



GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-441)

CONFIGURACIÓN DE SEGURIDAD DE ENTORNOS VIRTUALES VMWARE ESX

ENERO 2010

Edita:



© Editor y Centro Criptológico Nacional, 2010
NIPO: 076-10-072-4

Tirada: 1000 ejemplares

Fecha de Edición: septiembre de 2010

Raúl Siles ha participado en la elaboración y modificación del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el **Centro Criptológico Nacional** puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del **Centro Criptológico Nacional**, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

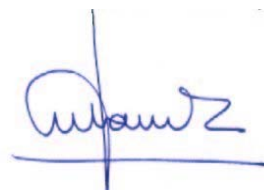
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Febrero de 2010



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN	6
2. OBJETO	7
3. ALCANCE	7
4. ENTORNOS DE COMPUTACIÓN VIRTUALES BASADOS EN VMWARE ESX	8
4.1. MECANISMOS DE GESTIÓN Y ADMINISTRACIÓN DE VMWARE ESX	8
4.2. DISEÑO DE LA ARQUITECTURA DEL ENTORNO VIRTUAL	9
4.2.1. COMUNICACIONES Y REDES DE DATOS EN VMWARE ESX	10
4.2.2. SEGMENTACIÓN FÍSICA DE LA RED Y FILTRADO DE TRÁFICO	11
4.2.3. SEGMENTACIÓN LÓGICA DE LA RED MEDIANTE VLANS	11
5. RECOMENDACIONES DE INSTALACIÓN DE VMWARE ESX	12
5.1. REQUISITOS	12
5.2. ACTUALIZACIÓN DE SOFTWARE DE VMWARE ESX	12
5.3. INSTALACIÓN DE VMWARE ESX	14
6. RECOMENDACIONES DE CONFIGURACIÓN DE VMWARE ESX	16
6.1. ACCESO AL ENTORNO VMWARE ESX	17
6.1.1. RESTRICCIONES DE ACCESO: BLOQUEO DE CUENTAS	17
6.1.2. RESTRICCIONES DE ACCESO CON EL USUARIO ROOT	18
6.1.3. RESTRICCIONES DE ACCESO CON USUARIOS REGULARES	21
6.1.4. CONFIGURACIÓN DE SSH	22
6.1.5. CONFIGURACIÓN DEL SERVIDOR WEB DE VMWARE ESX	23
6.1.6. GESTIÓN DE CONTRASEÑAS: COMPLEJIDAD Y CADUCIDAD	24
6.1.7. CONFIGURACIÓN DE SUDO	27
6.1.8. ACCESO SEGURO MEDIANTE SSL O TLS	28
6.2. CONFIGURACIÓN DE SEGURIDAD DE LAS COMUNICACIONES EN VMWARE ESX	31
6.2.1. CREACIÓN DE UNA RED DE GESTIÓN DEDICADA	31
6.2.2. MODO PROMISCO	31
6.2.3. PROTECCIÓN FRENTE A ATAQUES DE SUPLANTACIÓN DE MAC	34
6.2.4. CONFIGURACIÓN DEL FIREWALL EN EL SERVIDOR DE GESTIÓN	36
6.2.5. EXCEPCIONES A LA POLÍTICA DE FILTRADO POR DEFECTO	40
6.3. CONFIGURACIÓN DE SERVICIOS EN VMWARE ESX	41
6.3.1. ARRANQUE Y ACTIVACIÓN DE SERVICIOS	41
6.3.2. NTP (NETWORK TIME PROTOCOL)	43
6.4. PERMISOS DE FICHEROS EN VMWARE ESX	44
6.4.1. FICHEROS DE CONFIGURACIÓN	44
6.4.2. FICHEROS CON PERMISOS SETUID Y SETGID	46
6.5. LOGGING Y REGISTRO DE EVENTOS	46
6.6. CONFIGURACIÓN DEL ALMACENAMIENTO EN RED	48
6.6.1. iSCSI	48
7. RECOMENDACIONES DE CONFIGURACIÓN DE VIRTUALCENTER (VCENTER)	49
7.1. COMUNICACIONES DE RED DE VIRTUALCENTER	50
7.2. CONFIGURACIÓN DEL SERVIDOR WEB DE VIRTUALCENTER	50
7.3. ACCESOS DE GESTIÓN MEDIANTE VIRTUALCENTER	51
8. RECOMENDACIONES DE CONFIGURACIÓN DE LAS MÁQUINAS VIRTUALES (GUESTS) EN VMARE ESX	52
8.1. DESHABILITAR OPERACIONES SOBRE EL HARDWARE DE LAS MÁQUINAS VIRTUALES	52
8.2. DESHABILITAR LA OPCIÓN DE COPIAR Y PEGAR ENTRE MÁQUINAS VIRTUALES Y EL HOST	54
8.3. GESTIÓN Y ROTACIÓN DE LOS LOGS DE LAS MÁQUINAS VIRTUALES	56

