



UNIVERSIDAD DE QUINTANA ROO

División de Ciencias e Ingeniería

Esquema de Consolidación Tecnológica
para la Administración de un Laboratorio
de Cómputo.

Tesis para obtener el grado de

Ingeniero en Redes

Presenta

Marcos Aarón Hernández Meza

Director de tesis

M.T.I. Vladimir Veniamin Cabañas Victoria

Supervisores

Ing. Rubén Enrique González Elixavide

M.T.I. Melissa Blanqueto Estrada.



Chetumal, Quintana Roo, México.

Junio, 2010

Ø59887



UNIVERSIDAD DE QUINTANA ROO

División de Ciencias e Ingeniería

Trabajo de tesis elaborado bajo supervisión del Comité de Asesoría y aprobada como requisito parcial para obtener el grado de:

Ingeniero en Redes

Comité de Trabajo Tesis

Director:

M.T.I. Vladimir Veniamin Cabañas Victoria

Supervisor:

Ing. Rubén Enrique González Elixavide

Supervisor:

M.T.I. Melissa Blanqueto Estrada



Chetumal, Quintana Roo, México, Junio de 2010.

Chetumal, Quintana Roo, Junio de 2010.

AGRADECIMIENTOS

A mis padres, hermanos y a Dios por su apoyo y amor, que me han proporcionado la fuerza y voluntad para continuar en los momentos más difíciles.

A mi Director de Tesis,
M.T.I. Vladimir Veniamin Cabañas Victoria
por su asesoramiento, paciencia y compromiso
para guiarme en este trabajo.

A todos mis amigos y compañeros de la carrera de Ingeniería en Redes ya que permitieron que este pequeño viaje sea interesante y ameno.

DEDICATORIA

Dedico este trabajo aquella persona que con un solo roce de sus manos, con tan solo mirar sus ojos, pudo despertar en mí el amor, el deseo de estar siempre a su lado y entregarle lo mejor de mí. *C.J.D.C.*

Contenido

Capítulo 1. Introducción	1
1.1 Antecedentes	1
1.2 Definición del problema.....	2
1.3 Justificación.....	3
1.4 Objetivos.	3
1.5 Alcance	4
1.6 Metodología.	5
Capítulo 2. Marco Teórico.	6
2.1 Centro de cómputo.	7
2.2 Gestión de software y Hardware.....	9
2.3 Gestión de Actualizaciones.....	10
2.4 Gestión de Red.....	19
2.5 Plataformas de gestión de red.	23
2.6 SNMP (Simple Network Management Protocol).....	25
2.7 System Center Configuration Manager 2007.....	26
2.8 LANDesk Management Suite.....	28
2.9 Novell ZENworks 10 Configuration Management.	30
Capítulo 3. Desarrollo.....	32
3.1 System Center Configuration.....	32
3.2 LANDesk Management.....	34
3.3 ZENworks 10 Configuration Management.	36
Capítulo 4 Conclusiones.....	40
4.1 Complejidad.....	40
4.2 Seguridad	40
4.3 Trabajo futuro.	42
Anexos.	43
Anexo A Instalación de Active Directory en Windows Server 2008.	43
Anexo B Instalación de Web Server IIS.....	43
Anexo C Instalación y configuración de SQL Server Standard 2005.....	45
Anexo D Instalación y configuración de SCCM 2007.	46
Anexo E Instalación de WSUS 3.0 SP2.....	48

Anexo F Instalación de LanDesk en Windows Sever 2003.....	53
Anexo G Instalación de ZENworks 10 Configuration.....	59
Bibliografía	65

Índice de figuras.

Figura 1. Un solo servidor de actualizaciones.....	14
Figura 2. Un solo servidor de actualizaciones con grupos.....	14
Figura 3. US independientes.....	15
Figura 4. US sincronizados internamente.....	16
Figura 5. Servidores US sin conectividad a Internet.....	17
Figura 6. Administración centralizada.....	18
Figura 7. Administración distribuida.....	19
Figura 8. Jerarquía de zonas.....	24
Figura 9. Arquitectura de un sistema de gestión SNMP.....	25
Figura 10 Herramientas de SCCM 2007.....	26
Figura 11. LANDesk Management Suite.....	28
Figura 12 Herramientas de ZENworks 10.....	30
Figura 13. Configuración de Actualizaciones automáticas.....	50
Figura 14. Ubicación del servicio Windows Update en la intranet.....	50
Figura 15. Configuración de Actualizaciones automáticas.....	51
Figura 16. Ubicación del servicio Windows Update en la intranet.....	51
Figura 17. Actualizaciones automáticas en los equipos gestionados.....	52
Figura 18. LanDesk instalación.....	54
Figura 19. LanDesk agente.....	55
Figura 20. Ventana de resumen de ZENworks.....	60
Figura 21. ZENworks Instalación finalizada.....	60

Índice de tablas.

Tabla 1 Definiciones de clasificaciones.....	10
Tabla 2 Dispositivos de pruebas.....	32
Tabla 3. Requisitos mínimos de hardware.....	38
Tabla 4. Costos de las plataformas.....	38
Tabla 5. Requisitos de software.....	39

Capítulo 1. Introducción

1.1 Antecedentes

La industria de la computación ha experimentado muchos cambios desde los días de las computadoras centrales UNIVAC. A principios de 1980, la computadora de escritorio fue considerada como una herramienta comercial relativamente nueva. De hecho, la típica discusión de las corporaciones se centraba en el hecho de comprar una computadora de escritorio con una unidad de disco duro de 10 MB con un costo adicional de \$1,700, porque decían: “los usuarios nunca necesitarán ese espacio tan grande.” (1)

Desde entonces, la computadora usada como herramienta de productividad se ha convertido en una necesidad en la mayoría de las organizaciones, así como en las escuelas y en casa. El poner al alcance de la mano del usuario un poder de procesamiento se ha vuelto una necesidad. Como resultado de ello, la informática se ha convertido en una gran industria y, por consiguiente, potencialmente un gran dolor de cabeza para la administración. Los usuarios de las computadoras pueden ser territoriales sobre sus sistemas y las aplicaciones utilizadas. Por ejemplo: un usuario que está ejecutando tres programas de procesamiento de textos en varias versiones, ya que el usuario no está dispuesto a correr riesgos de convertir los documentos a una única versión de procesamiento de textos.

Por otra parte, más empresas están tomando ventaja de herramientas para la administración de su entorno de red, para proporcionar a sus usuarios una computadora que no sólo puede ser mantenida centralmente sino también que no puede ser modificada en absoluto por el usuario. Muchas empresas están extendiendo el uso de estas herramientas y otras herramientas, para apoyar a sus plataformas de servidor.

Ambos escenarios ejemplifican el hecho de que el apoyo a múltiples computadoras instaladas con una variedad de programas y aplicaciones de servidor puede ser un desafío hasta para el mejor equipado y financiado grupo de soporte de TI.

Muchos administradores de TI han reconocido la necesidad de proporcionar estándares para la computadora de escritorio y han comenzado a buscar y poner en práctica algún tipo de sistema de gestión centralizada de computadora. Los grupos de soporte de TI deben ser capaces de responder de manera activa y proactiva para aplicar y actualizar software en los sistemas cliente y responder a sus usuarios a las peticiones de asistencia rápida y eficaz.

El Grupo de soporte de TI debe ser capaz de administrar la mayor cantidad de equipos como sea posible mientras están sentados en sus propias computadoras. La clave para la gestión eficaz de escritorio remoto es crear una serie de herramientas de administración remota de TI que permiten a un grupo de soporte ser tan eficaz como si hubieran puesto realmente las manos en la computadora del usuario.

1.2 Definición del problema

Para un administrador de TI, no siempre es posible obtener información de los equipos de su red, información como los sistemas operativos, sus estados, si están actualizados o no, estadísticas tiempo de uso y que tipo de software está instalado en la computadora, tener información de las licencias, si los programas instalados están siendo utilizados de manera regular, así como la posibilidad de administrar los equipos de una manera más fácil.

La determinación de cuándo y qué actualizaciones se instalarán, ya sea del sistema operativo o de los programas, no siempre es sencillo, con frecuencia los usuarios descuidan esta tarea importante y el hecho de instalar actualizaciones y descargarlas en cada equipo conlleva a un uso mayor de ancho de banda afectando a otras aplicaciones.

1.3 Justificación.

Con un esquema de gestión tecnológica para la administración, el encargado de la red informática, podrá gestionar de manera centralizada y remota la distribución de software, instalar aplicaciones desde su estación de trabajo. Tener el control de las configuraciones, permitir o denegar la ejecución de algunas aplicaciones, permitir el uso de memorias flash, puertos serial, etc. Gestionar las actualizaciones, ya que las actualizaciones de software de aplicaciones y de sistemas operativos, permite incrementar la seguridad de una red, por consiguiente el tener una computadora no actualizada representa una seria posibilidad de comprometer el sistema y la red en la que se encuentra conectada, para tal caso, es necesario mantener actualizado el sistema.

Así como también se tendrá la posibilidad de realizar inventarios de las computadoras, control de las licencias de los programas, así como el control de las actualizaciones, poder definir, cuándo, cuáles y quiénes instalarán dichas actualizaciones y para qué aplicaciones.

1.4 Objetivos.

Objetivo General.

Consolidar el proceso de administración en la instalación, actualización del sistema operativo y otros paquetes de software, reduciendo el tráfico en la red generado por dichas actualizaciones y teniendo así un mejor control administrativo sobre el proceso de actualización. Así como también, facilitar el proceso de gestión de las computadoras en un laboratorio de computación de mediano tamaño, en un ámbito académico.

Objetivos Específicos.

- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.

- Unificar el proceso de instalación, configuración y actualización de los sistemas operativos y los programas.
- Maximizar la efectividad en el uso del ancho de banda, reduciendo el tráfico generado por las actualizaciones del sistema operativo y software de aplicación.
- Incrementar el nivel de seguridad en la red informática a través de la actualización de los sistemas operativos y de las aplicaciones instaladas en las computadoras.

1.5 Alcance

El alcance de este proyecto es el proponer un sistema de gestión para el laboratorio de telemática de la Universidad de Quintana Roo campus Chetumal. Determinar mediante una serie de pruebas a diversas plataformas de gestión, tales como las de descubrimiento de dispositivos, distribución de software y actualizaciones, instalación, desinstalación y bloqueo de aplicaciones, creación de reportes, herramientas de control remoto. Con base en el resultado de dichas pruebas, determinar qué sistema de gestión es el más adecuado para el laboratorio de telemática.

1.6 Metodología.

Se estudiarán diferentes aplicaciones de gestión de redes que implementan distintas herramientas para la administración. Lo anterior es con la finalidad de elegir una de ellas, la cual se adapte mejor a la gestión de redes para un laboratorio de cómputo.

Tipo de investigación:

- Descriptiva.
- Experimental

Método utilizado:

- Método Inductivo

Objeto:

- Aplicaciones de gestión de redes.

Medio:

- Recopilación de información bibliográfica y referencias electrónicas así como también investigación de campo.
- Pruebas de descubrimiento de dispositivos, distribución de software y actualizaciones, instalación, desinstalación y bloqueo de aplicaciones, creación de reportes, herramientas de control remoto.

Fin:

- Recomendar un modelo basado en software para la gestión de redes, la cual se adapte mejor a la administración de un laboratorio de cómputo.

Capítulo 2. Marco Teórico.

La dinámica de las infraestructuras de TI es cada vez más compleja y difícil de gestionar, hoy es común contar con diversas plataformas, arquitecturas y tecnologías que convergen en la red para proporcionar y acceder a los servicios ofrecidos por la red. La configuración de los dispositivos finales que se conectan a la red representa un gran reto para los administradores de red, ya que deben contar las herramientas que les permitan ejecutar los procesos de configuración de manera automática, supervisada

Sin embargo, la gestión de la configuración es sólo parte del reto, los administradores de TI deben proporcionar un equilibrio constante de gestión de la configuración con los requisitos de seguridad. Asegurar que los sistemas permanecen en el cumplimiento de las normas de seguridad es un proceso largo y costoso.

Para gestionar el cambio de manera eficaz, garantizando al mismo tiempo que todos los sistemas están actualizados y seguros, las organizaciones de TI deben automatizar los procesos para que la gestión pueda producirse automáticamente, con poca o ninguna intervención del personal de TI. Esto requiere herramientas centralizadas, escalables que reduce los costos al mismo tiempo que añaden nuevo valor a los servicios de red.

Por lo anterior, es necesario un esquema de consolidación tecnológica para la administración, que se ocupe de estas necesidades, ayudando a organizaciones de TI a gestionar eficazmente el cambio en la dinámica actual de las infraestructuras.

A través de racionalización de la política basada en la automatización, los administradores pueden gestionar de forma centralizada la planeación de todo el ciclo de vida de los sistemas, mediante la distribución de aplicaciones y la gestión de las actualizaciones de software en los servidores, clientes y dispositivos móviles a través de la red.

2.1 Centro de cómputo.

La administración se define como el proceso de crear, diseñar y mantener un ambiente en el que las personas al laborar o trabajar en grupos, alcancen con eficiencia metas seleccionadas. Las personas realizan funciones administrativas de planeación, organización, integración de personal, dirección y control. (2)

- La administración se aplica en todo tipo de corporación.
- Es aplicable a los administradores en todos los niveles de corporación.
- La administración se ocupa del rendimiento; esto implica eficacia y eficiencia.

El Administrador de Centros de Cómputo.

El Administrador de Centros de Cómputo o Administrador de TI es la persona con la autoridad y responsabilidad de planificar, organizar, dirigir y controlar el recurso informático de la institución con la finalidad de optimizar su uso y asegurar la calidad y permanencia del servicio dentro de la organización así como la prestación del servicio ininterrumpido y seguro.

El Centro de Cómputo.

Un centro de cómputo representa una entidad dentro de la institución, la cual tiene como objetivo satisfacer las necesidades de información de la empresa, de manera veraz y oportuna.

