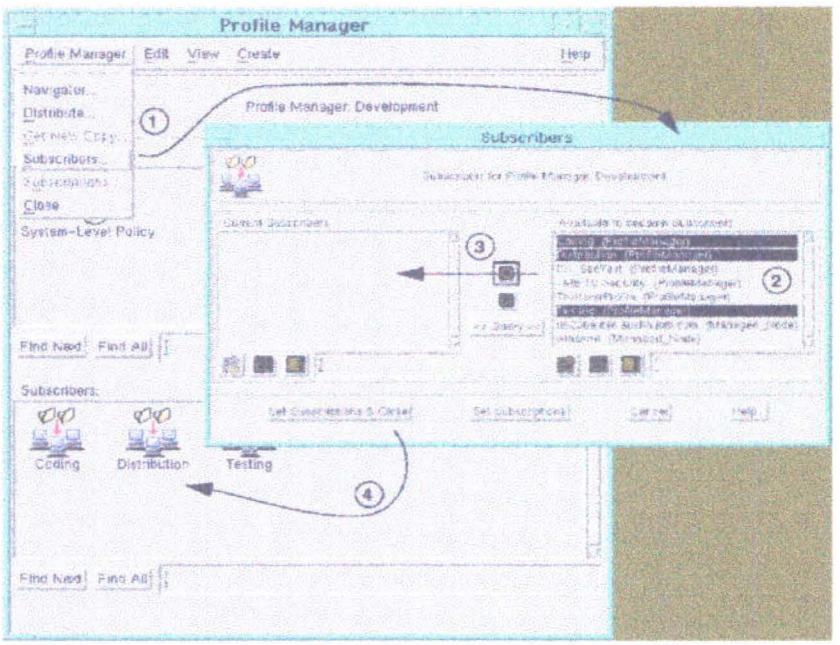


Figura. Políticas del sistema

4. Se agrega una entrada para cada tipo de política a implementar: globales, login, password y auditoría para cada plataforma (a modo de ejemplo ver Figura).



5. Se suscriben los *nodos destino* (o profile managers que contengan nodos destino) a los que deban aplicarse estas políticas generales (ver Figura)



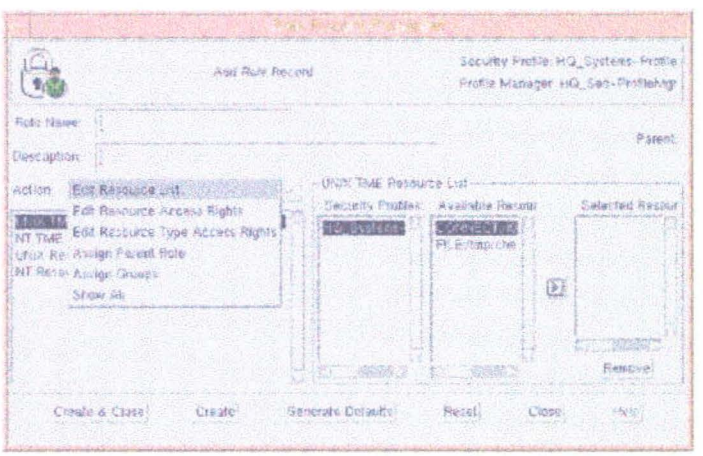


Figura. Suscripción de profile managers al profile manager de seguridad

6. Se definen y se protegen los *Recursos* que forman parte del sistema de seguridad (ver Figura).

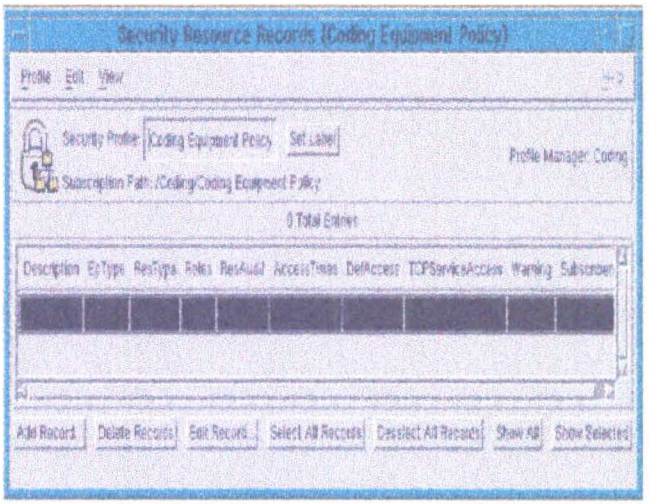


Figura. Crear una política de Recurso

7. Se definen los *Roles* del sistema (a qué recursos de la empresa y con qué permisos pueden acceder los usuarios). Ver Figura

8. Se definen los *Grupos* de seguridad (se agrupan las personas lógicamente según su trabajo o función).

9. Se asocian los *Recursos con* los *Roles* y los *Roles* con los *Grupos* correspondientes.

CAPITULO V

ADMINISTRACION DE DISTRIBUCION DE SOFTWARE

El modulo de Distribución de Software lo ayuda a distribuir y administrar software en una red multiplataforma, incluyendo maquinas UNIX, servidores Netware y PCs corriendo Windows, Windows NT, u OS/2.

El modulo de Distribución de Software ofrece un medio eficiente para la distribución, instalación y control de software en la red. Típicamente los usuarios de un sistema en red mantienen un gran stock de aplicaciones y herramientas de software. El modulo de Distribución de Software debe brindar capacidades para agregar aplicaciones, actualizar software existente con nuevas versiones, sincronizar software en sistemas client/server, etc.

Con la ayuda de este modulo se puede mantener actualizado el software de todos los sistemas en red (máquinas UNIX, sistemas Netware y PCs).

Distribución en Paralelo

Al distribuir copias de software a más de una estación, el modulo de Distribución de Software las debe realizar en paralelo. En lugar de enviar el software a la primer estación, y esperar hasta que esta termine con el proceso de distribución, se debe enviar el software a múltiples estaciones simultáneamente, resultando en una distribución mas veloz.

Inteligencia para WANs

Cuando se realizan distribuciones de software por vínculos de baja velocidad, o en momentos en que un incremento de tráfico en algún enlace puede afectar el rendimiento de sus aplicaciones de red, la aplicación debe permitir limitar este impacto en su red. Usted puede definir:

- A cuantas estaciones se distribuye software simultáneamente

- El máximo de kilobytes por segundo de tráfico a enviar
- Cuantos milisegundos deben transcurrir entre el envío de un paquete de datos y otro (con el fin de evitar picos en la red).

De esta manera el modulo de Distribución de Software le permite controlar y minimizar el impacto de la distribución en su red y a la vez llegar a tiempo con distribuciones urgentes.

Beneficios de utilizar el modulo de Distribucion de Software.

Los beneficios de utilizarlo para distribuir software en los servidores NT, Unix, AS/400 y en las PCs en lugar de usar scripts tradicionales o trasladarse hasta el lugar de la instalación para realizar esta ardua tarea, se describen a continuación:

- **Wan-Smart.** Para las distribuciones que abarcan redes WAN, se incluye una capacidad de "inteligencia en WANs" que reduce el tráfico de la red y asegura una distribución rápida y eficiente. Se envía una única copia del software a distribuir a través del vínculo WAN a una máquina remota y luego se utiliza esta máquina como punto de distribución local. Esto implica un uso mucho más efectivo de la red, que enviar múltiples copias de software a través del vínculo.
- **Capacidades "push" y "pull".** El modulo de Distribución de Software proporciona una herramienta que le permite al usuario final seleccionar el software a instalar según su conveniencia. Para aquellas aplicaciones mandatorias, se especifica en efectivizar la distribución.
- **Distribución en paralelo.** La distribución a múltiples nodos destino, donde no hay vínculos WAN, se realiza simultáneamente y en paralelo.

- **File Packages.** En los servidores NT y Unix (próximamente en AS/400), se mantiene el software actualizado creando "file packages". La máquina desde la cual se distribuyen los file packages es el *source host* para ese file package. Al distribuir un file package desde un único host se elimina la tarea de actualizar el software individualmente sobre cada host suscriptor de la red. Un mismo file package se distribuye a distintos hosts eliminando la posibilidad de utilizar distintas versiones del mismo software.

- **File Packages anidados.** Se utilizan file packages anidados para:

  - ✓ Crear file packages que tienen archivos en más de un source host
  - ✓ Ejecutar programas diferentes antes y después en una misma distribución
  - ✓ Distribuir conjuntos de archivos que tienen propiedades diferentes

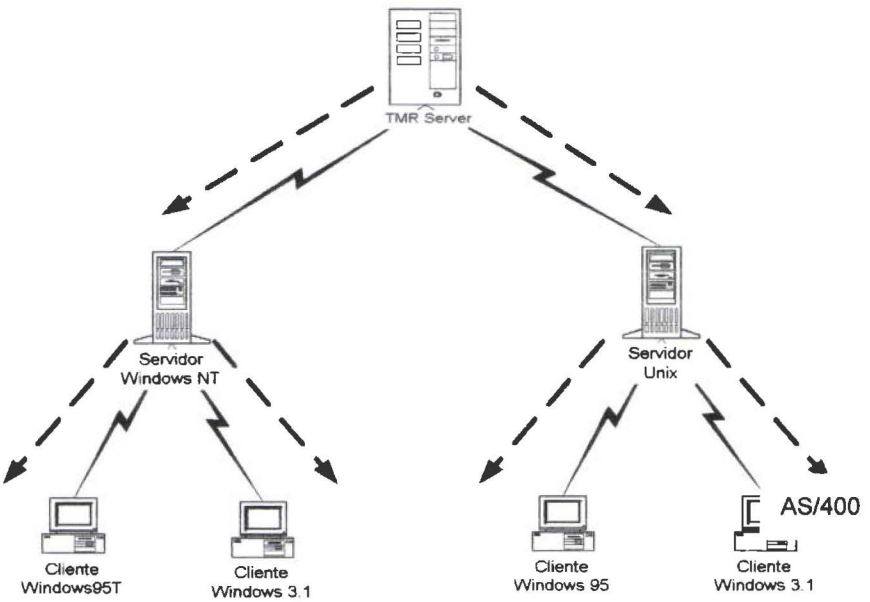
- **Opciones específicas de plataforma.** En la definición de un file package se especifican las opciones propias de cada plataforma relacionadas con la configuración y comportamiento de cada suscriptor.

- **Seguridad.** Para realizar una operación los administradores tienen los roles de autorización correspondientes para las tareas a ejecutar: algunos administradores solo podrán actualizar una aplicación en un grupo de máquinas en particular, otros sólo podrán distribuir software durante ciertas horas, etc.

- **Auditoría.** Este modulo permite conocer:

  - ✓ Si una distribución fue exitosa o si hubo fallas
  - ✓ La hora exacta de las distribuciones exitosas y las causas probables de fallas
  - ✓ Quién pidió la distribución

El modulo de Distribución de Software utiliza funciones genéricas de distribución provistas por el Framework. La topología Multiplexed Distribution (Mdist) permite dejar caer en cascada el flujo de información desde el MR server a los clientes (Ver Figura).



Distribución de Software

Los servidores que actúan como "repeaters" son clientes intermediarios que reciben una única copia de datos y la re-envían a otra estación designada como "repeater" o a su destino final (*endpoints*). De esta manera se realiza una distribución en cascada sobre las estaciones de la empresa.

La máquina que provee el software a distribuir se denomina *source host* y las personas con los niveles de autorización correspondiente son las encargadas de iniciar el proceso de distribución de software desde sus workstations.

Como parte de la distribución, se especifica uno o más de los siguientes tipos de programas a configuración:

- **Programas "Before"**: permiten ejecutar programas antes que el modulo de Distribución de Software ubique los datos descritos en el "file package" en el nodo destino (suscriptor)

- **Programas "After"**: permiten ejecutar programas después que el modulo de Distribución de Software haya ubicado los datos descriptos en el "file package" en el nodo destino (suscriptor)

- **Programas "Removal"**: permiten ejecutar programas antes que el modulo de Distribución de Software borre los datos descriptos en el "file package" en el nodo destino (suscriptor)

- **Programas "After Removal"**: permiten ejecutar programas después que el modulo de Distribución de Software haya borrado los datos descriptos en el "file package" en el nodo destino (suscriptor)

- **Programas "Commit"**: permiten ejecutar programas cuando el modulo de Distribución de Software realiza una operación de "commit" para el file package en el nodo destino (suscriptor). Esto es útil cuando los suscriptores están conectados a redes con vínculos de velocidades diferentes y el administrador de la red quiera que la información a distribuir esté disponible en todos los suscriptores al mismo tiempo. De esta manera, el nuevo software entra en producción una vez que todos los nodos hayan recibido el paquete.

- **Programas 'On Error'**: permiten ejecutar programas si un error detiene una operación de distribución o borrado en el nodo destino (suscriptor)

CAPITULO VI

ADMINISTRACIÓN DE INVENTARIO.

Provee una visión a nivel empresa de los componentes de hardware y software de los servers y clientes en todo el ambiente distribuido. Es una solución única para el descubrimiento automático y seguimiento de las configuraciones de software a través del ambiente, incluyendo aplicaciones desarrolladas internamente o adquiridas.

El modulo de administración de Inventario permite a los administradores de sistemas ejecutar, mediante una interfaz gráfica, Queries poderosos para identificar los servers y clientes apropiados para la distribución de software. Soportado en la base de datos relacional de su elección (Sybase, Oracle, DB2/6000 o MS-SQL Server), el diseño jerárquico ofrece escalabilidad así como una vista integrada de los componentes interdependientes de la aplicación.

Tiene que basarce en una tecnología licenciada de Intel, de esta forma su capacidad de autodescubrimiento automáticamente localiza hardware, software e información de configuración de estaciones y servidores PCs y Unix.

El modulo de administración de Inventario almacena información localmente en los servidores y clientes en el formato standard DMI MIF. Así puede trabajar con todas las estaciones DMI-compliant que se encuentren en su entorno, llevando esta información extra al repositorio de inventario.