8.4. EVITAR QUE LAS MÁQUINAS VIRTUALES DESBORDEN CON LOGS AL SERVIDOR VMWARE ESX.....	56
8.5. LIMITAR OPERACIONES DE MODIFICACIÓN DE LOS DISCOS VIRTUALES	57
8.6. SINCRONIZACIÓN DE TIEMPO ENTRE LAS MÁQUINAS VIRTUALES Y EL HOST	58
8.7. DESHABILITAR EL ARRANQUE MEDIANTE PXE	58
8.8. RESUMEN DE LOS PARÁMETROS DE CONFIGURACIÓN AVANZADOS DE LAS MÁQUINAS VIRTUALES.....	59
8.9. PERMISOS DE LOS FICHEROS DE LAS MÁQUINAS VIRTUALES	59
8.10. EVITAR EL USO DE DISCOS NO PERSISTENTES EN LAS MÁQUINAS VIRTUALES	60

ANEXOS

ANEXO A. LISTA DE LOS SERVICIOS MÍNIMOS RECOMENDADOS EN VMWARE ESX	62
ANEXO B. LISTADO DE PERMISOS DE LOS FICHEROS DE CONFIGURACIÓN DE VMWARE ESX (/ETC/VMWARE).....	63
ANEXO C. CHECKLIST	64
ANEXO D. REFERENCIAS	68

TABLAS

TABLA 1.- POLÍTICA DE FILTRADO POR DEFECTO DEL FIREWALL DEL SERVIDOR DE GESTIÓN.....	39
TABLA 2.- PERMISOS DE LOS PRINCIPALES FICHEROS DE CONFIGURACIÓN EN “/ETC”	45
TABLA 3.- PERMISOS DE LOS FICHEROS DE LAS MÁQUINAS VIRTUALES	60

FIGURAS

FIGURA 1.- CREACIÓN DE UN USUARIO EN EL CLIENTE VI CON ACCESO A SHELL.....	19
FIGURA 2.- CREACIÓN DE UN MENSAJE (O BANNER) EN EL ACCESO WEB	24
FIGURA 3.- ACCESO A LA CONFIGURACIÓN DE GESTIÓN DE VCENTER	29
FIGURA 4.- COMPROBACIÓN DE LOS CERTIFICADOS DIGITALES DE SSL EN VCENTER	30
FIGURA 5.- PROPIEDADES DE LOS SWITCHES DE RED VIRTUALES	32
FIGURA 6.- CONFIGURACIÓN DE LOS PARÁMETROS DE LOS SWITCHES DE RED VIRTUALES.....	33
FIGURA 7.- CONFIGURACIÓN DEL MODO PROMISCOU EN LOS SWITCHES DE RED VIRTUALES.....	34
FIGURA 8.- CONFIGURACIÓN DEL CAMBIO DE DIRECCIÓN MAC Y EL ENVÍO DE TRAMAS FALSAS EN LOS SWITCHES DE RED VIRTUALES	36
FIGURA 9.- POLÍTICA DE FILTRADO DEL FIREWALL DE VMWARE ESX EN EL CLIENTE VI.....	38
FIGURA 10.- CONFIGURACIÓN DE LA POLÍTICA DE FILTRADO DEL FIREWALL DE VMWARE ESX	38
FIGURA 11.- INFORMACIÓN DEL SERVICIO NTP DE VMWARE ESX.....	43
FIGURA 12.- CONFIGURACIÓN DEL SERVICIO NTP DE VMWARE ESX	44
FIGURA 13.- CONFIGURACIÓN DE AUTENTIFICACIÓN CHAP PARA ISCSI	49
FIGURA 14.- CONFIGURACIÓN DE UNA MÁQUINA VIRTUAL EN EL CLIENTE VI.....	53
FIGURA 15.- UBICACIÓN DEL FICHERO DE CONFIGURACIÓN DE UNA MÁQUINA VIRTUAL	53
FIGURA 16.- CONFIGURACIÓN DE LOS PARÁMETROS DE UNA MÁQUINA VIRTUAL DESDE EL CLIENTE VI	55
FIGURA 17.- CONFIGURACIÓN DE LOS DISCOS VIRTUALES EN MODO NO PERSISTENTE	