Misión de un Centro de Cómputo

La computadora como herramienta de solución para problemas de cálculo de operaciones, investigación de procesos, enseñanza, etc. establece las bases para determinar el objetivo de un centro de cómputo, como es el de prestar servicios a diferentes áreas de una organización ya sea dentro de la misma institución, o bien fuera de ella, tales como: control de operaciones, captura de datos, programación, dibujo, biblioteca, etc. Los diversos servicios que puede prestar un centro de cómputo, pueden dividirse en departamentos a áreas específicas de trabajo.

Elementos que Componen un Centro del Cómputo.

Para tener una visión organizada de los componentes básicos de un Centro de Cómputo como Sistema de Computación integral, se pueden dividir sus elementos en dos categorías: hardware y software.

Hardware.

Es el conjunto de elementos físicamente visibles en un sistema de computación. Es el equipo propiamente dicho. Incluye tanto a la computadora como a los equipos periféricos: impresoras, discos, monitores, unidades de respaldo, etc. Llamamos hardware al conjunto de dispositivos mecánicos y electrónicos que forman parte de la computadora.

Es el primer elemento de un sistema de computación y comprende a toda la maquinaria y al equipamiento relacionado al mismo. Contrasta con el elemento software, el cual puede ser descrito como el conjunto de instrucciones que le dicen a la computadora qué hacer.

Software.

El software es el segundo elemento de un sistema de computación, está constituido por los programas, por el conjunto de instrucciones que se suministran a la máquina para que resuelva algún problema.

En síntesis, el software está formado por instrucciones para que la computadora trabaje. El conjunto o serie de instrucciones para realizar una tarea en particular se llama programa o programa de software.

Bajo esta categoría se incluye a los programas preparados por el usuario (software de aplicación) como así también a aquellos programas provistos por el fabricante del equipo o comprado a terceras partes, como son el sistema operativo (software de base) y los lenguajes de programación, utilitarios y los productos para automatización de oficina como procesadores de texto, hojas de cálculo y otros productos de software.

2.2 Gestión de software y Hardware

La administración del hardware se basa en el control del inventario de hardware, y puede realizarse en forma básica, media o avanzada y puede requerir del uso de herramientas automatizadas dependiendo del nivel de control que se desea obtener.

Como eje de la administración, se requiere de un inventario de hardware, el cual consiste de un listado de todo el hardware en la organización.

El inventario de hardware debe incluir un listado completo de todos los componentes de la red incluyendo estaciones de trabajo, Servidores, periféricos y dispositivos de red y de comunicaciones. Entre los datos que debe contener el inventario, están los siguientes:

- Equipo, Marca, Modelo
- Tipo (servidor, computadora, concentrador, impresora, switch, etc.)
- Números de serie, Números de inventario.
- Códigos de barra.
- Todos aquellos definidos como políticas de la empresa.

También se requiere de un inventario de software, el cual debe contener información acerca del software instalado en cada una de los equipos de cómputo. Lo anterior debe incluir tanto Servidores como estaciones de trabajo.

Es recomendable que la información se concentre en un archivo central, también es muy recomendable que esta información se mantenga y actualice en forma periódica y que incluya los términos de las licencias de uso, fecha de adquisición, nombre del usuario que usa el software, detalles de instalación, acuerdos de mantenimiento, monitoreo de uso y otros datos que sean de importancia para su administración.

El inventario de software es de suma importancia pues permite administrar de mejor forma las licencias, negociar contratos de soporte, planear actualizaciones de software, resolver problemas relacionados con su uso.

2.3 Gestión de Actualizaciones.

Una actualización es una revisión, para su posible reemplazo parcial o total del software que está instalado en una computadora. Cada actualización disponible en los servidores del fabricante consta de dos componentes:

- Los **metadatos** ofrecen información acerca de la actualización. Por ejemplo, información de las propiedades de una actualización (a qué producto y/o plataforma es aplicable), etc. El paquete de metadatos descargado para una actualización por lo general es mucho más pequeño que el paquete verdadero del archivo de actualización.
- Los **archivos de la actualización** son los archivos binarios verdaderos de la actualización, instalados en un equipo.

Las actualizaciones son catalogadas por producto y por clasificación, según la vulnerabilidad que repara (ver tabla 1). Un **producto** es una edición específica de un sistema operativo o aplicación (Windows Server, Windows XP). Una **familia de productos** es el sistema operativo o la aplicación de base de la que se derivan los productos (Windows, de la que Windows Server, es miembro).

Clasificación	Definición
Crítica	Una vulnerabilidad cuya explotación podría permitir la propagación de un virus/gusano de Internet sin la acción del usuario.
Importante	Una vulnerabilidad cuyo aprovechamiento podría tener como resultado la puesta en peligro de la confidencialidad, integridad o la disponibilidad de los datos de usuarios, o de la integridad o disponibilidad del procesamiento de los recursos.
Moderada	La capacidad de aprovechamiento se reduce hasta un grado considerable debido a factores como una configuración predeterminada, una auditoría o debido a la dificultad de para aprovecharse.
Baja	Una vulnerabilidad cuyo aprovechamiento es muy difícil o cuyo impacto es mínimo.

Tabla 1 Definiciones de clasificaciones. ¹

¹ <http://technet.microsoft.com/es-es/updatesmanagement/bb229389.aspx>

De acuerdo a (3) el proceso para la administración de las actualizaciones se conforma de:

a. Valoración.

Los administradores tienen que valorar cuántos servidores y equipos cliente necesitan actualizar, cuáles son los requisitos de almacenamiento y de ancho de banda de la red y, finalmente, qué margen de tiempo es aceptable para implementar una actualización. Los administradores tienen también que determinar qué plataformas, productos e idiomas desean actualizar. Entre otros factores que pueden incluir en la actualización.

b. Identificación.

Los administradores deben determinar qué tipo de actualizaciones deben sincronizarse con el Servidor del proveedor y cuándo deben sincronizarse. Ya sea mediante una aplicación que reúna automáticamente datos acerca de todos los equipos conocidos, para así poder determinar si una actualización es relevante, los administradores pueden consultar rápidamente cuántos equipos necesitan esa actualización y cuál sería la repercusión en la red de su implementación antes de haberla instalado en el entorno de producción.

c. Evaluación y planeación.

Los administradores pueden probar las actualizaciones en un entorno separado del entorno de producción pero que se parezca a éste. Y determinar las tareas necesarias para implementar las actualizaciones en la producción, planear sus lanzamientos, crear las versiones y, a continuación, dirigir las pruebas de aceptación de dichos lanzamientos.

d. Implementación.

Los administradores deben especificar los grupos de equipos que se actualizarán y aprobar la implementación de las actualizaciones para esos grupos.

Servidor de Actualizaciones.

El servidor de actualizaciones o US (*Update Server*) permite a los administradores de redes implementar las últimas actualizaciones para diversas aplicaciones. Mediante el servidor de actualizaciones, los administradores pueden gestionar completamente la distribución de las actualizaciones lanzadas al mercado con el fin de corregir algún error o vulnerabilidades de seguridad (4). US ofrece una infraestructura de administración formada por:

- El sitio web del fabricante del software que distribuye actualizaciones.
- **Servidor US.** Este componente está instalado en Windows Server 2003 SP1 o Windows Server 2008 dentro del firewall corporativo. El servidor US permite a los administradores administrar y distribuir actualizaciones.
- **Automatic Updates.** Este componente se encuentra en los sistemas operativos y permite que tanto el servidor como los equipos cliente reciban actualizaciones.

Antes de planear e implementar una actualización para su instalación, el administrador puede analizar la repercusión que ésta podría tener en el equipo por medio de un informe de estado generado directamente desde la vista de la actualización para una sola actualización, un subconjunto de actualizaciones o bien todas las actualizaciones. Con los informes del servidor de actualizaciones, los administradores pueden consultar la siguiente información (4):

- **Estado de las actualizaciones:** Estos informes facilitan el estado para la aprobación e implementación de las actualizaciones por actualización, equipo y grupo de equipos, en función de los eventos que se envían al equipo cliente.
- **Estado del equipo:** se puede valorar el estado de las actualizaciones en los equipos cliente. Por ejemplo, pueden solicitar un resumen de las actualizaciones que se han instalado o que se necesitan para un equipo determinado.
- **Estado de cumplimiento del equipo:** información de cumplimiento relativa a un equipo específico, incluida información básica del software y hardware, la actividad del Servidor US y el estado de las actualizaciones.

- **Estado de cumplimiento de las actualizaciones:** información de cumplimiento relativa a una actualización específica, incluidas sus propiedades y el estado acumulativo para cada grupo de equipos.
- **Estado de sincronización (o descarga):** Los administradores pueden supervisar el estado y la actividad de sincronización durante un tiempo concreto. También pueden consultar las últimas actualizaciones descargadas.
- **Valores de configuración de US:** Los administradores pueden consultar un resumen de las opciones especificadas de la implementación de US.

Escenarios de implementación de US.

El servidor de actualizaciones es lo bastante flexible como para satisfacer las necesidades de administración de actualizaciones de una gran variedad de organizaciones, desde la pequeña empresa con conectividad de acceso telefónico hasta las empresas más grandes con miles de usuarios distribuidos entre múltiples lugares.

En función del tamaño de la organización, de su ubicación y de su infraestructura de conectividad, los administradores pueden determinar la manera más eficaz de escalar horizontalmente sus servidores US.

Implementación simple del US.

La implementación básica de un servidor de actualizaciones consiste en un servidor US dentro de la red corporativa. El servidor se conecta a los servidores del proveedor del software para descargar las actualizaciones. Esto es conocido como la sincronización, ver figura 1. Durante la sincronización, el servidor de actualizaciones determina si hay nuevas actualizaciones disponibles desde la última vez se sincronizó.

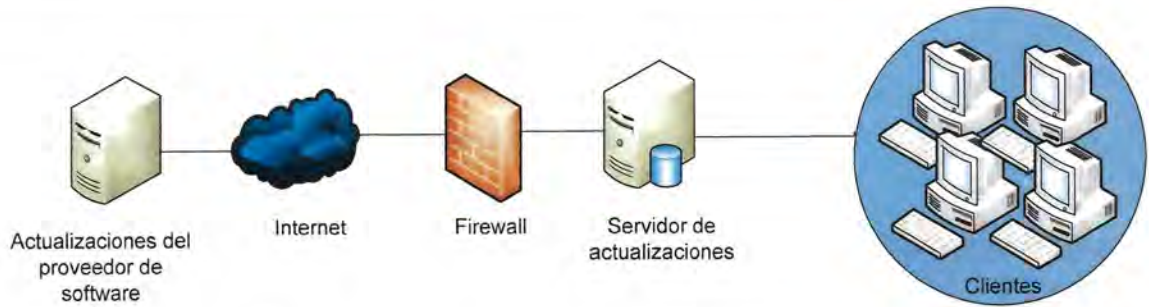


Figura 1. Un solo servidor de actualizaciones.

Implementación simple del servidor de actualizaciones con grupos.

Los grupos de equipos son una parte importante de las implementaciones de US, incluso una implementación básica. Los grupos de equipos permiten dirigir las actualizaciones de equipos específicos. Uno de los beneficios de la creación de grupos de equipos es que permite probar las actualizaciones. El grupo de Test contiene un pequeño número de equipos representativos de todos los equipos que figuran en el grupo de Contabilidad.

Las actualizaciones se prueban en el grupo de test. Si la prueba sale bien, puede distribuir las actualizaciones para el grupo de Contabilidad, ver la figura 2. No hay límite al número de grupos personalizados que puede crear.



Figura 2. Un solo servidor de actualizaciones con grupos.

Más de un servidor de actualizaciones.

a. Servidores de actualizaciones independientes.

Los administradores pueden implementar varios servidores configurados de forma que cada uno sea administrado independientemente y sincronice su contenido desde los servidores del proveedor.

El método de implementación en este escenario sería apropiado en situaciones en las que los diferentes segmentos de redes de área local o redes de área extensa se administran como entidades separadas (por ejemplo, sucursales), ver figura 3.

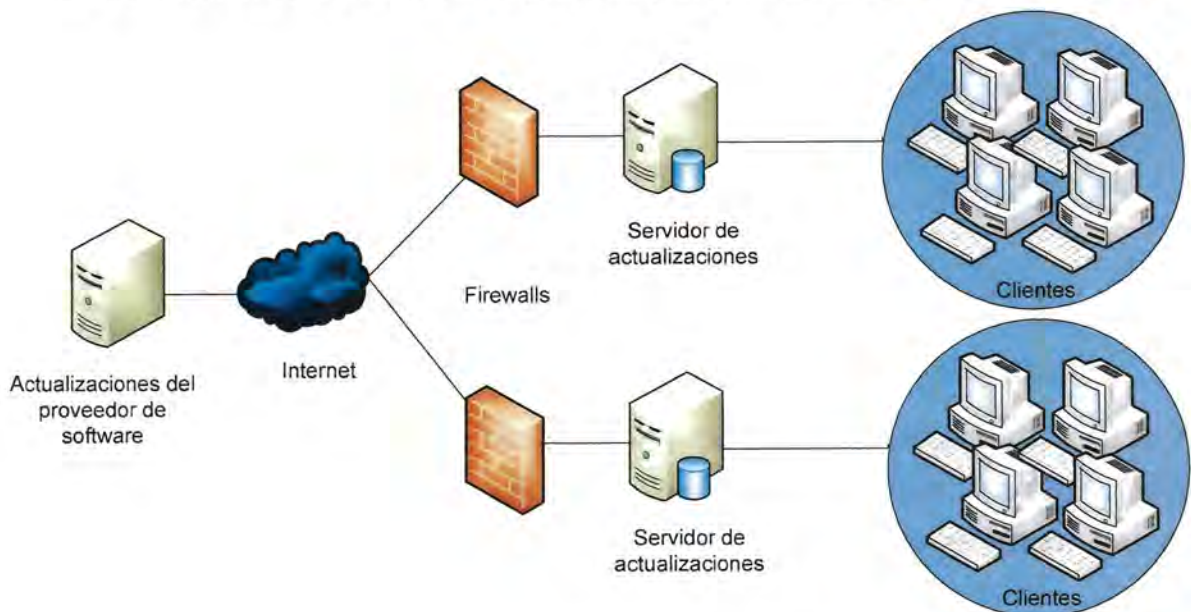


Figura 3. US independientes.

b. Servidores US sincronizados internamente.

