ANEXOS.

ANEXOS.

A. MANUAL DE AMANDA SOURCE BACKUP

Instalación De Amanda Source Backup.

Las versiones de SAMBA anteriores a la 2.0.3, en particular, deben ser parcheadas para que funcionen correctamente con Amanda. Sin estos parches, las copias de seguridad parecerán que se están realizando correctamente, pero las imágenes resultantes estarán corruptas.

Cuando AMANDA es configurada, las localizaciones de software adicional usado en los clientes, tales como GNU tar y SAMBA, se incorporan a los programas de AMANDA, de forma que el software adicional debe ser instalado en el mismo equipo donde se encuentra instalada AMANDA y en todos los clientes.

Definir el usuario y grupo a usar por AMANDA con las opciones –with-user y –with-group en ./configure. Por ejemplo, para usar Amanda para el nombre de usuario y backup como nombre de grupo:

```
#./configure --with-user=amanda --with-group=backup
```

No se necesitan obligatoriamente más opciones para ./configure, pero si se desea se puede ver todas las posibilidades con ./configure –help.

Una vez hemos ejecutado ./configure, teclea make para generar el instalador de AMANDA, y luego teclea make install para instalarlo. El paso make install debes hacerlo como root porque algunos programas de AMANDA requieren privilegios de sistema. Amenos que la se hayas cambiado la ubicación por defecto, AMANDA se instala en estas áreas:

/usr/local/sbin Programas que ejecutan los administradores.
/usr/local/lib Librerías.
/usr/local/libexec Programas privados que sólo usa AMANDA.
/usr/local/man Documentación.

Si la generación te da problemas o AMANDA necesita volver a ser generado, sobre todo si tienes nuevas opciones para ./configure, la siguiente secuencia garantiza que todo es perfectamente instalado, eliminando cualquier rastro de la instalación anterior:

```
#make distclean
#./configure
#make
#make install (as root)
```

Se pueden diagnosticar posibles problemas en los procesos de ./configure, mirando en el fichero config.log. Contiene una salida detallada de los tests que realiza ./configure. Tenga en cuenta que es normal que algunos de dichos tests 'fallen', como consecuencia de las pruebas que ./configure realiza para determinar cómo acceder a varias características del sistema.

Los sistemas operativos Unix normalmente incorporan características de los dispositivos en el nombre de fichero usado para acceder a una unidad de cinta. Las dos cosas a controlar son rewind y compression. AMANDA debe ser configurada con el dispositivo de cinta no-rebobinable , llamado así porque cuando el dispositivo es abierto y cerrado permanece en la misma posición y no hace un rebobinado automático. Normalmente es un nombre con una 'n', tal como /dev/nst0.

Se debe colocar al usuario AMANDA en el grupo al que actualmente pertenece el dispositivo de cinta, o selecciona un nuevo grupo para AMANDA y cambia los permisos de propietario de grupo del dispositivo. AMANDA necesita permisos de lectura y escritura. Desactivar el acceso al 'resto del mundo'.

Si es posible, se puede ubicar algún espacio de disco de almacenamiento para AMANDA en el servidor. El espacio de almacenamiento en disco puede reducir significativamente el tiempo de copia, permitiendo la realización de varias copias al mismo tiempo, mientras otra copia se está grabando en la cinta. Además, para dispositivos de cinta, AMANDA almacena la velocidad del dispositivo, y eso puede incrementar la capacidad. AMANDA puede ser configurada para limitar el uso de disco a un valor específico para que lo pueda

compartir con otras aplicaciones, pero una mejor aproximación es dedicar uno o dos discos de bajo coste dedicados exclusivamente a AMANDA.

En condiciones perfectas, debería haber suficiente espacio de almacenamiento en disco para las dos copias más grandes al mismo tiempo, de forma que una copia pueda pasar al disco de almacenamiento mientras que la otra está siendo grabada a la cinta. Si esto no es posible, cualquier cantidad que almacene al menos un poco de las copias más pequeñas ayudará. El reporte de AMANDA generado por cada ejecución con amreport muestra el tamaño de la imagen de copia tras la compresión software (si ésta se usa). Así, en adición a las herramientas amplot y amstatus, puede ser usado para conocer el espacio ocupado.

Decide con qué frecuencia AMANDA debería realizar copias completas. Esto es el ciclo de copia. Los períodos cortos facilitan la restauración porque hay menos partes, pero consumen más cinta o disco y tiempo. Períodos largos permiten a AMANDA hacer más cómoda la copia, pero se requieren más pasos durante una restauración.

Grandes cantidades de información a salvaguardar o dispositivos de cinta de menor capacidad también afectan al ciclo de copias. Selecciona un período lo bastante largo para que AMANDA pueda realizar una copia completa de cada área durante el ciclo de copias y todavía le quede espacio para la ejecución de las copias parciales. Los típicos ciclos de copias son una o dos semanas. Recuerda que el ciclo de copias es un límite máximo sobre con qué frecuencia se hacen las copias completas, y no un valor exacto. AMANDA los ejecuta con más frecuencia y en varios momentos durante el ciclo cuando equilibra la carga de copia. Sólo viola el límite si una copia falla repetidamente, y emite advertencias en el reporte si eso precisamente está a punto de pasar.

Por defecto, AMANDA asume que se ejecuta cada día. Si este no es el caso, establecer las ’ejecuciones por ciclo’ o runs per cycle (descrito a continuación) a un valor diferente. Por ejemplo, un ciclo de copias de siete días y ejecuciones por ciclo de cinco debería ser usado si las copias son ejecutadas sólo los días laborables.

Las ejecuciones por ciclo y el número de cintas por ejecución determinan el número mínimo de cintas necesarias, lo que llamamos el ’ciclo de cintas’, o tape cycle. Para asegurarse de que la ejecución actual no está sobre-escribiendo la última copia completa,

una más debería ser incluida. Por ejemplo, un ciclo de copias de dos semanas, con 14 ejecuciones por ciclo por defecto (cada día) y 1 cinta por ejecución por defecto, necesita al menos 15 cintas (14+1 ejecuciones*una cinta/ejecuciones). Usando dos cintas por ejecución se necesitan 30 cintas (14+1 ejecuciones*dos cintas/ejecuciones). Haciendo copias sólo en días laborables con un ciclo de copias de dos semanas, ejecutando 10 ejecuciones por ciclo, y dos cintas por ejecución necesita 22 cintas (10+1 ejecuciones*dos cintas/ejecuciones).

Deben asignarse más cintas que las mínimas para controlar situaciones de error. Una asignación de al menos el doble del mínimo permite usar la copia completa anterior si la copia completa más reciente no puede ser leída. Ubicar más cintas de las necesarias también incrementa el tiempo de recuperación de datos perdidos. AMANDA no tiene un límite sobre el número de cintas en el ciclo de cintas.

Configurando el Disco de Almacenamiento

Define cada disco de almacenamiento en una sección holdingdisk del fichero amanda.conf. Si las particiones están dedicadas a AMANDA, establece el valor de uso a un pequeño número negativo, como por ejemplo -10 MBytes. Esto le indica a AMANDA que use todo el espacio posible, menos ese límite. Si el espacio está compartido con otras aplicaciones, establece el valor a la cantidad que AMANDA puede usar, crea el directorio y establece los permisos de forma que sólo el usuario AMANDA pueda acceder.

Establecer un valor global para cada disco de almacenamiento. Los valores negativos provocan que AMANDA escriba copias más largas que el valor absoluto directamente a cinta, sobrepasando el disco de almacenamiento. Números positivos dividen las copias en el disco de almacenamiento en partes inferiores al valor global o chunksize. Aunque las imágenes estén divididas en varias en el disco de almacenamiento, éstas serán escritas en la cinta como una sola imagen. Por el momento, todas las partes para una imagen determinada van al mismo disco de almacenamiento.

Viejos sistemas operativos que no soportan ficheros mayores de 2 GBytes necesitan un tamaño chunk size ligeramente más pequeño, como 2000 MBytes, para que así el disco de almacenamiento todavía pueda ser usado por imágenes de copias muy grandes. Los

sistemas que soportan ficheros mayores de 2 GBytes deberían tener un valor muy grande, como 2000 GBytes.

Configurando las Copias de los Clientes

Se escoge o modifica un tipo de copia o dumptype ya existente que coincida con las opciones que deseas, o crea uno nuevo. Cada dumptype debería referenciar al dumptype global. Este es usado para establecer opciones para el resto de dumptypes. Por ejemplo, para usar la característica de indexación o indexing, actívala en el dumptype global, y los demás tipos que definas heredarán ese valor.

Crear un fichero llamado disklist en el mismo directorio donde reside tu amanda.conf o bien se copia el que se tiene en example/disklist. No sin antes asegurarse de que es legible por el usuario AMANDA. Cada línea en disklist define un área a ser copiada. El primer campo es el nombre de la máquina cliente (se aconsejan nombres completamente cualificados de dominio), el segundo es el área a ser salvaguardada en el cliente, y el tercero es el método de copia, o dumptype. El área puede introducirse como nombre de disco, sd0a, como nombre de dispositivo , /dev/rsd0a, o como nombre lógico, /usr. Los nombres lógicos son más fáciles para recordar qué es lo que se está copiando, así como a la hora de restauración o la reconfiguración del disco.

Para configurar un cliente Windows, se establece el nombre de la máquina al nombre de la máquina Unix que corre SAMBA y el área al nombre del recurso compartido de Windows, como por ejemplo //algún-pc/C$. Advierte que las barras que se usan como separadores son las deUnix, y no las de Windows.

Activa el acceso de AMANDA al cliente desde el servidor (a menos que el cliente sea el propio servidor) editando el fichero .amandahosts (o .rhosts, dependiendo de cómo se lo configuró en ./configure) en el directorio raíz del usuario AMANDA en el cliente. Se Introduce el nombre completamente cualificado de dominio del servidor de AMANDA y el usuario AMANDA, separados por un espacio o tabulador, asegurándose de que el fichero es propiedad del usuario AMANDA y no permite acceso a nadie más que al propietario.

Para los clientes Windows, en cambio se coloca la contraseña del recurso en /etc/amandapass en el servidor que corre SAMBA. El primer campo es el nombre de recurso compartido de Windows, el segundo es la contraseña en modo texto, y el tercer campo (opcional) es el dominio. Debido a que este fichero contiene contraseñas visibles, debería estar muy protegido, ser propiedad del usuario AMANDA y sólo accesible a él. Por defecto, AMANDA usa al usuario SAMBA. Esto lo puedes cambiar con –with-samba-user en ./configure.

Testeo y Depuración de la Configuración

Los test de la configuración con amcheck. Al igual que con la mayoría de comandos de AMANDA, se ejecutan como el usuario AMANDA, no como root:

#su amanda -c 'amcheck Daily'

Muchos de los tipos de errores que reporta amcheck están descritos en docs/FAQ o en la página man de amcheck. El error más común reportado a la lista de correo de AMANDA es selfcheck request timed out, que significa que amcheck no fue capaz de contactar con amanda en el cliente. En adición a la información que obtendrás de docs/FAQ, aquí se tiene algunas otras cosas para intentar, en caso de errores:

Ejecutarlo tanto en el servidor y el cliente, y asegúrate de que los números de puerto coinciden:

$cc check-service.c -lnsl lsocket (Solaris)
$a.out amanda udp amanda/udp: 10080
$a.out amandaidx amandaidx/tcp: 10082
$a.out amidxtape amidxtape/tcp: 10083

Ejecutar el programa amandad a través de la línea de comandos como el usuario AMANDA en el cliente. Debería permanecer durante unos 30 segundos, y luego de terminar. Se Introduce la ruta completa exactamente tal y como viene en inetd, usando copiar/pegar. No se debe proseguir hasta que amcheck esté de acuerdo con la configuración.

Ejecutando amdump

El script amdump controla una ejecución normal de AMANDA. Sin embargo, es normal realizar cosas específicas al sitio, así como meter un script de shell wrapper para amdump. Amdump está pensado para funcionar en modo desatendido desde el cron.

El script amdump hace lo siguiente:

Si un fichero llamado hold existe en el fichero de configuración, amdump para hasta que éste desaparezca. Este fichero puede ser creado y eliminado a mano para paralizar temporalmente las ejecuciones de AMANDA, sin tener que modificar las tareas definidas en el cron.

Si parece que otra copia de amdump está en ejecución, o se ha abortado una ejecución previa, amdump registra un error y termina. Si una ejecución anterior se abortó, debe ejecutarse amcleanup. Un paso amcleanup debería ser añadido a la secuencia de arranque del servidor de cintas para evitar ésta circunstancia. No se realizarán copias tras un fallo o aborto hasta que no se ejecute amcleanup.

Una vez el backup ha sido realizado, amreport es ejecutado para generar el reporte que se enviará vía email. También renombra el fichero de registro para la ejecución al log.

Los antiguos ficheros de registro amdump.NN son reorganizados, de forma que sólo los necesarios para mantener el ciclo de copias son mantenidos en el sistema.

El programa amtrmidx es ejecutado para eliminar los antiguos catálogos si la indexación ha sido usada.

Monitoreo del Estado del Disco de Almacenamiento

Mientras amdump está funcionando, amstatus puede monitorizar la ejecución. Amstatus se puede usar para generar estadísticas sobre cuántas copias fueron realizadas, qué pasó durante la ejecución, etc.

Una porción del área del disco de almacenamiento puede ser utilizada para realizar copias completas durante el modo degradado reduciendo el valor reservado en amanda.conf por debajo del 100%.

Un error o caída del servidor también puede dejar imágenes en los discos de almacenamiento. Ejecuta amflush, como el usuario AMANDA, tratará de pasar las imágenes del disco de almacenamiento a la próxima cinta, una vez se hayan corregido los problemas. Esto va a través del mismo mecanismo de peticiones de cintas que amdump. Si existe más de un juego de copias en el área del disco de almacenamiento, amflush permite que se escoja una o todas. Amflush genera un reporte vía email al igual que amdump.

Restaurando con AMANDA

Recuerde que a ninguna persona le puede interesar cuan información tiene salvaguardar, si luego no se la puede restaurar.

Una de las maneras de restaurar elementos con AMANDA es con el comando amrecover en el cliente. Antes de que amrecover pueda funcionar, AMANDA debe ejecutarse con el parámetro index del dumptype a yes, y los servicios amindexd y amidxtaped deben estar instalados y activados o preparados para ser automáticamente activados con inetd, normalmente en la máquina servidora de cintas (la secuencia de instalación por defecto los instala). Además, añade al cliente en el fichero .amandahosts (o .rhosts) para el usuario AMANDA en la máquina servidora. Como amrecover se debe ejecutar como root en el cliente, la entrada debe listar a root como al usuario remoto, no al usuario AMANDA. Amrecover no debería tener setup id root, ya que entonces cualquiera podría abrir los catálogos de todo el sistema.

Para éste ejemplo, el usuario jj ha solicitado dos archivos, ambos llamados molecule.dat, en los subdirectorios llamados work/sample-21 y work/sample-22 y dice que quiere las últimas versiones modificadas el 13 de enero. Antes de hacerte root en el cliente, cambia al área y luego ejecuta amrecover:

```
$su
Password:
#cd ~jj
#amrecover Daily
AMRECOVER Version 2.4.1p1. Contacting server on amanda.cc.purdue.edu ...
220 amanda AMANDA index server (2.4.1p1) ready.
200 Access OK
Setting restore date to today (2011-01-18)
200 Working date set to 2011-01-18.
200 Config set to Daily.
200 Dump host set to pete.cc.purdue.edu.
$CWD '/home/pete/u66/jj' is on disk '/home/pete/u66' mounted at '/home/pete/u66'.
200 Disk set to /home/pete/u66. amrecover>
```

En éste punto, una línea de interfaz de comandos te permite navegar por los catálogos de imágenes. Nos movemos con el comando cd, miramos lo que hay disponible con ls, cambia la fecha con setdate, añade ficheros y directorios para ser extraídos con add. El comando extract iniciará la extracción:

```
amrecover> setdate ---14
200 Working date set to 2011-01-14.
amrecover> cd work/sample-21
/home/pete/u66/jj/work/sample-21 amrecover> add molecule.dat
Added /jj/work/sample-21/molecule.dat
amrecover> cd ../sample-22
/home/pete/u66/jj/work/sample-22
amrecover> add molecule.dat
Added /jj/work/sample-22/molecule.dat amrecover> extract
Extracting files using tape drive /dev/rmt/0mn on host amanda.cc.purdue.edu.
The following tapes are needed: Daily-034
Restoring files into directory /home/pete/u66
Continue? [Y/n]: y
Load tape Daily-034 now
Continue? [Y/n]: y
```

Warning: ./jj: File exists

Warning: ./work: File exists

Warning: ./work/sample-21: File exists

Warning: ./work/sample-22: File exists set owner/mode for '.'? [yn] n amrecover> quit

El comando amrestore retorna imágenes completas de un respaldo. Primero, localiza el medio de almacenamiento que contienen las imágenes deseadas. La subopción find del comando amadmin genera una salida como ésta (abreviada):

#su amanda -c 'amadmin Daily find pete u66' Scanning /amanda...

date	host	disk	lv tape or file	file
2011-01-13		/home/pete/u6	1 Daily-033	26 OK
2011-01-14		/home/pete/u6	1 Daily-034	40 OK
2011-01-15		/home/pete/u6	1 Daily-000	34 OK
2011-01-16		/home/pete/u6	1 Daily-001	31 OK
2011-01-17		/home/pete/u6	0 Daily-002	50 OK
2011-01-18		/home/pete/u6	1 Daily-003	20 OK

El mensaje Scanning /amanda. . . indica que amadmin buscó en el disco de almacenamiento (/amanda) por si quedasen imágenes allí. Luego lista todas las cintas o ficheros en el disco de almacenamiento que contienen el área solicitada. La subopción info de amadmin muestra las cintas con las imágenes más recientes:

#su amanda -c 'amadmin Daily info pete u66' Current info for pete.cc.purdue.edu /home/pete/u66:

Stats: dump rates (kps), Full: 652.0, 648.0, 631.0

Incremental: 106.0, 258.0, 235.0 compressed size, Full: -100.0%,-100.0%,-100.0%

Incremental: -100.0%,-100.0%,-100.0%

umps:	lev	datestmp	tape		file	origK	compK	secs
	0	20110117	Daily-002	50	582239	582272	892	
	1	20110118	Daily-003	20	3263	3296	31	
	2	19981214	Daily-032	21	7039	7072	37	

Puede aparecer información antigua, tal como 19981214 (14-Dic-1998) en éste ejemplo. Aunque es cierto que era la última copia de nivel 2 de esa área, es de poco interés, debido a que al menos una copia completa de nivel 1 ha sido realizada desde entonces.

Los valores "compressed size" aquí pueden ser ignorados, debido a que ésta particular configuración usa compresión por hardware, así que no hay datos de software de compresión.

Una tercera forma de conocer qué cinta contiene una determinada imagen es generar una tabla de contenidos de cintas con "amtoc" tras cada ejecución de AMANDA:

El formato de cinta de AMANDA es deliberadamente simple, y gracias a ello la restauración de datos se podría realizar sin necesidad de ninguna de las herramientas de AMANDA, si fuera necesario. El primer archivo de la cinta es una etiqueta de volumen con la cinta VSN y la fecha en que fue grabada. Este no está en formato ANSI VOL1, pero es texto plano. Cada archivo tras de éste contiene una imagen usando bloques de 32 KBytes. El primer bloque es una cabecera de AMANDA con el cliente, el área y las opciones usadas para crear la imagen. Como en el caso de la etiqueta de volumen, la cabecera no está en formato ANSI, pero es texto plano. Sigue la imagen, comenzando en el siguiente bloque de cinta, hasta el final del archivo.

Para recuperar una imagen con las utilidades que trae el propio Unix, para el caso de no disponer del propio amrestore, posiciona la cinta en la imagen, y luego usa dd para leerla:

```
#mt rewind
#mt fsf NN
#dd if=$TAPE bs=32k skip=1 of=dump_image
```

La opción skip=1 le indica a dd que se salte la cabecera de AMANDA. Sin la opción of=, dd graba la imagen en la salida estándar, la cual puede ser redirigida con una tubería al programa de descompresión, si es necesario, y luego al programa de restauración del cliente. Como la cabecera de la imagen está en texto plano, puede ser visionada con:

```
#mt rewind
#mt fsf NN
#dd if=$TAPE bs=32k count=1
```

En adición a la descripción de la imagen, ésta contiene texto mostrando los comandos necesarios para realizar la restauración. Aquí se tiene una típica entrada para el sistema de archivos raíz en pete.cc.purdue.edu. Es una copia de nivel 1 hecha sin compresión, usando el programa comercial de compresión ufsdump:

AMANDA: FILE 19981206 pete.cc.purdue.edu /lev 1 comp Nprogram /usr/sbin/ufsdump

Para restaurarla, posiciona la cinta al principio del archivo y se ejecuta:

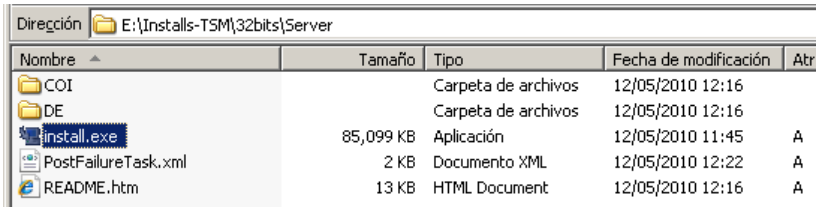
#dd if=$TAPE bs=32k skip=1 |/usr/sbin/ufsrestore -f... –

El mismo proceso aplica si se realiza una restauración desde disco, simplemente cambiamos el volumen del tape por la ruta al espacio de disco donde se almaceno el respaldo.