1. INTRODUCCIÓN

1. En los últimos años se ha producido un gran crecimiento en la utilización de entornos de computación virtuales (virtualización de sistemas) dentro de las arquitecturas de Tecnologías de la Información y las Comunicaciones (TIC).
2. Existen múltiples tecnologías, software y hardware, que ofrecen la capacidad de disponer de múltiples sistemas operativos virtuales ejecutándose sobre un mismo sistema físico o real.
3. En un entorno de computación virtual, los sistemas (y sistemas operativos asociados) que se ejecutan dentro de la infraestructura virtual se denominan sistemas (o máquinas) virtuales (o *guests*). El sistema que proporciona la plataforma hardware y software básico para la ejecución de la infraestructura virtual se denomina sistema físico o real (o *host*).
4. Las ventajas ofrecidas por las tecnologías de virtualización son:
 - Optimizar y reducir los costes de equipamiento hardware.
 - Gestionar de forma dinámica los recursos hardware.
 - Reducir el espacio físico asignado a los entornos de computación, en un proceso conocido como consolidación de servidores.
 - Simplificar y consolidar los mecanismos de gestión y mantenimiento de los sistemas.
 - Adicionalmente, implementan mecanismos que permiten fácilmente revertir el estado actual del sistema a un estado previo conocido.
5. El software de virtualización (también denominado comúnmente monitor de máquinas virtuales, *virtual machine monitor (VMM)*) permite crear un entorno virtual y ejecutar simultáneamente distintas máquinas virtuales.
6. Siendo evidentes las ventajas que ofrecen estas tecnologías, no debemos pasar por alto los riesgos añadidos a los ya existentes en cualquier sistema real y su sistema operativo asociado. Estos deben ser tratados de forma cuidadosa y específica con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de estas infraestructuras y los datos que se transmiten haciendo uso de ellas.
7. En el presente documento se ofrecen recomendaciones de diseño y configuración para disponer de un entorno virtual más seguro basado en la versión empresarial de VMware [Ref.- 1], denominada VMware ESX o VMware Infrastructure [Ref.- 2].