Usa varios servidores US y que sincronicen todo el contenido de la intranet de la organización. En esta configuración, solo un servidor debe descargar las actualizaciones desde los servidores del proveedor, ver la figura 4.

Este servidor está establecido como el servidor que precede en la cadena, con cuyo origen se sincroniza el servidor que sigue en la cadena. Si es necesario, los servidores pueden ubicarse a través de una red geográficamente dispersa para ofrecer la mejor conectividad posible a todos los equipos cliente.

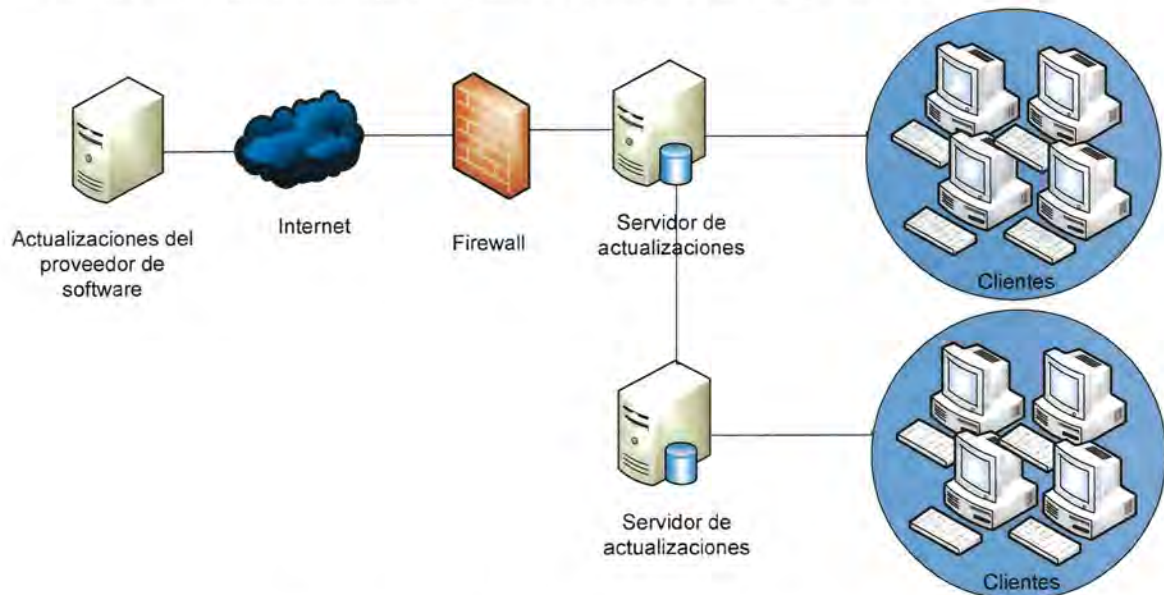


Figura 4. US sincronizados internamente.

Servidores US sin conectividad a Internet.

Si la directiva corporativa u otras condiciones limitan el acceso del equipo a Internet, los administradores pueden configurar un servidor US interno. En este ejemplo se creó un servidor para conectarlo a Internet; sin embargo, éste se encuentra aislado de la intranet.

Después de descargar, probar y aprobar las actualizaciones en este servidor, un administrador podría, a continuación, exportar los metadatos y contenido de las actualizaciones a los medios apropiados. Luego, desde estos medios, el administrador importaría los metadatos y contenido de las actualizaciones en los servidores US dentro de la intranet, ver la figura 5.



Figura 5. Servidores US sin conectividad a Internet.

Escenarios de administración de US.

Es posible administrar el servidor de actualizaciones de dos formas distintas: central y distribuida. Estos modelos de gestión permitirán administrar su solución de distribución de actualización en la forma en que tiene más sentido para la organización.

Administración centralizada.

La administración centralizada utiliza servidores sincronizados internamente. Estos servidores no se administran por separado, y sólo se utilizan para distribuir las aprobaciones a los grupos. Las actualizaciones aprobadas se replican del servidor principal a toda la organización. Los grupos deben ser creador localmente en cada servidor.

Para este esquema el administrador del servidor principal gestiona todos los servidores. (Figura 6).

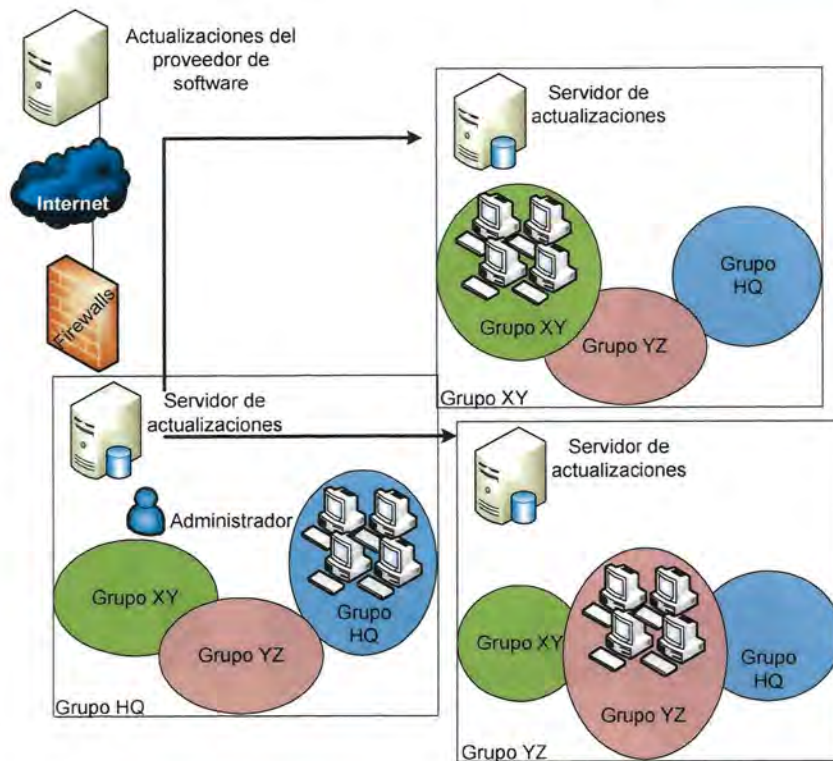


Figura 6. Administración centralizada.

Administración distribuida.

La administración ofrece un control total sobre las autorizaciones y los grupos de equipos para cada servidor de actualizaciones. Con el modelo de administración distribuida, suele haber un administrador en cada servidor, el cual decide el idioma de las actualizaciones, crea grupos de equipos, asigna actualizaciones a los grupos de equipos, ver la figura 7.

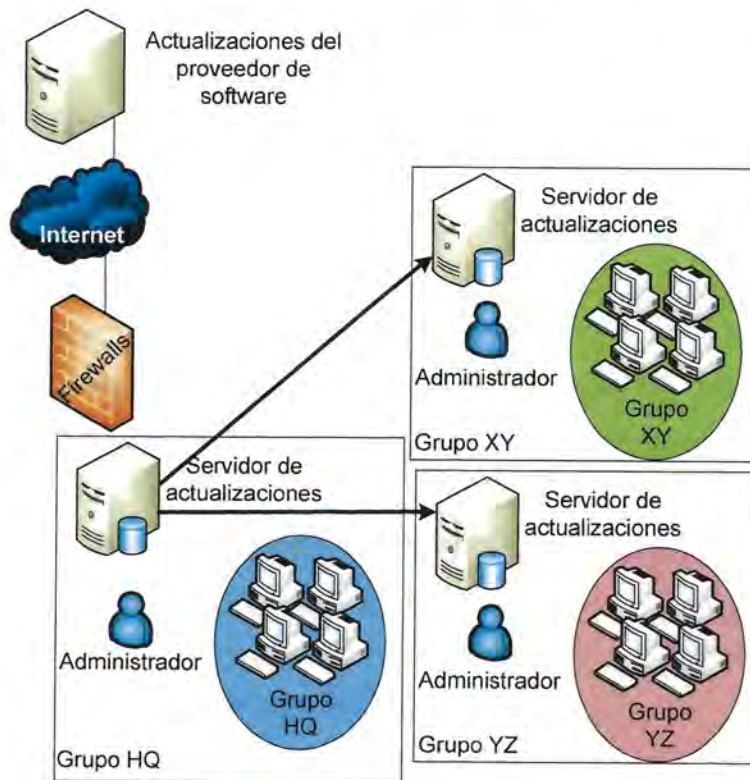


Figura 7. Administración distribuida.

2.4 Gestión de Red.

Una red se puede definir como todo el conjunto de equipos (computadoras y/o dispositivos) que están conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, los cuales comparten información (archivos), recursos (impresoras, etc.) y servicios (acceso a internet, e-mail, chat, juegos). Todo esto es lo que se conoce como redes informáticas, las cuales pueden clasificarse de acuerdo por su extensión, en:

- Local Area Network (LAN, Red de Área Loca)
- Metropolitan Area Network (MAN, Red de Área Metropolitana)
- Wide Area Network (WAN, Red de Área Extensa)
- Personal Area Network (PAN, Red de Área Personal)

Internet se crea por la interconexión de redes que pertenecen a los Proveedores de Servicios de Internet (ISP). Estas redes ISP se conectan entre sí para proporcionar acceso a millones de usuarios en todo el mundo. Garantizar la comunicación efectiva a través de esta infraestructura diversa, requiere la aplicación de tecnologías y protocolos consistentes y reconocidos comúnmente, como también la cooperación de muchas agencias de administración de redes. (5)

Junto con el crecimiento de las redes de datos, surgió la necesidad de su administración. La administración de redes incluye las tareas de diseño, integración y coordinación de los equipos de hardware, los programas de software y los recursos humanos necesarios para monitorear, testear, configurar, analizar, evaluar y controlar la red y sus recursos a los efectos de lograr la calidad de servicio requerida.

Administración de redes según la Organización Internacional para la Estandarización (ISO por sus siglas en inglés).

Las funciones de la administración, definidas por ISO, llamadas comúnmente "funciones FCAPS", debido a sus siglas en inglés, son las siguientes (6):

a. Gestión de Fallas. (Fault Management).

Se ocupa de mantener un funcionamiento correcto de la red, tratando de protegerla de los fallos que puedan aparecer en el sistema en su conjunto o en los elementos que lo componen. Ante un fallo:

- Diagnosticar y determinar rápidamente donde se localiza dicho fallo.
- Aislar a la red del fallo, reconfigurándola de forma que el impacto de éste sea lo menor posible.
- Resolver el problema de forma que la red vuelva a su estado inicial. Esto puede suponer la sustitución de los componentes fallidos.

b. Gestión de Configuración (Configuration Management).

Para poder gestionar las redes, es necesario saber qué elementos se disponen, cómo están interconectados, cual es la configuración específica de cada uno de los elementos, etc. La gestión de la configuración consiste en mantener esto en forma ordenada y documentada.

c. Gestión de Costos (Accounting).

Las redes de telecomunicaciones tienen costos asociados. Desde la amortización de los equipos, pasando por los costos de utilización de servicios, hasta los propios costos del gerenciamiento.

En general, podemos separar los costos en 3 categorías:

- *Costos directos de las telecomunicaciones:* Corresponden a los costos del uso de las redes. Estos costos tienen generalmente un componente fijo y un componente variable.
- *Costos de equipos:* Los equipos pueden ser propios o arrendados. En el caso de tener equipos propios, existe un costo de amortización, generalmente prorrateado en un período estimado como el de vida útil del equipo. Los equipos arrendados tienen un costo mensual prefijado.
- *Costos del Gerenciamiento:* Todos los aspectos de gerenciamiento (FCAPS – Gestión de configuración, de fallas, de seguridad, de desempeño y la propia gestión de costos) tienen costos asociados. Ya sea que se dispone de personal propio, o que se subcontrate el servicio a terceros, existen costos de gerenciamiento.

d. Gestión de Desempeño (Performance Management).

Tiene como objetivo asegurar el funcionamiento de las redes con la calidad de servicio deseada. Por ejemplo que el ancho de banda en los enlaces entre sucursales sea suficiente para el tráfico cursado, etc.

e. Gestión de la Seguridad (Security Management).

Es un tema complejo en sí mismo. La seguridad se enmarca dentro de los conceptos más generales de “Seguridad de la información”, que serán tratados más adelante. Como conceptos generales, la gestión de la seguridad en las redes se debe encargar de definir permisos de acceso, controlar el fraude y prevenir los ataques. El control de acceso debe definirse tanto para las redes de voz, como para las de datos. En las primeras, los controles típicos tienen que ver con los permisos para

realizar determinado tipo de llamadas y con las facilidades a las que cada usuario tiene acceso.

Administración de redes según la Unión Internacional de Telecomunicaciones-Sector de Normalización (ITU-T, siglas en inglés).

Las funciones se organizan en una estructura jerárquica de niveles que cubren todos los aspectos de gestión (en realidad, pensados para los prestadores de servicio) y clasifica las funciones que se deben realizar en cada nivel según criterios de responsabilidad. Los niveles son (6):

a. Gestión de Negocio (Business Management).

Incluye los aspectos relacionados con las estrategias de negocio; en él se definen las acciones para conseguir el retorno de la inversión, aumentar la satisfacción de los accionistas de la compañía y de los empleados, etc. Las decisiones tomadas en este primer nivel definen los objetivos estratégicos de la compañía, y condicionan las funciones y procesos de la capa de nivel de gestión de servicio. Es decir, la gestión del servicio debe estar alineada con la estrategia de negocio definida en la corporación.

b. Gestión de Servicio (Service Management).