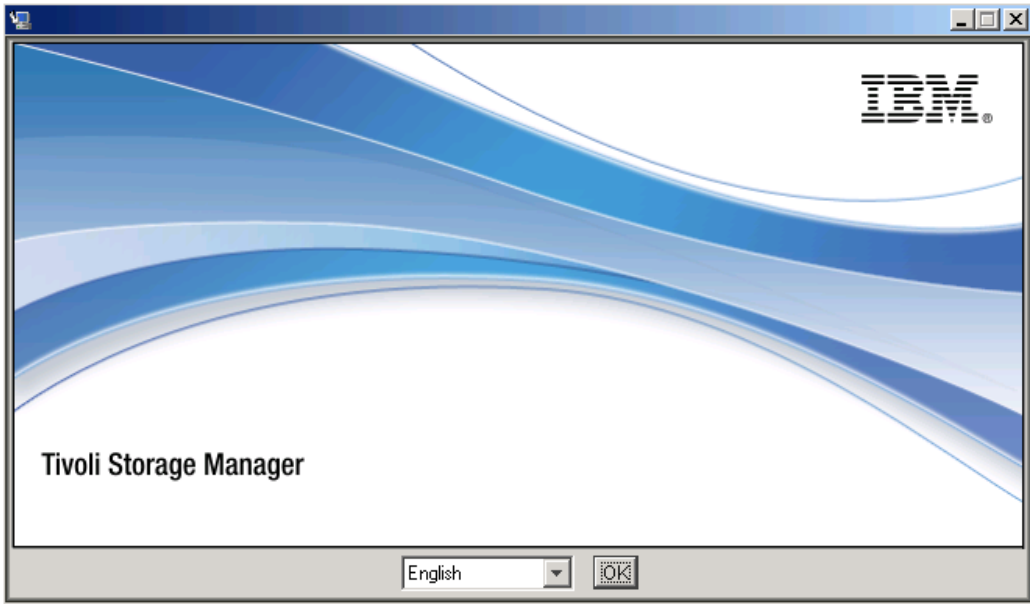
B. MANUAL DE IBM TIVOLI STORAGE MANAGER

INSTALACIÓN del SERVIDOR DE TSM 6.2.1.

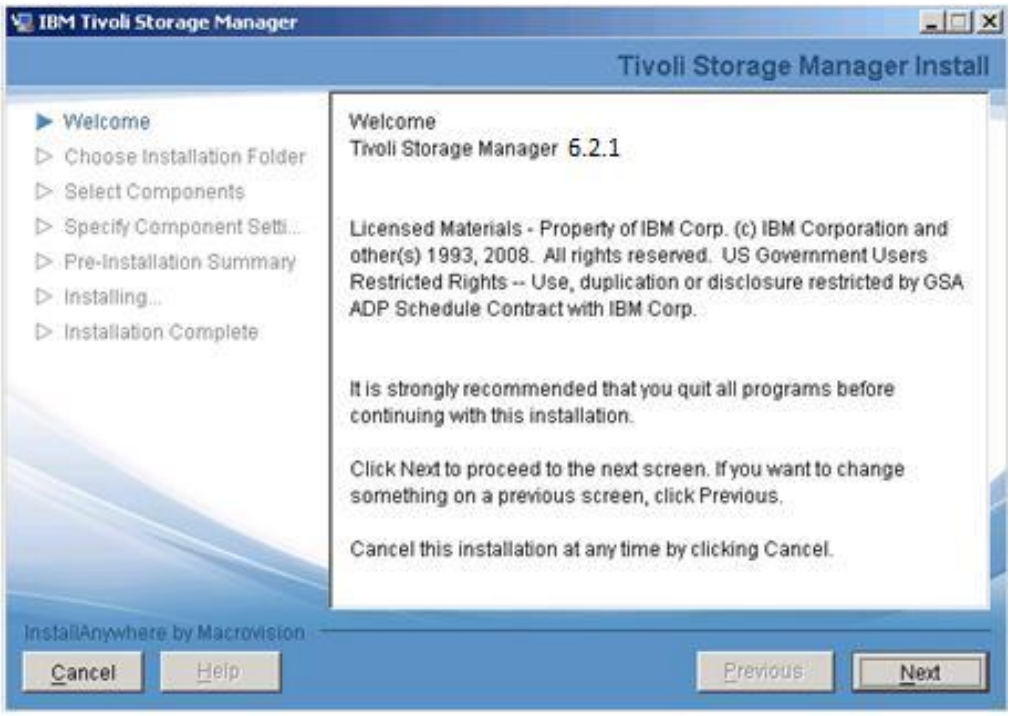
Como un usuario del grupo Administradores locales procedemos a la instalación de TSM Server, para esto nos ubicamos en el directorio del instalador y ejecutamos el archivo: install.exe



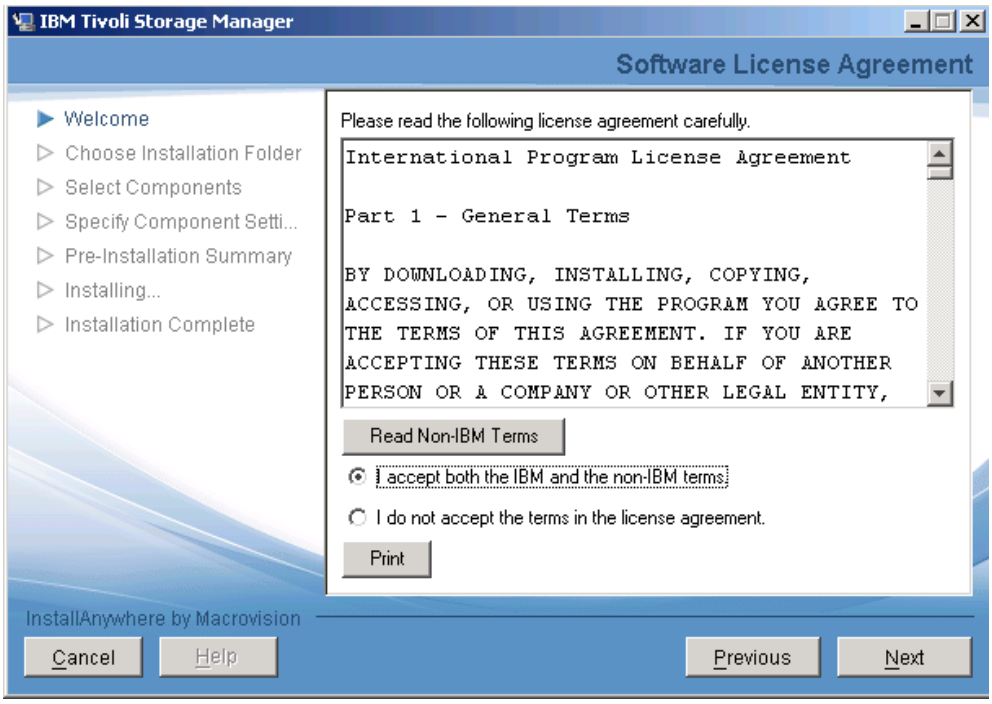
Escoja el idioma que le aparecerá en las pantallas de instalación (en este caso English).



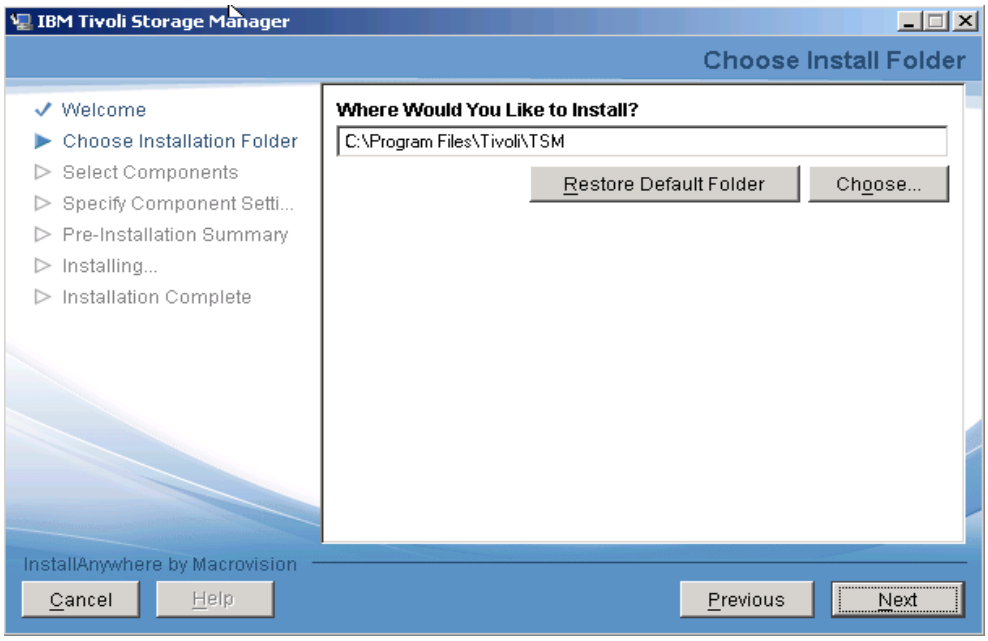
Aparecerá la pantalla de bienvenida, seleccione "Next"



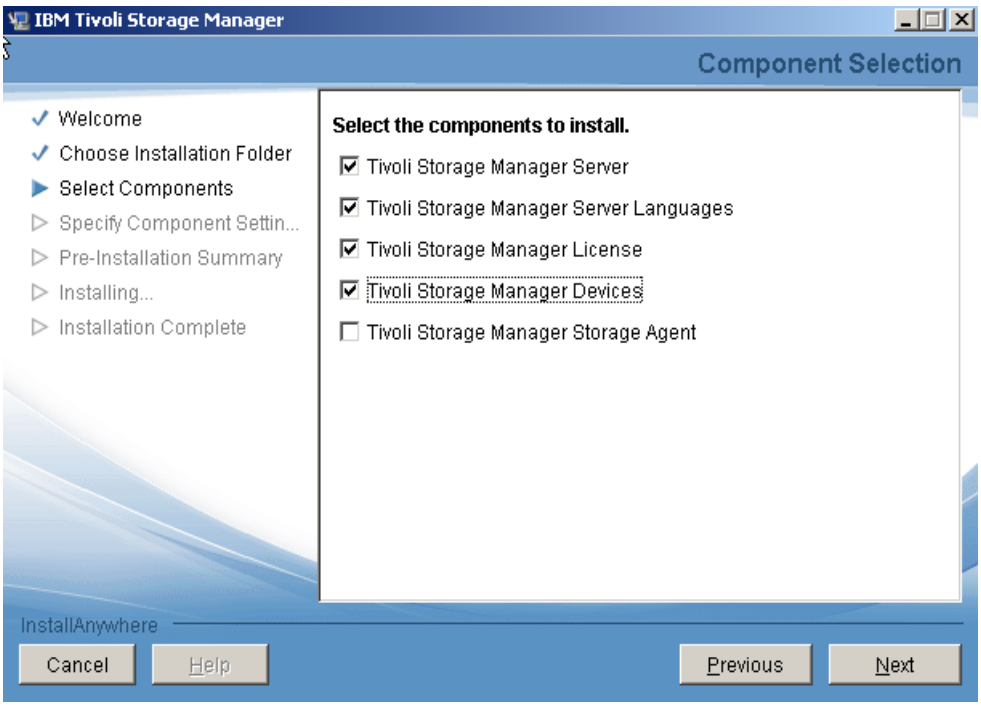
A continuación acepte la licencia y click en "Next"



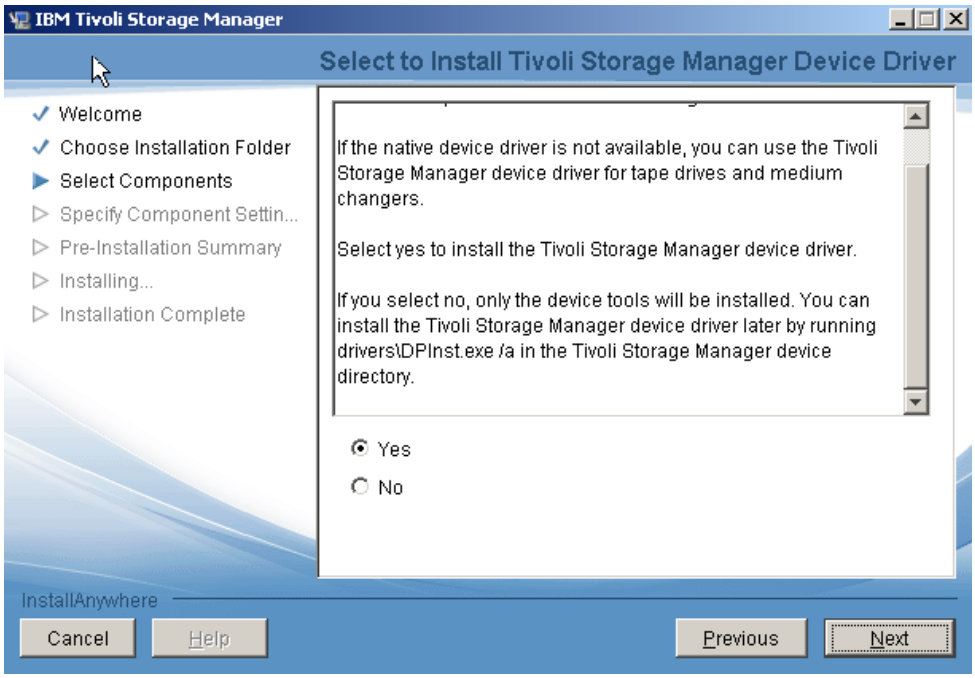
Se presentará un mensaje del asistente de instalación que solicita especificar la ruta de instalación.



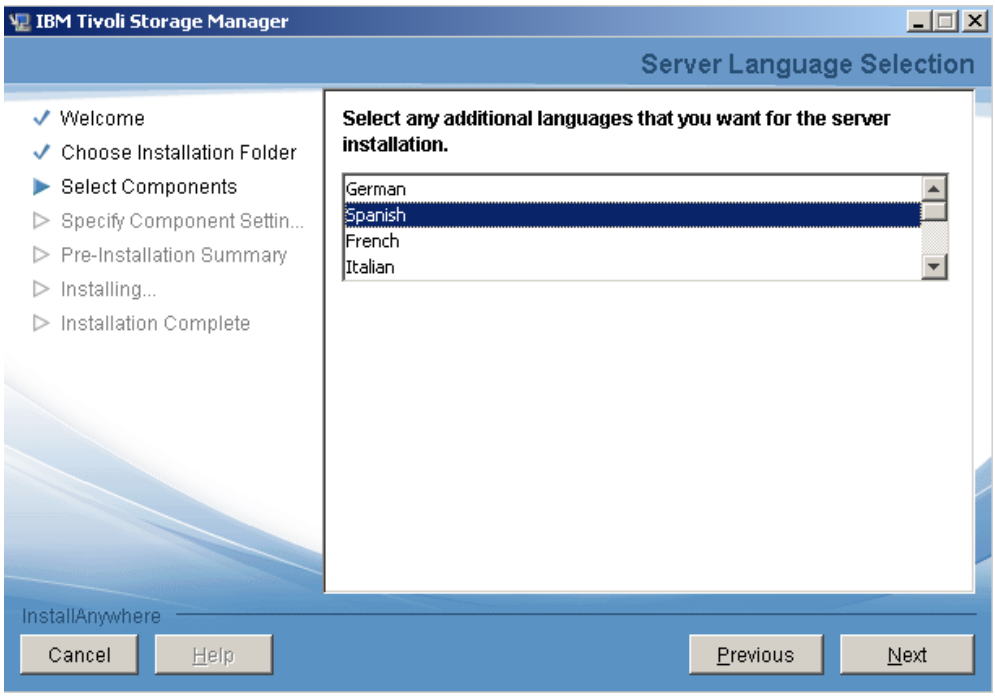
Seleccionamos los paquetes a instalar, no se instala **"Tivoli Storage Manager Storage Agent"**, ya que no se cuenta con un SAN.



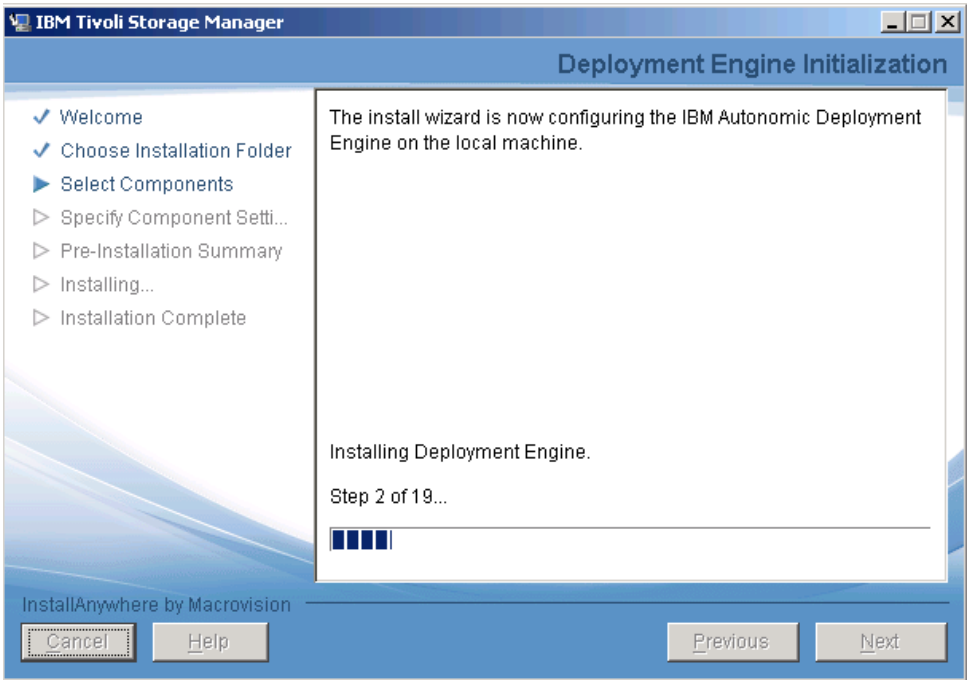
Luego de realizar click en el botón **Next.** Veremos la verificación de los paquetes seleccionados. Podremos seleccionar instalar los drives de TSM, para utilizar la librería conectada hacia el mismo.



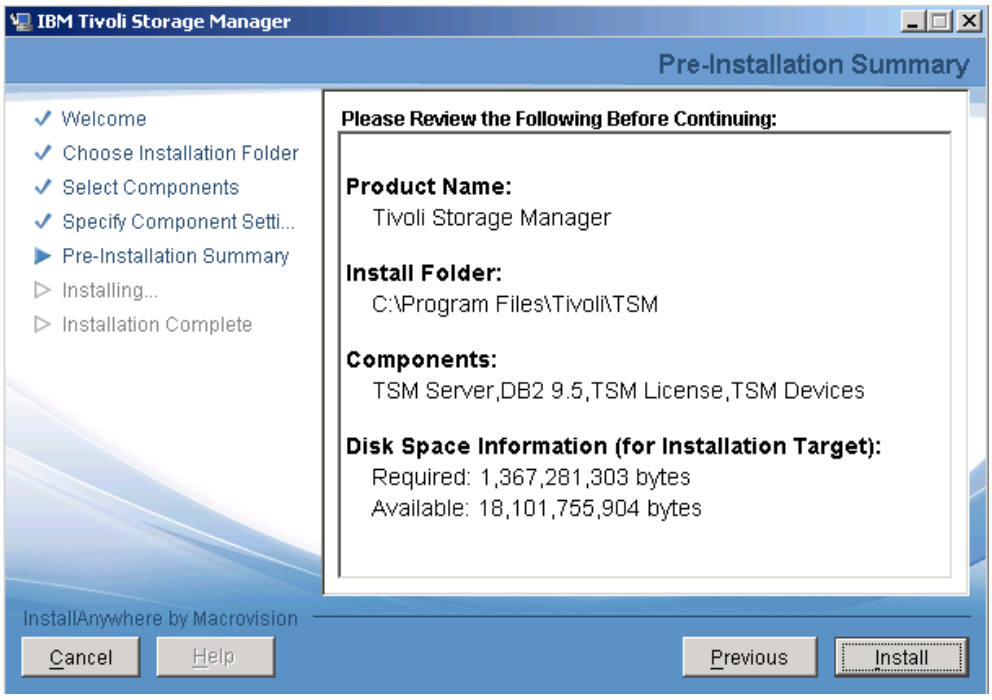
Luego de seleccionar Next, aparecerá el lenguaje con el cuan realizaremos la instalación de TSM.