8. El presente documento constituye una guía práctica para la configuración segura de entornos virtuales basados en VMware ESX, y complementa la guía CCN-STIC-956, denominada “Seguridad en Entornos de Computación Virtuales (Virtualización de Sistemas)” [Ref.- 3]. Esta guía general describe los riesgos, amenazas y ataques a los que se ven expuestos los entornos de computación virtuales en la actualidad.
9. Las recomendaciones de configuración segura deben complementarse con el diseño de una arquitectura de seguridad adecuada en el entorno dónde se ubiquen los entornos de virtualización, así como una correcta implementación, gestión, monitorización y auditoría de la infraestructura de virtualización. Todos esos elementos conjuntamente permitirán disponer de un entorno virtual más seguro.
10. Adicionalmente a las recomendaciones de configuración segura de la plataforma de virtualización, se recomienda consultar y aplicar otras guías y documentación con recomendaciones de seguridad para la instalación y configuración de los sistemas operativos y aplicaciones que se ejecutan en las máquinas virtuales [Ref.- 4].
11. Existen herramientas comerciales, como VMinformer [Ref.- 21], para analizar y auditar el nivel de seguridad de un entorno de virtualización basado en VMware ESX.
12. El entorno de virtualización VMware ESX dispone de múltiples componentes y aplicaciones complementarias para su gestión, realización de copias de seguridad, capacidades de distribución de recursos y tareas, desarrollos software personalizados, etc. La guía se centra en proporcionar recomendaciones de seguridad para la infraestructura principal de VMware ESX y no cubre todos los componentes adicionales.
13. Otros entornos virtuales software diferentes a VMware ESX quedan fuera del alcance de esta guía, sin embargo, es recomendable evaluar sobre ellos la validez de las recomendaciones de seguridad presentadas, ya que la mayoría de ellas serán aplicables.
14. Las recomendaciones quedan sometidas a una continua revisión debido al constante avance tecnológico, así como a la aprobación de nuevos estándares y la aparición de nuevas vulnerabilidades y herramientas.

2. OBJETO

15. Proporcionar recomendaciones de seguridad para el diseño y configuración de un entorno de computación virtual basado en VMware ESX.

3. ALCANCE

16. Las Autoridades responsables de la aplicación de la Política de Seguridad de las TIC (STIC) determinarán su análisis y aplicación a los Sistemas bajo su responsabilidad.

17. El objetivo de las recomendaciones de la presente guía es mejorar la seguridad de los entornos de virtualización, pero puede ser necesario evaluar detalladamente y adaptar las mismas a las particularidades y requisitos del entorno sobre las que serán aplicadas.
18. La guía proporciona recomendaciones y mejores prácticas para aumentar la seguridad de un entorno VMware ESX, pero debido a la complejidad, dependencias con la arquitectura de sistemas y redes existentes, y la flexibilidad en el diseño e implantación de este tipo de entornos, es necesario evaluar en detalle la aplicación de cada una de las recomendaciones a un entorno concreto.
19. Es conveniente tener en cuenta que la guía ha sido diseñada para ser aplicada sobre nuevos entornos virtuales. Su aplicación sobre un entorno virtual ya existente en producción debe ser evaluada minuciosamente, ya que algunas de las restricciones recomendadas pueden afectar a funcionalidad que está siendo utilizada actualmente y a los requisitos específicos del entorno sobre el que desea aplicar la guía.

4. ENTORNOS DE COMPUTACIÓN VIRTUALES BASADOS EN VMWARE ESX

20. VMware ESX proporciona una plataforma de virtualización software que permite la gestión de los recursos hardware del sistema sobre el que se instala. Dentro del entorno VMware ESX es posible llevar a cabo la instalación de múltiples máquinas virtuales, cada una de ellas con su sistema operativo asociado.
21. Las recomendaciones de seguridad detalladas a lo largo de la presente guía aplican a VMware ESX versión 3.5 Update 3 (U3, build 123630).
22. VMware ESX 3.X es referenciado también habitualmente como VMware ESX Server o VMware Infrastructure 3, aunque a lo largo de toda la guía se emplea el término VMware ESX.

4.1. MECANISMOS DE GESTIÓN Y ADMINISTRACIÓN DE VMWARE ESX

23. VMware ESX proporciona diferentes mecanismos para la gestión del entorno virtual:
 - Consola del servidor de gestión de VMware ESX (ESX Server/Service Console o CLI, Command Line Interface), accesible en la consola física del equipo mediante Alt+F1. Permite el acceso como usuario “root” por defecto.
 - Acceso remoto de terminal mediante SSH (Secure Shell). No permite el acceso como usuario “root” por defecto.