El modulo de administración de Inventario es un componente crítico para las empresas que quieren utilizar la información de inventario como input para el proceso de distribución de software o para reforzar las políticas de configuración en los servers y estaciones de trabajo. Asimismo, al proveer información vital sobre el hardware y software del entorno, permite evaluar

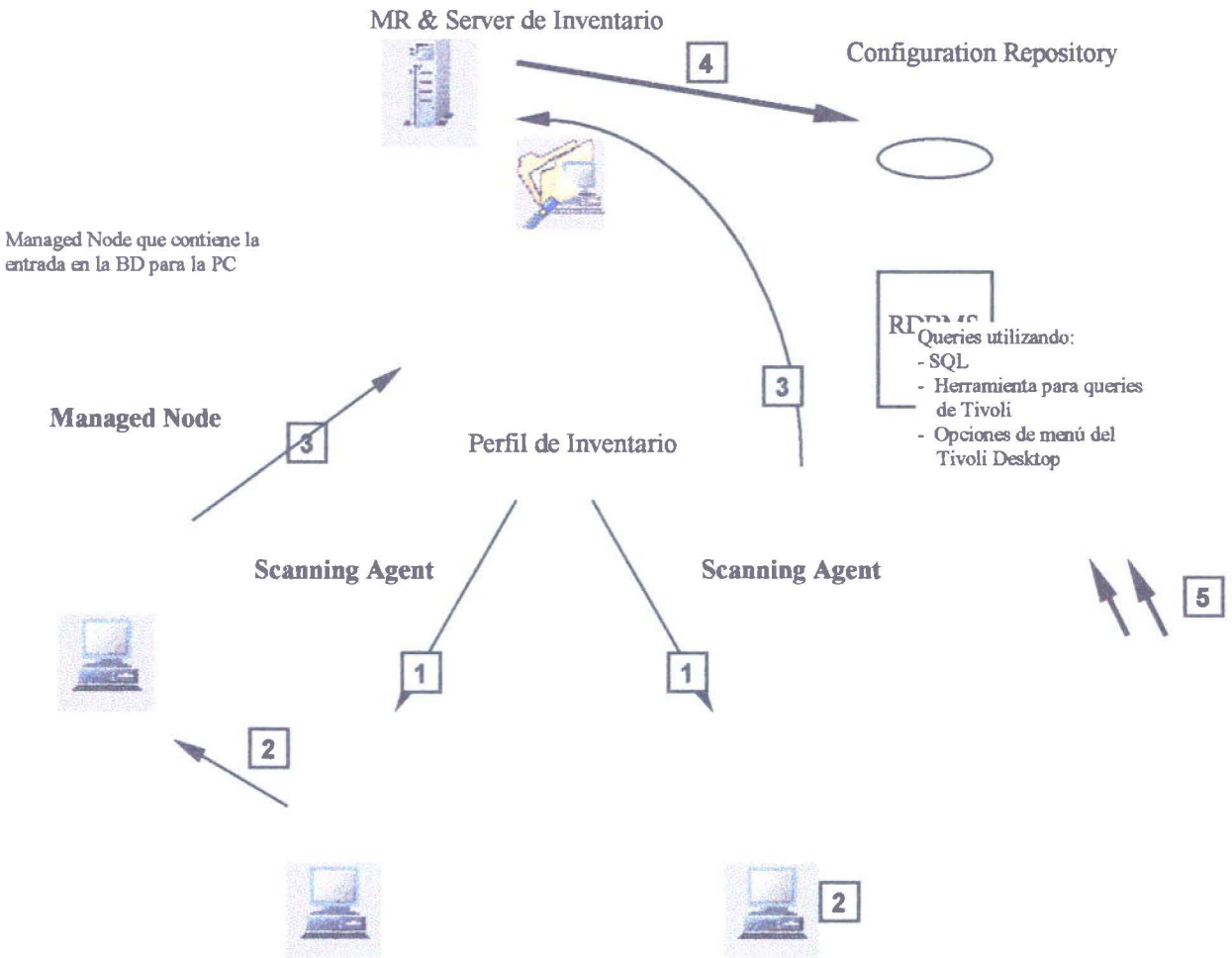
y tomar acción sobre reemplazos que se deban encontrar para evitar problemas asociados con el cambio de milenio.

El modulo de Administración de Inventario es una aplicación de administración centralizada que busca el hardware y software instalado en equipos de arquitectura Intel, Unix y AS/400, y almacena dicha información en una base de datos centralizada. Los componentes principales son:

- **Inventory Server:** porción del modulo de Administración de Inventario que se ejecuta en el servidor (MR). Es donde se definen los perfiles que contienen las instrucciones para "escanear" los sistemas.
- **PC scanning agent:** componente que se ejecuta en las Pcs (como es el caso de las estaciones Windows 95) y es quien realiza la búsqueda de hardware/software instalado y archivos de configuración en las PCs.
- **Managed node:** es el representante (o "sponsor") de una o más PCs (que ejecutan el agente) y donde se guardan los archivos de configuración.
- **Configuration repository:** lugar donde residen las tablas, allí se almacena toda la información de inventario. Es una base de datos relacional (Oracle 7, Sybase 10, DB2, Informix, MS SQL).

El flujo de información entre los componentes de la aplicación de inventario involucra los siguientes pasos básicos:

Figura. Flujo de información de modulo de Administración de Inventario



1. Se crea un perfil en el servidor con las instrucciones correspondientes para el relevamiento del inventario. Luego se distribuye a sus suscriptores.

2. Se almacenan los datos de inventario en un archivo con formato standard ASCII MIF (Management Information Format). Los agentes de PC envían su información de inventario (archivo MIF) y sus archivos de configuración a su "managed node" asociado.

3. Cuando el "managed node" recibe de los agentes los archivos de configuración de PC, los almacena en su base de datos local en formato Revision Control System (RCS). Luego la información de inventario se envía al servidor MR.

4. El servidor de inventario acumula toda la información de los suscriptores, la convierte en formato de base de datos standard, y la almacena en el "repositorio" de configuración, el cual es una Base de Datos Relacional (RDB).

5. Se pueden realizar consultas de distinto tipo sobre la RDB y/o utilizar los queries provistos con el producto.

La información de inventario que se obtiene pertenece a las siguientes categorías:

- ID del componente
- Conexiones IPX LAN
- Procesador
- Coprocesador
- Recursos del sistema
- Puertos
- Memoria
- Dispositivos de almacenamiento
- Drives lógicos
- Sistema Operativo
- IPX LAN
- Entorno
- Device drivers
- Archivos de configuración

CAPITULO VII

MONITOREO DISTRIBUIDO

El modulo de monitoreo distribuido es una herramienta diseñada para el monitoreo de recursos de sistemas y la generación de eventos y alarmas. Como todas las aplicaciones para administración debe funcionar en un entorno distribuido, en una variedad de plataformas.

El modulo de monitoreo distribuido, monitorea el status de una gran variedad de recursos, como máquinas, aplicaciones y procesos.

Mediante el uso de perfiles, este modulo debe permitir que los administradores de sistemas alteren los parámetros de monitoreo, para cualquier número de sistemas remotos relacionados, mediante una única acción. Los perfiles también definen respuestas automatizadas. Estas respuestas pueden incluir cambiar el status de un icono, abrir una ventana de alerta en el escritorio de un administrador, enviarle un e-mail, o ejecutar un procedimiento de recuperación remoto o local.

El modulo de monitoreo distribuido debe poseer componentes que brinden las siguientes funciones:

- El motor de monitoreo. El programa cliente se instala como un servicio adicional del framework en cada nodo administrado que va a ser monitoreado en forma directa. Dicho motor es el responsable de determinar si el monitor debe ser gatillado, crear un calendario con los monitores que se deben ejecutar y evaluar las respuestas de los mismos con respecto de los valores obtenidos con anterioridad para determinar que acciones se deben tomar.
- Colecciones de monitoreo. Una colección de monitoreo contiene el código que define como se recolecta información sobre un recurso. Una colección también fija parámetros que determinan como se interpreta la información obtenida. Todas las capacidades de monitoreo

se encuentran definidas en diversas colecciones de monitoreo que agrupan en forma lógica los mas de 2000 monitores disponibles.

Mecanismo de Configuración Centralizada

El modulo de monitoreo distribuido debe proveer un mecanismo de configuración centralizada para la distribución de fuentes de monitoreo para monitorear cualquier recurso disponible en entornos Windows NT, Netware o UNIX. Esto incluye dispositivos fisicos, dispositivos lógicos, aplicaciones, intentos de acceso y otras actividades. Una vez configurados los recursos y actividades a monitorear, la aplicación automáticamente realiza decisiones distribuidas y acciones remotas sin intervención necesaria de los administradores.

Recolección de Datos / Respuesta Automatizada

El modulo de monitoreo distribuido le otorga la capacidad de recolectar información específica de su entorno que no este contemplada dentro de las colecciones de monitoreo. Si se puede acceder a información mediante un comando o script, este modulo puede recolectar dicha información, realizar decisiones remotas inteligentes basadas en esa información, y responder automáticamente.

Políticas para el Monitoreo distribuido.

Cada región o segmento de la red puede tener sus propias políticas de monitoreo para administrar los diferentes recurso de la red antes de lo cual se pueden configurar dichos seteos.

Para cada tipo de configuración se van a crear diferentes archivos llamados profiles con características específicas de configuración. El administrador de la red debe ser el encargado de disenar y crear diferentes profiles dependiendo de las necesidades de la red.

Para mantener una presentación más adecuada de los resultados se cran unos indicadores de colecciones los cuales se pueden asociar a los profiles para de esta manera agrupar la mayor cantidad de políticas de cada región en cada indicador de colección.

Presentacion grafica del monitoreo distribuido.

Una de la grandes facilidades que tiene el usar un software de administración es las ventajas de la representación gráfica, para lo cual se pueden presentar diferentes tipos de representaciones gráficas de los eventos que están sucediendo en la red.

El modulo de Monitoreo Distribuido provee las herramientas fundamentales para monitorear los recursos o eventos sobre un conjunto arbitrario de nodos administrados y disparar acciones basadas en el estado del nodo administrado. Los componentes principales que permiten estas funciones son los siguientes:

- **Sentry engine:** Proceso que se ejecuta en cada nodo administrado y controla y supervisa los recursos según se defina. Determina cuándo disparar el monitor y cuándo ejecutar respuestas automáticamente. El motor de modulo de Monitoreo Distribuido se ejecuta de manera autónoma en cada sistema monitoreado.

- **Monitoring Collections:** Conjunto de fuentes de monitoreo. Una fuente de monitoreo representa un aspecto específico de un sistema que puede ser monitoreado (ej. Porcentaje de espacio en disco utilizado).

- **Monitor:** Es un *registro* de un *perfil* Sentry. Es una entidad que monitorea, en los intervalos especificados, un aspecto específico de un recurso. Su definición contiene múltiples valores para cada umbral y el curso de acción a tomar al alcanzar dicho umbral. Los monitores se distribuyen a los "Sentry engines" de los nodos administrados a través de los perfiles Sentry.

- **Indicator collection:** Proporciona una ventana que contiene indicadores y alertas de estado de los monitores.

- **Indicator:** Reside en una colección de indicadores y permite visualizar gráficamente el estado de los perfiles Sentry asociados a él. Hay cinco niveles de severidad: Normal, Advertencia, Severo, Crítico y Fatal.

A continuación se ilustra la interacción entre el MR Server y los Sentry engines.