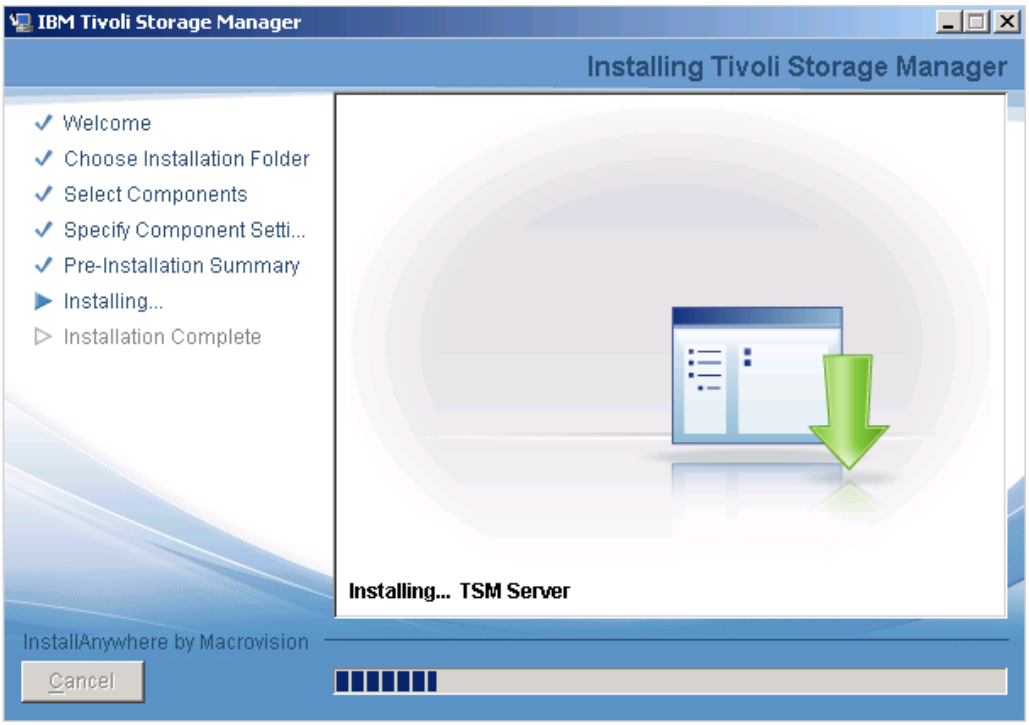
Damos click en next, y podremos observar el inicio de la instalación de Tivoli Storage Manager V6.2.1 con la configuración realizada anteriormente.



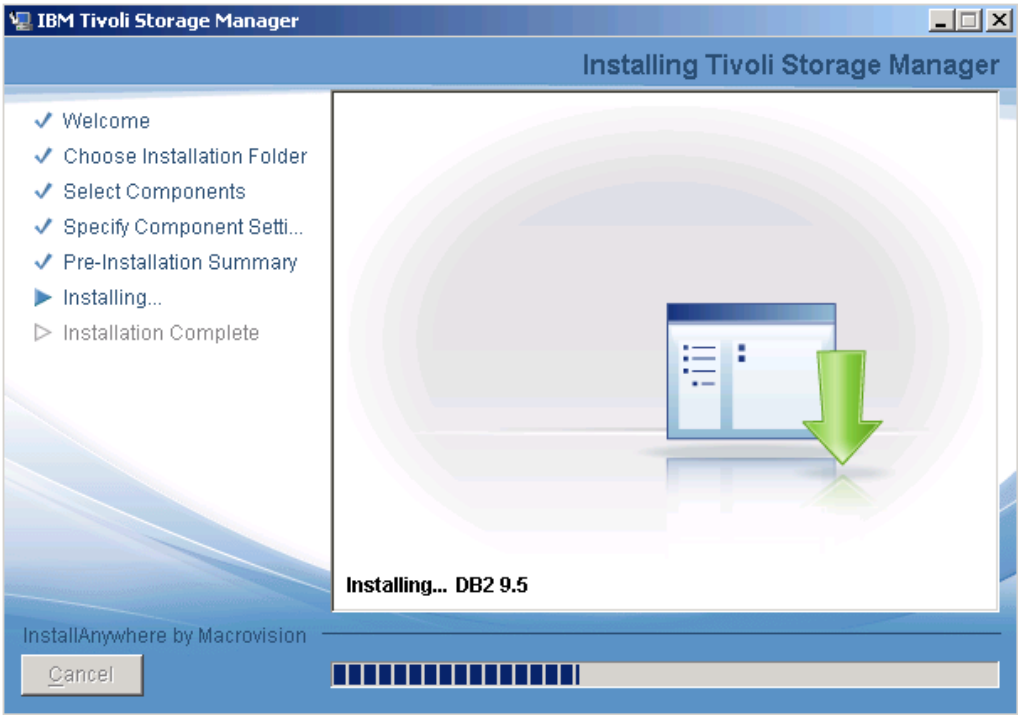
Verifique los productos a instalar y presione en el botón **Install.**



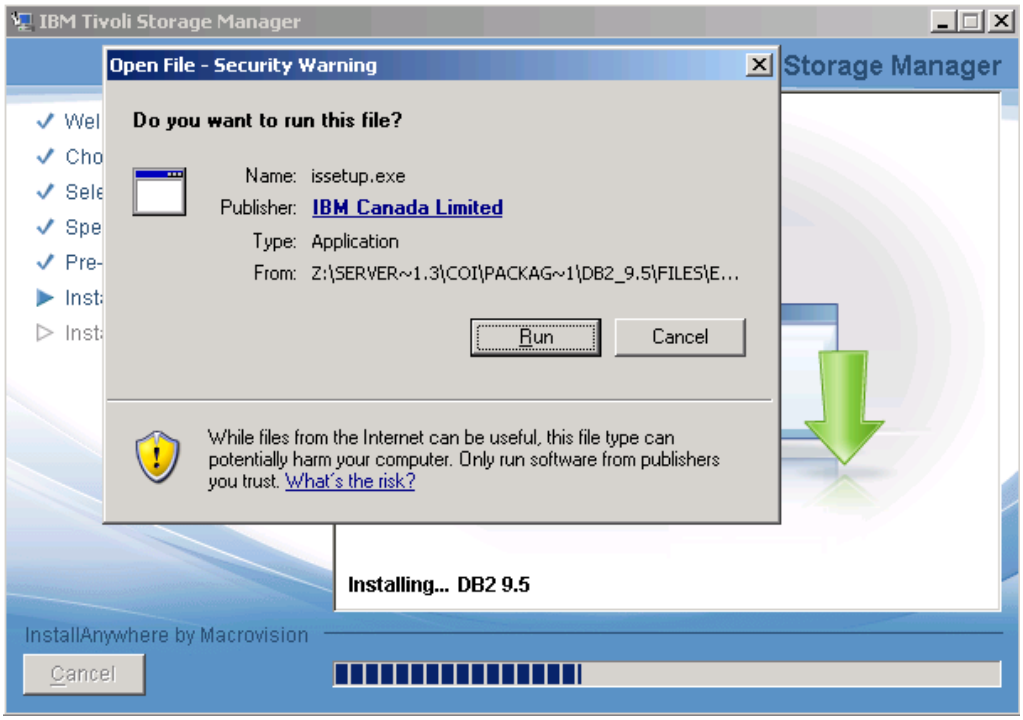
Una vez iniciada la instalación podremos ver el proceso de instalación de los diferentes paquetes: Instalación de **TSM Server.**



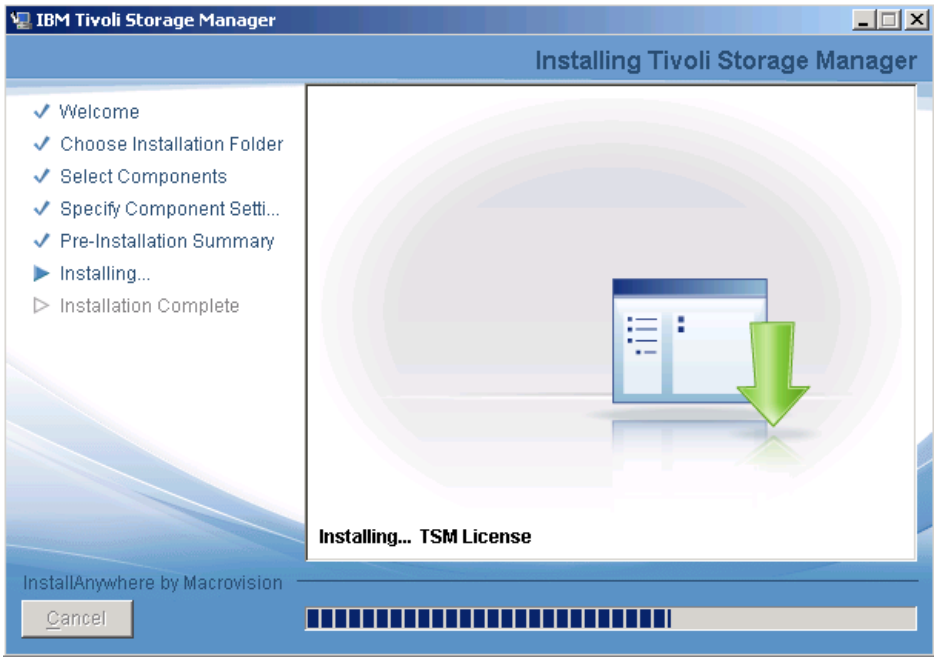
Instalación de DB2 para el uso con Tivoli Storage Manager v6.2.1



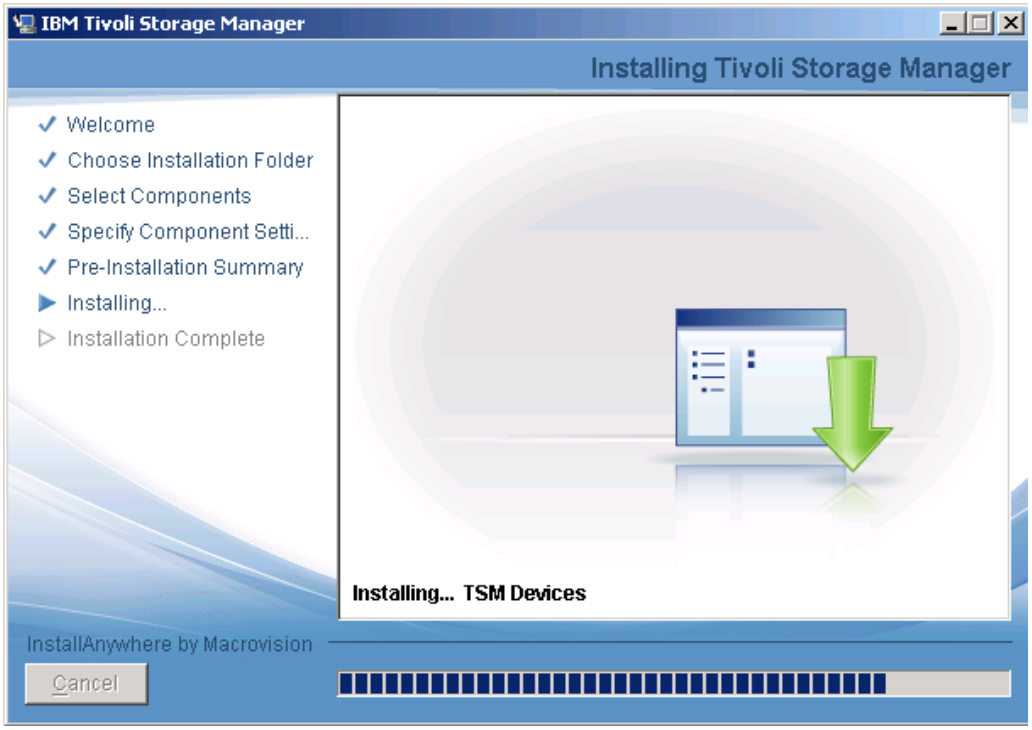
En el mensaje emergente aceptamos “Run”, el proveedor del instalador para continuar.

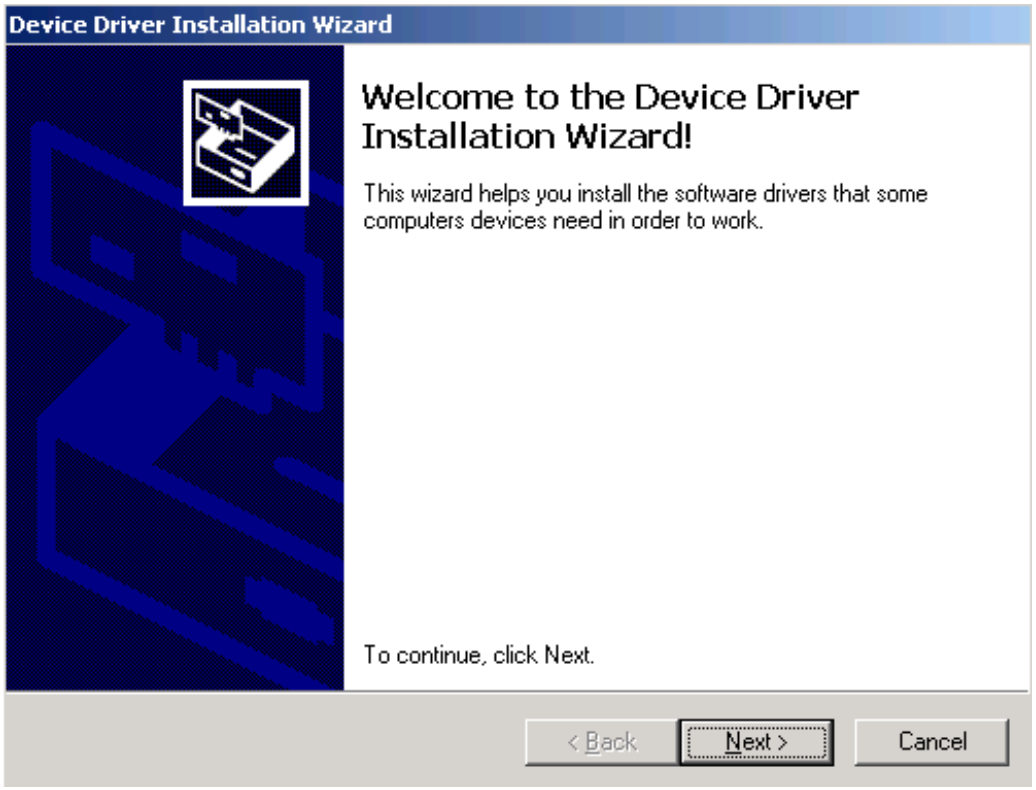


Ahora veamos el proceso de instalación de la licencia para Tivoli Storage Manager v6.2.1

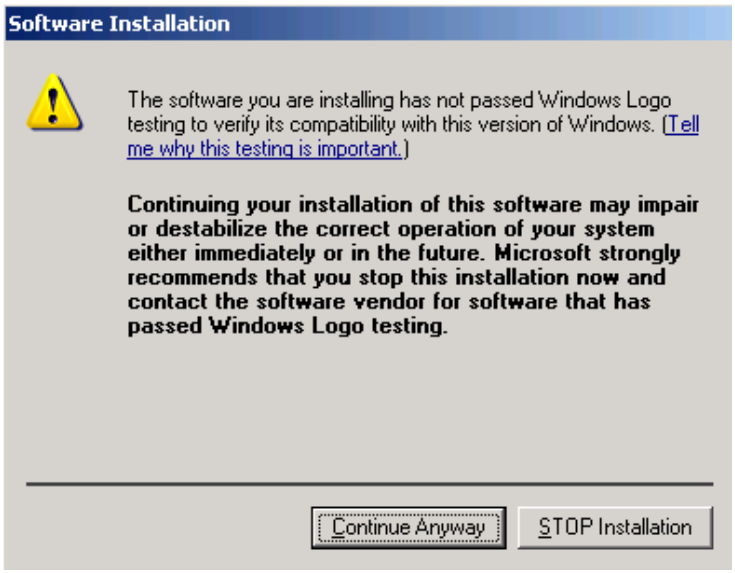


Observamos el proceso de instalación de los drivers necesarios de TSM. Donde se desplegará el asistente para dicha instalación.

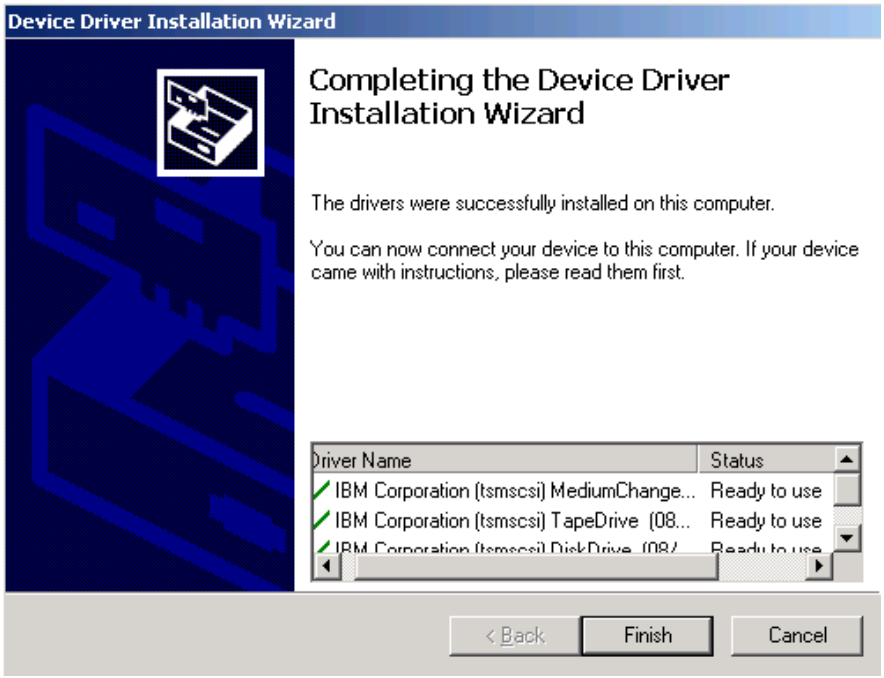




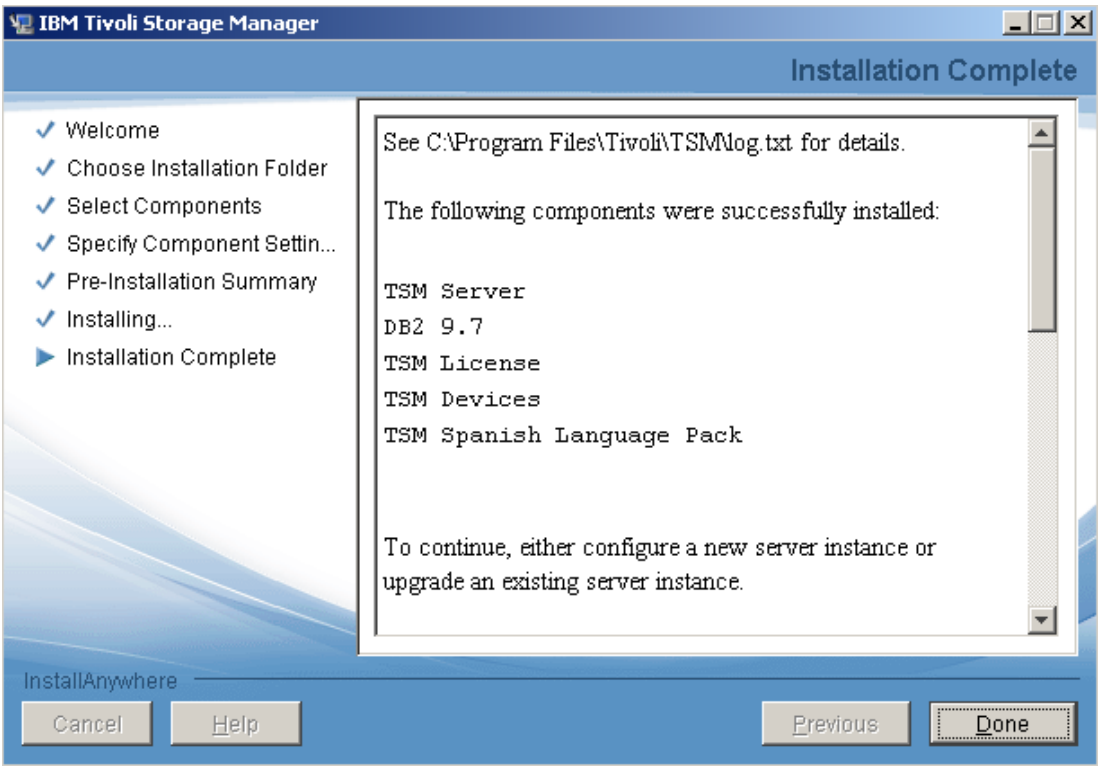
Aceptamos, la licencia de software de terceros para continuar.