- Acceso de administración web, denominado “VMware Virtual Infrastructure (VI) Web Access”, y disponible desde el enlace web <https://192.168.1.23/ui/>, considerando la dirección IP 192.168.1.23 como la IP asociada al servidor de gestión. Permite el acceso como usuario “root” por defecto.
 - VMware Infrastructure Client (también conocido como VI Client): cliente Windows para la gestión remota de VMware ESX. El cliente está disponible para su descarga desde la página principal del interfaz de administración web de VMware ESX. Permite el acceso como usuario “root” por defecto.
 - VMware VirtualCenter (vCenter) Server: software de gestión empresarial de VMware ESX que permite la administración remota y gestión de recursos de múltiples servidores VMware ESX. Este software está disponible en la web de VMware. Emplea por defecto las credenciales de Windows para permitir el acceso a la gestión y administración de ESX.
 - VMware proporciona un cliente remoto denominado Remote Client (RCLI).
24. Las recomendaciones de seguridad de la presente guía indican cuál de estas opciones es el mecanismo de gestión sugerido para la aplicación de cada cambio y modificación en la configuración de VMware ESX. Por abreviar, la denominación de cada uno de los diferentes mecanismos de gestión es, respectivamente: CLI, SSH, web, cliente VI, vCenter y RCLI.
25. Como principio general de diseño, se recomienda emplear el cliente VI o VirtualCenter como mecanismo principal y/o único de administración y gestión del entorno VMware ESX, frente a por ejemplo, el acceso mediante consola o SSH. Ambos accesos permiten la realización de las tareas necesarias en el entorno, y minimizan la ejecución arbitraria de comandos de sistema operativo permitidos en la consola o por SSH. Adicionalmente, VirtualCenter permite realizar la autenticación de usuarios empleando las bases de datos de credenciales existentes, como por ejemplo el directorio activo de Windows, gestionar roles y usuarios, y mantiene un registro de todas las acciones realizadas.

4.2. DISEÑO DE LA ARQUITECTURA DEL ENTORNO VIRTUAL

26. Como paso previo a la instalación y configuración de VMware ESX se recomienda planificar y diseñar la arquitectura de sistemas y redes del entorno de virtualización [Ref.- 10].
27. Existen múltiples factores de seguridad a considerar en el diseño de una arquitectura de sistemas y redes, pero los elementos críticos desde el punto de vista del entorno de virtualización son:

- Diseñar la arquitectura de red del entorno de virtualización, aplicando una adecuada segmentación de la red tanto a nivel físico como lógico, incluyendo dispositivos encargados del filtrado de tráfico entre redes y sistemas, tales como cortafuegos (o *firewalls*).
- Deberían crearse diferentes segmentos de red (físicos o lógicos, mediante VLANs) para propósitos diferenciados, como la red de servicio, de gestión, de backup, de almacenamiento IP, de VMotion (migración dinámica de máquinas virtuales), etc.
- Diseñar la arquitectura de almacenamiento del entorno de virtualización, aplicando una adecuada segmentación entre sistemas y los dispositivos de almacenamiento (físicos y lógicos).

4.2.1. COMUNICACIONES Y REDES DE DATOS EN VMWARE ESX

28. VMware ESX proporciona múltiples elementos para el diseño y creación de infraestructuras de comunicaciones avanzadas, basadas en la definición de múltiples redes de datos.
29. Existen diferentes tipos de redes de datos que pueden definirse y conectarse al sistema VMware ESX:
 - Red de gestión mediante consola remota. Por ejemplo, consola remota basada en HP iLO (Integrated Lights-Out), Dell Remote Access Card (DRAC), IBM management module (MM), o Remote Supervisor Adapter II (RSA II).
 - Red de gestión estándar, que permite el acceso al servidor de gestión o consola de servicio y administración a través de diferentes mecanismos, como la consola por SSH, el acceso web, el cliente VI, vCenter y RCLI.
 - Red para la migración de máquinas virtuales con VMotion.
 - Red de producción o servicio donde se ubican las máquinas virtuales.
 - Red o redes de almacenamiento, definidas según la tecnología de almacenamiento empleada, como por ejemplo fiber-channel (FC) SAN, iSCSI o NFS.
30. Se recomienda segmentar e independizar todas y cada una de estas redes entre sí, ya sea físicamente o lógicamente mediante VLANs. VMware proporciona información detallada sobre la seguridad del entorno VMware ESX mediante el uso de VLANs [Ref.- 11] (capítulo 10).