En la capa de gestión del nivel de servicio se decide cómo gestionar los servicios que se van a prestar en la red. En este nivel se incluyen todos los aspectos relacionados con la atención a los clientes o usuarios y los de desarrollo y operación de los servicios, y se realiza la gestión de las peticiones de servicio, la calidad del servicio —Quality of Service (QoS)—, la gestión de problemas, la facturación, etc.

c. Gestión de Red (Network Management).

Los servicios están soportados sobre las redes de telecomunicaciones. El nivel de gestión de red es responsable del transporte de la información entre dos extremos y de asegurar que ésta se realiza de forma correcta. Cualquier error o problema que se detecte en este nivel y que afecte a los servicios que se prestan a los clientes o usuarios debe ser notificado hacia el nivel de gestión de servicio.

d. Gestión de Elementos de Red (Network Element Management).

Se encarga de todos los aspectos relacionados con switches, sistemas de transmisión, etc., considerados como elementos aislados. Cualquier error o evento que se produzca en un equipo que pueda afectar al transporte de la información debe ser notificado hacia el nivel de gestión de red.

2.5 Plataformas de gestión de red.

En el mercado existen plataformas o sistemas de gestión de red con los cuales se podrá aumentar la eficiencia de TI al reducir las tareas manuales y lo que le permite centrarse en proyectos de alto valor, maximizar las inversiones de hardware y software, y la autonomía de la productividad del usuario final. Un esquema de consolidación tecnológica para la administración contribuye a mejorar la eficacia del departamento de IT permitiendo la seguridad y escalabilidad del sistema operativo, la implementación de aplicaciones y gestión de la configuración deseada, aumentar la seguridad del sistema, y la gestión de los servidores, escritorios y dispositivos móviles.

Tipos de zonas de gestión.

Una zona define el alcance del control administrativo. Una zona consta de un servidor, sistema de funciones de la zona, clientes y recursos. Una zona siempre requiere el acceso a una base de datos. Existen varios tipos de zonas. Una zona utiliza límites para determinar a los clientes que estén bajo su administración. Múltiples zonas se pueden configurar en jerarquías y conectado de tal forma que puedan gestionar la utilización del ancho de banda entre las zonas. Al instalar una zona, puede ser una zona primaria o secundaria.

Entonces, al instalar otras zonas, se tienen la facultad de disponer de relaciones jerárquicas de modo que hay zonas que gestionan a otras zonas.

Zona Primario. La zona principal será el servidor primario de almacenamiento para el esquema de administración, el cual guardara los datos de sí mismo y de todas las zonas por debajo de él en una base de datos.

Zona Secundaria. Es aquella zona que se adjunta e informa a una zona principal. Remite la información que recoge de sus clientes, como los datos de los inventarios e información de estatus del sistema a su zona principal. La zona principal luego almacena los datos de las zonas primarios y secundarios en la base de datos, ver la figura 8.

La ventaja principal de usar zonas secundarias es que no se necesita un mantenimiento adicional de las base de datos. Estas se gestionan desde la zona principal al que se conectan, por lo que son utilizados con frecuencia en zonas sin administrador local. La desventaja es que se deberán unir a una zona principal y no puede ser trasladada a otra zona principal sin borrar y volver a crear la zona. Además, zonas secundarias no puede tener zonas debajo de ellos en la jerarquía.

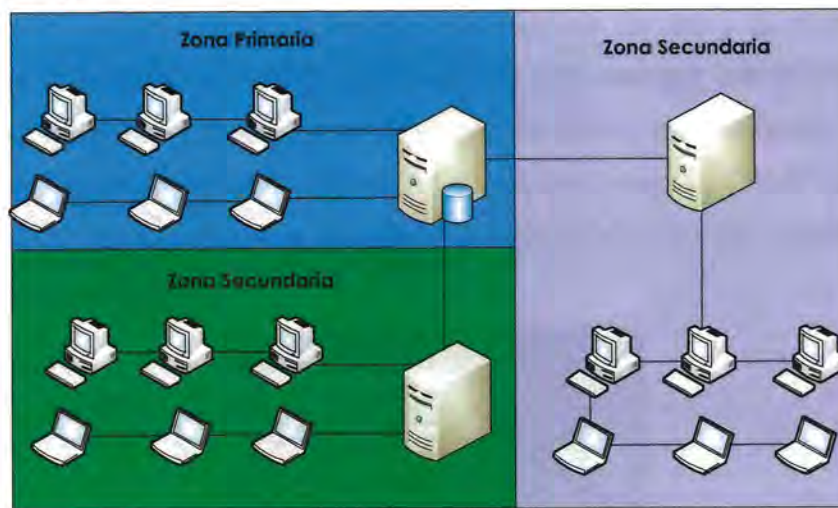


Figura 8. Jerarquía de zonas.

Las zonas son generalmente configuradas para tener una conexión rápida con sus clientes, por lo general la red de área local (LAN). Sin embargo, es común encontrar clientes que se mueven entre las zonas, dispositivos móviles que se conectan a la red, los clientes que se conectan a la red de la organización a través de dial-up o redes privadas virtuales (VPN).

2.6 SNMP (Simple Network Management Protocol).

SNMP (Simple Network Management Protocol) fue definido por el IETF (Internet Engineering Task Force) en 1989, en el RFC-1098. Desde entonces, se ha convertido en un estándar de la industria de las comunicaciones para controlar dispositivos de red desde estaciones de gerenciamiento y administración centralizadas.

SNMP es un conjunto de protocolos y funciones especialmente diseñadas para la administración de redes, que utilizan el protocolo IP. SNMP permite a los administradores de red aislar fallas y monitorear el status y la performance de las redes de comunicaciones corporativas. SNMP define dos componentes (6) (ver la figura 9):

- SNMP Manager: Es una aplicación de software desde la que se realiza la administración, en forma centralizada, de la red.
- SNMP Agent: Residen en los diversos dispositivos de red y generan información estadística acerca de sus funciones y recursos (por ejemplo, información estadística de tráfico). Esta información es almacenada en una base de datos local, llamada MIB (Management Information Base). A su vez, los "Agentes SNMP" pueden recibir y enviar información desde y hacia el "Administrador SNMP" (SNMP Manager), utilizando el protocolo UDP.

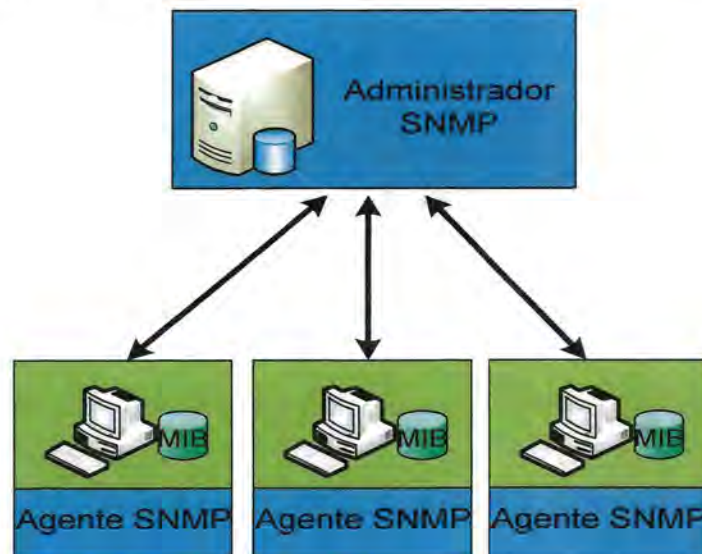


Figura 9. Arquitectura de un sistema de gestión SNMP.

2.7 System Center Configuration Manager 2007.

Con esta plataforma se podrá evaluar, desplegar y actualizar los servidores, clientes y dispositivos a través de entornos físicos, virtuales, distribuidos y móviles. Aprovechando las tecnologías de Microsoft, tales como Microsoft Windows Server Update Services (WSUS), Active Directory en Windows Server y la arquitectura de Windows, System Center Configuration Manager 2007 mejora su visión interior y control de su infraestructura de red.

Las organizaciones pueden asegurarse que los sistemas cumplen con los estados de configuración deseados para mejorar la disponibilidad, seguridad y rendimiento de los sistemas en toda la red. Algunas de las características que esta plataforma brinda son las siguientes (ver figura 10):



Figura 10 Herramientas de SCCM 2007.

- *Gestión de Activos*. Permite gestionar recursos de hardware y software, genera inventarios, para la documentación de los activos. La información que permite obtener es, que software hay instalado, cuantas copias, tiempos de las licencias, estadísticas de uso, etc.

- *Gestión de Actualizaciones de Software.* Esta herramienta usa el WSUS previamente instalado para la gestión de las actualizaciones de productos Microsoft, así como también software de tercero.
- *Gestión de la Configuración Deseada.* Con esta opción se puede verificar el estado de aplicaciones requeridas y aplicaciones opcionales, así como si hay aplicaciones prohibidas instaladas.
- *Distribución del Software.* Permita crear paquetes para ser distribuidos, ya sea a todos los clientes o a una selección de ellos, también la distribución puede ser opcional u obligatoria, esto con la ayuda de reglas de distribución.
- *Control Remoto.* Esta herramienta permita tomar el control de la computadora remota, transferir archivos.

2.8 LANDesk Management Suite.

Esta herramienta permite al personal de TI automatizar las tareas de gestión del sistema. Se podrá aumentar el rendimiento, reducir gastos y ahorrar tiempo de administración, con esta solución se podrá gestionar el hardware y software aplicable a todos los sistemas y usuarios en un entorno de red complejo. Ayuda a la asistencia técnica para los usuarios de forma fácil y segura, reduciendo así los costos y las demandas de recursos de asistencia.

Colabora a la protección de la productividad del usuario y reduce el tiempo y ancho de banda de red con tecnologías de distribución de software de eficacia superior con tolerancia a errores. Entre las herramientas que ofrece esta plataforma de administración se encuentran las siguientes (ver figura 11):



Figura 11. LANDesk Management Suite

- *Supervisión de licencia de software.* Detecta aplicaciones instaladas, permite o niega la ejecución de aplicaciones, permite la generación de informes.
- *Distribución de software.* Esta función proporciona el despliegue de las aplicaciones, mediante la creación de paquetes, cabe mencionar que esta

herramienta requirió de una configuración especial para que funcionara correctamente, esto se describe en el anexo F.

- *Implementación de sistemas operativos y migración de perfiles.* Mediante la tecnología de proxy pxe se podrá realizar la instalación de SO en equipos nuevos, así como la captura de configuración de usuario, aplicaciones y escritorios.
- *Control remoto.* Esta herramienta de la opción de tomar el control del equipo remotamente, comunicarse con el cliente para proporcionar una mejor asistencia técnica, así como transferir archivos. Con esta opción se puede reiniciar o apagar el equipo.
- *Administración de inventarios.* Crea inventarios detallados de hardware y software. Se podrá acceder a un panel de informes y publicar éstos en archivos compartidos en formato HTML, PDF, Doc, RTF o XLS.
- *Administración de dispositivos de mano.* Esta herramienta es usada para la administración de dispositivos de mano, con un consumo bajo de ancho de banda, esto es configurable.
- *Gestión de Actualizaciones de Software.* Se usa el WSUS para la distribución de actualizaciones de productos Microsoft, la administración se hace de forma independiente.

2.9 Novell ZENworks 10 Configuration Management.

Esta plataforma de administración proporciona funciones completas de gestión de servidores y estaciones de trabajo con sistemas Windows, a los que se hace referencia en conjunto con el término “dispositivos”. Se pueden emplear dispositivos Windows o Linux como servidores. Esta plataforma proporciona herramientas de gestión, tales como (ver figura 12):



Figura 12 Herramientas de ZENworks 10.

- *Gestión de Software.* Permite configurar, distribuir e instalar aplicaciones de software en los dispositivos, así como deshacer la instalación.
- *Gestión de dispositivos basada en directivas.* Directivas para crear un conjunto de configuraciones. Las directivas ayudan a gestionar los favoritos de Internet Explorer, las directivas de grupos de Windows, los derechos de archivos locales, las impresoras, etc.

- *Imágenes.* Permite tomar una imagen de discos duros y restaurar en el dispositivo.
- *Gestión remota.* Con esta herramienta se podrá administrar de manera remota, esta herramienta proporciona operaciones como el Control remoto, la Vista remota, la Ejecución remota, el Diagnóstico remoto y la Transferencia de archivos.
- *Recopilación de inventarios.* Recopila inventarios completos de software y hardware de todos los dispositivos gestionados e inventariados y permite crear y exportar informes.
- *Asset Management.* Realiza un seguimiento del uso de las aplicaciones de software (tiempo de ejecución, el tiempo de actividad, el usuario que ha entrado, el equipo y la aplicación utilizada), y gestionar las licencias.
- *Personality Migration.* Automatiza el proceso de migración de un conjunto de valores de sistema y de aplicaciones personalizados, tales como fondo de escritorio, valores de cuentas de correo electrónico, valores de servidor proxy del navegador, archivos y carpetas, correos electrónicos archivados, plantillas de Microsoft Office, macros de MS Excel, etc.
- *Linux Management.* Para gestión completa de Linux que reduce de forma significativa el trabajo del departamento de TI al disminuir la supervisión necesaria para gestionar sistemas Linux.
- *Handheld Management.* Con esta función se podrá gestionar dispositivos de mano Palm, Windows CE, Pocket PC y BlackBerry.
- *Endpoint Security Management.* Gestiona directivas de seguridad para soportes de almacenamiento extraíbles, sistemas de comunicaciones inalámbricas (incluidos MESH y WiMAX).

Capítulo 3. Desarrollo.

Para este trabajo se realizaron diversas pruebas con 3 de las principales plataformas de gestión de redes. Los equipos que se usaron se especifican en la tabla 1, el equipo Dell Studio 1537, fue usado como servidor:

Dispositivo	Fabricante	Modelo	Unidades
Laptop	Dell	Studio 1537	1
Laptop	Compaq	V3218La	1
Desktop	Compaq	EVO	1
Router	Linksys	WRT54G2	1

Tabla 2 Dispositivos de pruebas.