Se observa la petición de aceptación para la instalación de certificados.



Al final el servidor de TSM está instalado, presione en el botón "**Done**".

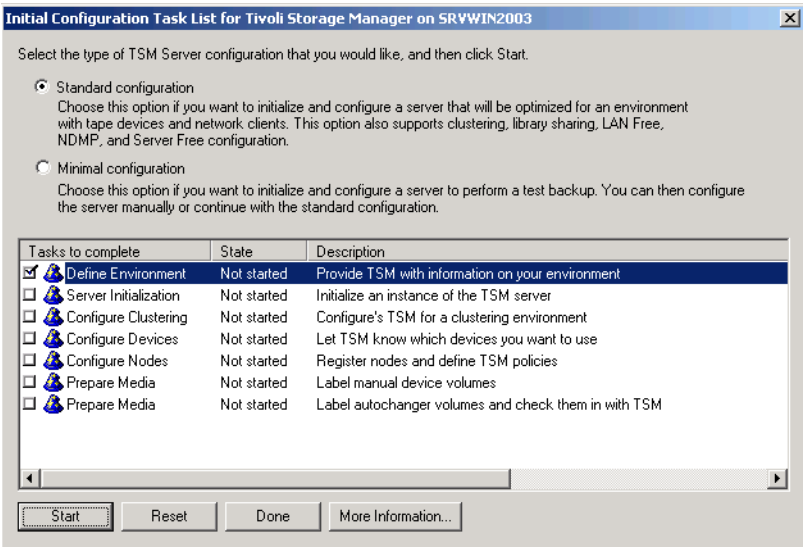


CONFIGURACIÓN INICIAL de IBM TIVOLI STORAGE MANAGER SERVER V6.2.1

Al momento el software ya se encuentra instalado en el servidor seleccionado, ahora continuaremos en proceso de configuración inicial. Para eso, es necesario ejecutar la consola de TSM Server.

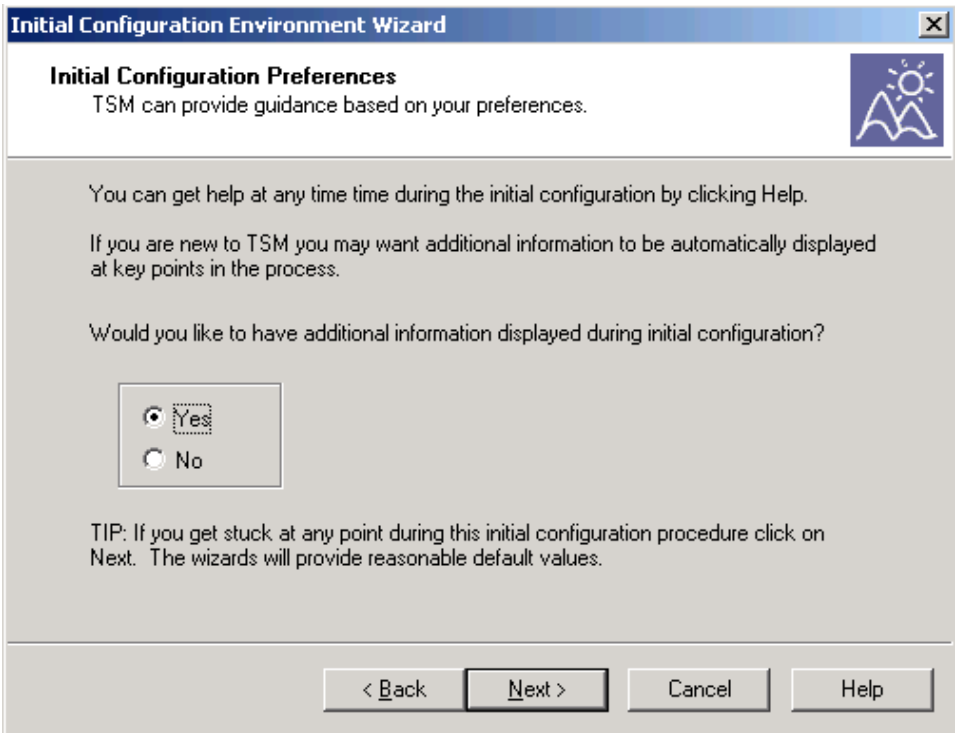
Start ->All Programs->Tivoli Storage Manager->Management Console

Al ejecutar la consola de TSM, aparecerá el "**Wizard de Configuración**", el cual nos ayudará a configurar los parámetros y dispositivos que utilizará TSM Server. Seleccionamos la opción de configuración standard "**Standard Configuration**" y a continuación presionamos en el botón "**Start**".

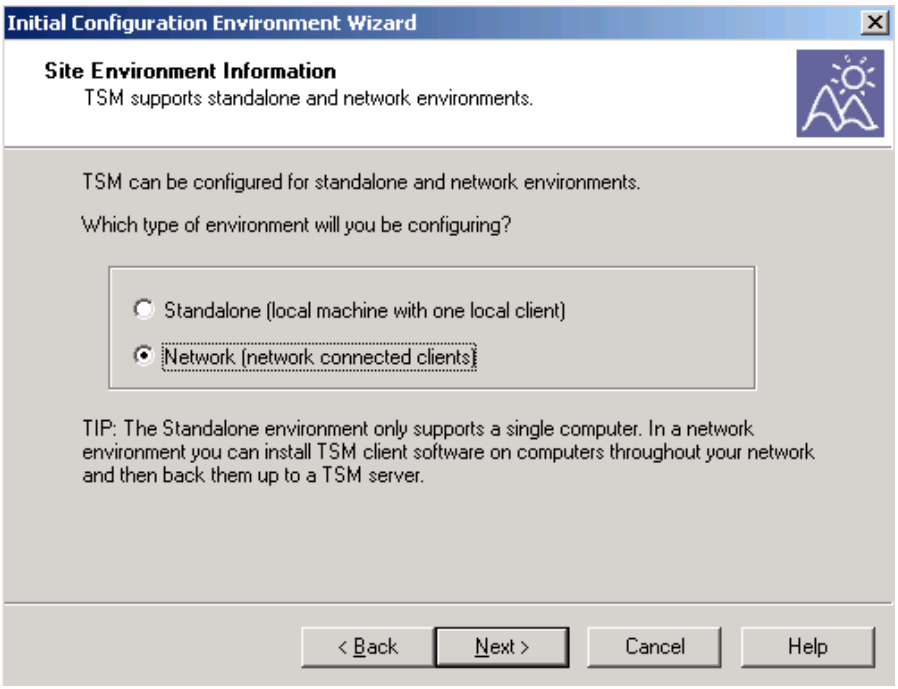


Aparecerá la ventana de bienvenida, presione en el botón **Next**.

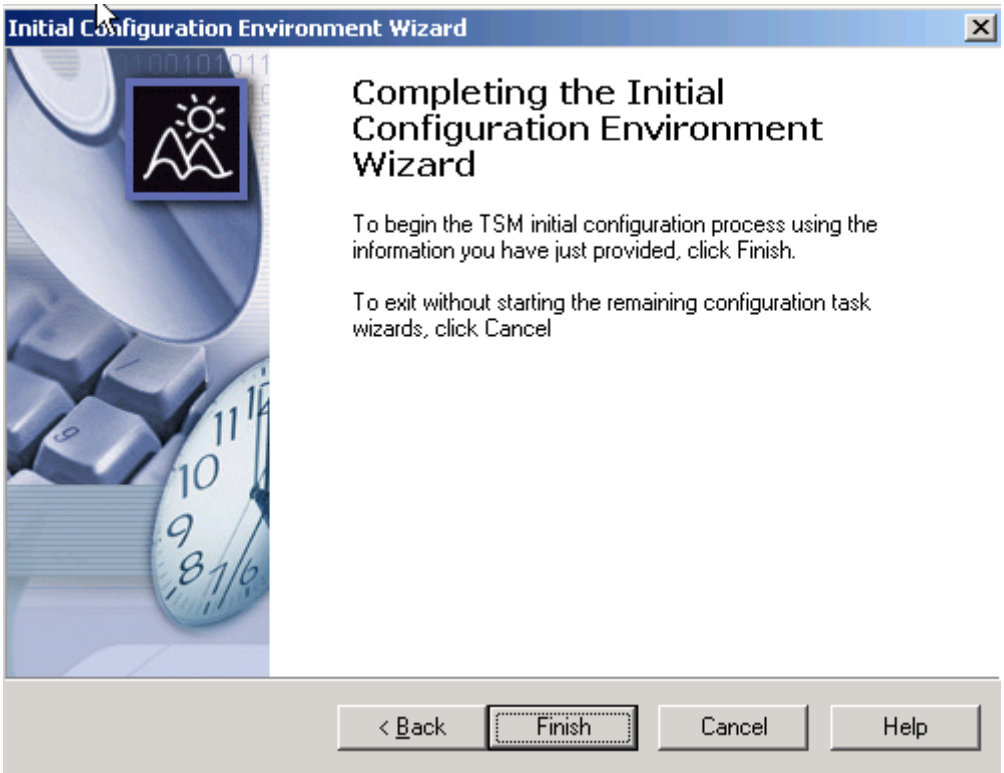
Seleccione "**Yes**" para que pueda tener una guía extendida durante el proceso de instalación y presione en el botón **Next**.



Los clientes se conectarán a TSM utilizando la red, entonces, seleccione el método de comunicación "**network**", presione luego en **Next**.



Presione en el botón **Finish**.

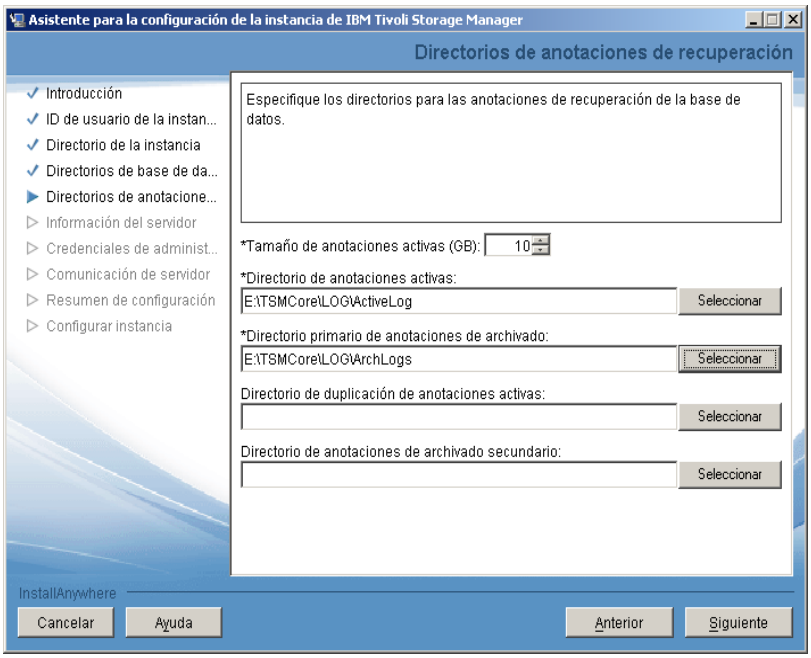


ASISTENTE de INICIALIZACIÓN

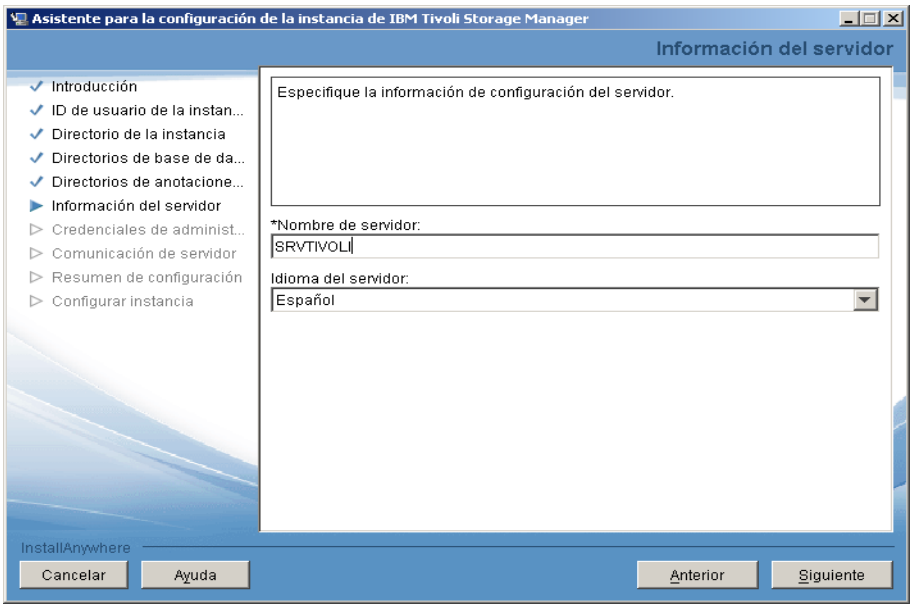
Presione en el botón **Next**.

Asignamos un espacio en disco, para poder almacenar los diferentes componentes de la base de datos de TSM.

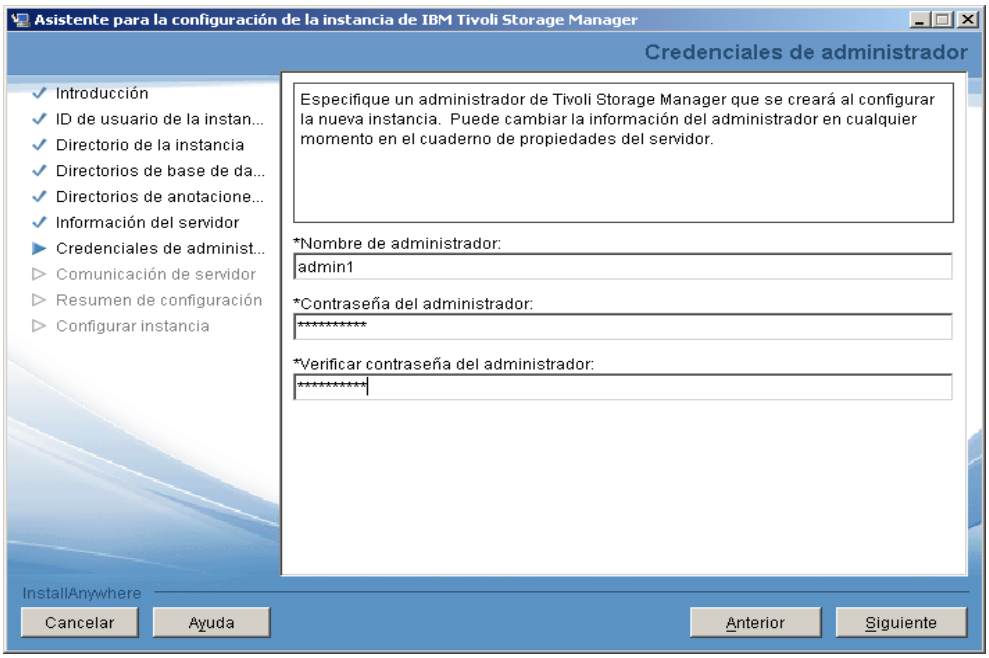
Definimos la ruta en la que previamente se instaló TSM, y lo agregamos la ruta totalmente identificada y tamaño para el primer grupo de almacenamiento de disco.



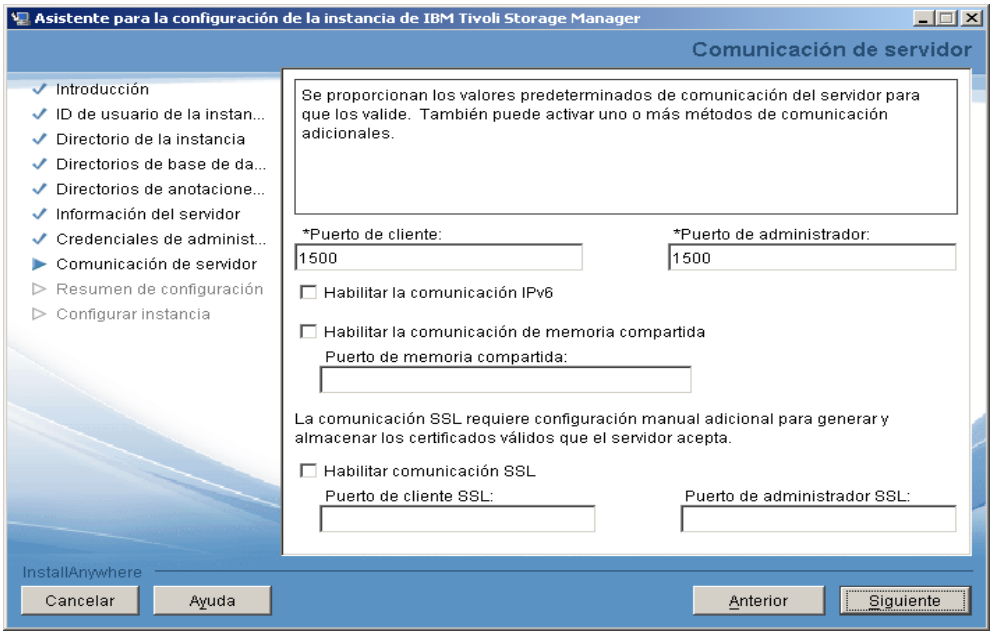
Se sugiere que se mantenga el mismo nombre del servidor en el cual se procedió a instalar la herramienta así como el idioma pre-establecido para el Sistema Operativo.



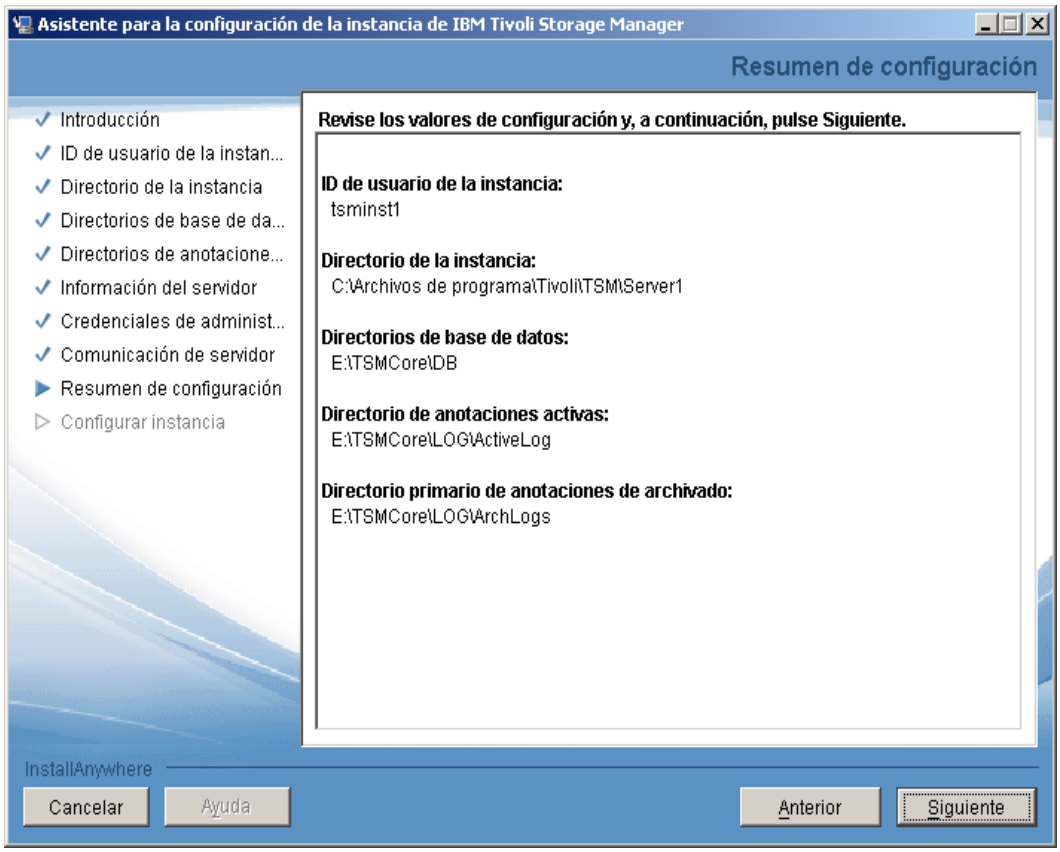
En este caso se utilizará el usuario "***admin1***", como administrador de la herramienta de respaldos en primera instancia se utiliza "***Passw0rd***" como contraseña para el usuario antes mencionado.