31. Aplicando los principios de segmentación de la lista previa, es posible y recomendable segmentar cada red en otras subredes, como por ejemplo segmentar la red de producción en una red para la realización de copias de seguridad, una red DMZ para las máquinas virtuales que deban estar expuestas a Internet, una red interna para las máquinas virtuales internas, etc.

4.2.2. SEGMENTACIÓN FÍSICA DE LA RED Y FILTRADO DE TRÁFICO

32. Se recomienda disponer de tarjetas de red físicas independientes para cada una de las redes necesarias en el entorno de virtualización. A través de la utilización de vSwitches (o switches de red virtuales) es posible asociar los interfaces de red virtuales, tanto del servidor ESX como de las máquinas virtuales, a los vSwitches y los interfaces de red físicos de forma independiente [Ref.- 18].
33. Se recomienda desplegar dispositivos de filtrado de tráfico para proteger tanto los interfaces de gestión del entorno VMware ESX, como el tráfico de servicio hacia el servidor VMware ESX y entre las máquinas virtuales. La guía de configuración de VMware ESX [Ref.- 11] (capítulo 10) proporciona información detallada del tráfico de red (incluyendo puertos TCP y UDP) empleado por los diferentes componentes del entorno VMware ESX, necesaria para el diseño de las políticas de filtrado.
34. Las políticas de filtrado deberían permitir únicamente el tráfico mínimo necesario para las comunicaciones necesarias según la funcionalidades empleadas en el entorno específico de VMware ESX.

4.2.3. SEGMENTACIÓN LÓGICA DE LA RED MEDIANTE VLANS

35. VMware ESX proporciona capacidades de configuración de VLANs mediante el estándar 802.1q en los interfaces de red de las máquinas virtuales o los vSwitches.
36. Se recomienda crear una red física separada, o al menos independizar mediante VLANs, la red de gestión (asociada a la consola de servicio o servidor de gestión de VMware ESX) y las redes de servicio de las máquinas virtuales.
37. La guía de configuración de VMware ESX [Ref.- 11] (capítulo 10) proporciona información general sobre las mejores prácticas para la configuración de VLANs desde el punto de vista de seguridad. La configuración final específica de VLANs es dependiente de la arquitectura de red del entorno.
38. La segmentación a nivel 2 de la red, por ejemplo mediante VLANs, mitiga los ataques de nivel 2, como *ARP poisoning*.
39. Adicionalmente, VMware proporciona información sobre los detalles de implementación de los vSwitches en VMware ESX y los tipos de ataques de nivel 2 frente a los que no son vulnerables.

5. RECOMENDACIONES DE INSTALACIÓN DE VMWARE ESX

5.1. REQUISITOS

40. Para llevar a cabo la instalación de VMware ESX es necesario disponer de una plataforma hardware soportada por VMware, tal y como detalla la HCL, Hardware Compatibility List [Ref.- 5].
41. Los elementos hardware más críticos y fundamentales desde el punto de vista de una adecuada compatibilidad para el correcto funcionamiento de VMware ESX son el disco duro (incluyendo su interfaz, SCSI) y la tarjeta de red.
42. La presente guía ofrece recomendaciones de seguridad para el entorno VMware ESX, y complementa las guías estándar oficiales de inicio, instalación y configuración de VMware ESX 3.5 [Ref.- 6].
43. Cuando el entorno VMware ESX arranca, se inicia una máquina referida como el servidor de gestión (o consola de servicio) de VMware ESX, que está basada en el sistema operativo RHEL 3, RedHat Enterprise Linux 3.
44. Con el objetivo de proporcionar una plataforma de virtualización segura, se recomienda aplicar las mejores prácticas de seguridad para entornos Linux, y en concreto RedHat, al servidor de gestión de VMware ESX, ya que éste está basado en una versión restringida de RedHat Enterprise Linux.
45. La guía CCN-STIC-614, denominada “Seguridad RedHat Linux (FEDORA)” proporciona recomendaciones de seguridad para la configuración de RedHat Linux [Ref.- 7].