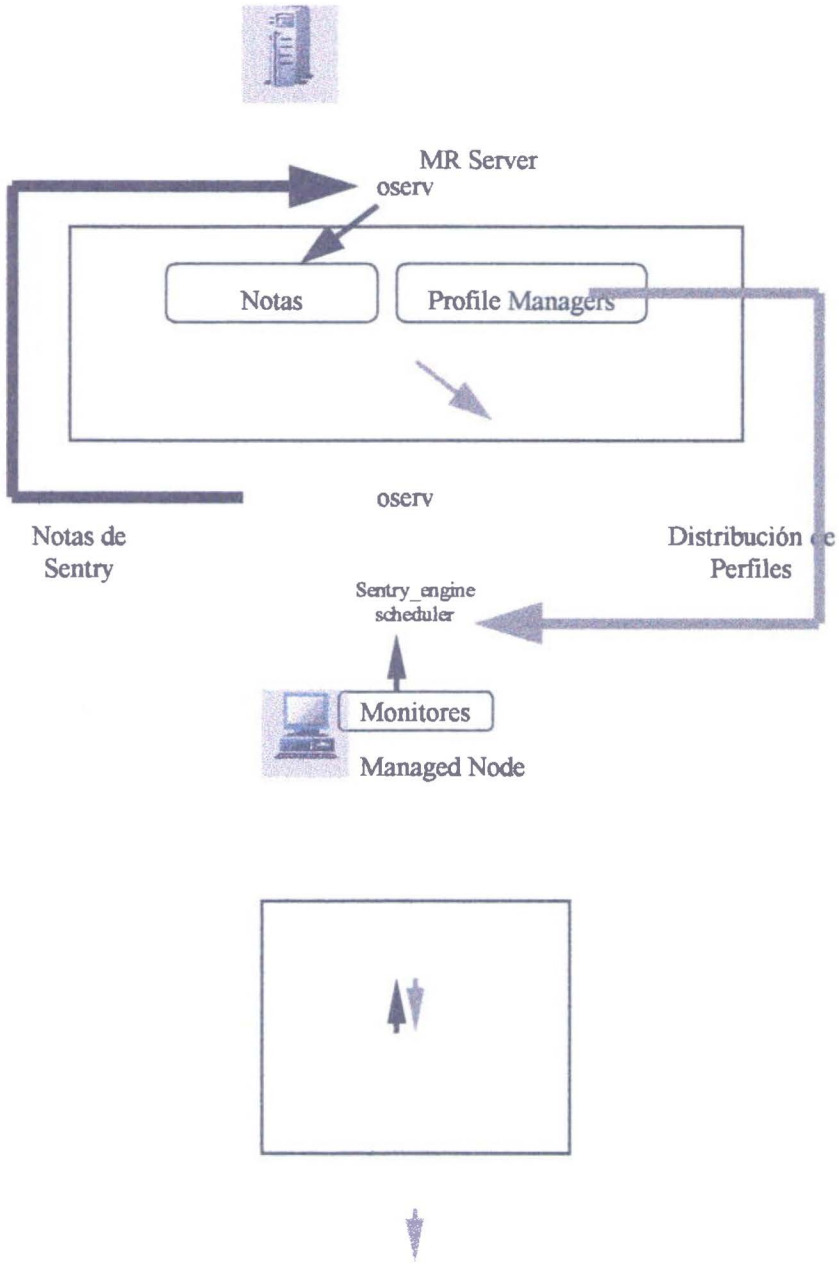


Figura . Configuración interna de modulo de Monitoreo Distribuido

CAPITULO VIII

CONSOLA EMPRESARIAL

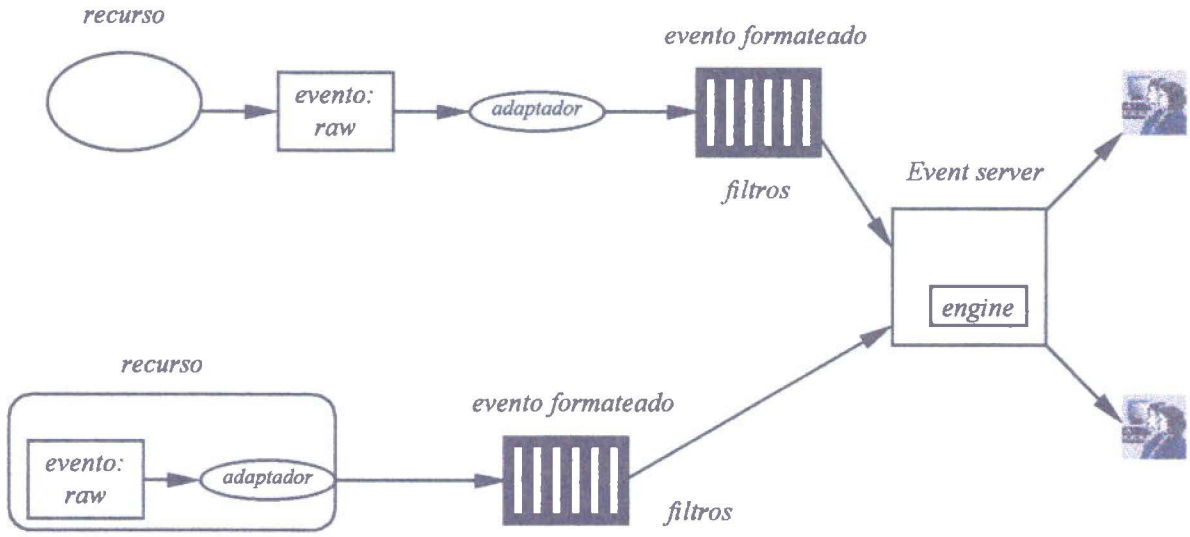
La Consola Empresarial es una herramienta de administración que ayuda a mantener la disponibilidad de los recursos de la red, sistemas, aplicaciones y bases de datos. Provee un punto de control centralizado para la recepción y correlación de eventos. Posee la habilidad de integrar *eventos* provenientes de cualquier fuente de información importante.

Procesa los eventos a través de un conjunto de *reglas.*

La Consola Empresarial ayuda a reducir la complejidad de la administración actuando como punto central de mensajes y alarmas provenientes de las redes, sistemas y aplicaciones. Los eventos se clasifican en grupos que los administradores de sistemas consideren relevantes para la empresa, los que se visualizan en las consolas de cada uno de ellos. Los administradores le definen un conjunto de respuestas que corrigen automáticamente ciertos problemas de rutina, lo que les permite dedicarse a responder los problemas más críticos y relevantes.

Los componentes principales de Consola Empresarial son los siguientes:

- **Evento:** es la unidad mínima de información, e indica el estado de un componente.



- **Event Adapter:** es un programa que transforma la información que recibe para enviarla al servidor de eventos. Figura. Configuración de la Consola Empresarial.
- **Event Server:** Es el responsable de la recepción de todos los eventos. Crea un registro en la base de datos para cada evento entrante, luego lo evalúa según un conjunto de reglas, y determina la acción a tomar. Ver Figura
- **Event Console:** Interfase gráfica que permite al administrador visualizar y responder a los eventos. Permite tener distintas vistas de los eventos dependiendo de la función. Está representado por un ícono en el desktop.

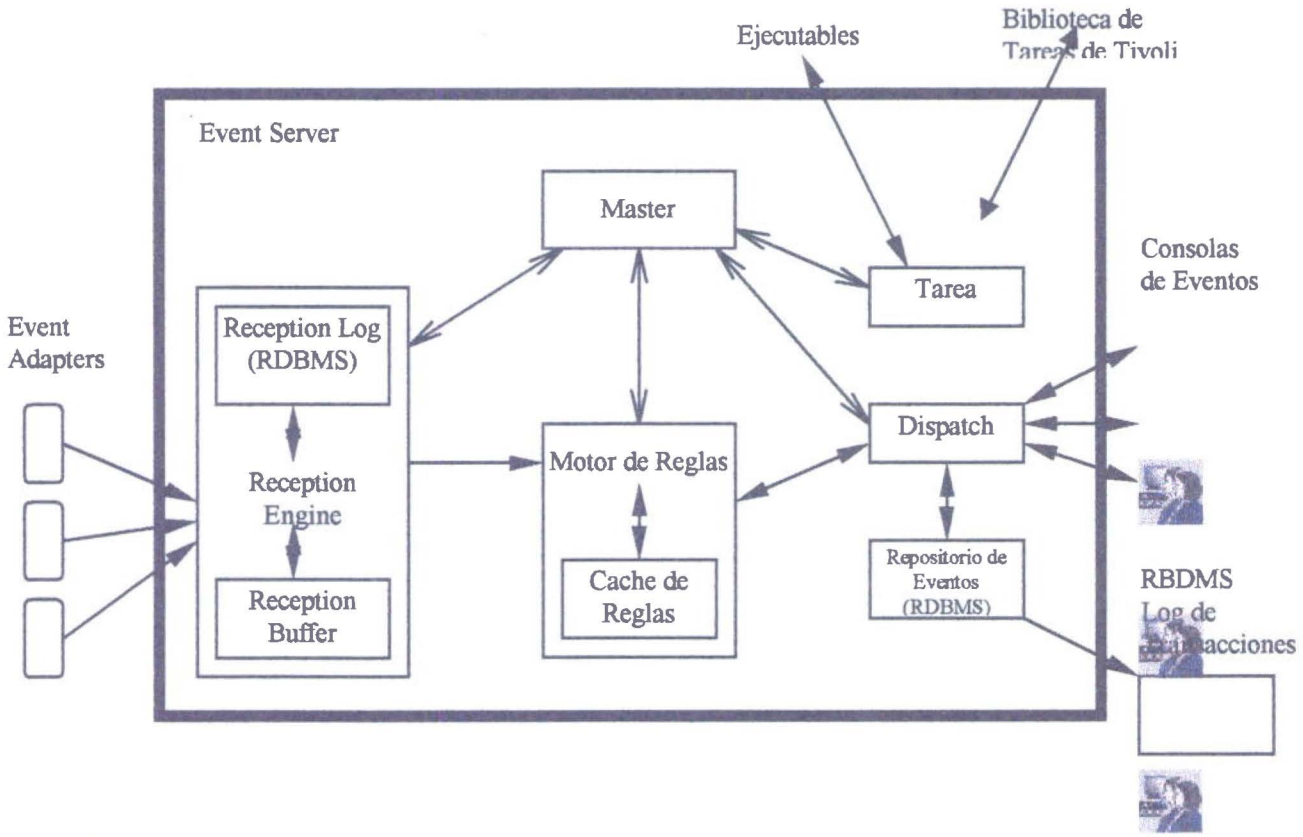


Figura. Componentes internos de la Consola Empresarial

Entre los eventos que acepta la Consola Empresarial se incluyen los siguientes:

- **Network:** Informa sobre la infraestructura de conexión física y lógica del entorno distribuido
- **System:** Informa sobre los estados de hardware, sistema operativo y servicios de red de los sistemas
- **Performance:** Informa sobre las medidas de performance de sistemas y aplicaciones
- **Database:** Informa sobre el estado de bases de datos relacionales
- **Application:** Informa sobre el estado de aplicaciones críticas de negocio

CAPITULO IX

CONTROL REMOTO

Control Remoto es el primer producto en su tipo diseñado para manejar sistemas empresariales completos. Esto significa control remoto en tiempo real, la capacidad de establecer conexiones rápidamente donde puede haber miles de potenciales recursos objetivos, la habilidad de controlar no sólo los desktop sino también aplicaciones distribuidas en distintas plataformas y una administración de gran seguridad que protege en contra de abusos.

De esta forma el Control Remoto permite:

- soportar a miles de usuarios desktop,
- mejorar la cantidad de problemas resueltos al primer llamado,
- reducir la cantidad de despacho de técnicos,
- asegurar el éxito cuando los técnicos son despachados debido a un mejor diagnóstico previo,
- ahorrar tiempo ocioso entre fallas gracias a una reparación más rápida, y
- reducir los llamados repetitivos permitiendo una mejor educación de usuarios.

Control completo en tiempo real

Control Remoto provee control de los sistemas que se desean administrar tanto sobre una red de área local (LAN) o extendida (WAN). La herramienta entrega un menú para iniciación remota, incluyendo un grupo seleccionado combinaciones de teclas, las cuales pueden ser realizadas en la estación administradora. Las combinaciones de teclas que pueden ser transmitidas a través del menú incluyen "Ctrl+Alt+Del", "Alt+Esc", "Alt+Tab" y "Ctrl+Esc".

Rápida conexión al nodo correcto

Una solución de control remoto para toda una empresa debe proveer facilidades que permitan una rápida conexión al nodo que se desea administrar. Para hacer esto posible, el modulo de Control Remoto provee un listado de búsqueda con los nombres de los sistemas a ser controlados, el que se actualiza automáticamente. Las sesiones se establecen simplemente tecleando sobre el nodo deseado. Adicionalmente, para asegurar que la conexión es posible, es auto-instalable a través del ambiente de administración.

Optimizado para aplicaciones distribuidas

En una gran empresa, las aplicaciones de negocio críticas están típicamente distribuidas a través de una serie de diferentes sistemas. El modulo de Control Remoto permite administrar aplicaciones distribuidas claves, no solo a estaciones de trabajo individuales. Dos capacidades claves que se ofrecen simultáneamente son:

Primero, puede no sólo controlar estaciones de trabajo sino también servidores Windows NT y OS/2 y **Segundo**, provee la capacidad de mantener múltiples sesiones de control simultáneas sobre una misma consola administradora.

Los administradores pueden moverse fácilmente entre las ventanas de control o tener ventanas Telnet por medio de un producto Telnet de terceros o una emulación de terminal para servidores corporativos.

Procedimientos basados en autorizaciones

El uso de tecnología de control remoto en una gran empresa sólo es posible cuando existen mecanismos para prevenir las violaciones de seguridad. La seguridad del usuario final controlado, dejado de lado en la mayoría de las implementaciones de sistemas de control remoto, tiene un diseño líder especialmente para detectar intrusos en grandes instalaciones. Control Remoto ofrece una exclusiva facilidad que permite administración de IT por medio de un procedimiento

previamente determinado, el cual define los nodos a los cuales se tiene acceso y los permisos que tienen asignados. El Framework de administración fuerza estas políticas. Control Remoto ofrece delegación de autoridad basada también en políticas de procedimientos. Los nodos que deseen ser administrados son agrupados en Policy Regions. de esta forma se le asignan roles a cada uno de los administradores, los cuales pueden incluir la capacidad de "control" y "reboot".

Para proteger más allá en contra de las violaciones de seguridad, los usuarios finales pueden ser consultados si permiten que tomen el control de su estación y pueden recuperar ese control en cualquier momento. Este modulo está desarrollado con componentes de software separados para el "controlador" y el "controlado", lo que reduce dramáticamente el número de puntos de entrada en la red. Se ha utilizado tecnología de encriptación para asegurar que la estación administradora pueda sólo ser ejecutada dentro del ambiente de administración. Además una conexión log es mantenida para proveer una auditoría de las conexiones remotas.

En grandes corporaciones, los administradores deben resolver problemas que surgen en PCs que están ubicadas fisicamente lejos de sus oficinas (en otro piso, edificio o ciudad). A veces los problemas pueden resolverse telefónicamente, pero muchas veces se requiere el traslado del administrador hacia el lugar del inconveniente, provocando demoras y pérdida de tiempo al usuario final.

Control Remoto permite al administrador tomar control del teclado y mouse visualizando en pantalla lo que está ocurriendo en una PC remota. Además, el administrador puede monitorear la PC y dejar que el usuario repita los pasos que causaron el error.

El siguiente diagrama ilustra el entorno de Control Remoto:

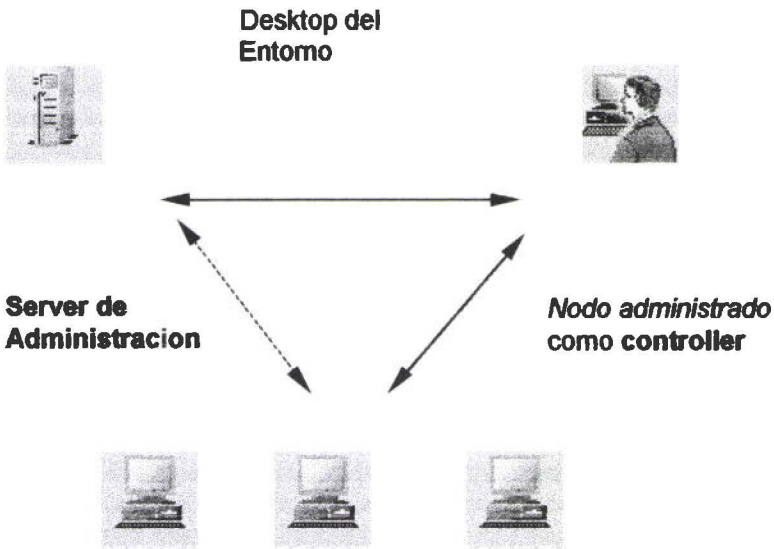


Figura Entorno de Control Remoto

CAPITULO X

ADMINISTRACION DE APLICACIONES.