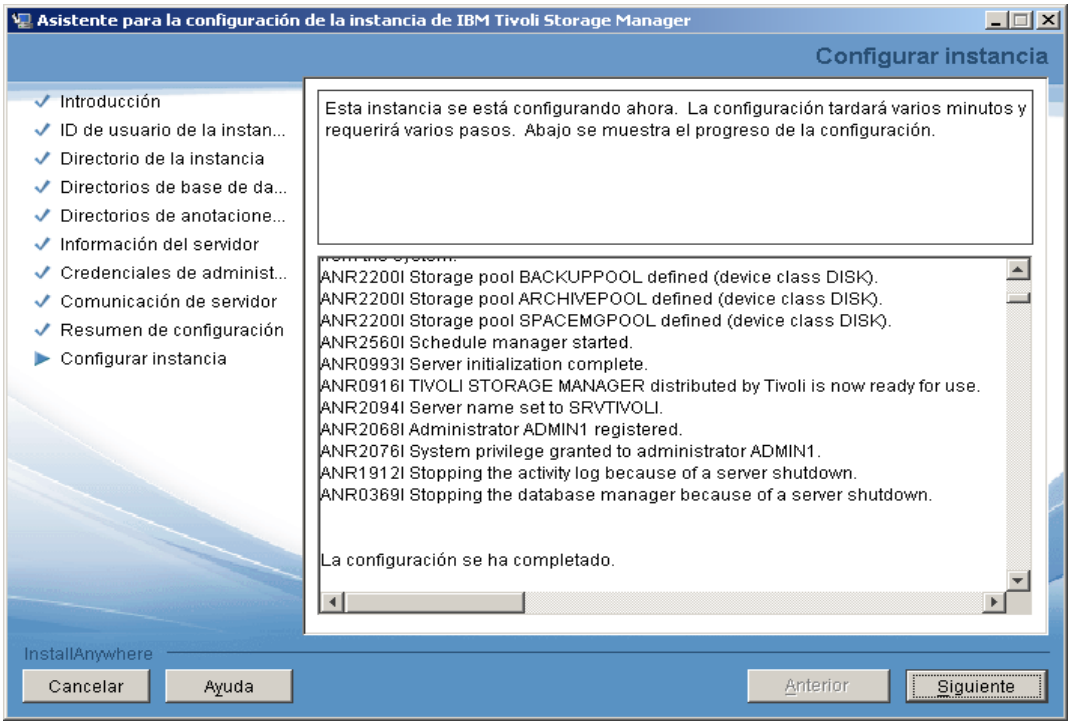
El puerto por defecto para la generación de la primera instancia de TSM es 1500, el cual no debe ser modificado si no existe la necesidad.



Al finalizar el asistente Ud. puede ver un resumen de las configuraciones realizadas, donde solo necesita hacer click en siguiente para continuar con el asistente de configuración.



Se detalla el resumen de la configuración realizada y la cual será aplicada.



CONFIGURANDO USUARIO “tsminst1” PARA ADMINISTRAR y LEVANTAR TSM COMO SERVICIO

Antes de continuar con el asistente de inicialización de dispositivos, debemos otorgar permisos al "**tsminst1**" para que pueda subir a TSMServer como servicio.

Debe previamente crear un usuario cualquiera en este caso "**tsminst1**", el mismo que debe agregarlo a los grupos DB2ADMNS y DB2USERS terminado este proceso desde la consola de administración de db2 (dsmcmd) digitamos los siguientes comandos.

C:\>**db2 get instance**
The current database manager instance is: SERVER1

C:\>set db2instance=server1

C:\>db2 connect to TSMDB1
Database Connection Information
Database server = DB2/NT 9.7.1
SQL authorization ID = ADMINIST... Local database alias = TSMDB1

C:\>**db2 "select grantee,securityadmauth from syscat.dbauth"**
GRANTEE SECURITYADMAUTH

ADMINISTRATOR Y
1 record(s) selected.

C:\>**db2 grant dbadm with dataaccess with accessctrl on database to user tsminst1**
DB20000I The SQL command completed successfully.

C:\>**db2 grant secadm on database to user tsminst1**
DB20000I The SQL command completed successfully.

C:\>**db2 "select grantee,securityadmauth from syscat.dbauth"**

GRANTEE SECURITYADMAUTH

ADMINISTRATOR Y

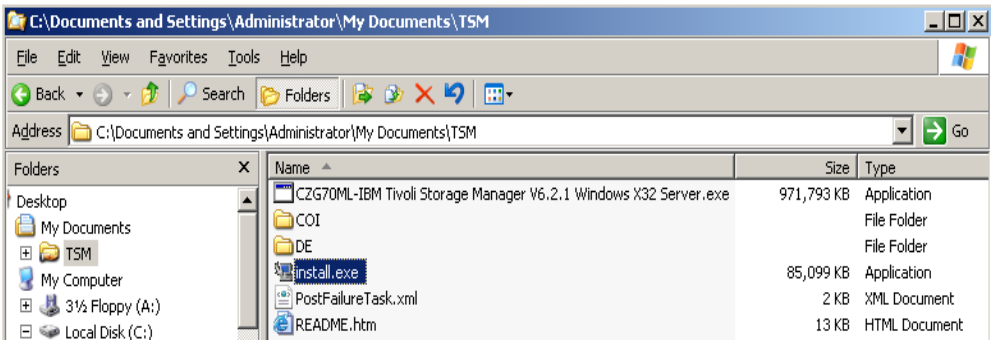
TSMINST1 Y

2 record(s) selected.

Ahora solo necesitamos ingresar en el administrador de servicios de Windows, he iniciar el servicio de TSM en el cual tenemos que asignar al servicio TSMServer1 el propietario de login al usuario "**tsminst1**", de igual manera realizamos la misma tarea para el servicio "***DB2 – DB2TSM1 – SERVER1***", para que inicie automáticamente.

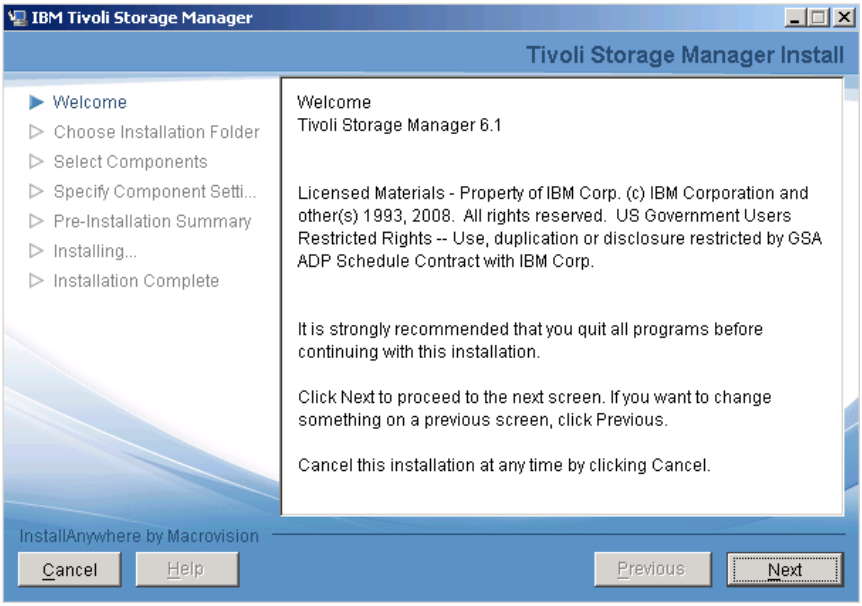
INSTALACIÓN del TSM ADMINISTRATION CENTER V6.1

Como un usuario del grupo administradores, procedemos con la instalación del **Admin Center (AC**), para esto nos ubicamos en el directorio del instalador y ejecutamos el archivo: **install.exe**

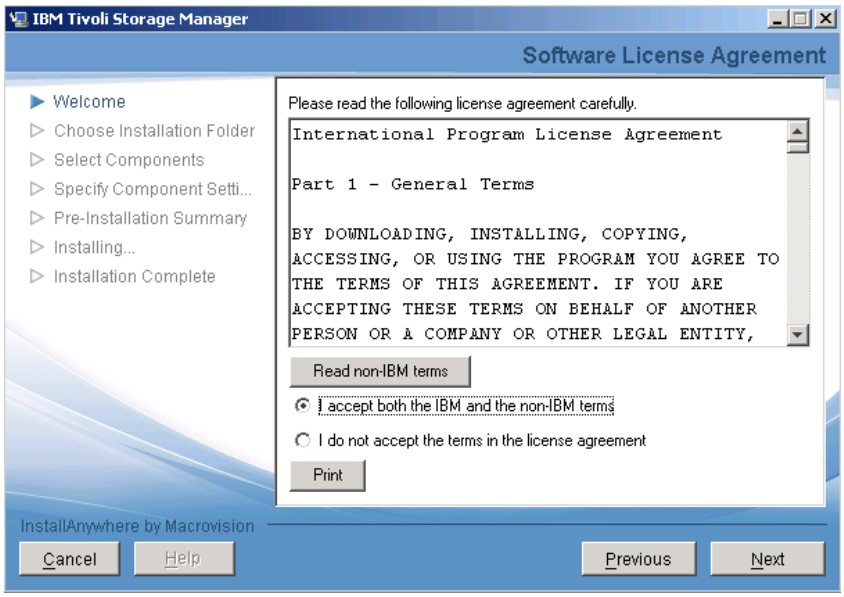


Tras la ejecución del archivo de instalación, aparecerá la ventana donde se deberá seleccionar el idioma de instalación.

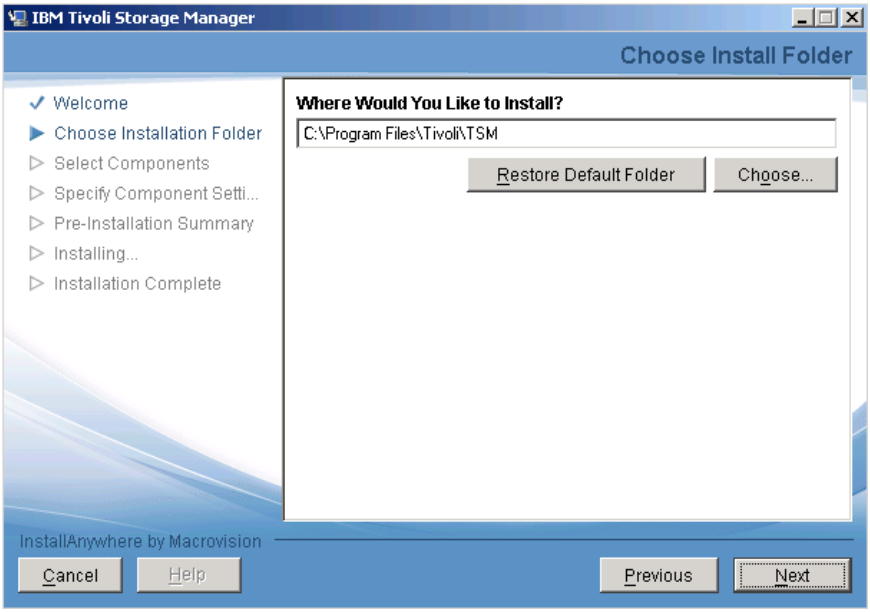
Aparecerá la ventana de bienvenida del "**Asistente de Instalación**", presione en el botón **Next**.



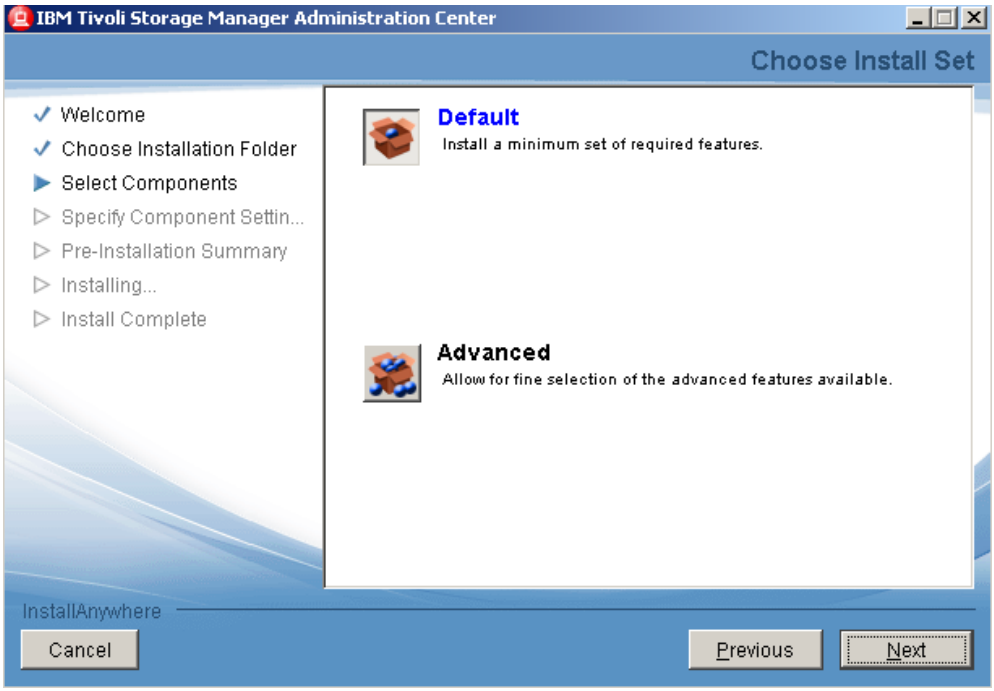
En esta ventana aparecerá el requerimiento de Licencia, la cual se deba aceptar poder continuar, presione en el botón **Next**.



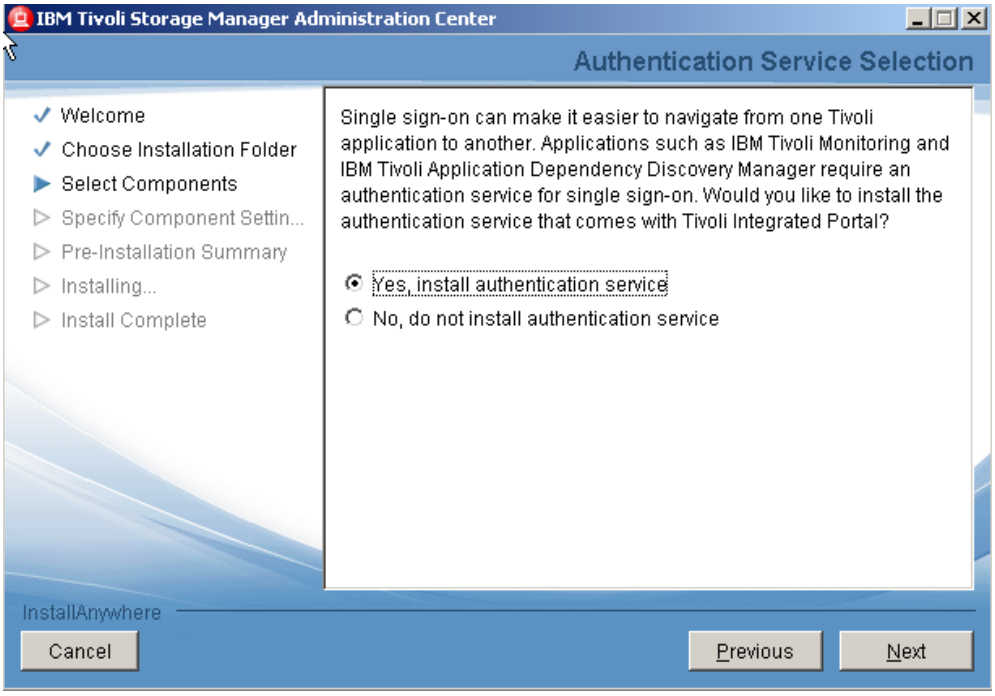
Acepte la ruta predeterminada para la instalación del Portal (**C:\Program Files\Tivoli\TSM**) y presione en el botón **Next**:



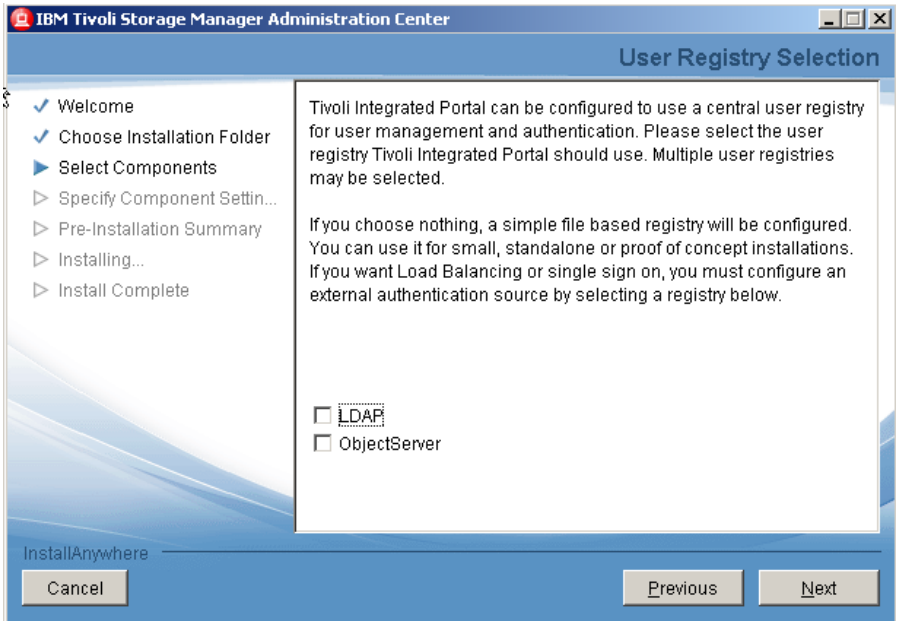
Seleccionamos la manera que deseamos instalar ya sea Default o Advanced, en este caso se utilizará el modo “Advanced”, ya que de esta manera podemos decidir instalar o no “Tivoli Integrate Portal”, presione en el botón **Next**.



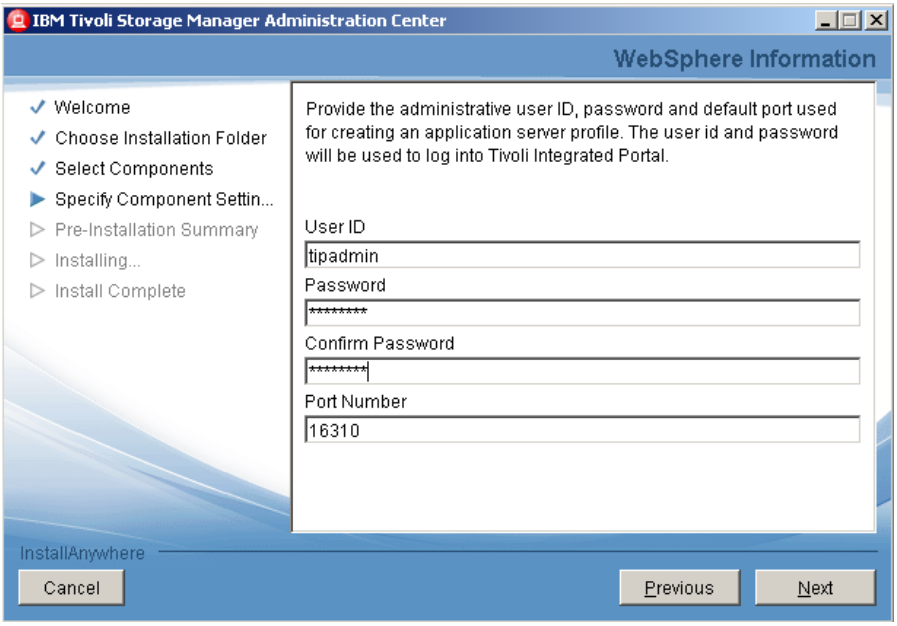
Se selecciona la opción Advanced para generar una instalación personalizada.



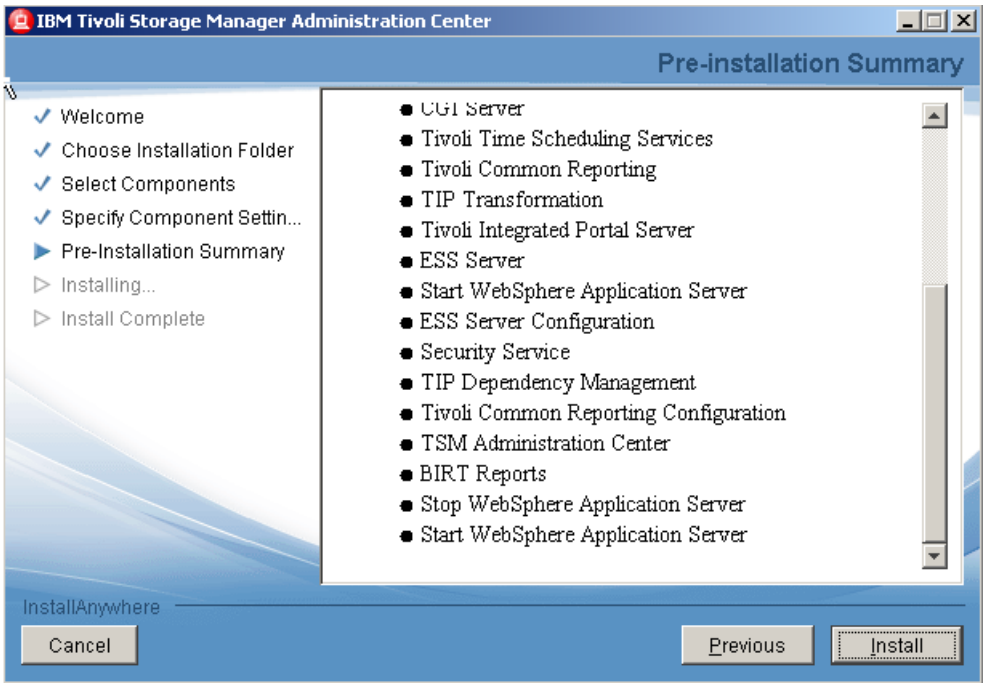
Adicionalmente, se puede optar una validación a través de LDAP para usuarios ya existente caso contrario se utiliza la autentificación normal de la herramienta.