Las pruebas realizadas fueron bajo un entorno virtual, usando la herramienta, VirtualBox de Sun Microsystems. Esta herramienta es de licencia GNU-GPL. Se usa la configuración básica, excepto la interfaz de red, la cual se configura como adaptador puente y elegir una interfaz de red física.

3.1 System Center Configuration.

La versión usada para este trabajo fue SCCM 2007 SP1, con una licencia de evaluación de 180 días. Consultar la tabla 3 para conocer el costo de la aplicación.

- **Instalación.** Para la instalación de esta aplicación se creó la máquina virtual de acuerdo a sus especificaciones de requisitos mínimos de hardware (ver tabla 2), el sistema operativo para el servidor fue el Windows Server 2008, antes de proceder con la instalación se cubrieron los requisitos de software (ver tabla 4 y anexos A, B, C y E), seguidamente se instaló la aplicación (ver anexo D).
- **Configuración de clientes.** Para la configuración de los clientes, se procedió usando el Active Directory previamente instalado y configurado. La herramienta presenta otras opciones las cuales fueron probadas y no funcionaron, como método alternativo se agregaron los clientes de manera manual:
 - a. Compartir la carpeta "Client" localizada en el servidor de SCCM en
x:\Program Files\Configuration Manager\Client

b. Desde el cliente abrir una ventana de línea de comandos y ejecutar:

```
\\server\share\ccmsetup.exe /source:\\server\share\ /mp:servidorSCCM /logon  
SMSSITECODE=XXX
```

Dónde:

Server= Nombre del servidor de Configuration Manager

Share= Folder compartido donde está el archivo ccmsetup.exe

MP= Management Point asignado al cliente.

XXX= Nombre del Site de SCCM al que será asignado el cliente.

Ejemplo:

```
\\ServidorSCCM\Client\ccmsetup.exe /source:\\ServidorSCCM\client\  
/mp:ServidorSCCM /logon smssitecode=SC1
```

NOTA: este método resultará tedioso si se considera agregar muchos clientes. Pues se tendrá que repetir el método una y otra vez, por cada computadora.

- Herramientas de administración: Entre las herramientas que se probaron se encuentran las siguientes.
 - *Gestión de Activos.* Excepto el problema de descubrimiento de clientes, las funciones como Software Metering, Reporting, funcionan correctamente.
 - *Gestión de Actualizaciones (Software Update).* Esta herramienta integra el WSUS, funciona correctamente.
 - *Gestión de la Configuración Deseada (Desired Configuration Manager).* Se bloqueó la aplicación Messenger, la cual al tratar de ejecutar en el cliente, no inicio, también se configuraron permisos de lectura, escritura, instalación de software, obteniendo un resultado positivo.
 - *Distribución del Software (Software Distribution).* Cuando se realizó la primera prueba, se distribuyó 2 paquetes (Firefox y Office 2007), el tiempo fue de instalación a un cliente fue de 10 minutos y poco más de 24 hrs

respectivamente, para solucionar el problema se instaló Hotfix (KB932303), al realizar por segunda vez la prueba, esta tardo 1 min y 15 min respectivamente.

- *Control Remoto.* Al realizar la primera prueba arrojó un error "Unable to locate Remote Assistance file", para solucionar el problema, hay que habilitar esta función en ambos lados tanto en el Server como en el Cliente.

3.2 LANDesk Management.

La versión usada para este trabajo fue LANDesk Management 8.8, con una licencia de evaluación de 60 días. Consultar la tabla 3 para conocer el costo de la aplicación

- *Instalación.* Para la instalación de esta aplicación se creó la máquina virtual de acuerdo a sus especificaciones de requisitos mínimos de hardware (ver tabla 2), el sistema operativo para el servidor fue el Windows Server 2003, antes de proceder con la instalación se cubrieron los requisitos de software (ver tabla 4 y anexo F).
- *Configuración de clientes.* Para la configuración de los clientes, se procedió usando la herramienta Agente Landesk, con la cual se obtuvo un resultado erróneo, por consiguiente se usa la opción manual, la cual se describe en el anexo 6.6.

NOTA: este método presenta el mismo problema que SCCM.

- *Herramientas de administración:* Entre las herramientas que ofrece esta solución, se encuentran las siguientes:
 - *Supervisión de licencia de software.* Al agregar de manera correcta a las computadoras clientes, esta función presenta información de las aplicaciones instaladas, versión, tiempo de licencia, funciona de manera correcta.

- *Distribución de software.* Al realizar la primera prueba se distribuyó 2 paquetes (Firefox y Office 2007), usando las guías proporcionadas por el fabricante, da como resultado un error de distribución. Para resolver este problema se configuraron algunos parámetros extras al IIS, para compartir una carpeta, en la cual se guardaron las aplicaciones a distribuir, al realizar la prueba de nuevo. Así como también se bloqueó la aplicación Messenger, la cual al tratar de ejecutar en el cliente, no inicio, bloqueo de memorias flash, bloqueo de puertos serial, obteniendo resultados positivos.
- *Control remoto.* Al iniciar esta herramienta, se tendrá la opción de apagar o reiniciar la computadora cliente, entablar una conversación con el usuario vía chat, transferir aplicaciones mas no la instalación automática. Su interfaz es un poco lenta y tiende a bloquearse por segundos así como también al momento de iniciar la aplicación primero pide permiso al usuario cliente, dando la posibilidad de rechazar y de esta forma cerrar el control remoto.
- *Administración de inventarios.* Para la recolección de inventarios funciona de forma correcta, no requiere mayor configuración, a menos que se desee lanzar inventarios de forma personalizada.
- *Gestión de Actualizaciones de Software.* Puesto que LANDesk no posee de forma integrada una función para la actualización, se instaló un servidor de actualizaciones de forma independiente.

3.3 ZENworks 10 Configuration Management.

La versión usada para este trabajo fue ZENworks 10 CM SP1, con una licencia de evaluación de 60 días. Consultar la tabla 3 para conocer el costo de la aplicación.

- Instalación. Para la instalación de esta aplicación se creó la máquina virtual de acuerdo a sus especificaciones de requisitos mínimos de hardware (ver tabla 2), el sistema operativo para el servidor fue el Windows Server 2008, antes de proceder con la instalación se cubrieron los requisitos de software (ver tabla 4 y anexos G).
- Configuración de clientes. Para la configuración de los clientes, esta aplicación presenta diferentes opciones, entre las que se encuentran, mediante Active Directory, Descubrimientos de dispositivos mediante direcciones IP, entre otras. Para este caso, se usó la segunda opción, la instalación se realizó de una forma sencilla y sin mayores problemas, como de configuraciones extras.
- Herramientas de administración: Entre las herramientas que ofrece esta solución, se encuentran las siguientes:
 - Gestión de Software. La aplicación funcionó de forma correcta, solo se configuraron los paquetes de distribución para este caso Firefox y Office 2007, está se lanzó de manera correcta.
 - Gestión de dispositivos basada en directivas. Funcionó de manera correcta, se bloqueó el Messenger en el cliente, dando resultados positivos.
 - Gestión remota. Presenta una interfaz sencilla, pero sin problemas de bloqueos, al correr la función se tienen 2 opciones, por permiso o derechos, la primera se debe obtener la aprobación del usuario, la segunda no requiere aprobación, pero se debe contar con el usuario y contraseña del administrador. Las sesiones se protegen mediante Secure Socket Layer (protocolo TLSv1).

- *Recopilación de inventarios.* Para la recolección de inventarios funciona de forma correcta, no requiere mayor configuración, a menos que se desee lanzar inventarios de forma personalizada.
- *Asset Management.* Con esta función se obtuvo la información de las aplicaciones (tiempo de ejecución, el tiempo de actividad, el usuario que ha entrado, el equipo y la aplicación utilizada), y gestionar las licencias, no requiere mayor configuración.
- *Endpoint Security Management.* Con esta función se probó el bloqueo de memorias flash, bloqueo de puertos serial, obteniendo resultados positivos, ya sea dando permiso lectura o escritura.

Tablas Comparativas.

Producto	Procesador	RAM	Disco Duro
SCCM 2007 ²	1.2 GHz	1 GB	1.5 GB
LANDesk Management 8.8 ³	2.0 GHz	2 GB	2.0 GB
ZENworks 10 Configuration Management ⁴	2.0 GHz	2 GB	2.0 GB

Tabla 3. Requisitos mínimos de hardware.

Producto	Costo	Características
SCCM 2007	\$579.00 ¹	Licencia de servidor para la plena aplicación, servidor y cliente de administración.
SCCM 2007 / SQL Server	\$1,321.00 ¹	Licencia de servidor para la plena aplicación, el servidor y administración de clientes.
ZENworks 10 Configuration Management	\$199.00 ³	El precio corresponde a la versión Enterprise.
LANDesk Management 8.8	\$107.00 ⁵	Más \$92.00 por cada computadora que se agregue.

Tabla 4. Costos de las plataformas.

En las tablas anteriores se puede observar una comparación entre las diferentes plataformas, tanto en los requisitos de hardware como el costo de las licencias, se aprecia que SCCM 2007 es la plataforma que menos recursos de hardware requiere, pero la solución más costosa; a diferencia de LANDesk y ZENworks que sus requerimientos de hardware son iguales, la variación se encuentra en sus costos, siendo el más económico ZENworks.

² <http://www.microsoft.com/systemcenter/configurationmanager/en/us/default.aspx>

³ <http://www.landesk.com.mx>

⁴ <http://www.novell.com/es-es/products/zenworks/configurationmanagement>

⁵ LANDesk Sales Representatives, via email

Sistema	Clientes	Active Directory	IIS	Base de Datos	Otros
System Center Configuration Manager 2007	Todas las versiones de Windows.	Requerido para instalar el server y agregar dispositivos. Su instalación requiere parámetros especiales.	Versión 6 o 7. Con extensiones WebDAV	SQL Server 2005/2008 Standard/Enterprise.	WSUS 3.0 SP2
LANDesk Management Suite 8.8	Windows 2000/2003/XP Windows 95/98 Macintosh UNIX Linux.	No requerido para instalar server. Usado en una de las opciones para agregar dispositivos.	Versión 6 o 7. Debe instalarse antes que .NET Framework 2/3.	SQL Server 2005/2008 Express.	.NET Framework 2/3 Monitorización/Alertas (SNMP). Microsoft WSE 2.0SP3.
Novell ZENworks 10 Configuration Management	Windows Server 2003/2008. Linux SUSE 10.	Usado en una de las opciones para agregar dispositivos.	No requerido.	Sybase SQL Anywhere 10.0.1 ó Microsoft SQL Server 2005 Enterprise/Standard ó Oracle 10g Standard	.NET Framework 2/3

Tabla 5. Requisitos de software.

En la tabla anterior se puede observar que SCCM 2007 es la aplicación que más requisitos de software necesita para ser instalada, haciendo de su implementación la más complicada de las plataformas, LANDesk no presenta tantos requisitos de software en comparación con SCCM 2007 pero si más que ZENworks, siendo esta última la plataforma más sencilla de instalar con menos requisitos.

Capítulo 4 Conclusiones.

4.1 Complejidad

La complejidad creciente y el alcance del uso de la computación han propiciado que la información se concentre en manos de unas cuantas personas. Los sistemas de administración en la organización son elementos importantes para la seguridad en la computación. Las funciones principales, tales como las funciones de control se deben definir con claridad. Todos los procedimientos deben incluir evidencias sistemáticas.

4.2 Seguridad

La seguridad de los sistemas constituye una parte muy técnica y compleja de la administración. Se requiere un enfoque metódico para identificar las "puertas falsas", definir controles discretos y garantizar que estos se lleven a cabo y se vigilen. Esta revisión debe incluir el equipo y los programas, de las computadoras principales y terminales.

El seguimiento del desempeño del computador central y las terminales es una función administrativa y de seguridad importante. Se deben considerar cuidadosamente los recursos disponibles de los programas existentes o sus modificaciones.

Nos hemos acostumbrado a que los sistemas informáticos siempre tienen que funcionar, pero la creciente complejidad y la presión de dependencia hacen que su gestión y administración deban ser las adecuadas. A continuación se describen las tres plataformas de gestión que abarca este trabajo:

System Center Configuration Manager 2007.

Este programa brinda grandes opciones de configuración con equipos los cuales tengan Windows como sistema operativo, pero nos limita en cuanto al servidor ya que solo es compatible con Windows Server, además de tener un entorno Active Directory tanto para la instalación del servidor como para la de los clientes. Requiere la instalación de una instancia de base de datos SQL Server Enterprise esto aumenta el costo de implementación. La gestión de las actualizaciones es

mediante un servidor de actualizaciones, este puede ser instalado en el mismo servidor o en otro.

En general la instalación es más complicada en comparación a los otros productos. La administración puede ser mediante consola o vía web. Y la instalación de los clientes es mediante el Active Directory, esta no presenta ningún problema si se cuenta con esta herramienta y que los equipos y usuarios estén debidamente configurados. Presento algunos problemas al usar sus herramientas, las cuales se pudieron resolver.

LANDesk Management Suite 8.8

En la versión 8.8 no es compatible con Windows server 2008 pues presenta un problema con el IIS y .NET Framework 2. Es un requisito tener instalado primero el IIS y después instalar el .NET Framework 2, pero en particular la versión Server 2008, ya tiene instalado el .NET, es por ello que no es posible instalarlo, aunque podemos usar otro sistema operativo para el servidor. En general la instalación no presenta mayor complicación.

El agente se instala mediante Active Directory o de forma manual, esto no representaría ningún problema en redes con pocas terminales. La gestión de actualizaciones se hace mediante un servidor de actualizaciones, que se debe instalar por separado, es similar al SCCM 2007, se podrá usar el servidor de actualizaciones. Soporta las versiones Express del SQL Server, esto no incrementa el costo de implementación. La administración puede ser mediante consola o vía web.