Cuando se desarrollan aplicaciones propias, generalmente no se tiene en cuenta cómo se van a operar y a administrar las mismas en el entorno de producción. El personal de soporte desconoce el ciclo de vida completo de la aplicación. El personal de operaciones, no puede hacer el deployment eficiente de las aplicaciones a través de toda la empresa, teniendo en cuenta las múltiples plataformas y dependencias que generalmente están asociadas con las aplicaciones del entorno distribuido. También se observa que los operadores no saben cómo monitorear apropiadamente la aplicación para asegurar su disponibilidad.

Tradicionalmente, el equipo que desarrolla o integra la aplicación es el responsable del soporte completo de la aplicación. Desarrollan, prueban e instalan la aplicación, entrenan a los usuarios y por lo general se convierten en el soporte de nivel 2.

Se puede mejorar la administración de las aplicaciones, según las siguientes prácticas recomendadas:

- **Enlazar formalmente los procesos de implementación de la aplicación entre los grupos de desarrollo y de operaciones**. Un deployment eficiente requiere una manera estándard para especificar los paquetes de instalación con las correspondientes dependencias entre los distintos componentes de la aplicación. Los desarrolladores, generalmente son quienes mejor conocen como monitorear la aplicación para asegurar su disponibilidad y mejorar el tiempo de respuesta ante eventuales anomalías

- **Desarrollar políticas y tareas para la administración de las aplicaciones**. Esto incluye un conjunto de políticas y roles que aseguran que las tareas operativas correctas sean ejecutadas por el operador apropiado y autorizado.

- **Proveer un conjunto abierto de API's para la comunicación entre los datos de management y que puedan ser interpretados por el sistema de Administración**.

* Ver Apéndice A para más información.

CAPITULO XI

CONSOLA EMPRESARIAL

Una de las mayores prioridades del departamento de Information Technology (IT) a cargo de la administración de entornos de computación distribuidos es asegurar que los problemas sean manejados de una manera eficiente y a tiempo. También es una responsabilidad esencial del grupo de IT asegurar la alta disponibilidad de las aplicaciones que corren en este entorno.

La Consola Empresarial provee las herramientas para manejar problemas dentro de un entorno de computación distribuido (DCE).

La unidad central de información dentro de la Consola Empresarial es el evento. Un evento es cualquier cambio significativo en el estado de un recurso del sistema o de una aplicación. Un evento puede indicar que un host dejó de estar operativo, el intento no autorizado de conexión a un host como usuario root o un disco rígido a punto de llenarse. La consola Empresarial acepta virtualmente cualquier tipo de evento, incluyendo los siguientes:

Tipo de evento	**Descripción**
Network	Informa sobre la infraestructura de conexión fisica y lógica del entorno distribuido.
System	Informa sobre los estados de hardware, sistema operativo y servicios de red de los sistemas en la red.
Performance	Informa sobre las medidas de performance de sistemas y aplicaciones.

Database	Informa sobre el estado de bases de datos relacionales y otras.
Application	Informa sobre el estado de aplicaciones críticas para el negocio.

Como cada tipo de evento incluye muchos eventos diferentes, el grupo de IT debe evaluar:

- Cuáles son los eventos más importantes para manejar
- Cómo deben ser manejados estos eventos
- Que eventos debería ver cada operador

La Consola Empresarial utiliza reglas para realizar la correlación de eventos ayudando al personal de IT en la determinación de la severidad y relación de los distintos eventos. La Consola Empresarial también permite a los responsables del grupo de IT asignar la responsabilidad de diferentes eventos a diferentes operadores. Esta característica ayuda al grupo de IT a evitar problemas tales como sobrecarga de información y duplicación de esfuerzo entre los operadores.

La Consola Empresarial también brinda respuesta automática a muchos eventos comunes. Por ejemplo, si un disco duro alcanza la marca de un 80% completo, este modulo puede borrar automáticamente archivos de logging que no sean esenciales para ayudar a asegurar que haya espacio disponible en el disco cuando se necesite salvar una gran cantidad de datos. Al proveer un sistema de administración proactivo, la Consola Empresarial puede resolver problemas mas rápidamente y el grupo de IT estará disponible para trabajar en problemas más críticos que requieran alguna forma de intervención del operador.

Componentes de La Consola Empresarial. La Consola Empresarial utiliza event adapters para recolectar información, un server de eventos central para procesar la información y consolas de eventos para presentar la información al grupo de IT.

Los event adapters son procesos que residen típicamente en el mismo host que la fuente administrada. Una fuente es una aplicación (como una base de datos) o un recurso del sistema (como espacio en disco disponible). Cuando un adaptador de eventos recibe información desde su fuente la direcciona al server de eventos correspondiente. Un adaptador puede ser configurado para descartar eventos inocuos seleccionados en lugar de enviarlos al server de eventos, reduciendo el tráfico de la red.

El server de eventos es un server central que maneja todos los eventos de los sistemas distribuidos. El server de eventos crea una entrada en la base de datos relacional para cada evento entrante. Luego evalúa estos eventos contra un conjunto de reglas para determinar si puede responder o modificar el evento automáticamente. Finalmente actualiza la consola de eventos con la información actualizada. Si se requiere intervención humana, el server notifica al usuario correspondiente. Este usuario realiza la tarea requerida y notifica al server de eventos cuando la condición que generó el evento ha sido rectificada

Las consolas de eventos brindan una interface gráfica de usuario (GUI) que permite al grupo de IT visualizar y responder los eventos recibidos. El responsable de la administración puede configurar múltiples consolas de eventos basadas en las responsabilidades del grupo de IT. Los usuarios pueden tener vistas de estos eventos en forma independiente o compartida.

Glosario

- **Object Request Broker (ORB):** proceso que corre en el TMR server y en todos los nodos administrados.
- **Base de datos distribuida y orientada a objetos:** cada Servidor de Objetos almacena información sobre los objetos del entorno ME en una base de datos propia orientada a objetos.
- **ME Desktop:** interfase gráfica que permite el acceso a todas las aplicaciones.
- **Policies:** políticas o reglas a las que están sujetas todas las operaciones del entorno ME.
- **Resource o Managed resources:** representación en el entorno ME de los elementos reales de la empresa, tangibles (ej. Computadora) o intangibles (ej. Política).
- **Profiles:** una colección de información específica que puede ser manejada y distribuida a las máquinas del entorno ME.
- **Profile Manager:** contenedor de perfiles que los enlaza con otros Resources a modo de suscriptores. Puede contener más de un perfil de igual tipo o diferente.
- **Subscribers:** Resources que representan el destino final (*endpoint*) de un perfil o profile manager.
- **Management by subscription:** concepto que implica administrar recursos creando un conjunto de perfiles y distribuirlos, a través de profile managers, a múltiples Subscribers u otros Profile Managers actuando como listas de distribución.
- **Policy Region:** conjunto de recursos administrados (*managed resources*) que comparten las mismas reglas.
- **Policy Subregion:** una policy region que reside dentro de otra policy region.

- **Roles de las máquinas:**
  - ✓ *TMR server:* máquina que ejecuta el software y la base de datos necesaria para administrar los clientes. Cada TMR tiene un TMR server, el cual almacena objetos y código ejecutable que sus suscriptores puedan requerirle; adicionalmente es el encargado de autenticar y validar todas la operaciones que se deseen realizar sobre sus clientes.
  - ✓ *ME clients:* estaciones que ejecutan el software para poder interactuar con el server y con otros clientes.
- **Administrador:** persona en quien, mediante roles de autorización, se delegan responsabilidades de administración sobre recursos específicos del sistema.

CONCLUSIONES

Al finalizar el desarrollo del tema planteado para el presente trabajo, se pueden establecer las siguientes conclusiones.

Debido al cambio que esta sufriendo la computación en red es cada vez más necesaria una correcta administración de los recursos que se encuentran en la red debido a que estos pueden ser de diferentes arquitecturas, plataformas y por supuesto de diferentes proveedores.

Sin una adecuada administración, el hecho de realizar rutinas de calendarización de procesos, iniciar y monitorear tareas, resetear colas de impresión, calendarizar backups, compresión de datos, así como administrar el espacio en disco de diferentes equipos y diferentes localidades, se ha vuelto casi imposible a menos que se realice una movilización de recursos que realicen este tipo de trabajo.

Es lógico que cada marca tenga su especial modo de administración lo cual provoca la necesidad de una serie de conocimientos por parte del personal de sistemas, encadenando esto una serie de gastos extras para la empresa, por lo cual, es indispensable él ir estableciendo políticas de trabajo es decir estándares en los procesos de administración por ejemplo, establecer una política de usuarios ayudaría a tener un mayor control sobre el tipo de usuarios y evitar la repetición de claves etc.

Por esto el trabajo de administración de redes se lo ha considerado como muy complejo, limitando en muchas ocasiones el implementar soluciones informáticas que mejoren el rendimiento de una empresa.

Además de establecer esta serie de políticas es fundamental el contar con una herramienta de administración (Software) que colabore con toda esta planificación es decir, esta herramienta debe cumplir con una serie de características que ayuden de forma eficiente en la labor de administración, debe ser una aplicación que de forma centralizada administre la totalidad de la red, esto implica que la administración de diferentes plataformas y arquitecturas debe ser transparente para el usuario evitando de esta forma la necesidad de tener un especialista para cada plataforma.

El poder realizar la administración desde un sitio centralizado implica la reducción de costos de movilización de personal y de recursos en general para de esta forma permitir a la organización un mejor aprovechamiento de sus recursos.

REFERENCIAS

- Redes LAN y de Area Extensa (Prentice Hall)
- Tivoli Framework (Publicación de IBM Corporation)
- Tivoli Enterprise Console (Publicación de IBM Corporation)
- NetView (Publicación de IBM Corporation)
- Security Management (Publicación de IBM Corporation)
- Software Distribution (Publicación de IBM Corporation)
- Revistas Técnicas
- Internet (www.ibm.networking.com)
- Network Computing (Publicación de IBM Corporation)

Apéndice A: Applications Management Specification

Address Application Complexity and Uniqueness

Client/server applications typically consist of several distinct, heterogenous components. In addition, every client/server application may be different in structure. To effectively manage such applications, it is essential that the application manager have access to information describing the application architecture and layout. The AMS facilitates the transfer of knowledge from the application provider to the application manager.

The centerpiece of AMS is the specification of the format and contents of Application Description Files (ADFs). Each client/server application can provide its own set of ADFs. The ADFs act as a bridge between the application provider and a management application by describing in a standard way the management information associated with a particular application. This management information describes elements of the entire application life cycle, including the initial deployment of the application, configuration of the various deployed components, monitoring and controlling the running application, and updating systems with new versions of the application.

Provide a Lightweight and Flexible Solution.

The AMS can be applied to all classes of distributed applications, ranging from commercial software to in-house development. AMS puts a minimal burden on application providers to make their applications *management ready*, while establishing an open framework that management tools can both provide and use to effectively manage applications. Supporting AMS does not require that applications be substantially modified, re-linked or re-compiled. The process of making an application management ready can be done by the original application developer or by a third-party developer after the application is developed.

Support Existing Standards.

The ADF format is based on the Management Information Format (MIF) as specified by the Desktop Management Task Force (DMTF). ADF files are DMTF-compliant MIF files. The ADF specification expands the existing Software Standard MIF, taking it from single-desktop software management to distributed, client/server applications management.

Compliance with the DMTF enables an easy integration with management environments that support the DMTF Desktop Management Interface (DMI). On the other hand, AMS can just as easily be used in environments that do not use DMI, as it does not require DMI. AMS is also neutral with respect to other existing management protocols (for example, SNMP).

Enable Application Deployment.

The AMS enables application providers to notify administrators of how an application should be distributed and installed on a variety of platforms and for a variety of application functions (for example, client components and server components). The component description files are also used to declare the software and hardware dependencies that must be met by the target systems in a production environment before the application can be successfully deployed.

Enable Application Monitoring.

The AMS specifies a way for application providers to notify administrators of what statuses, metrics, or events it offers that can be monitored. The application provider can also specify how this information can be accessed or retrieved by management tools.

Support Application-Specific Management Tasks

The AMS specifies a way for application providers to notify administrators of what operational tasks can be run against the application components. These tasks might include starting, re-starting, or stopping an application server, or backing up application databases.

Apéndice B: Tivoli Implementation Methodology

The Tivoli Implementation Methodology (TIM) consists of documents, guidelines, templates, and tools that assist with the planning, management, and deployment of the Tivoli Management Environment (ME) family of products at one or more customer locations. It is used by consultants in the Tivoli Professional Services (TPS) and IBM Global Services (IGS) organizations, as well as certified and approved Business Partners.

Tivoli has designed the TIM to be a full-cycle process that covers the Sales,Concept, Planning, Deployment (Development), Quality, Launch, and Life Cycle Phases of a Tivoli Deployment project. When using the TIM, the consultant determines the customer's Information Technology process strategy, gathers the customer's high and low-level detailed requirements, creates the project plan documents, develops the architecture and system design, develops deployment plans, and aids with the actual deployment of the products at the customer's site.

Throughout the entire project, the Project Manager manages and monitors the progression of the deployment using documents and plans developed through the TIM.

The TIM documents, guidelines, tools, and templates were developed by a team of consultants, with representatives from Tivoli Headquarters, Tivoli Strategic Alliances, Tivoli Sales, and Tivoli Professional Services. It has been sanctioned by management and includes the key elements often covered in Tivoli's best proposals.

NOTE: Both the Tivoli Consultant and the customer should remember that since Tivoli products are highly customizable and every customer is unique, each document, guideline, tool, and template should be tailored to match the customer's specific environment. The documentation is inherently linear, but customer situations are never that way due to the myriad of circumstances that can influence the environment. The Tivoli Consultant and the customer must work together to determine specific customer requirements and needs during each phase of TIM.