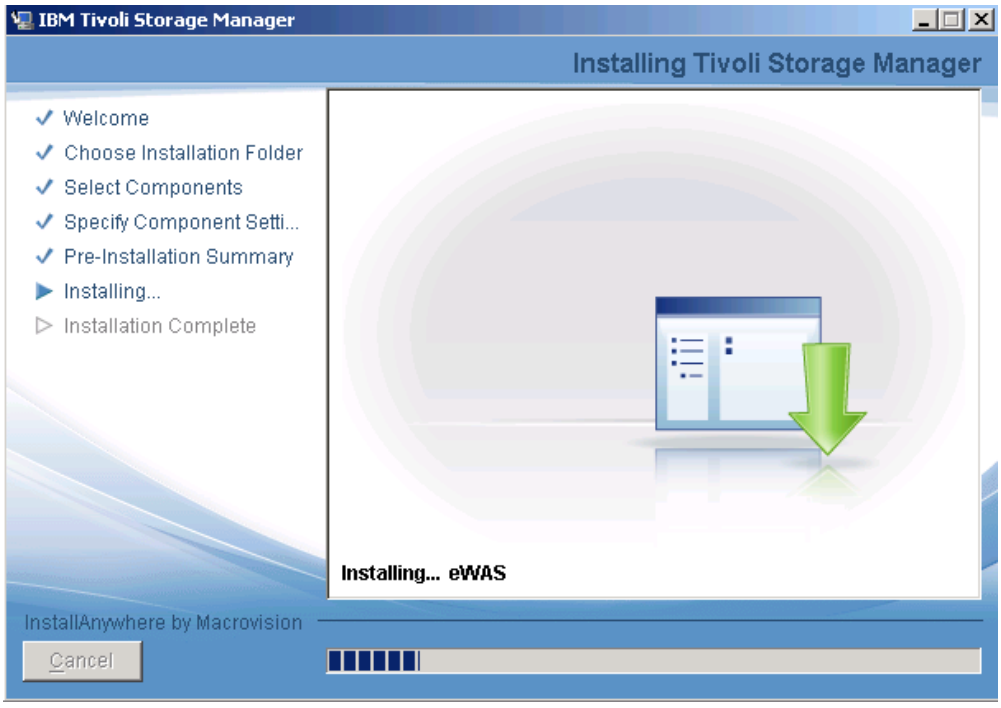
Para esta instalación se utilizará el usuario "***tipadmin***" con su respectiva contraseña "***Passw0rd***" a través del puerto 16310.



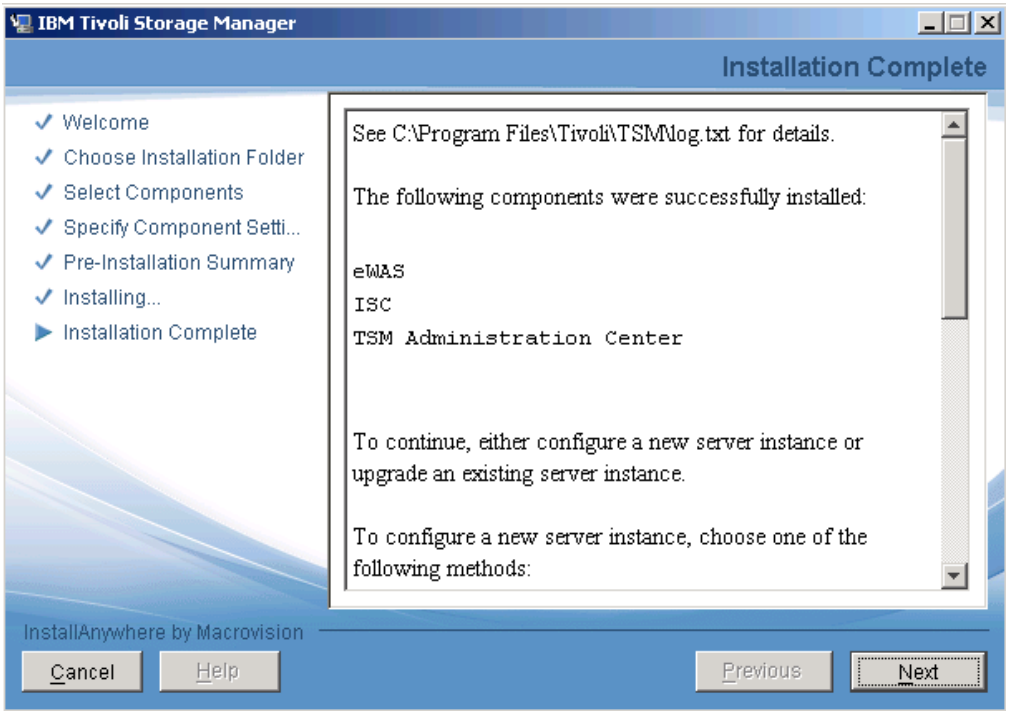
Se presentará el resumen de los paquetes que serán instalados conjuntamente con el "***Administration Center***"



Inicia el proceso de instalación:



Al final aparecerá la ventana en la que se indica que el proceso de instalación ha finalizado satisfactoriamente, presione en el botón **Next**.



Aparecerá la ventana final, presione en el botón **Finish**. Automáticamente se desplegará el navegador con la consola de administración web de Tivoli Storage Manager.

Para validar la instalación de Tivoli Integrated Portal manualmente, es necesario ejecutar un explorador web y abrir la siguiente URL:

http://<hostname>:16310

PARAMETRIZACIÓN DE LA SOLUCIÓN DE ADMINISTRACIÓN DE RESPALDOS IBM TIVOLI STORAGE MANAGER

A continuación se resume la definición de atributos y componentes de la solución de administración de respaldos a través de IBM TSM:

SETEO DE PARÁMETROS de CONECTIVIDAD

Desde una consola de comandos administrativos de TSM (**dsmadmc**) ejecutamos lo siguiente:

SETOPT COMMTIMEOUT 7200

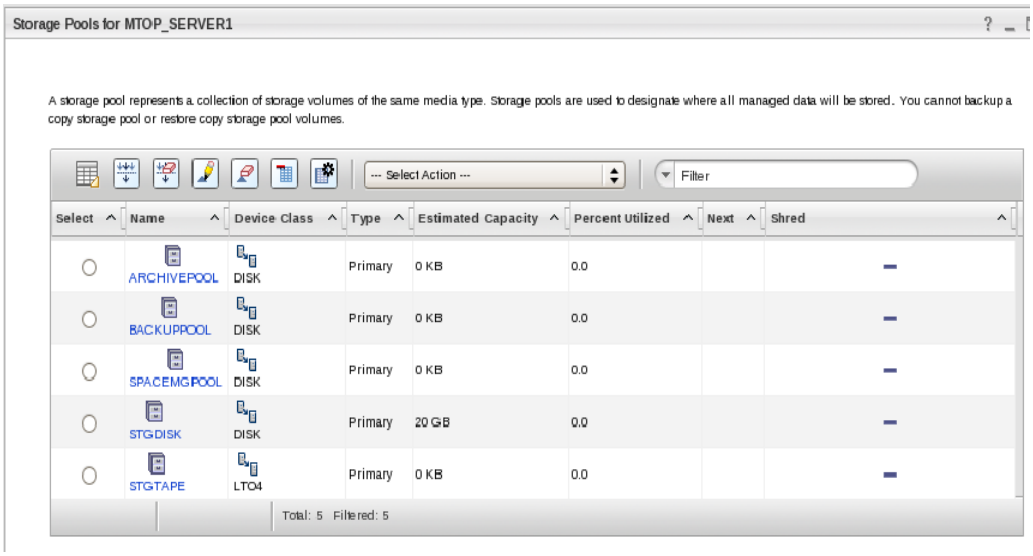
SETOPT IDLETIMEOUT 30

CREACIÓN DEL DEVICE CLASS TIPO FILE

La definición de las “clases de dispositivos” puede realizarse mediante el portal web (Tivoli Integrated Portal) o mediante la línea de comandos:

DEFINE DEVCLASS FILEDEV DEVTYPE=FILE FORMAT=DRIVE MAXCAP=10485760K MOUNTL=4 DIR=/TSMdata/FILEDEV SHARED=NO

CREACIÓN de STORAGE POOLS para el DEVICE CLASS tipo LTO y tipo DISK
Al igual que el resto de componentes, la definición de “storage pools” puede realizarse vía web o mediante comandos administrativos.



DEFINICIÓN DE STORAGE POOL DE ALMACENAMIENTO.

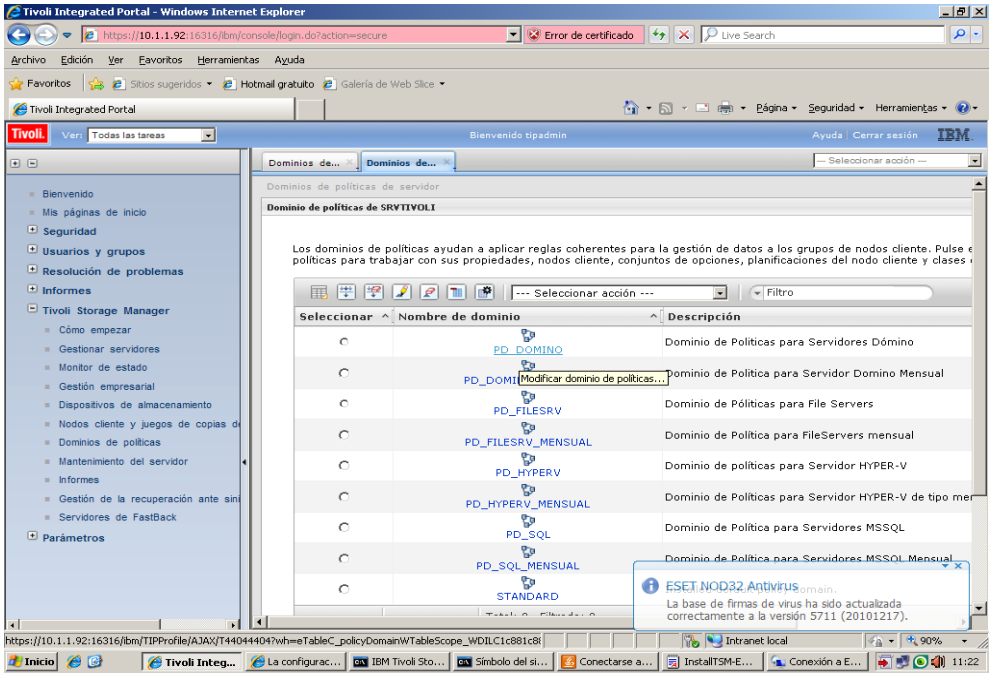
DEFINE STGPOOL STGDISK DISK POOLTYPE=PRIMARY
DESCRIPTION=”Storage Pool Primario de tipo DISK para stage de datos previos a tape**” NEXTPOOL=STGTAPE HI=90 LO=0**
DEFINE VOL STGDISK C:\TSMData\STGDISK\diskvol01.dsm
FORMATSIZE=20480 WAIT=yes
NOTA: El tamaño se especifica en MB, si se desea un pool de 20 GB el valor a setear es 20 x 1024 MB=20480 MB.

PROCESO de REGISTRO de NODOS en TSM

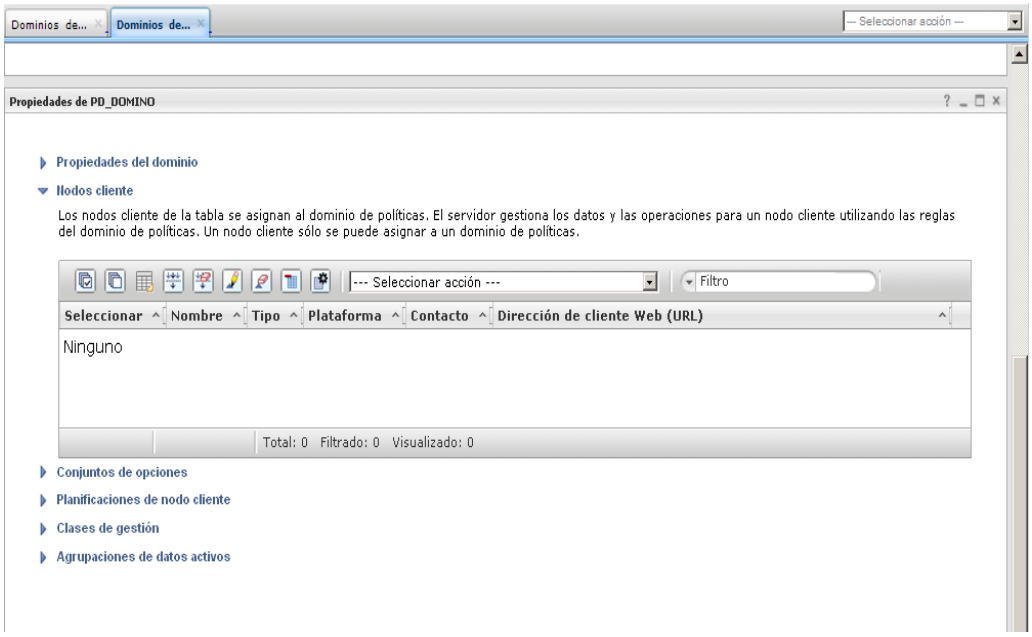
El proceso de registro de nodos bajo un Policy Domain de TSM Server es relativamente sencillo. Se lo puede realizar vía comandos administrativos (**dsmadmc**) o vía web mediante el Tivoli Integrated Portal. En este ejemplo registramos vía comandos el nodo Linux **SRVINSTRANET** bajo el Policy Domain **PD_FILESERVER**:

register node SRVINTRANET admin passexp=0 backdel=yes archdel=yes domain=PD_FILESERVER

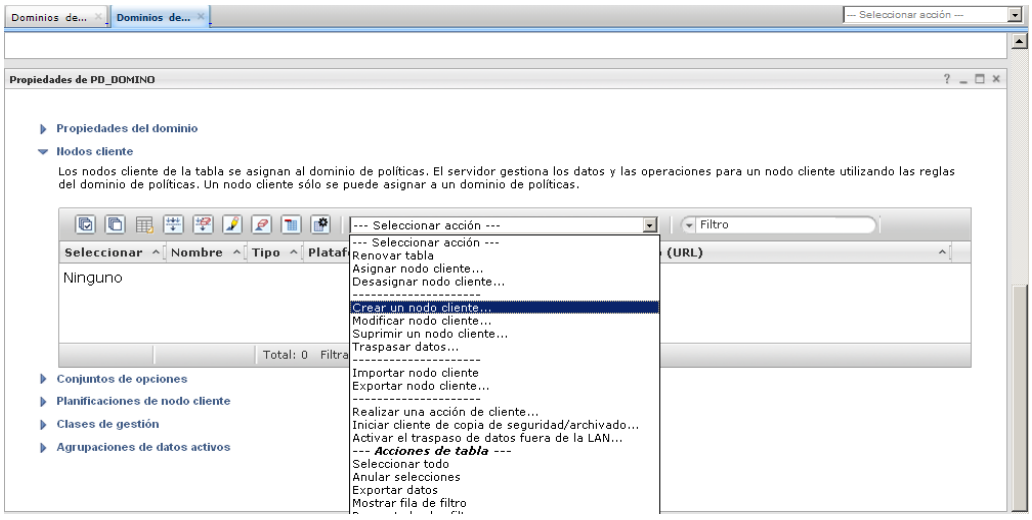
Desde el Tivoli Integrated Portal el proceso se resume en las siguientes pantallas:



En el combobox, seleccionamos, Crear un nodo cliente para poder iniciar con el asistente.

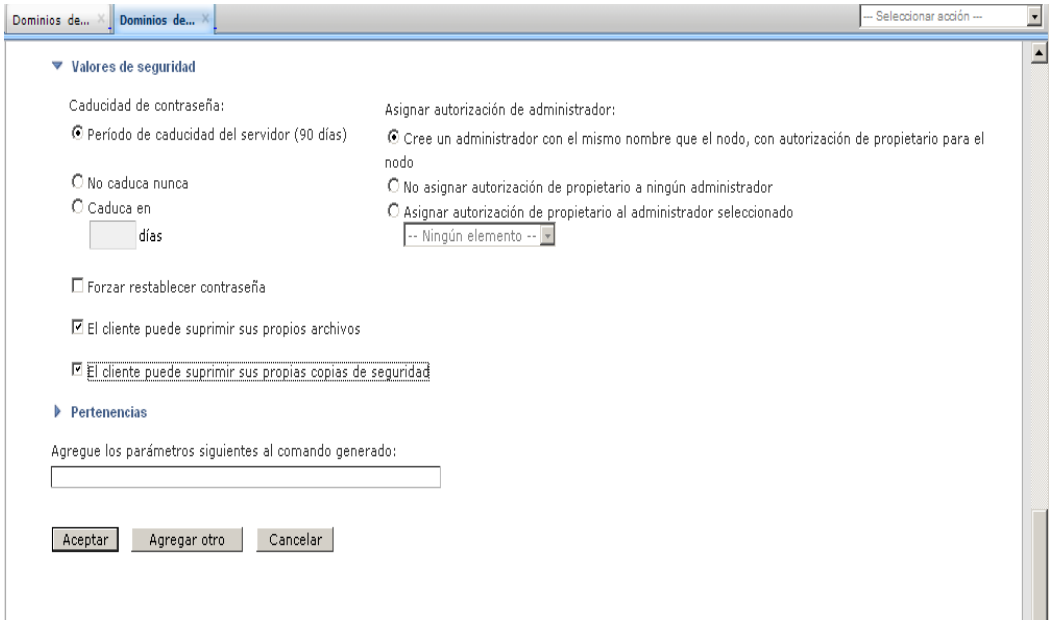


Se desplegará una ventana de configuración donde se podrá establecer el medio de comunicación y demás parámetros de configuración de conectividad para cada nodo nuevo que se registre en TSM.

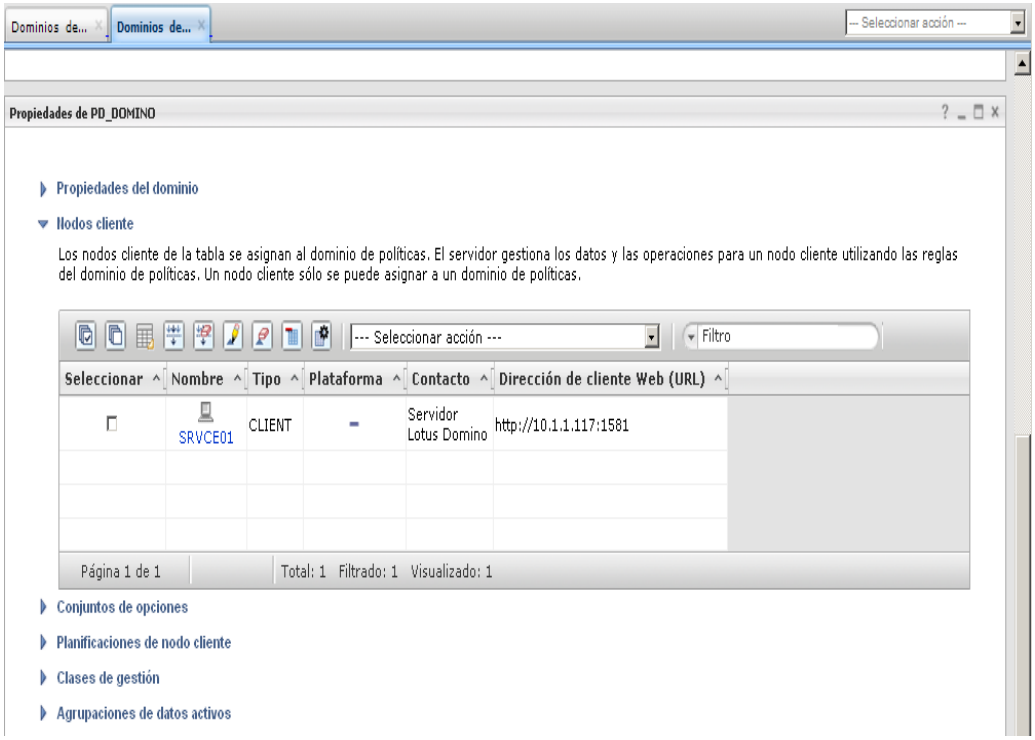


Se recomienda que el nombre del nodo sea el mismo del equipo en primera instancia o un identificativo que ayude con la pronta identificación de los servicios que ofrece. La clave aquí suministrada es totalmente independiente de la consola de comandos, la base de datos o la consola web.