Novell ZENworks 10 Configuration Management.

Puede ser usado tanto en Windows Server 2008 o en sistemas Linux, no presenta ningún problema al momento de su instalación. La instalación es mucho más sencilla con respecto a los anteriores. Los requisitos de software son

mínimos. Si no se cuenta con un servidor de base de datos, se instalará un manejador propio en el proceso. La instalación del agente puede ser por Active Directory o mediante descubrimiento por rango de direcciones IP, para ello basta con proporcionar los datos de la cuenta del administrador del equipo a gestionar, esto es muy útil en redes con grandes terminales. La administración es vía web. La herramienta de control remoto así como de transferencia de archivos es más rápida que en las plataformas anteriores. En general presenta una interfaz vía web más sencilla pero potente, la cual se enfoca en la administración y el consumo mínimo de recursos.

Con base a las pruebas realizadas, se llegó a la conclusión de que la distribución de Novell ZENworks 10 es la más adecuada para la administración de un centro de cómputo, pues es la de menor costo, al momento de su instalación no requiere modificar la infraestructura y no presenta mayor problema, además que es muy sencilla. Ofrece una gama de herramientas, una interfaz fácil de comprender y en las pruebas realizadas no se presentó mayor inconveniente. Esta herramienta no presente ningún problema en las pruebas.

Como parte de la solución, para la administración de las actualizaciones se trabajará con Windows Server Update Services que es una distribución de Microsoft.

4.3 Trabajo futuro.

Puesto que todas las pruebas e instalaciones se realizaron en un entorno virtual, el siguiente pasó, sería la implementación de la plataforma de gestión, con esto los administradores podrán controlar y administrar de manera centralizada y a distancia utilizando Internet para ingresar al sitio Web de la aplicación, para poder entrar al sitio web de la aplicación. Además, esta plataforma permitirá el control de las aplicaciones que se deseen instalar o las que deban de ser denegadas, por no ser aplicaciones necesarias e incluso que solo consuman recursos.

Anexos.

Anexo A Instalación de Active Directory en Windows Server 2008.

1. Abrir el Administrador del servidor.
2. Clic derecho sobre Funciones y clic sobre agregar funciones.
3. Elegir Servicios de Dominio de Active Directory, y clic en siguiente.
4. Al terminar, clic en cerrar, saldrá un asistente para configurar el AD.
5. Clic en Crear un Dominio nuevo en un bosque nuevo y siguiente.
6. Tecleamos el FQDN del dominio. Ejemplo *lab.net* y clic en siguiente.
7. En nivel funcional del bosque, elegir Windows Server 2008.
8. Seleccionar Servidor DNS y clic en siguiente.
9. En la siguiente pantalla se debe elegir el tipo de direccionamiento (Estático o dinámico), en este caso elegir el estático.
10. Cuando se termine la instalación, el sistema se reiniciará.

Anexo B Instalación de Web Server IIS.

Web Server IIS versión 6.

1. Herramientas administrativas / Administre su servidor.
2. Agregar o quitar Función. Elegir Configuración Personalizada
3. Clic en Servidor de Aplicaciones (IIS, ASP.NET).
4. Elegir las opciones: Extensiones de Servidor de FrontPage y Habilitar ASP.NET.
5. Presenta un resumen de lo que se instalara. Clic en Finalizar.

Web Server IIS versión 7.

1. Abrir el Administrador del servidor.
2. Clic derecho sobre Funciones y clic sobre agregar funciones.
3. Elegir Servidor Web IIS 7, instalar otras características requeridas.
4. Elegir las opciones que se desea instalar.
 - a. Desarrollo de Aplicaciones:
 - Extensiones ISAPI, Filtros ISAPI, Extensibilidad de .NET.

5. Instalar. Al finalizar la instalación, se instala WebDAV.
6. Ejecutar el instalador. Se acepta el acuerdo de licencia e Install.
7. Herramientas administrativas, en el menú inicio.
8. Abrir Administrador de IIS. Seleccionar el servidor y clic en sitios.
9. Clic a Default Web Site. Abrir WebDAV Authoring Rules.
10. Clic sobre Enable WebDAV. Después clic en Add Authoring Rule.
11. Seleccionar las siguientes opciones:
 - a. All content.
 - b. Specified roles or user groups: teclear administrator.
 - c. Permissions: Read, Source y Write.
12. Dar clic en aceptar.
13. Abrir el administrador del servidor.
14. Clic en funciones, en Servidor web y en agregar servicios de función.
15. Elegir: Autenticación básica, Autenticación de Windows.
16. Clic en siguiente y en instalar.
17. Al terminar, abrir el administrador de IIS, y clic en Autenticación.
18. En Autenticación de Windows, clic derecho y habilitar.
19. Agregar a los servicios del IIS compatibilidad con la administración de IIS 6.
20. Abrir el administrador del servidor.
21. Clic en funciones, en Servidor web y en agregar servicios de función.
22. Elegir Compatibilidad con la administración de IIS 6. Instalar.
23. Abrir el administrador del servidor. Clic derecho en Características. Y en agregar características.
24. Elegir Extensiones de servidor BITS. Clic siguiente / Instalar.
25. Instalar ASP en IIS, abrir el administrador del servidor.
26. Funciones, en Servidor web (IIS) y en agregar servicios de función.
27. Seleccionar ASP, clic en siguiente y en instalar.
28. Con esto se termina la instalación de IIS 7.

Anexo C Instalación y configuración de SQL Server Standard 2005.

1. Insertar el DVD de SQL Standard 2005.
2. Al iniciar la instalación, aparece un cuadro en el cual indica que este programa tiene un problema de compatibilidad. Para solucionar este problema, al terminar la instalación se debe instalar el SP2 de SQL. Clic en Ejecutar programa.
3. Se acepta la licencia y clic en Next.
4. Clic en Install. Al terminar la instalación dar clic en Next.
5. Mostrará un Wizard para terminar de instalar el SQL. Clic en next, he iniciara un check al finalizar. Clic en next.
6. Proporcionar el nombre del propietario y compañía. clic en Netx.
7. En **Components to Install**, elegir todas las opciones y clic en next.
8. En **Instance Name**, elegir Default instance y clic en next.
9. En **Service Account**, seleccionar *Customiza for each account*, en Service: elegir *SQL Server Agent*, en *Use the built-in System account: Local system*. En Start services elegir todas las opciones excepto SQL Browser.
10. En **Authentication Mode**, elegir *Windows Authentication Mode*. Clic en next.
11. En **Collation Setting**, elegir *Latin1_General*, y clic en next.
12. Clic en next, en la siguiente pantalla dar clic en Finish.
13. Instalar el SP2 de SQL.
14. Abrir el instalador. Mostrará la bienvenida, dar clic en Next.
15. Aceptar los términos de la licencia / Elegir las funciones que se instalaran.
16. En **Authentication**, seleccionar *Apply selection to all instances*, Authentication: Windows Authentication. Clic en next.
17. En **Running Processes**, elegir MSSQLSERVER y next. Clic Install.
18. Mostrar una advertencia, clic en Aceptar.
19. Al terminar el proceso de la instalación, dar clic en next.
20. En **Installation Complete**, dar clic en next.
21. En **Additional Information**, solo dar clic en Finish.
22. En **SQL Server 2005 User Provisioning Tool for Vista**, elegir las 2 opciones y clic en OK. Con esto se termina de instalar SQL Server 2005.

Anexo D Instalación y configuración de SCCM 2007.

Para poder instalar el SCCM 2007 (descargar de la página oficial del producto), es necesario que en el servidor este instalado los siguientes aplicaciones o que estén presentes en el entorno de red.

- a. **Active Directory** ver anexo A.
 - b. **IIS 7** ver anexo B.
 - c. **SQL Server 2005** ver anexo C
 - d. **WSUS 3.0** ver anexo E.
- a. Ejecutar el instalador de SCCM 2007, dar clic en *run the prerequisite checker*. Esto para comprobar que el servidor cumpla con todos los requisitos necesarios para la instalación de este paquete.
 - b. Escribir el nombre del servidor en el cual está instalado SQL Server, y en el cual se instalará SCCM 2007, y clic en ok.
 - c. Hasta este punto, sólo muestra 1 error y 1 warning:
 1. Microsoft Remote Differential Compression (error).
 - Administrador del servidor / agregar características.
 - Elegir Compresión Diferencial Remota. Clic en siguiente, instalar.
 2. Schema extensions (warning).
 - Ejecutar en el símbolo de sistema con propiedades de administrador, extadsch.exe que se encuentra en `|\SCConfigMgr07_EVAL_EN\SMSSETUP\BIN\I386`, dentro del disco de instalación de SCCM 2007.
 - Abrir *Editor ADSI*, para crear el contenedor de SCCM 2007.
 - Dentro de *CN=System*, clic derecho, *Nuevo/Objeto*, elegir *Container*.
 - En valor, escribir *System Management*, clic en siguiente y terminar.
 - Dentro de *CN=System*, dar clic derecho a *CN= System Management*, y clic en *propiedades*. Y clic en la pestaña de seguridad.
 - Clic en *agregar*, en tipos de objetos elegir, computadoras y escribir el nombre del servidor, ejemplo: *WSUS* y clic en comprobar. Aceptar.
 - En Permisos, dar clic en control total.
 - Clic en opciones avanzadas, buscar *WSUS* y doble clic.
 - En *Aplicar a*: elegir Este objeto y todos los descendientes. Aceptar.

- Nuevamente clic en aceptar.
- d. Abrir el SCCM 2007, clic en *Install Configuration Manager 2007 SP1*.
- e. Elegir *Install a Configuration Manager site server*. Clic en siguiente.
- f. Aceptar los términos de la licencia y clic en siguiente.
- g. Elegir *Custom settings*, clic en siguiente.
- h. Elegir *Primary site*, clic en siguiente.
- i. Pedirá la clave del producto, escribirla y clic en siguiente.
- j. Elegir donde se desea instalar el SCCM y dar clic en siguiente.
- k. Teclar el *Site code* y *Site Name*. Ejemplo *PPR* y *Lab de Redes*. Siguiendo.
- l. En *Site mode* elegir *Configuration Manager mixed Mode*. Siguiendo.
- m. Elegir todas las opciones que se desean instalar, Siguiendo.
- n. Teclar el nombre del servidor SQL Server, y clic en siguiente.
- o. Escribir el nombre del proveedor de SQL, clic en siguiente.
- p. Elegir *Install a management point* y clic en siguiente.
- q. Especificar un número de puerto, Ejemplo: *Use default port (80)* y siguiente.
- r. Configurar las actualizaciones solo dar clic en siguiente.
- s. Especificar el directorio en el cual guardara las descargar. Siguiendo.
- t. Para este paso el servidor debe tener acceso a internet, pues iniciara la descarga de los manifiestos de Microsoft de sus aplicaciones. Este paso puede demorar, dependiendo de la velocidad de la conexión. Siguiendo.
- u. Mostrará un resumen de lo que instalara. Siguiendo.
- v. Mostrará una ventana la cual indica que se han completado todos los requisitos, dar clic en *Iniciar Instalación*.
- w. Comenzará la instalación. Al finalizar dar clic en terminar.

Anexo E Instalación de WSUS 3.0 SP2.

Prerrequisitos de Software.

1. Microsoft .NET Framework 2.0 o versiones posteriores.
2. IIS 6.0 o versiones posteriores. Además de la configuración predeterminada, seleccione ASP.NET, Autenticación de Windows, Compresión de contenido dinámico y Compatibilidad con la administración de IIS 6. Clic en Siguiente
3. Una de las siguientes bases de datos:
 - a. Microsoft SQL Server 2008 Express, Standard o Enterprise Edition
 - b. SQL Server 2005 SP2
 - c. Windows Internal Database
4. Microsoft Management Console 3.0
5. Microsoft Report Viewer 2008 redistribuible.

Instalando WSUS 3.0 SP2.

1. Ejecutar el paquete. La primera pantalla, es la bienvenida, clic en siguiente.
2. Elegir Instalación completa incluida la consola de administración o solo la consola de administración. Clic en siguiente.
3. Aceptar el contrato de licencia. Clic en siguiente.
4. Especificar el directorio en el cual se almacenaran las actualizaciones, por default es C:\WSUS. Clic en siguiente.
5. De no contar con una base de datos, WSUS instalara *Windows Internal Database*. Clic en siguiente.
6. Definir la dirección Web del WSUS, por default usara el nombre del servidor y el puerto 80. Clic en siguiente.
7. Mostrará un resumen de lo que se instalara. Dar clic en finalizar.

Configurar el WSUS 3.0 SP2.

1. Elegir el servidor del cual se descargarán las actualizaciones, en caso de tener otro servidor WSUS proporcionar dirección y puerto, de lo contrario, elegir Sincronizar desde *Microsoft Update*. Clic en siguiente.
2. Si se tiene un servidor proxy proveer los datos relevantes. Clic en siguiente.
3. Dar clic en *Iniciar conexión*, para que el servidor descargue los catálogos de *actualizaciones disponibles, tipos de productos e idiomas*. Clic en siguiente.

4. Elegir el idioma de las actualizaciones. Clic en siguiente.
5. Definir los productos para los cuales se obtendrán las actualizaciones. Siguiente.
6. Determinar la clasificación de actualizaciones para sincronizar. Siguiente.
7. Programar la sincronización del servidor con *Microsoft Update*. Siguiente.
8. Elegir si se desea iniciar la consola de administración de WSUS y la primera sincronización. Clic en finalizar.

Agregar Grupos en WSUS 3.0 SP2.

1. Clic en *Herramientas Administrativas > Windows Server Update Services*.
2. Clic en *Equipos*, clic derecho sobre *Todos los equipos*, elegir *Agregar grupos de equipos*. Ejemplo 1. *En AD*, Ejemplo 2. *PPR*. Clic en *Aceptar*

Autorizar las actualizaciones en WSUS 3.0 SP2.