The ultimate goal is a successful implementation of the Tivoli Implementation Project, as defined as being on schedule, within budget, and to the customer's specifications.

Employ sound judgement, experience, and discretion when using the TIM and it will be a very valuable contributor to a successful deployment.

TIM Key Benefits

TIM Provides Accelerated Deployments: TIM enables accelerated deployments and reduces the time required to deliver Tivoli benefits to the customer. The documentation, templates, and tools that make up the TIM are designed to reduce the time to deployment for customers and professional services groups.

TIM Captures "Best of Breed" Tivoli Intellectual Capital: TIM captures years of Tivoli architecture and deployment experience available in the Tivoli organization, providing access to best of breed methods and practices.

TIM is the Standard Methodology: Specific versions of the TIM are available to Tivoli Professional Services, certified and approved Business Partners, and certified and approved current Tivoli customers. It provides an industry-wide, best of breed methodology and delivers market confidence in the ability to deploy enterprise-wide solutions.

Guidelines for Using TIM

The TIM contains a massive amount of documentation and information that is logically divided into Phases, Segments, Tasks, and Steps. These correspond to their respective entries in the TIM to help guide you through the entire process.

Phases are the underlying time-oriented divisions of a project and reflect the progress of a project from pre-sales to project completion. In each phase, it is possible that each Segment has some activity that occurs during that timeframe.

Segments are the major divisions of the document. Each segment involves a major undertaking or phase in the process, has clear inputs, and yields definitive deliverables. They are documented in a linear two-dimensional

fashion, but since all the segments are interrelated, you will find that you are frequently cross-referencing between segments in a three-dimensionalfashion throughout the entire project. Segments can span Phases.

Tasks are necessary sub-units of a Segment. A high-level process chart shows dependencies between the Tasks and an implied order in which they should be completed. Various Tasks may be omitted at a particular customer site, depending upon the local conditions.

Steps break down the work into even smaller units. Not all Tasks will be broken down to this degree, but long and complicated ones benefit from the clarity of this additional level of granularity. Steps are especially useful in the Deployment Segments.

If you are viewing the TIM online, there are options available on the TIM Home Page to download all or selected files. Files are either "documentation" files or "attachment" files. Attachments are files containing templates you can edit, or that have additional information, or that are examples. You can view selected Segments by clicking on the icon box in the TIM charts. From the TIM Home Page, you can also view the files in sequence or by alphabetical order. "View list of Files in Sequential Order" shows a list of all the Segments and their accompanying documents, in the logical order in which they appear in the TIM. "View List of Files in Alphabetical Order" is self-explanatory. The documentation files are all in HTML format, for online viewing. To print those, view them from an internet browser and print them out.

As stated above, the TIM is to be used as a set of guidelines, but there is no substitute for experience when investigating the requirements for a customer. The purpose of the templates is not to provide a standard files where the names can be changed and a final copy printed. They provide descriptions of major elements in a "basic" implementation. Each document should be closely examined to determine if it meets the client's objectives and what customizations are required. Each document is not intended to be "all-inclusive." However, templates will reduce the amount of time required to generate quality documents, allowing consultants time to focus on the more complex issues.

Overview

The TIM is a logical sequence of project phases and segments that cover all the tasks of a project, from the pre-sales activities to the actual product deployment steps.

The underlying phases of a project are Sales, Concept, Planning, Development (Design and Deployment), Quality, Launch, and Life Cycle. The Sales Phase is handled by the salesperson, who quickly gathers high-level information about the customer and their requirements, and gives that information to the Tivoli Consultant for analysis. The next phase is the Concept Phase, in which high level an detailed requirements gathering is done. The purpose in this phase is to determine if the customer can benefit from a Tivoli deployment, and to get information to start an architecture and specific recommendations. In the Planning Phase, both project deliverables, such as the Statement of Work and Project Timelines, and the System Design and Architecture document, are produced and agreed upon. Then the Development Phase begins with Detailed Design and actual Deployment (installation and configuration) of the Tivoli products. The next phase, Quality, is very important, and preparation for this phase in made early on in a project. During the deployment and before the final launch to the customer, the consultants must verify that the deployment meets the customers objectives by conducting a series of tests. After that, in the Launch Phase, the customer receives a document describing the Tivoli environment, and consultants archive project documentation for future reference.

During the Life Cycle Phase, the customer is on their own, relying upon Tivoli Customer Support for assistance.

Each segment has clearly defined inputs and deliverables. Some segments span multiple Project Phases and overlap other segments. Many interact concurrently.

The TIM Overview chart (on the TIM Home Page and in this file) shows the overall project timeline and primary deliverables of each segment. Segment 0000, Information Technology (IT) Process Assessment, starts in the Sales Phase, and continues throughout the project. Segment 1000 is done during the Sales and Concept Phases. Segment 2000, Project Management, covers the entire timeline of the project starting with Concept, but its major focus starts after the sale is made and continues until the project is completed. Segment 3000 starts during the concept and continues through the Development-Design Phase. Segment 4000, Architecture and Detailed Design, actually gets started in the Sales Phase and concludes (in theory) just prior to the Quality Phase. Segment 9000, Quality Assurance, is the primary focus of the Quality Phase, but it needs to be started early in a project. It is conceivable

that the order and range for any segment could vary in various situations. Each segment has one or more definitive deliverables that determine the activities done within the segment.

The following sections present an overview to all the segments of the Tivoli Implementation Methodology.

Segment 0000: Information Technology Strategy Assessment

Understanding the Customer's Information Technology (IT) structure and systems management processes are key steps in the development of a Tivoli architecture and ultimately a successful Tivoli deployment. For this reason Segment 0000 should be used by consultants to help bridge the gap between Process, Organization and Technology. Technology is defined for the purpose of this Segment as ME applications, as well as any other applications with which the Tivoli solution many need to integrate. Some companies, such as IBM Consulting and some 10/Plus Business Partners, help other companies with corporate process and organizational re-engineering. Tivoli does not perform such services at this time. However, it is beneficial to the project if the consultants understand the level of information technology strategy that Tivoli's customers have developed.

Process changes can drive organizational changes, which can drive technology changes, or technology changes can drive process and organizational changes, or organization changes can drive process or technology changes. It is important to keep these relationships in mind when working with customers regardless of the technology. It is especially important with a Tivoli Solution due to Tivoli's special ability to be highly customizable to fit the customer's organization and processes.

Without a clear understanding of the customer's technology, organization and processes, the Tivoli solution will not deliver to its full potential.

Major Input

Needs Analysis Document

Interviews with the Customer

Major Output

Information Technology Organization, Policies, and Systems Management

Process Summary

Segment 1000: Pre-Sales Project Planning

When the Tivoli consultant is called in to assist in an implementation, the first major deliverable is to provide technical and cost proposals for the work to be performed.

In a set of formal meetings with the customer staff, sales engineers (SEs) interview the customers to determine their requirements and working environment. They also do a risk assessment, to determine the possible pitfalls in the potential project. Based on this information gathering, the SEs determine the Tivoli products that are to be deployed. The SE also completes the "Request for Tivoli Deployment Proposal" form, summarizing the recommendations as well as the names of key contacts. The Request form and the interview forms are submitted to the consultants. The consultants evaluate the information and begin to formulate the Project Proposals, which include both the Technical Proposal and Cost Estimates. The consultant meets with the customer and they agree upon a suggested timeline and sequence of events that will lead to a successful solution for the customer. These elements are estimated and detailed for the customer in a formal proposal. This defines the consultant's understanding of the business and technical issues to be solved at the customer's sites, the products to be delivered, the resources of both the consultants and the customer required for the installations, and the approximate timeframes.

The project proposals give the customers an idea of the amount of effort required to deploy the distributed system management products in their environment. This effort is usually done as a pre-sales activity, and as such is very short in duration. It is impossible at this phase to determine all of the detailed requirements that will be addressed in the implementation. For this reason only estimates can be made for the effort required to deploy the products. These estimates are based on experience with deploying the product in hundreds of customer sites, and are usually within a reasonable range of the actual effort required. Once the detailed deployment plans, including the Statement of Work, are complete, the customer will have a plan that will detail the exact amount of effort required. The consultant staff, in conjunction with customer personnel, perform the actual deployment of the products.

Major Input

Request for Tivoli Deployment Proposal

Sales and SE Interviews

Tivoli Customer Survey

Tivoli Customer Interviews

Major Output

Technical Proposal

Signed Cost Proposal

Pre-work Checklist

Segment 2000: Project Management

The intent of this Segment is to aid the Project Manager and implementers in achieving a long term referenceable account deployment. It is assumed that the Project Manager is trained in the basic rudiments of Project Management. It is ideal if the person is a Certified Project Manager. This segment highlights the key project management principles that are often neglected under the usual time pressures of production schedules. Primarily, Project Management does not occur at any one point in time of a project, but it is an on-going and pervasive activity. This segment establishes the roles of all personnel involved in the deployment of the products. The responsible personnel should clearly be defined, and the levels of escalation should also be well understood. The responsible personnel should have the complete authority to sign off on deployment and design decisions throughout the life of the project. These issues must be made clear at the project launch meeting.

The roles of project management and reporting mechanisms should be clearly defined in the project launch meeting as well. Each of these responsibilities will be critical as new plans are developed and agreed to. The customers and Tivoli will both be signing off on the plans, and the plans will be the binding agreement as to what will be deployed. The establishment of clear responsibilities will make dispute resolution much easier during the course of the project.

Project Validation

Once the Project Manager is assigned the project, the following steps should be the initial ones taken to validate the project. At this stage all issues, concerns about the project should be addressed, i.e. not enough hours in the contract, problems with the technical solution, etc. This is the Project Manager's "day in court". Beyond this point the Project Manager is now accountable for the project. The Project Manager must do the following:

Read and evaluate the Technical and Cost Proposals Is the work effort (scope) realistic and achievable? Are the deliverables clearly defined? Is the solution technically sound?

Consult with:

Systems assurance

Proposal team

Sales/account team

Write the Statement of Work and Project Task Plan. At this point, the answer should be "yes" to the following questions:

Is the scope clearly defined?

Is the estimate reasonable?

Is the schedule realistic?

Is the project profitable?

Determine customer's expectation and reset as necessary.

Elements of a Successful Project

The successful development of a Tivoli system will depend on these basic elements:

Use of proven project management techniques

A sound, disciplined approach, with a detailed statement of work

Participation by a team of dedicated data processing professionals that possess the skills required for the development of this system

The key attributes of a successful project are that the project completes on time, that it stays within budget, and that a quality product results which satisfies the client. The successful completion of any project depends upon the careful execution of a well structured and detailed plan for each of the major components of a project.

While planning is one of the most important responsibilities of the project manager, there are other activities that also must be performed. This segment offers examples and suggestions to aid in these activities and should be considered and applied as necessary to the unique situation. Enhancements and additions are always welcome as each project teaches us more about our customer's needs and expectations.

Major Input

Information Technology Strategy

Customer Surveys and Interview forms

Technical Proposal

Cost Proposal

Major Output

Customer enrolls in training classes

Common understandings of the project objectives, roles, and responsibilities.

Statement of Work (SOW)

Project Task Plan (tasks, resources, timeline)

Project Deployment Summary

Project Status Reports (weekly, monthly)

A successful project, as defined as:

Complying with specifications

Meeting the schedules

Staying within the budget

Segment 3000: Detailed Requirements Gathering

The Detailed Requirements Gathering Segment of TIM is when you really get into the nitty-gritty of the Tivoli deployment requirements. It is a series of product-specific interviews with key customer personnel to identify all the detailed requirements and configuration parameters for deploying Tivoli products in the customer's environment. It is the logical extension of Segment 1000 and is intended to discover information that was too detailed for the initial phases of the project.

The consultant will spend several weeks individually interviewing the customer's personnel. In these interviews, the customers must be open and honest about their problems and their objectives for the automation of their software environment. The interviews are ME Framework, ME Region, and product-oriented, and focus on the concepts familiar to the customer. The objective of this phase is to obtain enough raw information to complete the next segment of TIM, the detailed architectural design.

The questionnaires define, in detail, all of the configuration parameters, such as Tivoli Management Regions (TMRs), Policy Regions, Administrators, ProfileManagers, Profiles, Distributed Monitoring Monitors, Software Distribution File Packages, User Definitions, and more. Tivoli consultants use the forms to provide the customers with the details of what will be configured and how. These worksheets are also used to supply information to later Segments in order to configure the products.

Major Input

Signed Proposal for Tivoli Deployment

Prior Interviews with customers

Major Output

Completed detailed questionnaires for the entire customer environment, including the framework, network, and products.

A detailed description and logical picture of the customer's environment

A sense for the customer's requirements, phasing,and high-level goals

Segment 4000: Architecture and Detailed Design

The Architecture and Detailed Design Segment is primarily active during the Technical Phase of the project. By now the customer and the consultants have identified the objectives and key people involved in the project. They

have also gathered detailed information about the customer site. The interviews in the previous Segment are used to document a detailed System

Design and Architecture document.

The purpose of this segment is to design a high-level architecture for the project, followed by an Architecture and System Design for the customer's entire Tivoli environment. This will be carefully documented so that everyone understands what is to be deployed.

Another very important activity in this segment, which can be done during either the Sales, Concept, or Planning Phases, is the determination and ordering of the hardware and software that will be required for this project. The determination is based on the early high-level design. This is necessary so that the right equipment will be ready when the deployment begins. The customer can decide whether to order systems for just the test lab or for the entire rollout.

Segment 4000 is critical in that it assures a good customer understanding of the entire process. It also makes the subsequent Segments go much more smoothly.