Active por defecto que la clave del nodo no caduque y que el nodo pueda suprimir tanto sus respaldos como sus archivamientos generados (backups y archives).



Una vez finalizado el asistente podremos observar el nuevo cliente creado pero en el campo plataforma no se observa ningún cambio ya que el mismo se genera una vez que se haya realizado el proceso de registro del nodo creado.



SCRIPTS GENÉRICOS para BACKUP y ARCHIVE hacia IBM TSM

Los scripts genéricos para realizar el backup tanto de los Servidores de Archivos, Domino y Hyper-V son: "**bkp_nombreservidor.cmd**", "**bkp_nombreservidorHV.cmd**" y "**bkp_dominc.cmd**", los cuales se encuentran en el los diferentes servidores de la solución implementada. Dichos scripts se encuentran bajo el directorio del cliente de respaldos de IBM TSM (**C:\Archivos de Programa\Tivoli\TSM\baclient**).

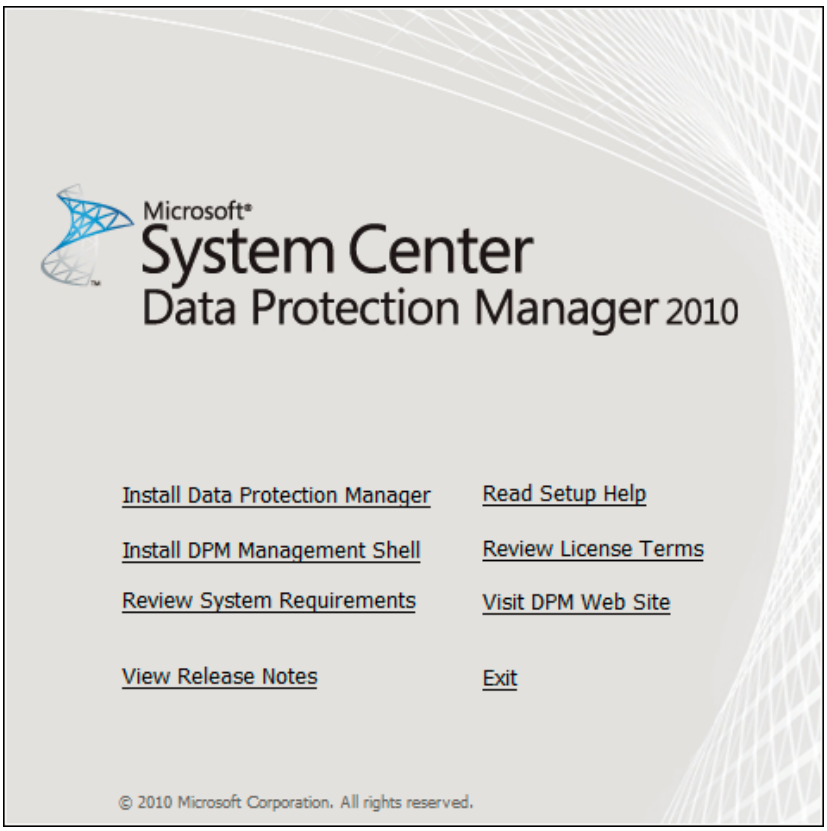
Ejemplo de Script para respaldo de File Servers.

bkp_srvcorreo.cmd
TSM_DIR="C:\Archivos de Programa\Tivoli\TSM\baclient" cd $TSM_DIR date < /dev/null > $TSM_DIR/bkp_srvuepro.log time < /dev/null >> $TSM_DIR/ bkp_srvuepro.log #OJO: en una sola línea la siguiente instrucción $TSM_DIR/**dsmc incr** "D:*" -subdir=yes -optfile=$TSM_DIR/dsm.opt >> $TSM_DIR/bkp_srvuepro.log

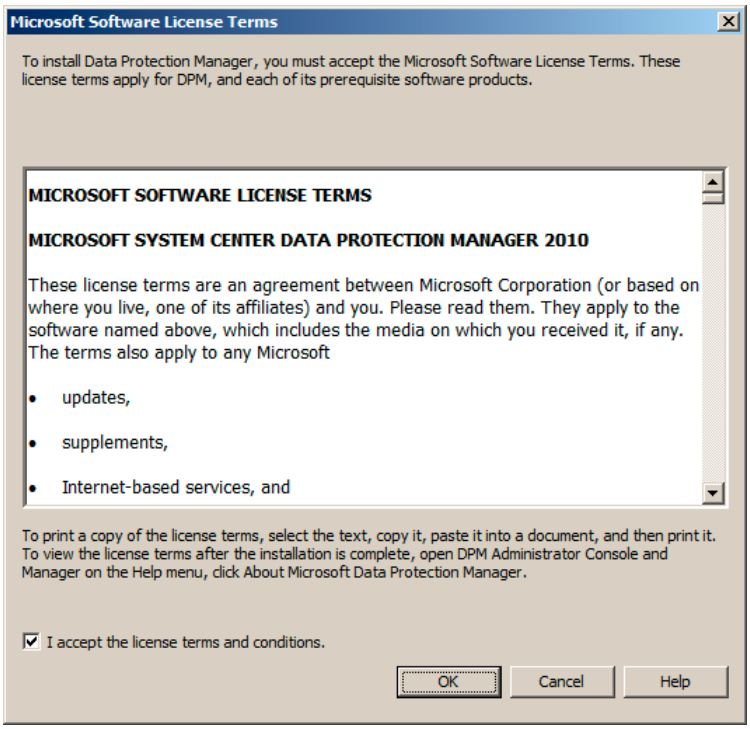
C. MANUAL DE MICROSOFT SYSTEM DATA PROTECTION MANAGER

Instalación de Data Protection Manager 2010

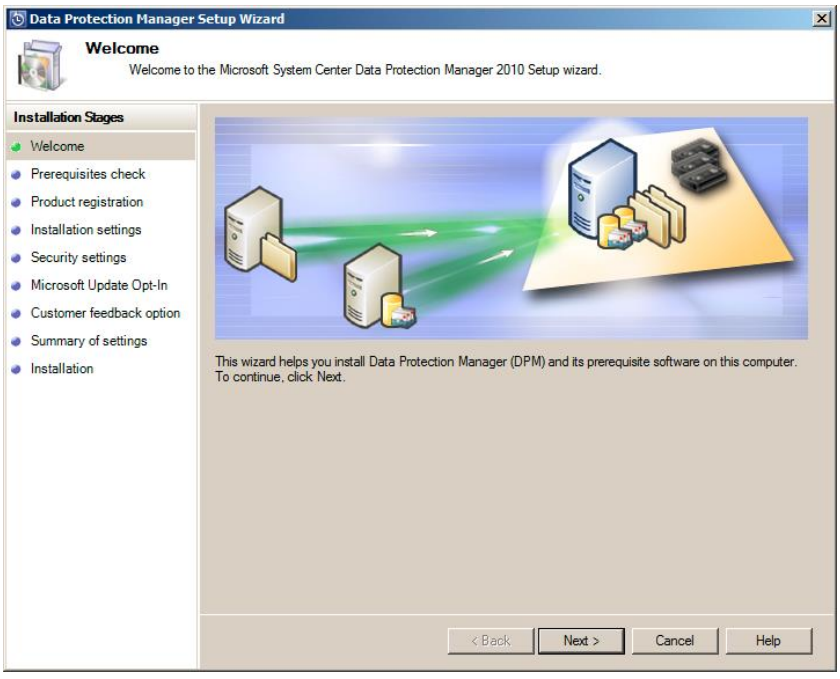
El primer punto a comprobar es que el servidor de Microsoft que será utilizado para DPM este unido a un dominio caso contrario la instalación no podrá concluir con éxito.



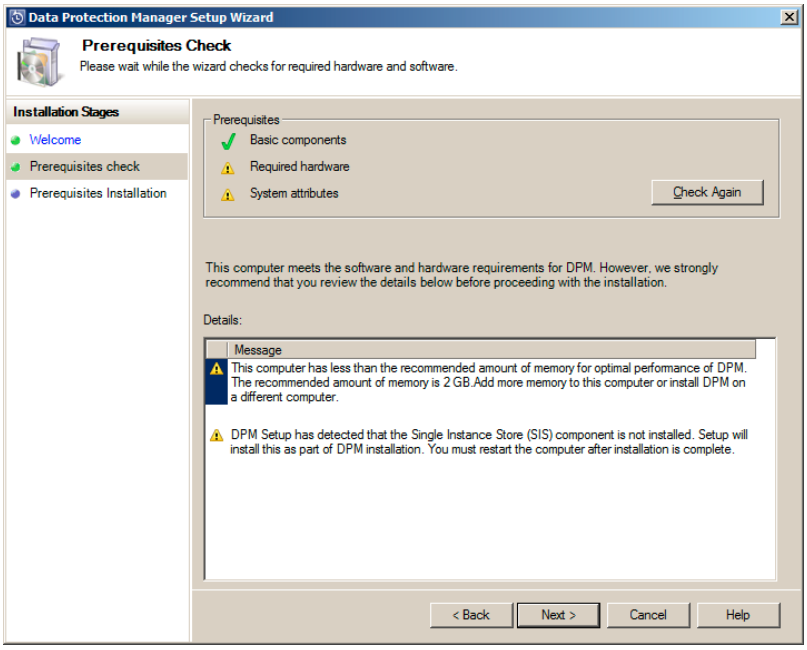
Seleccionamos “Install Data Protection Manager” o “Instalar Administrador de protección de datos” (si se lo descargaron en español)



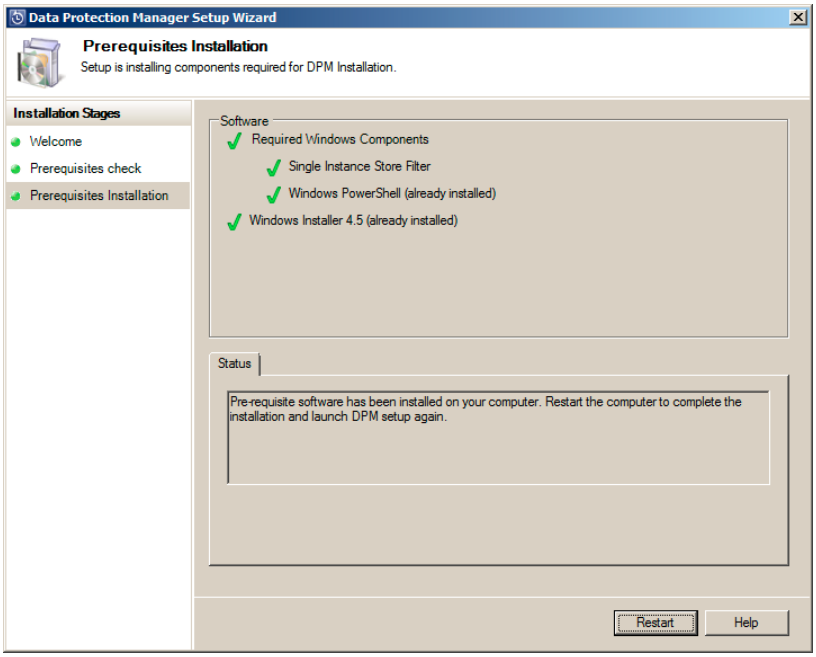
Marcamos la casilla de licencia para poder continuar con la instalación, y OK/Siguiente. Antes de continuar con la siguiente ventana el asistente instalará algunos componentes necesarios como "Microsoft .Net Frameworks 3.5 SP1" si no lo teníamos instalado.



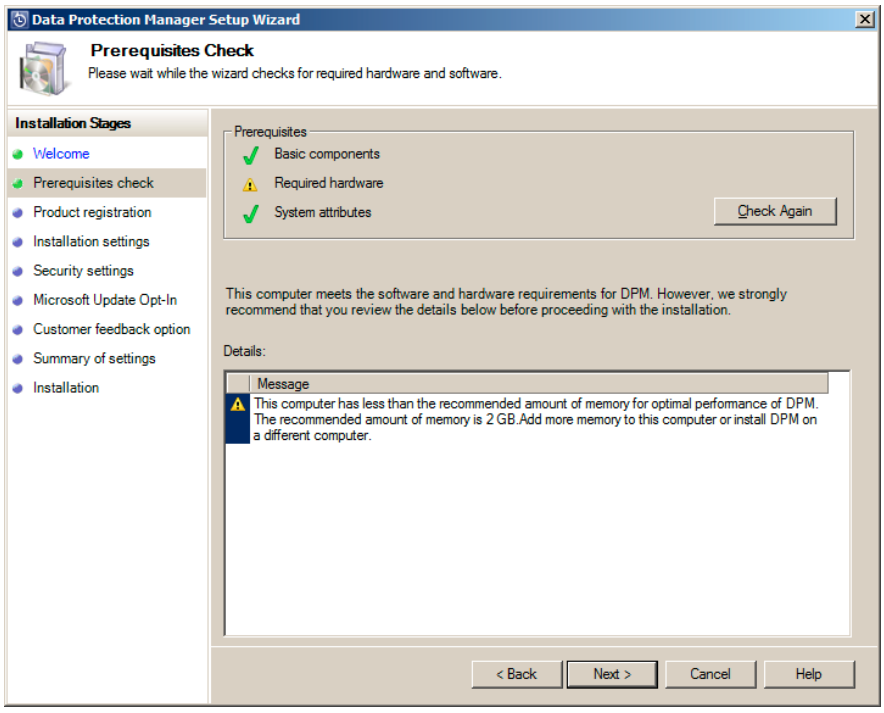
Luego de la instalación procedemos a continua con la instalación.



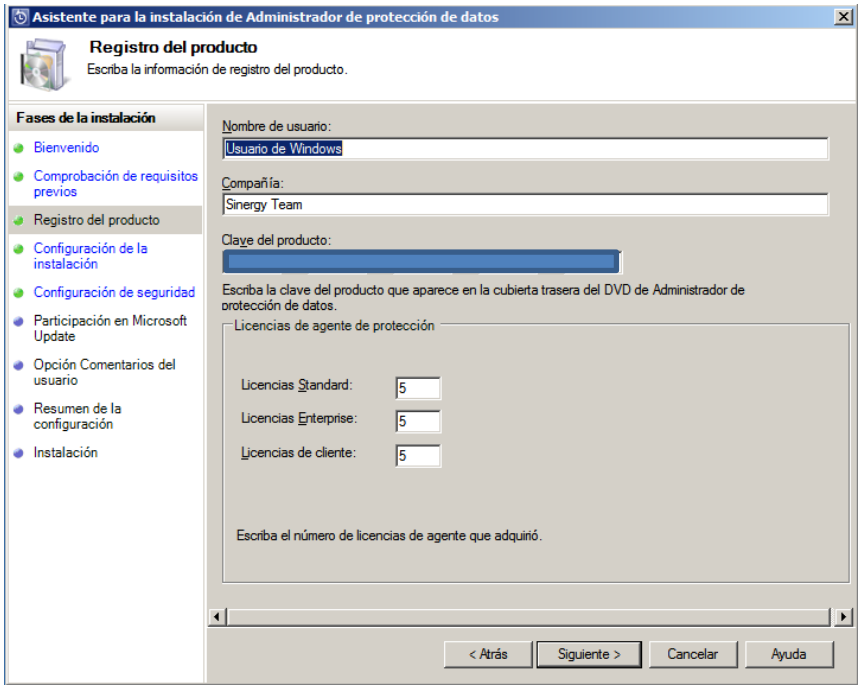
El asistente ahora ha comprobado los prerrequisitos, y se puede observar que el sistema no cumple con el mínimo de memoria ram (2GB) y que no tiene instalado el componente SIS. Estas alertas son informativas ya que por la memoria se tornará más lento pero instalará la herramienta en el caso del componente faltante el asistente lo instalará.



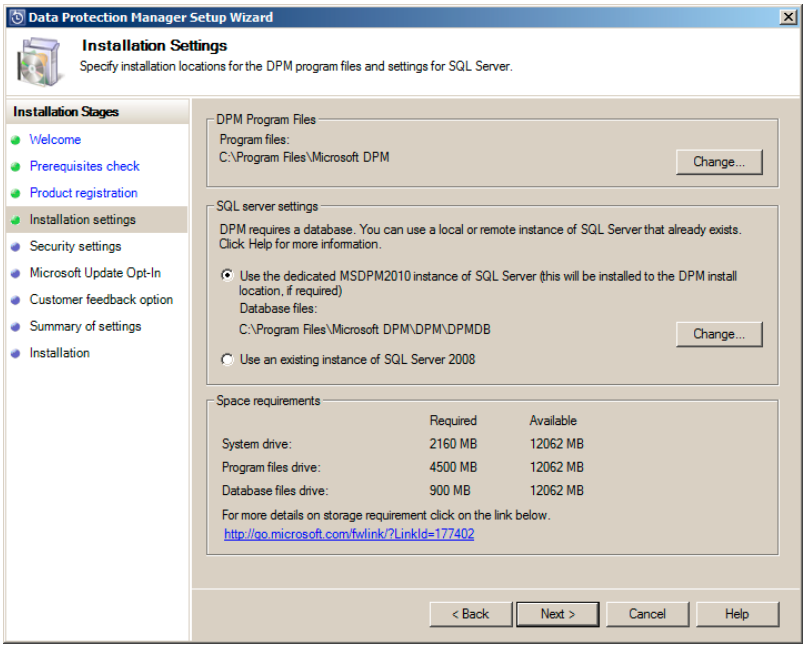
Debemos proceder a reiniciar el equipo para que aplique y active los componentes recién instalados.



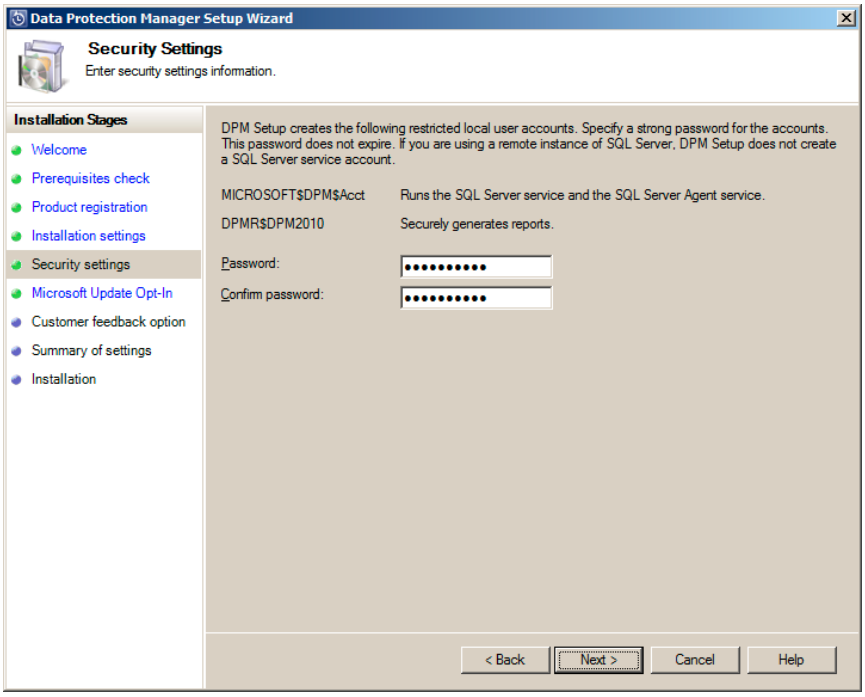
Lanzamos nuevamente el instalador pero esta vez solo aparecerá la alerta de la memoria ya que el resto de componentes ya los ha instalado.



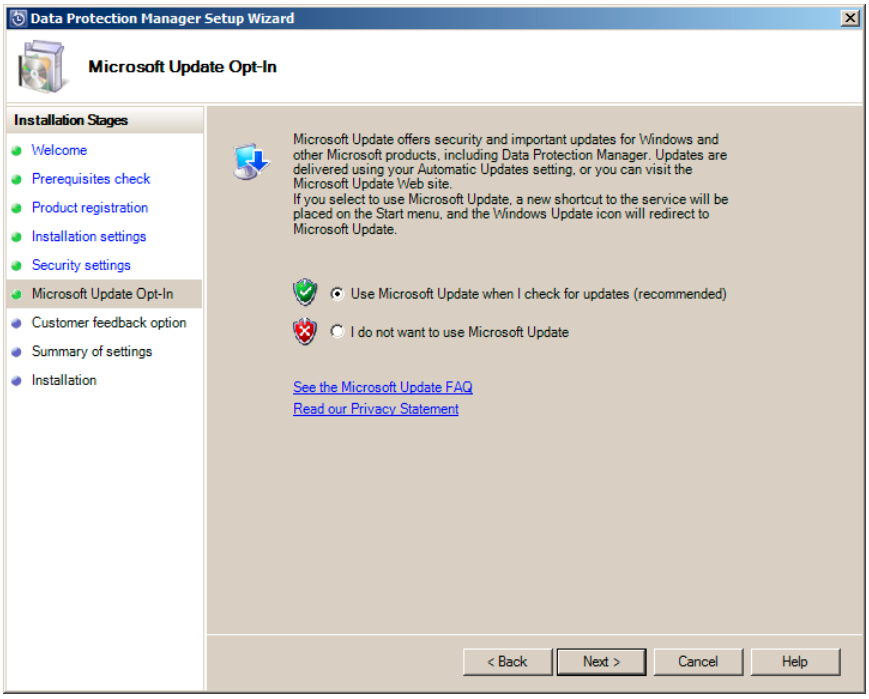
Nos pedirá un nombre de usuario y empresa.