1. Clic en *Herramientas Administrativas > Windows Server Update Services*.
2. Clic en *Actualizaciones* y elegir la categoría que desee.
 - a. Todas las Actualizaciones, Actualizaciones críticas, Actualizaciones de seguridad y Actualizaciones de WSUS.
3. Elegir la o las actualizaciones que desee aprobar. Clic derecho y *Aprobar*.
4. Definir el grupo de equipos para el cual se aprobarán las actualizaciones. Clic derecho sobre el grupo y elegir *Aprobar para su instalación*, clic en *aceptar*. Saldrá un cuadro del proceso de aprobación dar clic en *cerrar*. La actualización no estará disponibles hasta que el servidor la haya descargado.

Agregando clientes al WSUS 3.0 SP2.

Antes de iniciar esta tarea, es necesario configurar el WSUS.

1. Clic en *Herramientas Administrativas > Windows Server Update Services*.
2. Clic en *Opciones*. Clic en *Equipos*, elegir *Usar directivas de grupo o la Configuración de Registro de los equipos*. Clic en *Aceptar*.

Para agregar equipos que obtengan las actualizaciones desde un servidor WSUS existen 2 formas de realizar esta tarea:

a. Equipos gestionados por medio de Active Directory (AD).

1. Como primer requisito, el servidor debe estar en un entorno AD.
2. Ir a *Herramientas Administrativas, Administración de directivas de grupo*.
3. Clic en el dominio el cual se desea configurar > *Objetos de directivas de grupo*.

4. Clic derecho sobre *Default Domain Policy* y clic en editar.
5. Clic sobre *Configuración del Equipo, Directivas, Plantillas de Administración, Componentes de Windows, Windows Update.*
6. Editar las siguientes reglas:
 - a. Configuración de Actualizaciones automáticas.

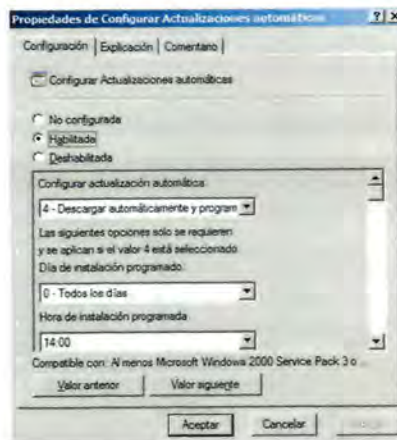


Figura 13. Configuración de Actualizaciones automáticas

- b. Especificar la ubicación del servicio Windows Update en la intranet.

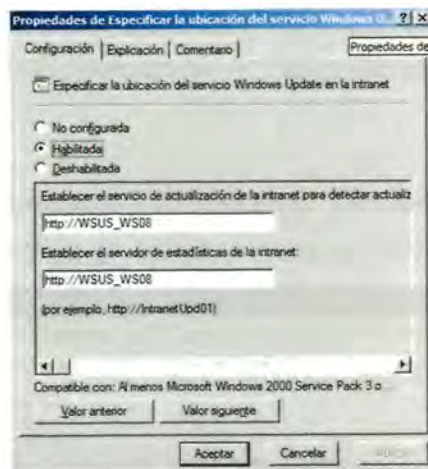


Figura 14. Ubicación del servicio Windows Update en la intranet

- c. Frecuencia de detección de Actualizaciones automáticas.
 - d. Habilitar destinatarios del lado cliente. En esta opción se especifica el grupo definido en el servidor WSUS. Ejemplo *En AD*.

b. Equipos no gestionados por medio de Active Directory (AD).

1. Dirigirse directamente al equipo el cual se agregará al servidor WSUS.
2. Clic en Inicio, Ejecutar y teclear *gpedit.msc.* (Windows XP)
3. Clic en Directiva de equipo local.
4. Clic sobre *Configuración del Equipo, Directivas, Plantillas de Administración, Componentes de Windows, Windows Update.*
5. Editar las siguientes reglas:

a. Configuración de Actualizaciones automáticas, ver la figura 15.

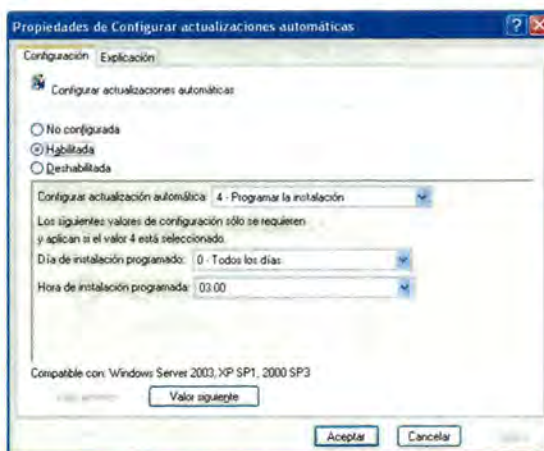


Figura 15. Configuración de Actualizaciones automáticas

b. Especificar la ubicación del servicio Windows Update en la intranet (en esta caso http://WSUS_WS08 o dirección IP), ver la figura 16.

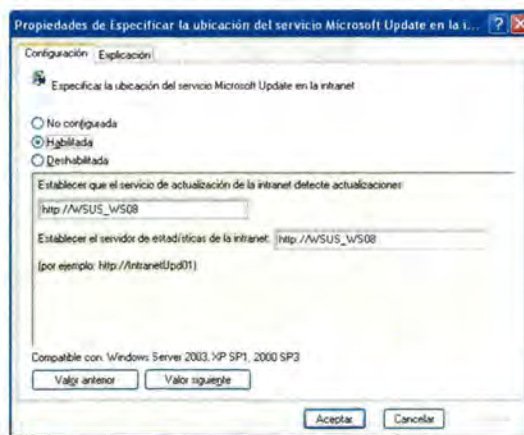


Figura 16. Ubicación del servicio Windows Update en la intranet.

- c. *Frecuencia de detección de Actualizaciones automáticas.*
- d. *Habilitar destinatarios del lado cliente.* En esta opción se especifica el grupo definido en el servidor WSUS. Ejemplo *PPR*.

En ambos casos para verificar que la configuración fue correcta, ir a *Panel de Control, Actualizaciones Automáticas*, en la cual la opción estará deshabilitada, ver la figura 17.



Figura 17. Actualizaciones automáticas en los equipos gestionados.

Anexo F Instalación de LanDesk en Windows Sever 2003.

1. Instalar .NET Framework 2.0 y 3.0

- a. Descargar el .NET Framework 2.0. Ejecutar el instalador.
- b. Descargar el .NET Framework 3.0. Ejecutar el instalador.

2. Microsoft WSE 2.0 SP3.

- a. Descargar el Microsoft WSE 2.0 SP3. Ejecute el instalador.

3. Monitorización/Alertas (SNMP).

- a. Clic en Inicio, panel de control, Agregar o quitar programas
- b. Clic en Agregar o quitar componentes de Windows.
- c. Seleccionar Herramientas de administración y supervisión.
- d. Clic en Detalles y verificar que se encuentre seleccionado el SNMP.
- e. Clic en aceptar > siguiente > Finalizar.

Después de haber instalado estos paquetes, lo siguiente es, instalar LanDesk.

4. Instalación de LanDesk.

Antes de iniciar la instalación, se necesita configurar, algunos parámetros de seguridad:

1. Haga clic en Inicio, Ejecutar y escribir ***gpedit.msc***. Haga clic en Aceptar.
2. Ir a Directiva de equipo local, Configuración del equipo, Configuración de Windows, Configuración de seguridad, Directivas locales, Opciones de seguridad.
3. Las siguientes políticas deben configurarse como se muestra:
 - ***Miembro de dominio***: Cifrar o firmar digitalmente datos de un canal seguro (siempre): Deshabilitado.
 - ***Cliente de redes de Microsoft***: firmar digitalmente las comunicaciones (siempre): Deshabilitado.
 - ***Servidor de red Microsoft***: firmar digitalmente las comunicaciones (siempre): Deshabilitado.
 - ***Acceso de red: deja los permisos de Todos para aplicarse a usuarios anónimos***: Habilitado.
 - ***Acceso de red: restringir acceso anónimo a canalizaciones con nombre y a recursos compartidos***: Deshabilitado.

- **Seguridad de red:** no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña: Habilitado.
- **Seguridad de red:** Nivel de autenticación de LAN Manager: Enviar respuestas LM y NTLM.

Ahora iniciar con la instalación:

- Ejecutar el programa de instalación. Elegir el directorio temporal.
- Elegir que se instalará en este caso, LanDesk Management Suite.
- Elegir el Idioma que se instalará. Mostrará una ventana de bienvenida.
- Aceptar los acuerdos de licencia, siguiente.
- Elegir la carpeta donde se instalará LanDesk, siguiente.
- Elegir la base de datos, Ejemplo: crear una nueva base de datos, siguiente.
- Definir la contraseña de la base de datos, siguiente.
- Determinar el nombre de la organización y el nombre del certificado que se creará, siguiente.
- Presentará un resumen, siguiente. Al terminar mostrará el siguiente cuadro, ver la figura 18.



Figura 18. LanDesk instalación.

- Proceder a configurar los servicios.
- Aun no se ha instalado el SQL server, LanDesk lo instala automáticamente.
- Al finalizar notificará que ha concluido con éxito la instalación.

Agregar dispositivos para administrar.

1. En el servidor compartir la carpeta **LDLOGON**, que se encuentra en C:\Archivos de programa\LANDesk\ManagementSuite\

2. Ir al dispositivo que se agregará, abrir el explorador de Windows y teclear \\IP_Server_LanDesk. Entrar a la carpeta **LDLOGON**.
3. Ejecutar WSCFG32.EXE, (el programa de configuración de dispositivos), ver la figura 19.

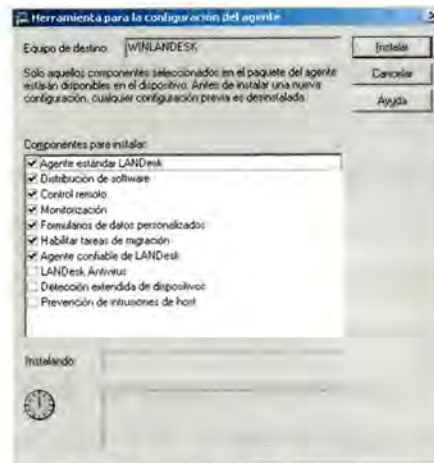


Figura 19. LanDesk agente.

4. Seleccionar los componentes a instalar.
5. El dispositivo se agregará automáticamente al servidor LanDesk.

Distribución de software.

Para configurar un servidor Web para la distribución de software:

1. Cree un directorio en el servidor Web. Ejemplo: c:\inetpub\wwwroot.
2. Copiar los paquetes que se distribuirán en este directorio.
3. Panel de control, doble clic en Herramientas administrativas > Administrador de servicios Internet.
4. En el panel derecho, doble clic en el icono con el nombre del dispositivo y haga clic en Sitio Web predeterminado.
5. En una zona vacía del panel derecho, clic derecho en Nuevo y haga clic en Directorio virtual.
6. En el asistente, clic en Siguiente e introduzca un alias para el directorio. Siguiente.
7. Introduzca la ruta de acceso o desplácese hasta ella, clic en Siguiente.
8. En el cuadro de diálogo *Permisos de acceso*, habilite *Ejecutar archivo de comandos* y *Examinar*. Clic en Siguiente > Finalizar.

9. En el menú contextual del directorio virtual que ha creado, clic en Propiedades.
10. En la ficha Documentos, desmarcar la opción *Habilitar página de contenido predeterminado* y Aceptar.
11. En la ficha Seguridad del directorio, haga clic en el botón Editar en el cuadro Acceso anónimo y control de autenticación. Seleccione la opción *Autenticación integrada de Windows*. Deshabilitar Digest authentication para servidores de dominio de Windows.
12. Habilitar el puerto 80 del servidor Web, en el panel izquierdo, haga clic con el botón derecho en Sitio Web predeterminado.
13. Clic en Propiedades. En el cuadro de diálogo Identificación del sitio Web, Puerto TCP: 80. De no ser así, clic en *Avanzadas* y añadir el puerto.
14. Asegúrese de que el sitio Web se encuentre disponible al abrir un explorador e introducir la URL del servidor Web y el directorio virtual. Por ejemplo, si el nombre del servidor Web es Test y el nombre del directorio virtual es Paquetes, introduzca la URL siguiente:

http://Test/Packages

Debería aparecer una lista de los paquetes que se han copiado en este directorio.

Configuración de servidores Web de IIS 6 para la distribución de software:

- Configurar el directorio virtual que almacena los paquetes.
- Registrar un tipo MIME con IIS.

Para registrar los tipos de archivo MIME

1. Inicie Internet Information Services (IIS) Manager.
2. Expanda el equipo local en el árbol.
3. Clic en Sitios Web > Sitio Web predeterminado.
4. Menú contextual en carpeta compartida Web del paquete, clic en Propiedades.
5. Clic en la ficha Encabezados HTTP. Clic en Tipos MIME.
6. Clic en Nuevo. En el cuadro Extensión, escribir un asterisco (*).
7. En el cuadro Tipo MIME, escribir un nombre.
8. Clic en Aceptar dos veces para aplicar los cambios.

Distribución de paquetes

Se requieren tres pasos principales para distribuir paquetes a los dispositivos.

1. Crear un paquete distribución para el paquete que desee distribuir.
2. Crear un método de entrega.
3. Programe el paquete y el método de entrega para la distribución.

Para crear un paquete de distribución

1. Clic en Herramientas > Distribución > Paquetes de distribución.
2. En el menú de acceso directo del grupo de paquete que desee, clic en Nuevo paquete de distribución > tipo de paquete que desee crear.
3. En el cuadro de diálogo Paquete de distribución, escribir información del paquete. Recordar que debe escribir el nombre del paquete, la descripción y el archivo principal. Clic en Ayuda para obtener información.
4. Al terminar, clic en Aceptar. La secuencia de comandos aparece debajo del elemento de árbol del tipo de paquete y del propietario que ha seleccionado.