Major Input

Considerations for Hardware Decision

Project Management Documents

Signed Proposal for Tivoli Deployment

Interviews with customers to define the detailed requirements

Major Output

Hardware and Software Recommendations

Purchase Orders for Server Hardware

Detailed System Design and Architecture Document, which describes the way the Tivoli implementation will look

Customer attends training now, if not done earlier Deployment worksheets are completed in preparation for configuration

Segments 5000-8000: Products Deployment

The Products Deployment Segments are essentially product-specific how-to documents. They also sometimes contain automated installation and configuration scripts and tools to help facilitate the deployment. These Segments detail all of the steps that are necessary to deploy the products, based on the information that Segments 3000 and 4000 provide.

These Segments make the connection between the logical concepts and the real products. They use information from the worksheets to configure the products, thus removing much possible human error from the actual population of the objects that are specific to the customer's environments.

These Segments can be very long and detailed, but as consultants become more familiar with the entire methodology, their need to refer to these Segments diminishes. As Tivoli adds new products to its product line, the methodology will be expanded to include them, and these Segments will be the how-to manuals for smooth deployment of the new products.

Major Input

Project Management Deliverables

System Design and Architecture Document

Detailed Product and Framework Questionnaires

Completed Deployment Spreadsheets

Major Output

Fully Deployed Installation and Configuration of the Tivoli Products Fully Tested Deployment

Segment 9000: Quality Assurance

The Quality Assurance Segment is possibly the most important segment of all. Without this segment, the consultant is gambling with the quality of the entire deployment. The primary goal of this segment is to be able to verify that the consultants successfully deployed what they planned to deploy, according to the Statement of Work document. This segment starts early on in a project with the writing of test plans and designing of deployment test labs. This is especially important for complicated and geographically disperse deployments. With carefully designed, written, and executed test scenarios and test cases, the goal of satisfied customers is more likely to be achieved.

Major Input

Project Management Deliverables

System Design and Architecture Document

Completed Deployment Spreadsheets

Major Output

Test Plans, Test Scenarios, Test Cases

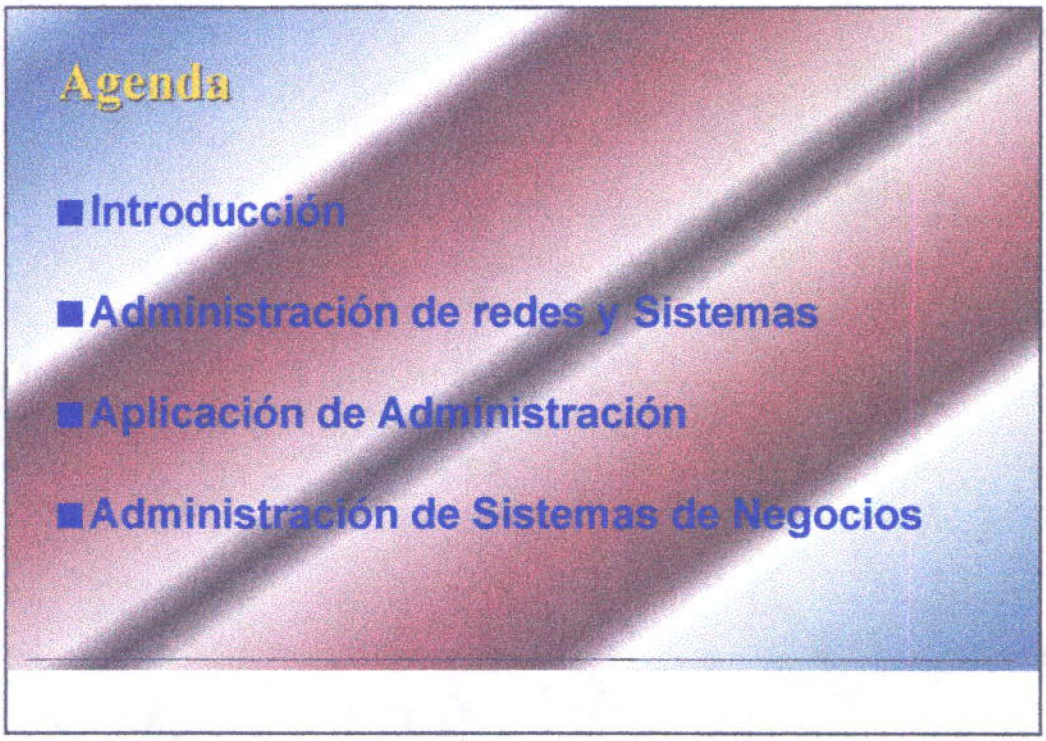
Fully Tested and Quality Deployment

Summary

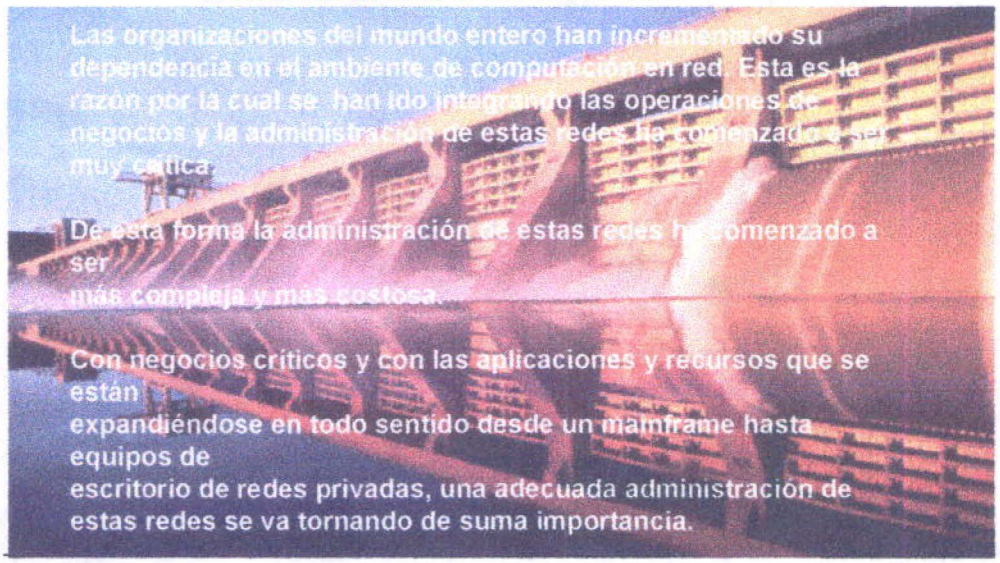
The TIM is a logical sequence of project phases and segments that cover the pre-sales activities to the actual product deployment steps. Each segment has clearly defined inputs and deliverables. Some segments overlap and interact concurrently.

The TIM Overview chart (on the TIM Home Page and in this file) shows the overall timeline and deliverables of each segment. Segment 0000, Information Technology (IT) Process Assessment, starts in the Sales Phase, and continues throughout the project. Segment 1000 is done during the Sales and Concept Phases. Segment 2000, Project Management, covers the entire timeline of the project starting with Concept, but its major focus starts after the sale is made and continues until the project is completed. Segment 3000 starts during the concept and continues through the Development-Design Phase. Segment 4000, Architecture and Detailed Design, actually gets started in the Sales Phase and concludes (in theory) just prior to the Quality Phase. Segment 9000, Quality Assurance, is the primary focus of the Quality Phase, but it needs to be started early in a project. It is conceivable that the order and range for any segment could vary in various situations. Each segment has one or more definitive deliverables that determine the activities done within the segment.b


Geographically dispersed sites
Heterogeneous Environments
PRINCIPIOS BASICOS Y HERRAMIENTAS
para la
ADMINISTRACION DE REDES
Thousands of events and alerts
Host + Distributed Networks


Agenda
Introducción
Administración de redes y Sistemas
Aplicación de Administración
Administración de Sistemas de Negocios

Introducción ....



Las organizaciones del mundo entero han incrementado su dependencia en el ambiente de computación en red. Esta es la razón por la cual se han ido integrando las operaciones de negocios y la administración de estas redes ha comenzado a ser muy crítica.

De esta forma la administración de estas redes ha comenzado a ser
más compleja y mas costosa.

Con negocios críticos y con las aplicaciones y recursos que se están
expandiéndose en todo sentido desde un mainframe hasta equipos de
escritorio de redes privadas, una adecuada administración de estas redes se va tornando de suma importancia.

Introducción.

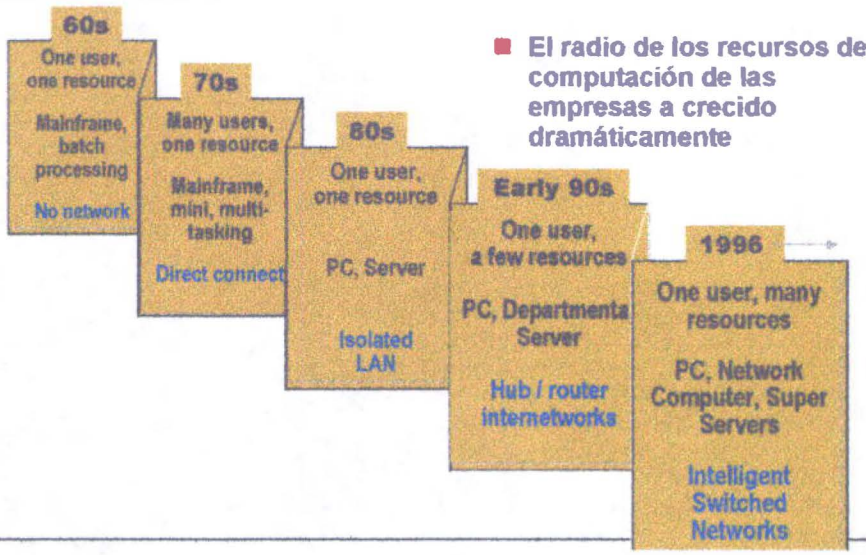
La administración de las redes puede ir estableciendo la diferencia, ya que grandes plataformas en ambientes escalables requieren de soluciones de administración prácticas.
El departamento técnico de una empresa requiere ingresar al ambiente de computación en redes de manera continua, así adquiere el conocimiento de los cambios que se deben hacer en su organización para tener claras las perspectivas de las aplicaciones que van a ser ejecutadas en su negocio.
Una herramienta de administración debe proveer una vista común y simple de los recursos del ambiente de red así como también debería ser una verdadera integración para los diferentes ambientes de sistemas.
Disciplinas de administración o aplicaciones de administración deben operar de una forma transparente a través de diferentes ambientes operativos.
Esto permite al usuario ejecutar cualquier actividad de administración u operación sobre múltiples plataformas con un solo comando consistente.

Objetivos:

- Indicar las ventajas de tener establecidas políticas de administración de red.
- Mostrar las nuevas tendencias de administración de red
- Mostrar nuevas tecnologías que de una forma fácil y simple nos permitan realizar la administración de redes a través de distintas plataformas.

La visión de las Cosas

La naturaleza de la computación esta cambiando

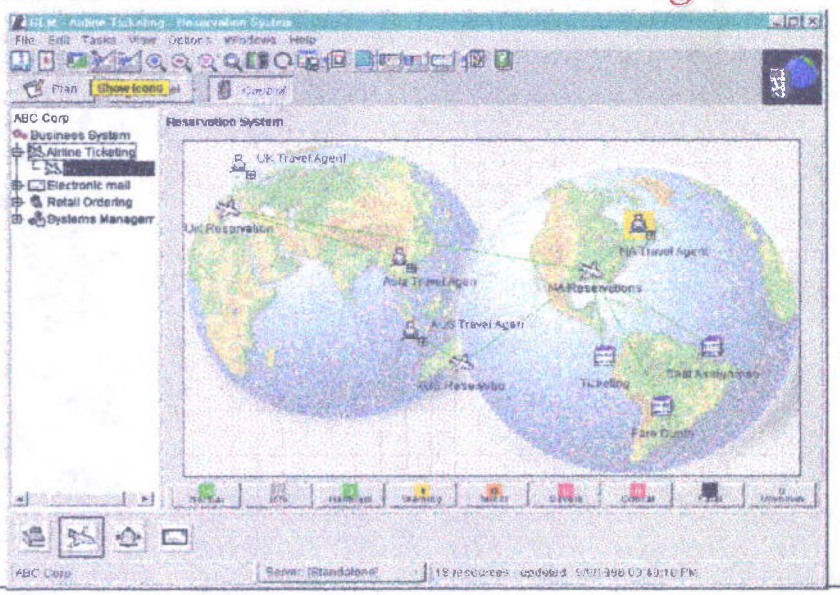


- El radio de los recursos de computación de las empresas a crecido dramáticamente

La naturaleza de los negocios está cambiando

- **Factores significantes:**
  - Cambios hacia IP
  - Más gráficos, imágenes, video y sonido
  - Centralización de recursos en el servidor
  - Grandes servidores (super servers)
  - Transición desde Novell a NT
  - Web, Java, Internet, intranets
  - Más aplicaciones de trabajo en grupo (ejm, Notes)
  - Continuo crecimiento del tamaño en la infraestructura computacional.
  - Computación cooperativa
  - Se incrementa la importancia de la seguridad
  - Usuarios móbiles
  - Usuarios remotos

Esto es .... Administrar un Negocio



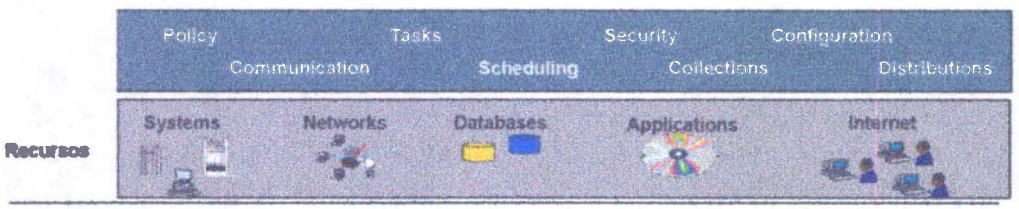
Estructura de un Producto

Recursos a Administrar

- Componentes de Red
- Sistemas Operativos
- Bases de Datos
- Software Medio
- Aplicaciones de Usuario
- Usuarios Finales