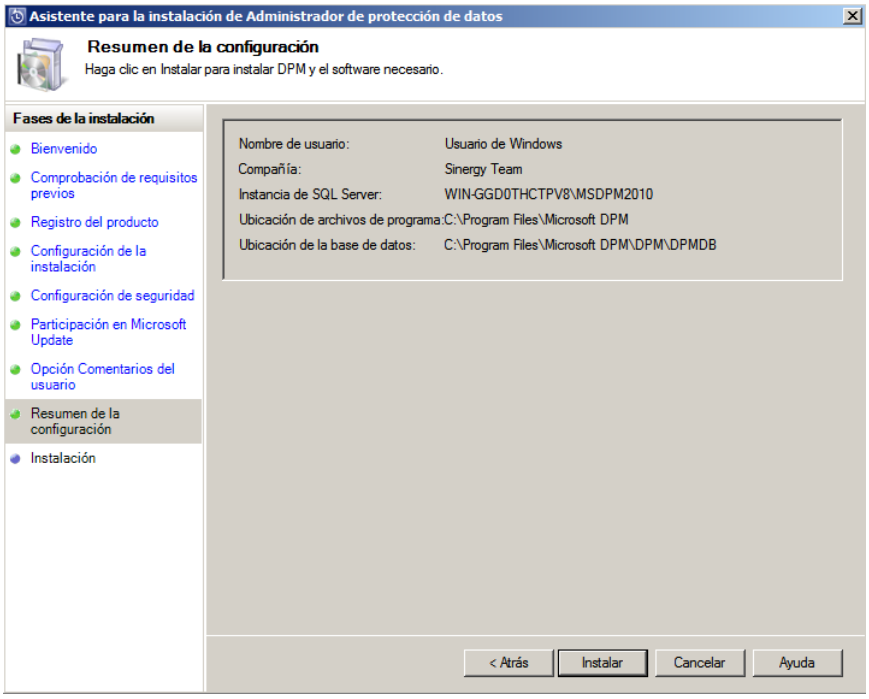
Data Protection Manager necesita una base de datos en SQL Server 2008 / R2. Podemos seleccionar la opción que yo seleccioné y el asistente instalará una base de datos en local, o decirle que utilice una instancia de SQL Server 2008 ya existente. En este caso instale el motor de SQL.



Especificamos una contraseña segura y proseguimos.

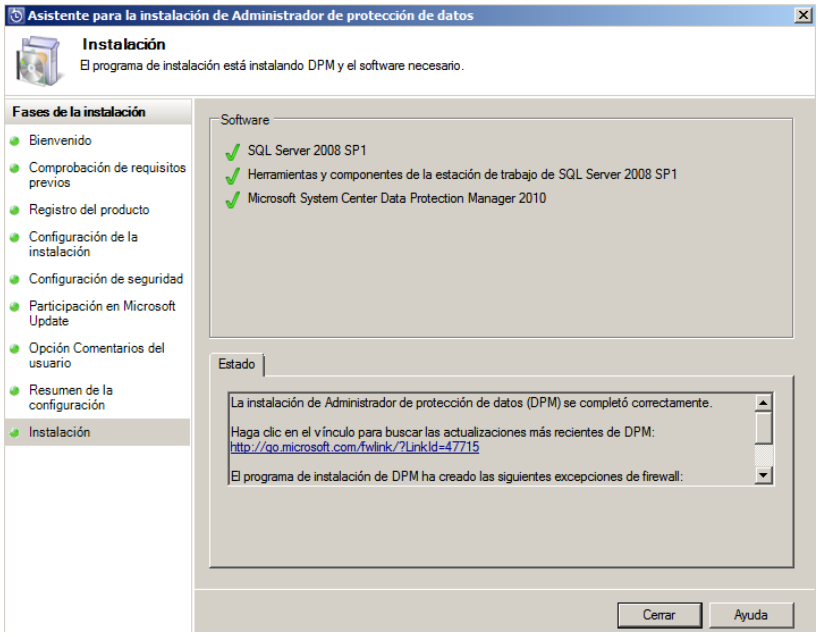


Podemos enlazar a la herramienta para que descargue automáticamente actualizaciones o parches necesarios.

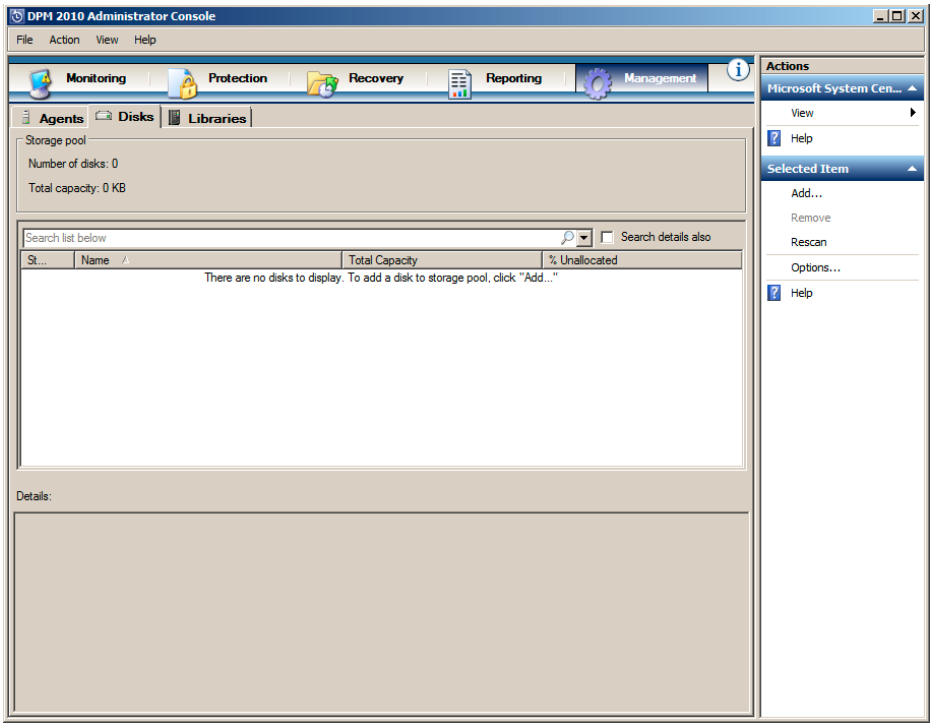


Aparece el resumen de nuestra configuración y procedemos a instalar la misma.

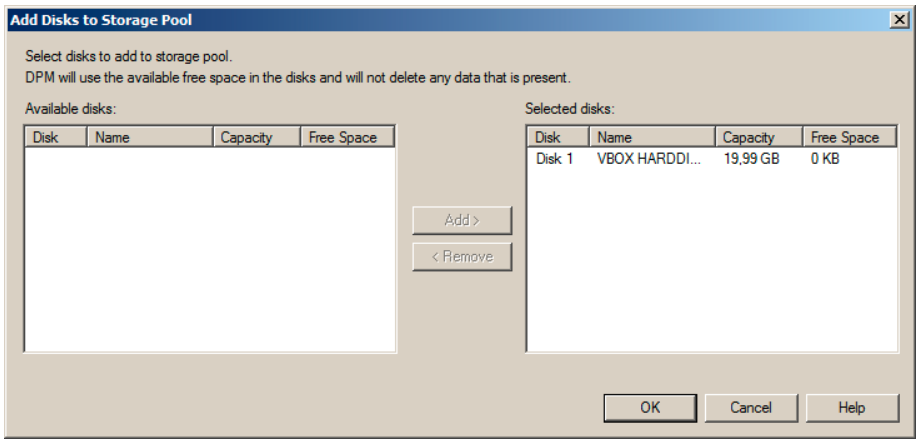
Una vez terminada la instalación tendremos algo como lo siguiente.



Procedemos a ingresar a la herramienta y a asignarle el espacio en disco que utilizará para los respaldos de sus clientes.



Hacemos click en **Management** y a **Disks**. Y hacemos click en **Add…** para añadir un disco duro.



Con lo cual queda operativa nuestra herramienta DPM de Respaldos.

D. PROCEDIMIENTOS DE RESPALDO Y RESTAURACIÓN DE INFORMACIÓN

Los procedimientos de "respaldos" y "restauraciones", establecidos en el presente documento tienen como objetivos proteger los datos y aplicaciones de software contra todo tipo de fallas que puedan ocurrir y posibilitar la recuperación de fallas en el menor tiempo posible y sin la pérdida de datos.

Se deberán establecer los procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los Sistemas o aplicativos de la Compañía.

Archivos que deben tener copias de respaldo

1. Backups del Sistema Operativo (en caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos).

2. Backups del Software Base (Paquetes con los cuales interactúan los Aplicativos de la Compañía).

3. Backups del Software Aplicativo (Considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software o procedimiento que también trabaje con la información, para producir los resultados con los cuales trabaja el usuario final).

4. Backups de los Datos y de estructura de datos (Bases de Datos, Índices, tablas de validación, contraseñas, tablespaces, usuarios, roles y todo archivo necesario para el funcionamiento de los Sistemas de Información de la Institución y la pronta recuperación de los mismos en caso de fallas).

5. Backups de archivos de usuarios (Archivos utilizados por el personal de la Universidad en cada Departamento).

Especificaciones y normas para la elaboración de los backups

Para backups de Sistemas Operativos y de Software Base

1. Los backups de los Sistemas Operativos y de Software Base utilizados en el Centro de Sistemas de Información deberán estar almacenados en CD's o DVD's con etiquetas que contengan la siguiente información:

   - ✓ Código de numeración del CD/DVD [tipo][número].
   - ✓ Identificación del Sistema Operativo.
   - ✓ Número de CD/DVD (en formato [número]de[cantidad total de CD´s].
   - ✓ Versión.
   - ✓ Idioma

2. Las claves de instalación de los diferentes Sistemas deberán ser administradas por el Administrador de la Base de Datos y proporcionada al personal de soporte técnico cada vez que sea necesario manteniendo un registro sobre las instalaciones realizadas.

3. La ubicación de resguardo de dichos backups será la Sala de Servidores del Centro de Sistemas de Información que cuenta con las condiciones apropiadas para el mantenimiento de los medios.

4. La frecuencia de obtención de estos backups deberá ser anual o cada vez que se deteriore el medio de almacenamiento de los mismos.

Para Backups del Software Aplicativo

1. Los backups del Software Aplicativo deberán estar almacenados en CD´s con etiquetas que contengan la siguiente información:
   - ✓ Código de numeración del CD [tipo][número].
   - ✓ Nombre del Sistema.
   - ✓ Versión.
   - ✓ Ubicación de las fuentes (formato: [nombre sistema]/[fuentes]).
   - ✓ Ubicación de los compilados (formato: [nombre sistema]/[compilados]).
   - ✓ Ubicación de los instaladores (si se tienen) (formato: [nombre sistema] /[instaladores]).
   - ✓ Número de CD (en formato [número]de[cantidad total de CD´s], ej. 2 de 3)

2. La ubicación de resguardo de dichos backups será la Sala de Servidores del Centro de Sistemas de Información y una máquina de la red.

3. La frecuencia de obtención de éstos backups es anual en caso de que no se registren modificaciones; y cada vez que se elabore una nueva versión del sistema.

Para Backups de datos

1. Los backups de datos y de estructura de las bases de datos deberán realizarse para cada base de datos que se encuentre a cargo del Centro de Sistemas de Información, a la fecha son:
   - ✓ Bases de Datos ubicadas en los Servidores en custodia de Centro de Sistemas de Información: UCBL, UCB2 e IISEC (Base de Datos del Instituto de Investigaciones Socio Económicas)
   - ✓ Bases de Datos externas ubicadas fuera del Centro de Sistemas de Información: MPDL y MPDS (Bases de Datos de Maestrías para el Desarrollo de La Paz y Santa Cruz)
2. Los backups de datos deberán elaborarse según su importancia de la siguiente manera:
   - o Backups completos diarios en épocas críticas como inscripciones y backups día por medio en épocas normales.
   - o borrado de los backups anteriores semanalmente.

- backups completos semanales.
- borrado de los backups anteriores mensualmente

Los backups se guardan en dos lugares fijos distintos, en el directorio backups del disco donde se halla el motor y en un directorio creado para tal fin.
Para todos los servidores copiar los últimos backups de configuraciones he instaldores de la herramienta cada semana.

3. La nomenclatura de los backups sigue este patrón: años (4 dígitos), mes (2 dígitos), día (2 dígitos). Ejemplo: el backup del 4 de Junio del 2000 es 20000406.dmp, donde dmp es la extensión del archivo.

   Para los directorios donde se almacenan los backups: [NOMBRE_SERVIDOR]/ [NOMBRE_BAKCUP]

4. Al sacar un backup se debe necesariamente crear un archivo log, en el mismo directorio en el que se está creando el backup. Debe seguirse la misma nomenclatura usada en los archivos bmp en el nombre de los archivos log.

5. Una vez que se han creado los dos archivos, el dmp y el log, deben comprimirse con algún compresor de archivos (actualmente se lo realiza con el Winzip) y almacenarse en dos lugares físicos distintos. Una copia debe quedar en el directorio Backups del disco denominado motor, mientras que la otra copia en un directorio creado con tal fin, en alguna de las máquinas de la red.

Backups de archivos de usuarios

1. Los archivos de usuarios se almacenarán en un disco duro bajo la responsabilidad del personal de Soporte Técnico de la Universidad y en base a la siguiente configuración de carpetas:
   - ✓ [Fecha]/[Nombre Departamento]/[Nombre Usuario]/.
   - ✓ [Fecha]: Semestre-Año, ej: 2-2004.
   - ✓ [Nombre Departamento]: sigla o nombre según corresponda, ej: ADM ó PERSONAL

- ✓ [Nombre Usuario]: inicial nombre y apellido, ej: mTorrez
- ✓ La nomenclatura de los subdirectorios del usuario se realizarán según la información que almacene el usuario.

2. Se obtendrán backups de archivos de usuarios semestralmente para todos los usuarios de la red de la Universidad.

3. Se verificará la información que se almacene, íntegramente, tanto el original como las copias (en caso de encontrarse empaquetada, desempaquetarla como comprobación). Asimismo, debe verificarse que la información no esté contaminada con virus informático.

4. En el modo de trabajo monousuario, los usuarios son los responsables de hacer el respaldo de la información.

5. En el modo de trabajo multiusuario el responsable de hacer el respaldo de la información es el administrador de la red, previa orden de trabajo por parte del usuario.

Medidas de seguridad

1. Se grabará el trabajo que se está realizando cada cierto tiempo (10 - 20 minutos aproximadamente).
2. Los medios magnéticos deben estar alejados de los campos magnéticos y no se les debe acercar ningún cuerpo con propiedades magnéticas (como los imanes, teléfonos), ya que podrían provocar la pérdida irrecuperable de los datos ya almacenados.
3. No se debe mover la CPU conteniendo al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco.
4. Los ambientes donde se depositan los medios magnéticos deben cumplir con las condiciones adecuadas de temperatura y no presentar humedad.

5. Los medios magnéticos en los cuales se almacenará los respaldos de la información serán completamente nuevos (primer uso), verificándose su buen estado operacional.
6. Sólo el personal responsable de la seguridad de los archivos tendrá acceso al ambiente donde se encuentren estos medios magnéticos.
7. Antes de descolgar el servidor de la red el supervisor debe enviar con 15 minutos de anticipación un mensaje a los usuarios para que salven su información.

Recomendaciones para realizar un backup

Para cumplir los requerimientos esenciales que se necesitan para efectuar el proceso de backup, se debe tener en cuenta los siguientes aspectos:

Consideraciones técnicas

Las principales consideraciones técnicas que pueden mencionarse son las siguientes:

1. Capacidad de Procesamiento: El criterio de capacidad de procesamiento se basa fundamentalmente en la capacidad de almacenamiento en memoria externa disponible por el usuario de la computadora, con el fin de poder efectuar procesos de respaldo de información (backup), de acuerdo a los equipos existentes.
   Esta clasificación incluye las siguientes categorías:

   - Microcomputadoras - Computadoras personales.
   - Computadora de mediana capacidad (Minicomputadoras).
   - Computadora de alta capacidad (Mainframes).
   - Ambiente de Red

   De acuerdo a esta clasificación, se debe considerar qué tipo de backup es recomendable usar para satisfacer las necesidades existentes.

2. Posibilidades respecto al uso de utilitarios interactivos de respaldo de información: En este aspecto, en el mercado se disponen de un conjunto de utilitarios de propósito general que permiten efectuar procesos de respaldo de información.
   Para ello se debe disponer de criterios o metodologías apropiadas que permitan el uso de estos utilitarios de acuerdo a:

   - Volumen de información que es posible procesar.
   - Frecuencia de proceso de la información .
   - Importancia de la información (Información sensitiva) con la finalidad de disponer de un utilitario único "estándar", que se adopte en cada Institución.

3. Potencia: Es la capacidad de memoria operativa y velocidad de procesamiento. Este criterio indica la cantidad de Kbytes de memoria operativa real o virtual, accesibles al usuario en la computadora y la velocidad de la misma, las cuales se pueden clasificar de acuerdo a las siguientes categorías:

   - Computadora de poca potencia.
   - Computadora de mediana potencia.
   - Computadora de alta potencia.

   Con los criterios mencionados, se debe seleccionar los utilitarios o el tipo de backup a usar en un proceso determinado.

Consideraciones de sistemas

Los sistemas que van a ser utilizados se clasifican por los siguientes criterios:

1. Volumen de información de entrada: Este criterio implica considerar sistemas que trabajen con información de entrada que permitan procesar:
   - Pequeño volumen de información.
   - Mediano volumen de información.
   - Gran volumen de información.

   De acuerdo al volumen se debe usar el tipo de backup más apropiado.

2. Volumen de información de salida: De manera similar al anterior, se debe considerar el tamaño de la información de salida para seleccionar el tipo de backup adecuado.

   Se puede clasificar en:

   - Sistemas de poca complejidad: Poseen un número reducido de archivos y de unidades de tratamiento o procesos independientes.
   - Sistemas de complejidad media: Tienen gran cantidad de archivos y procesos diferentes y requieren un tratamiento de sus datos por diferentes programas, para lograr un resultado.
   - Sistemas de gran complejidad: Tienen características especiales, como calcular gran cantidad de iteraciones u operaciones para los datos.

   De acuerdo a lo mencionado, se debe indicar el tipo de backup a usar.

3. Sistemas que trabajan bajo la modalidad en tiempo real: Este aspecto es muy importante para realizar un proceso de respaldo de información, puesto que no es lo mismo realizar backups de archivos que son permanentemente usados (accesados) por los usuarios, para ello es necesario tener en cuenta ciertos tipos o metodologías de respaldo de información apropiada.

4. Organización del ambiente: Los backups realizados en disco o en cinta, deben ser etiquetados y correctamente organizados para conocer en todo momento las últimas versiones y pueda localizarse fácilmente cuando se quiera restablecer los datos en el disco duro.

De respaldo de seguridad

1. La información almacenada debe ser verificada íntegramente, tanto el original como las copias (en caso de encontrarse empaquetada, desempaquetarla como verificación). Asimismo, debe verificarse que la información no esté contaminada con virus informático.

2. Los archivos que son textos, hojas de cálculo, gráficos, etc., mientras no se concluyan, serán guardados en una sola copia por cada actualización para facilitar

su almacenamiento. Una vez concluidos se debe guardar una copia adicional de respaldo, en forma empaquetada o no, dependiendo del tamaño del archivo.

3. Cuando se quiera almacenar un archivo de respaldo este deberá guardarse físicamente en otra unidad magnética (diskette, cinta o disco) diferente a la que contiene el archivo original.

Del almacenamiento físico

1. Los ambientes donde se depositan los medios magnéticos deben contar con adecuadas condiciones de temperatura y no presentar humedad.

2. Los medios magnéticos en los cuales se almacena la información histórica deben ser completamente nuevos (primer uso), verificándose su buen estado operacional.

3. Sólo el personal responsable de la seguridad de los archivos tendrá acceso al ambiente donde se encuentren estos medios de almacenamiento.

Recuperación ante siniestros.

Utilizando la herramienta seleccionada e instalada que es Tivoli Storage Manager, se procede a indicar cuál es el proceso para restaurar información de los diferentes servidores presentes en la compañía.