Para crear un método de entrega

1. Si ya se ha configurado el método de entrega que se utilizara, ir al siguiente procedimiento, "*Para programar una distribución de tareas*".
2. Clic en Herramientas > Distribución > Métodos de entrega.
3. En el menú de acceso directo del método de entrega que se utilizara, clic en Nuevo método de entrega.
4. En el cuadro de diálogo Método de entrega, escribir la información de entrega. Clic en Ayuda para obtener información. Al terminar, clic en Aceptar.

Para programar una tarea de distribución

1. Clic en Herramientas > Distribución > Tareas programadas.
2. Clic en el botón de la barra de herramientas *Crear tarea de distribución de software*.
3. En Paquete de distribución, seleccionar el paquete de distribución que ha creado.
4. En Métodos de entrega, seleccionar el método de entrega que se desea utilizar.
5. Clic en Guardar para guardar los cambios.
6. En la vista de red, arrastrar los destinos a la tarea en la ventana *Tareas programadas*. Los destinos pueden incluir los dispositivos individuales, grupos de

equipos, objetos LDAP (usuario, equipo y grupo), consultas LDAP y consultas de inventario.

7. En el menú contextual de esa tarea, seleccionar Propiedades.

8. La página Dispositivos destino muestra los dispositivos que recibirán la tarea.

9. En Tarea programada, escribir el nombre de la tarea y la programación.

10. Ir a la página Introducción y confirme que la tarea se haya configurado debidamente. Al finalizar, haga clic en Guardar.

Observe el progreso de la tarea en la ventana Tareas programadas.

Anexo G Instalación de ZENworks 10 Configuration.

Requisitos previos a la instalación:

- a. Microsoft .NET Framework 2.0 y las actualizaciones más recientes.
 - b. El servidor debe estar dentro de un dominio.
 - c. Disponer de una dirección IP estática o dirección DHCP de forma permanente.
-
1. Introducir el DVD de instalación de Novell ZENworks 10 Configuration Management SP2. Seleccione el idioma. De no mostrar automáticamente, ejecute el archivo *setup.exe* en la raíz del DVD.
 2. Leer las indicaciones y clic en siguiente.
 3. Aceptar los términos de la licencia y clic en siguiente.
 4. Elegir el directorio en el cual se instalara la aplicación y clic en siguiente.
 5. Elegir entre crear una zona de gestión o si va a instalar un servidor nuevo en una zona existente y clic en siguiente.
 - a. Zona de gestión nueva.
 - i. Proporcionar Nombre de la zona.
 - ii. Contraseña de administrador de la zona.
 - b. Zona
 - i. Proporcionar dirección del servidor.
 - ii. Puerto SSL que se usará.
 - iii. Nombre de usuario del administrador y contraseña.
 6. Elegir el tipo de base de datos que usara la aplicación, y clic en siguiente.
 7. Elegir abrir los puertos (80, 443, 8005, 8009, 2645, 2638) que usará la aplicación, clic en siguiente.
 8. Elegir el tipo de certificadora (interna o externa), en esta caso *interna* y clic en siguiente.
 9. Introduzca la clave de uno o varios de los productos y clic en siguiente.
 10. Presentará un resumen de lo que se instalara, ver la figura 20, y clic en Instalar.

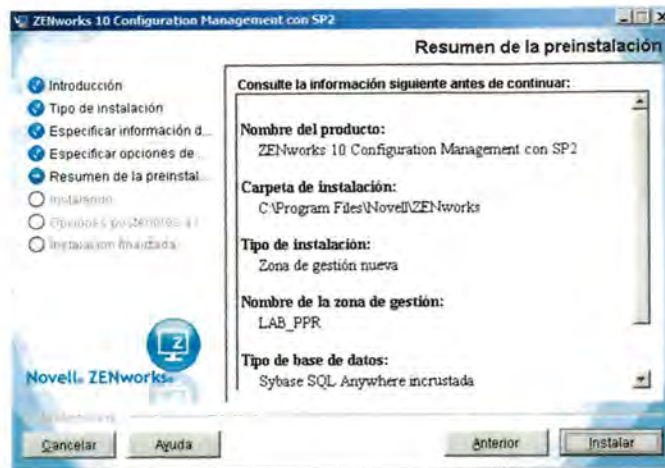


Figura 20. Ventana de resumen de ZENworks.

11. Al concluir la instalación mostrará la siguiente ventana, ver la figura 21.

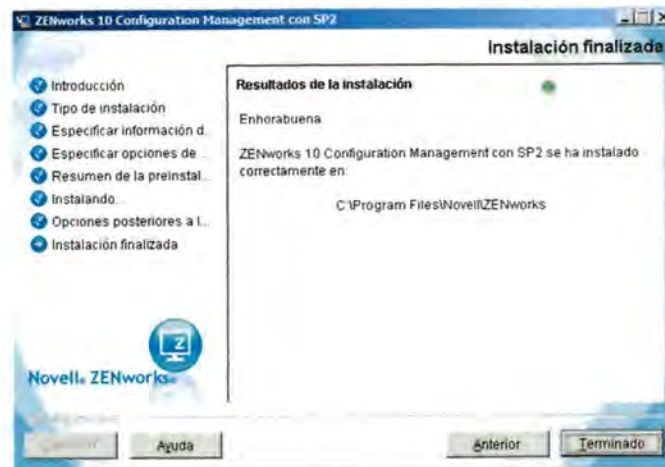


Figura 21. ZENworks Instalación finalizada.

Agregar dispositivos a la zona de gestión.

a. Creación de una tarea de descubrimiento de IP.

1. En el Centro de control de ZENworks, clic en la pestaña **Distribución**.
2. En el panel Tareas de descubrimiento, haga clic en **Nuevo** para lanzar el Asistente de nueva tarea de descubrimiento.
3. Complete los campos del asistente con la información:

- a. Opción que se usará para el descubrimiento, Ejemplo: IP, Nombre y una breve descripción. Clic en siguiente.
 - b. Definir la tecnología de descubrimiento, clic en siguiente.
 - c. Definir el rango de direcciones IP que se usaran para la tarea.
 - d. Definir las credenciales.
 - e. Definir la programación de descubrimiento.
 - f. Seleccionar servidor primario.
 - g. Seleccione el servidor proxy de Windows que debe llevar a cabo la tarea de descubrimiento. De lo contrario solo dar clic en finalizar.
- NOTA:** es necesario que en los dispositivos a descubrir este habilitado en el firewall la opción de respuestas de ICMP (ping).

b. Creación de una tarea de distribución.

Requisitos previos para distribuir a un dispositivo.

Windows 2000, Windows 2003 y Windows XP

1. Clic derecho en *Mis sitios de red > Propiedades*. Accederá a la ventana *Conexiones de red*.
2. Clic derecho en *Conexión de área local > Propiedades*. Accederá al recuadro de diálogo *Propiedades de Conexión de área local*.
3. En la pestaña General, comprobar que esté seleccionada la opción *Compartir impresoras y archivos para redes Microsoft*. clic en Aceptar.

Windows Vista y Windows Server 2008

1. Clic derecho en *Red > Propiedades*. Se mostrará la ventana *Centro de redes y recursos compartidos*.
2. En el panel izquierdo, clic en *Administrar conexiones de red*.
3. Clic derecho en *Conexión de área local > Propiedades*. Accederá al recuadro de diálogo *Propiedades de Conexión de área local*.
4. En la pestaña *Funciones de red*, comprobar que esté seleccionada la opción *Compartir impresoras y archivos para redes Microsoft*. Clic en Aceptar.

Habilitación del uso compartido de archivos e impresoras mediante el firewall de Windows

1. En el menú *Inicio*, clic en *Configuración > Panel de control*.
2. Doble clic en *Firewall de Windows*. Se mostrará la ventana *Firewall de Windows*. Clic en la pestaña *Excepciones*.
3. En la lista *Programas y servicios*, seleccionar *Compartir archivos e impresoras* y clic en *Modificar*. Aparecerá la ventana *Modificar un servicio*.
4. Clic en *Cambiar ámbito* para incluir la dirección IP del servidor primario y de la subred local. Clic en *Aceptar*.

Habilitación del uso compartido de archivos clásico.

Windows 2003

1. En el escritorio del dispositivo con Windows 2003, clic en el menú *Inicio > Configuración > Panel de control*.
2. Doble clic en *Herramientas administrativas > Directiva de seguridad local*. Se abrirá la ventana *Configuración de seguridad local*.
3. *Configuración de seguridad > Directivas locales > Opciones de seguridad*.
4. Cambie el valor de *Acceso de red: modelo de seguridad y recursos compartidos para cuentas locales a Clásico: usuarios locales autenticados como ellos mismos*. Clic en *Aceptar*.

Windows XP

1. En el dispositivo con XP, clic derecho en *Mi PC* y clic en *Abrir*.
2. Clic en el menú *Herramientas > Opciones de carpeta* para mostrar el recuadro de diálogo *Opciones de carpeta*. Clic en *Ver*.
3. En la lista *Configuración avanzada*, desmarcar la opción *Utilizar uso compartido simple de archivos* y clic en *Aceptar*.

Al desactiva la opción, cambiar el valor para la opción *Acceso de red: modelo de seguridad* y para *compartir para cuentas locales* de la directiva de seguridad local (*Directivas locales > Opciones de seguridad*) a Clásico: usuarios locales autenticados como ellos mismos.

Windows Vista

1. Abrir el Registro de Windows y acceda a la siguiente entrada:
HKLM/Software/Microsoft/Windows/CurrentVersion/Policies/System/LocalAccountTokenFilterPolicy.
Si la clave de registro no existe, deberá crearla.
2. Cambie el valor de DWORD (32 bits) a 1. Esto permite que los usuarios remotos puedan entrar y se les fuerce a ser "invitados". Cierre el registro.
3. Abrir la ventana Servicios y establezca que el servicio de registro remoto se inicie automáticamente e iniciarlo.
4. Clic en *Inicio > Configuración > Panel de control.*
5. Doble clic en *Centro de redes y recursos compartidos.*
6. Elegir *Activar el uso compartido de archivos* y clic en *Aplicar.*

Windows Server 2008

1. En el escritorio del dispositivo con Windows Server 2008, haga clic en el menú *Inicio > Configuración > Panel de control.*
2. Haga doble clic en *Centro de redes y recursos compartidos.*
3. Elegir *Activar el uso compartido de archivos* y haga clic en *Aplicar.*

Iniciando la tarea de Distribución.

1. Para instalar el agente de Zenworks en los dispositivos descubiertos, solo es necesario ir a la opción ***Dispositivos distribuibles.*** Seleccionar los dispositivos a los que se le instalara el agente y en la pestaña ***Acción*** dar clic en ***Instalar.***
2. Pedirá un nombre para la tarea de distribución y una breve descripción. Clic en siguiente.
3. Ahora seleccione los dispositivos a los cuales se les instalara el agente. Clic en siguiente.
4. Introduzca las credenciales que se deben usar para distribuir el software a los dispositivos seleccionados, proporcionar login y password del administrador del equipo a gestionar.

5. Cree una programación para la distribución.
6. Seleccione el servidor que realizará la tarea de distribución.
7. Seleccione el servidor proxy de Windows que debe llevar a cabo la tarea de descubrimiento, sólo en caso de ser necesario.
8. Elija el Paquete de distribución dependiendo del tipo de procesador (32 o 64 bits), Especifique la carpeta en la que se debe instalar el agente de ZENworks Adaptive. Si no se especifica nada, el agente se instalará por defecto en %ZENWORKS_HOME% o en %PROGRAMFILES%\Novell\ZENworks. Y por último elegir el modo para reiniciar el dispositivo de destino (de inmediato, manual o programado).
9. Elegir una clave de registro válida, o dejar en blanco.
10. Acciones previas/posteriores a distribución (Introduzca si es necesario los comandos para la distribución). Clic en finalizar.
11. Ir al menú Tareas de Distribución, seleccionar la tarea, clic en Acción y elegir Lanzar tarea de Distribución.

Bibliografía

1. **Kaczmarek, Steven D.** *Microsoft System Center Configuration Manager 2007 Administrator's Companion*. Estados Unidos : Microsoft Press, 2008. ISBN 0-7356-2385-6.
2. **Fine, Leonard H.** *Seguridad en Centros de Computo*. Mexico : Trillas, 2000.
3. **Microsoft Corporation.** Centro de administración de actualizaciones. [En línea] 2009. [Citado el: 18 de Abril de 2009.] <http://technet.microsoft.com/es-es/updatemanagement/bb245736.aspx>.
4. **Microsoft Corporation.** Windows Server Update Services 3.0 SP2. [En línea] 2009. [Citado el: 10 de Noviembre de 2009.] <http://technet.microsoft.com/en-us/wsus/default.aspx>.
5. **Cisco Systems.** Cisco Exploration 4.0. [En línea] 2007. [Citado el: 16 de Abril de 2009.] <http://www.cisco.com/web/learning/netacad/index.html>.
6. **Joskowicz, Ing. José.** *Redes de Datos*. Montevideo, Uruguay : Universidad de la República Montevideo, 2007.
7. **Robert, Williams.** *Windows Server 2003 Administracion de sistemas*. España : Grupo ANAYA, S.A., 2003. ISBN 84-415-1595-6.
8. **Novell.** ZENworks 10 Configuration Management SP2. [En línea] 2009. [Citado el: 15 de Julio de 2009.] <http://www.novell.com/es-es/documentation/zcm10/>.
9. **LANDesk Software.** LANDesk Management Suite. [En línea] 2009. [Citado el: 10 de Junio de 2009.] <http://www.landesk.com.mx/SolutionServices/product.aspx?id=762>.
10. **Microsoft Corporation.** Fundamentals of Configuration Manager 2007. [En línea] 2009. [Citado el: 6 de Mayo de 2009.] <http://technet.microsoft.com/en-us/library/bb693852.aspx>.