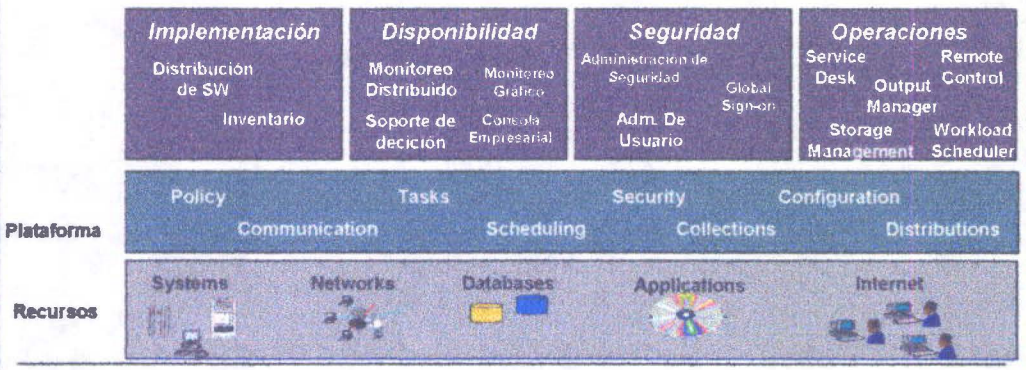
Base de Conocimientos de Objetos Distribuidos (Framework)

- Facilita Administrar los Recursos
- Diferentes plataformas son vistas desde el mismo sistema de administración
- Tiene que soportar (UNIX, NT, NetWare, OS/390,...)
- Conjunto de servicios comunes para administrar todas las aplicaciones



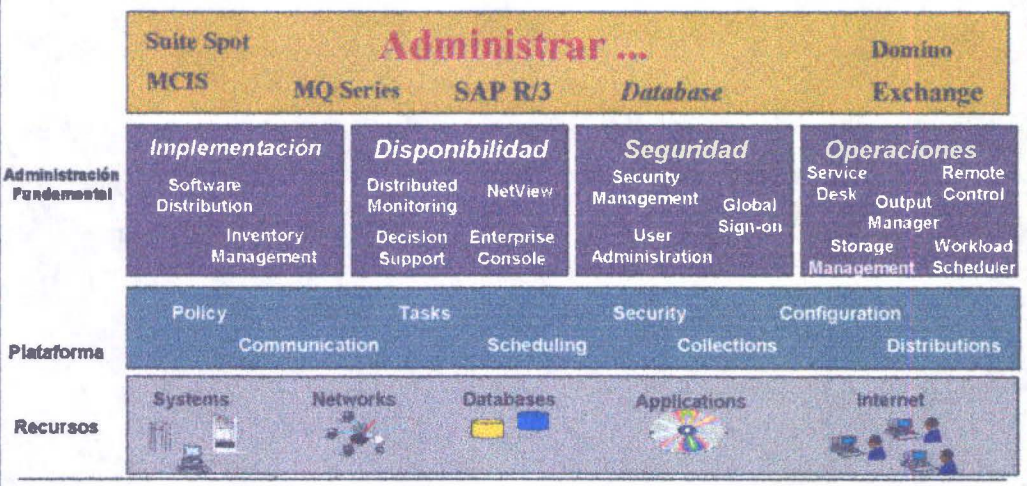
Administración de Sistemas y Redes

- Debe proveer un conjunto de productos para administración
  - Disponibilidad
  - Implementación
  - Seguridad
  - Operación

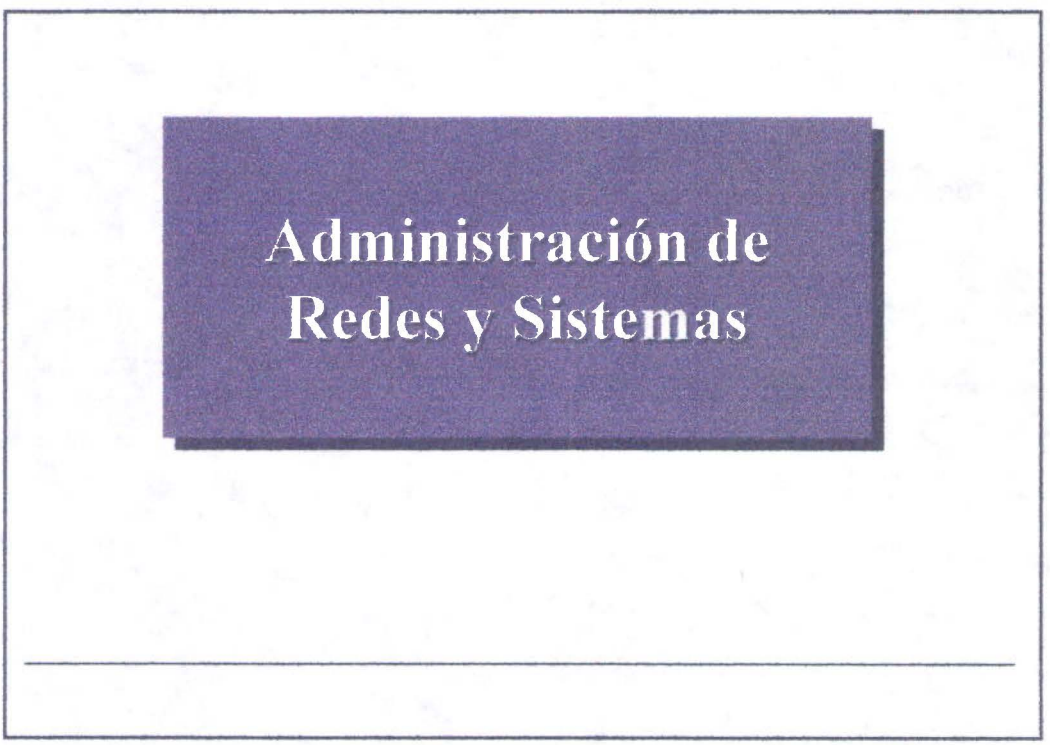


Administración de Aplicaciones

- Módulos para administrar aplicaciones específicas de negocios
- Usos y avances de productos para la administración de la compañía

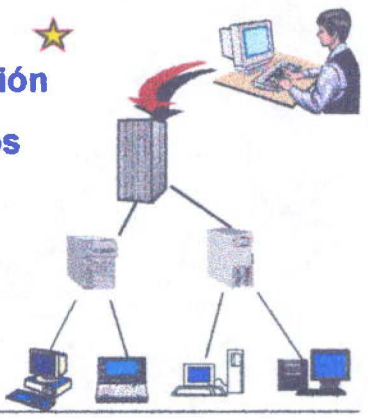



Administración de Sistemas de Negocios
Administración Global de la Compania
Administración de Aplicaciones
Suite Spot
MCIS
Adminitrar ..
MQ Series
SAP R/3
Database
Domino
Exchange
Fundamental Management
Implementación
Software Distribution
Inventory Management
Disponibilidad
Distributed Monitoring
NetView
Decision Support
Enterprise Console
Seguridad
Security Management
Global Sign-on
User Administration
Operaciones
Service Desk
Output Manager
Remote Control
Storage Management
Workload Scheduler
Framework
Policy
Tasks
Security
Configuration
Communication
Scheduling
Collections
Distributions
Recursos
Systems
Networks
Databases
Applications
Internet

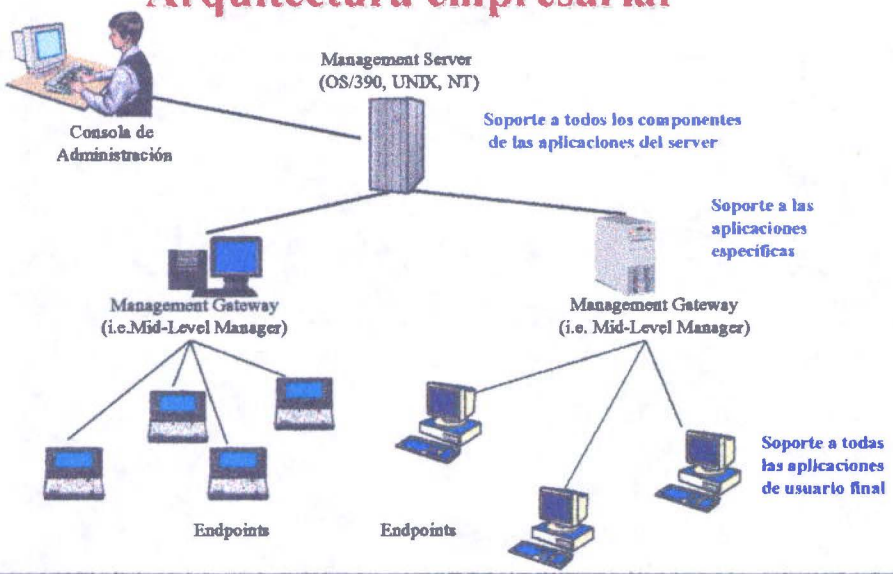

Administración de
Redes y Sistemas

Framework

- Seguridad, centralizado, jerárquico, y escalable
- Mayor soporte para servers y clientes heterogéneos
- Servidores y servicios replicados
- Políticas basadas en la automatización
- Un conjunto de estandares, servicios y APIs abiertos

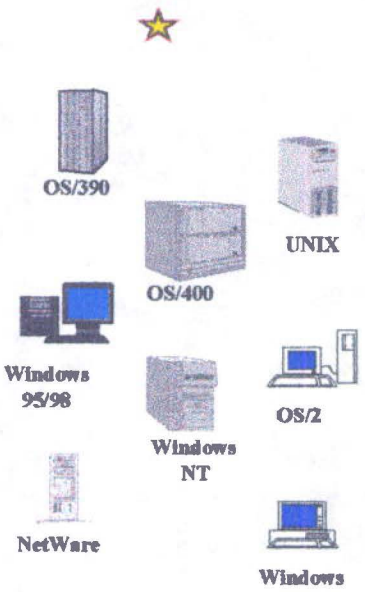


Arquitectura empresarial



Agente de Administración

- Arquitectura con un agente
- Características de Administración
  - Extensible
  - Autónomo y con conexión
  - Menores datos
- Provee una admnistración de un-toque
  - Actualización automática
- Enfoque hacia
  - Adaptadores de Red
  - Sistemas operativos
  - Aplicaciones



Disciplinas fundamentales de Administración

Inplementación	Disponibilidad	Seguridad	Operaciones
Habilitar configuración global Cambio de Administración	Colecta y rutea información para una administración proactiva	Asegura acceso apropiado para los usuarios y proteje a la empresa	Automaitza actividades para asegurar el nivel de servicio

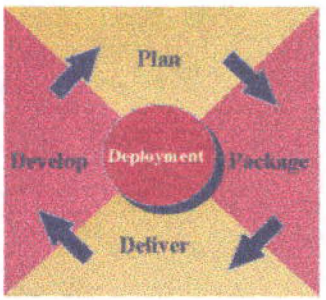
Inplementación

El desafío:

- Proveer el software correcto a las personas correctas
  - Muchos tipos de plataformas
  - Millones de partes en movimiento
- Diferentes tipos de aplicaciones
  - Client/Server
  - Desktop

El Dilema:

Cada paso en la implementación puede ser una labor intensiva en el ciclo de vida



La solución:

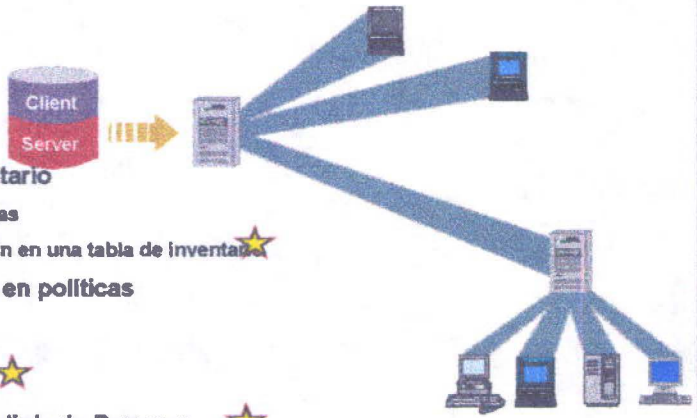
- Administración de Inventario
- Administración de la distribución de SW

Administración de Inventario

- Busqueda de HW y SW
  - Nuevo HW, BIOS y DMI scans ☆
- Soporte a base de datos abiertas
- Integrar consultas/reportes
- Arquitectura WAN-Smart ☆

Administración de Distribución de SW

- **Packaging**
  - AutoPack
  - File package GUI
- **Planeamiento**
  - Integración de inventario
    - Consultas pre-definidas
    - Estatus de distribución en una tabla de inventario
  - Distribución basada en políticas
- **Entrega**
  - WAN-Smart
  - Mobile support, Userlink via Browser
  - Delegación de Autoridad
  - Integración de Eventos



Disponibilidad de Administración

El desafío:

Maximizar la disponibilidad de negocios las aplicaciones y los recursos de computación para los diferentes niveles de servicio hacia los usuarios

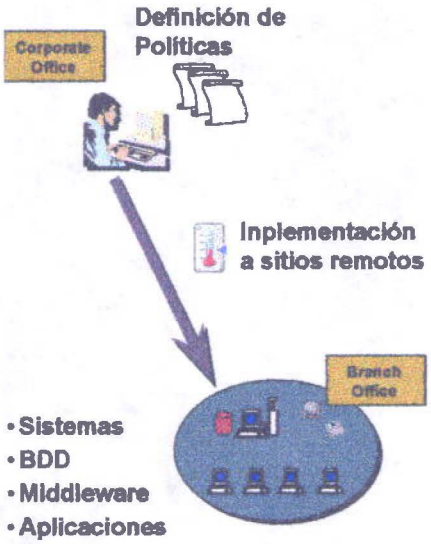
El dilema:

- Miles de elementos, alarmas y eventos
- Multiples consolas = pruebas de productividad
- Administracón de redes, sistemas y aplicaciones

La solución:

- Monitoreo distribuido
- Monitoreo gráfico
- Soporte de decisión

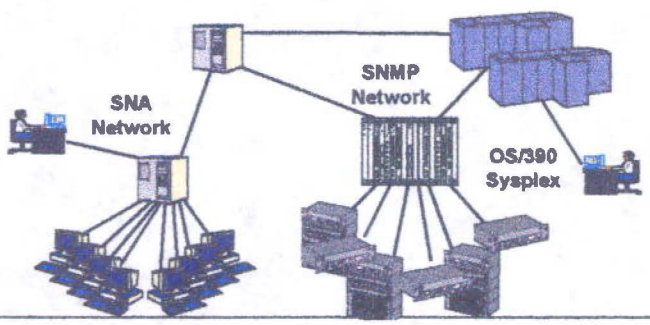
Monitoreo Distribuido



- Configuración basadas en políticas
- Distribución automática para ambientes dinámicos
- Inteligente, multi-threshold, agente de respuesta local
- Añadir sus propios monitores y eventos
- Monitoreo de recursos a través del Web y por medio charts, gráficos y reportes

Monitoreo Gráfico

- Integrar administración de redes y sistemas
- Administración a través de múltiples plataformas y sistemas
- Automatización extensiva y capacidades escalables
- Administración SNMP, SNA y OS/390

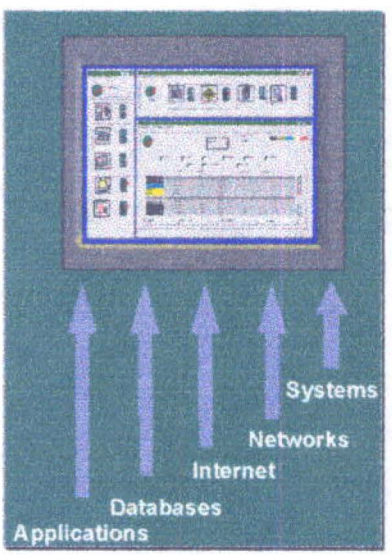


S/390 Administración de Rendimiento

- **Monitor de Rendimiento (PM)**
  - Monitoreo, registra, y reporta el rendimiento y utilización de la red
  - Flujo de tráfico, tiempos de transmisión y uso de componentes
  - SNA y TCP/IP
- **Medida de la facilidad de recursos**
  - Monitoreo, registro y reporte del rendimiento y utilización del S/390
  - Maximizar el uso de los recursos del S/390
  - Determinación rápida de problemas
- **Reportes de Rendimiento del S/390**
  - **Consolidación de disciplinas y administración con tecnología JAVA**
  - **Listo para el uso y personalización de reportes**
  - **Reportes a nivel empresarial**

Consola Empresarial

- **Integración y colección de eventos**
  - Windows NT, Unix, OS/390, Tandem, ...
  - NT Event Logs, NT Registry, Syslog, SNMP, non-SNMP, App. logs, ...
  - Construir sus propios colectores de eventos
  - Nuevos adaptadores: OS/2, Tandem, Cabletron Spectrum, OS/390
  - Integración con el monitoreo gráfico
- **Correlación de recursos y eventos**
  - Eliminar sobrecarga de información
  - Rutear y determinar la causa de un problema
- **Atomatización**
  - Inatención, establecer reglas
  - Iniciativas del operador



Soporte de Decisión

- Transformar datos dentro de una base de conocimientos para informar a las decisiones del negocio
- Evaluar como están funcionando las herramientas de administración
- Ejecutar reportes parametrizados y poder personalizarlos
- Herraminentas de navegación para los datos
- Calendarizar regularmente la publicación de reportes

Administración de seguridad y usuarios

El Desafío:

Implementación & Hacer cumplir

Cumplir reglas de seguridad

Cumplir con las políticas de la empresa

La Solución:

- Administración de usuarios
- Administración de seguridades
- Global Sign-on

El Dilema:

Diferentes herramientas de seguridad:

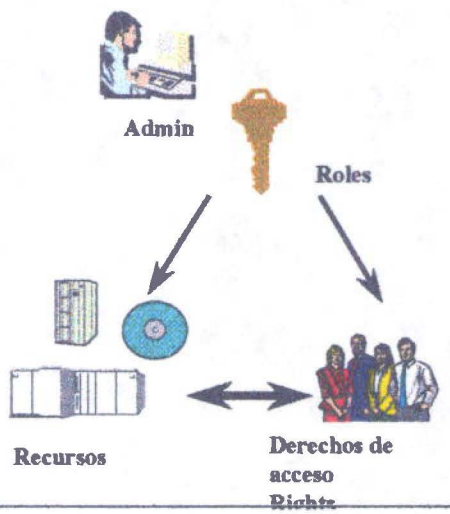
- Control de acceso
- Protección de virus
- Alarmas/Monitoreo
- Detección de intentos de acceso
- Administración de usuarios
- Identificación & Autentificación
- Aplicaciones de usuario

Administración de usuarios

- **Cross-Platform**
  - Administrar atributos de usuarios NT, UNIX y NetWare
  - Administrar todos los elementos de la red
- Consistencia con las políticas de validación establecidas
- **Un Password que sirve de interface entre las tecnologías**

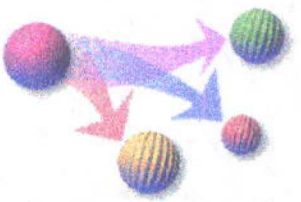
Administración de Seguridad

- **Políticas consistentes en base a la cobertura de todas las plataformas**
  - NT, UNIX, OS/390, ...
- **Control centralizado**
- **Resolver inconsistencias en los modelos de seguridad**
- **Integrado con los mejores productos asociados**
- IBM Global Sign On, PassGo, Firewall-1, Norton Antivirus, Axent ERM, ITA ...



IBM Global Sign-On

- Coordina logons entre recursos distribuidos
- Un UserID y password
- Incrementa la productividad del usuario
- Un abierto y expandible framework
  - Añade nuevos mecanismos de autentificación
  - Añade nuevos tipos de objetivos
- Reduce exposiciones de seguridad



Operaciones

El desafío:

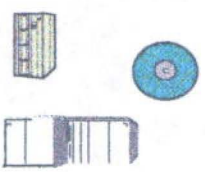
Reducir las tareas y procedimientos requeridos para mantener los niveles adecuados de soporte I/T

El dilema:

- Inversiones existentes en I/T
- Control Cross-Platform
- Delegación de tareas
- Duplicación de trabajo

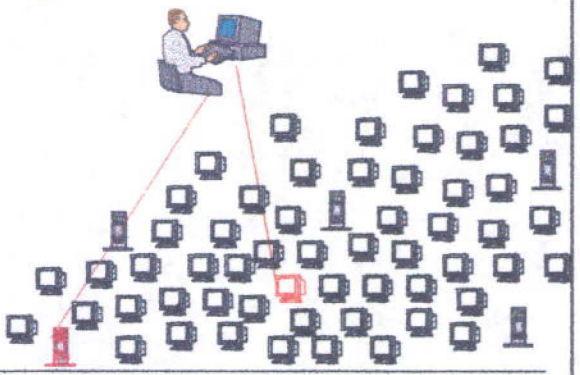
LA SOLUCION:

- Control Remoto
- Calendarización de tareas
- Servicio de escritorio
- Administración de almacenamiento



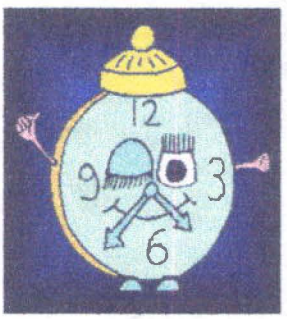
Control Remoto

- Control remoto completo en tiempo real
- Conexión rápida al objetivo correcto
- Autorizaciones basadas en políticas establecidas



Calendarización de Trabajo Operaciones, Planeamiento, Control (OPC)

- Administración del trabajo en los host y en los ambientes distribuidos
- Automatización de Operaciones
  - Procesos basados en reglas
  - Recuperación automática
  - Iniciadas por el operador
- Arquitectura Fault tolerant
- Consistencia, control centralizado
- Integrado con aplicaciones de misión crítica
  - R/3, Oracle Financials, Baan, PeopleSoft



Administración de Salidas
Sistema de Administración de Distribución

- **Administración de salidas**
  - **Centralizado** Administración de la distribución de información
  - **Automatizado**, fault tolerant, distribución
  - **Seguro**, acceso flexible de los usuarios hacia los recursos

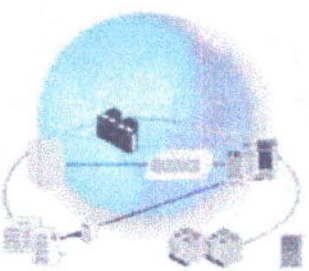
Sistema de Administración de Distribución de Reportes

- Distribución basada en el tipo de información
- Vistas y almacenamiento de reportes On-Line

Adminsitración de Almacenamiento

- **ADSTAR Distributed Storage Manager (ADSM)**
  - **Políticas basdas en backups, restore y archivo**
  - **Proveer administración de recuperación ante desastres**
  - **Base de datos de backups**

- **Data Facility System Manage Storage (DFSMS)**
  - **Administración de almacenamiento jerárquico**
  - **Administración de medios removibles**
  - **Rendimiento en almacenamiento**



Administración de APLICACIONES

Administración de Aplicaciones

El desafío:

Proveer herramientas para administrar aplicaciones críticas para cumplir con la misión del negocio

El Dilema:

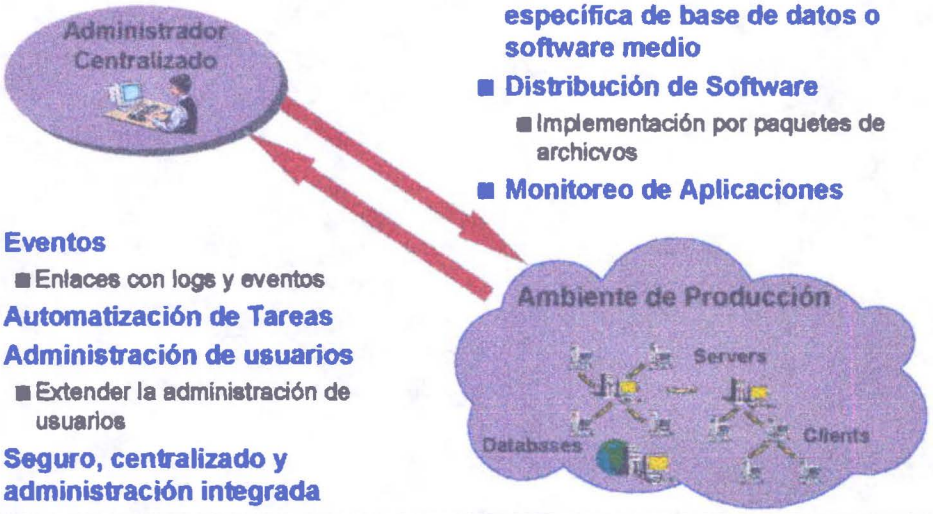
- Muchas herramientas
- No integradas
- Aplicaiones no administradas en contexto con la infraestructura IT

La Solución:

- Administración para:
  - Base de Datos
  - Aplicaiones de e-mail
  - Recursos de Internet
  - R/3, MQ Series
- Toolkits y Asociados

Administración para ...

- Aplicación para administración específica de base de datos o software medio
- Distribución de Software
  - Implementación por paquetes de archicvos
- Monitoreo de Aplicaciones



- Eventos
  - Enlaces con logs y eventos
- Automatización de Tareas
- Administración de usuarios
  - Extender la administración de usuarios
- Seguro, centralizado y administración integrada

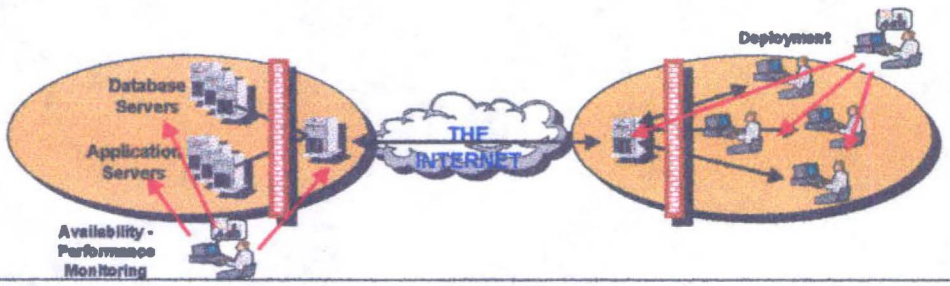
Administración para ... "*BDD*"

- Administración de base de datos a nivel empresarial
  Oracle, Sybase, Informix, DB2, MS SQL Server
- Disponibilidad
  - Monitoreo de Base de Datos
- Escalas para administrar el ingreso a las bases de datos
- Administración de usuarios centralizada
  - Sincronización de la definición de las cuentas de usuarios
- Habilitar la administración de las bases de Datos en el contexto de los sistemas críticos del negocio

IBM Microsoft SQL Server SYBASE INFORMIX ORACLE

Administración para el exterior

- **Administrar los internet servers:**
  - Microsoft and NetScape
  - Mail, Directory, News, Web, Proxy
  - Others: Apache, INN, NCSA, Sendmail
- **Realizar análisis de Web site**
- **Control centralizado de los Internet servers**



Administración de Sistemas de Negocios

Administrar Estratégicamente los Sistemas de Negocios

El Desafío:

Proveer formalidad, disponibilidad y servicio a niveles empresariales. Sistemas de soporte IT para los procesos críticos de los negocios.

El Dilema:

- **Compreneder como las aplicaiones trabajan juntas para satisfacer los objetivos del negocio**
- **Relaciones entre aplicaiones, software medio y dispositivos**
- **Espacio entre host y ambientes de distribución**

La Solución:

- **Administración Global de la EMPRESA**

Administración Global de la Empresa

- ***Administración de Sistemas de Negocios***
  - **Administración de múltiples aplicaciones en un contexto de negocio**
  - **Administración basada en estandares abiertos**
  - **Habilitar la administración y el control de:**
    - Aplicaciones de negocios desarrolladas a nivel comercial o interno.
    - Herramientas de administración existentes (Tivoli, IBM, & partners)

Interface para centralizar el negocio