5.2. ACTUALIZACIÓN DE SOFTWARE DE VMWARE ESX

46. Al igual que sucede con cualquier otro software, desde el punto de vista de seguridad es necesario definir y aplicar un procedimiento de actualización de software formal, que permita disponer de la última versión de VMware ESX que soluciona vulnerabilidades de seguridad conocidas. Se recomienda probar y evaluar las actualizaciones en un entorno de desarrollo o pruebas, previo a su aplicación en el entorno de producción.
47. VMware publica actualizaciones y las divide en tres categorías: Security, Critical y General. Es necesario mantenerse al día en las actualizaciones de tipo Security, ya que resuelven vulnerabilidades de seguridad públicamente conocidas y que podrían ser empleadas por un potencial intruso para atacar el entorno virtual.

48. Los parches y actualizaciones de software de VMware ESX, clasificados en tres categorías (General, Security y Critical), están disponibles en la web de descarga de parches de VMware [Ref.- 13] siguiendo las mejores prácticas recomendadas para la gestión de software en VMware ESX [Ref.- 14].
49. El portal de seguridad de VMware [Ref.- 12] contiene información sobre alertas de seguridad actualizadas de productos VMware y descarga de actualizaciones de seguridad. Se recomienda disponer de la última información publicada en dicho portal.
50. Pese a que el servidor de gestión está basado en una versión modificada de RHEL 3 (RedHat Enterprise Linux), no deben aplicarse directamente actualizaciones de RedHat, sino únicamente las proporcionadas por VMware para el producto ESX.
51. Debe tenerse en cuenta que algunas actualizaciones requieren un reinicio completo del entorno virtual, por lo que es necesaria su planificación de cara a minimizar el impacto en el servicio.
52. El software denominado VMware vCenter Update Manager puede emplearse para la gestión de actualizaciones de VMware ESX a nivel empresarial.
53. Desde la consola de VMware ESX (CLI) es posible obtener los detalles de las últimas actualizaciones instaladas en el sistema mediante el siguiente comando:

```
# esxupdate query
```

Por ejemplo, para VMware ESX 3.5 U3:

```
# esxupdate query
Installed software bundles:
----- Name ----- Install Date --- Summary ---
3.5.0-64607 01:12:04 01/04/80 Full bundle of ESX 3.5.0-64607
ESX350-200802303-SG 01:12:05 01/04/80 util-linux security update
ESX350-200802305-SG 01:12:05 01/04/80 openssl security update
ESX350-200802408-SG 01:12:05 01/04/80 Security Updates to the Python Package.
ESX350-200803209-UG 01:12:06 01/04/80 Update to the ESX Server Service Console
ESX350-200803212-UG 01:12:06 01/04/80 Update VMware qla4010/qla4022 drivers
ESX350-200803213-UG 01:12:06 01/04/80 Driver Versioning Method Changes
ESX350-200803214-UG 01:12:07 01/04/80 Update to Third Party Code Libraries
ESX350-200804405-BG 01:12:07 01/04/80 Update to VMware-esx-drivers-scsi-
megara
ESX350-200805504-SG 01:12:07 01/04/80 Security Update to Cyrus SASL
ESX350-200805505-SG 01:12:08 01/04/80 Security Update to unzip
ESX350-200805506-SG 01:12:08 01/04/80 Security Update to Tcl/Tk
ESX350-200805507-SG 01:12:08 01/04/80 Security Update to krb5
ESX350-200805514-BG 01:12:09 01/04/80 Update to VMware-esx-drivers-net-e1000
ESX350-200808203-UG 01:12:09 01/04/80 Update to Backup Tools
ESX350-200808206-UG 01:12:09 01/04/80 Update to vmware-hwdata
ESX350-200808210-UG 01:12:10 01/04/80 Update to VMware-esx-drivers-net-ixgbe
```

ESX350-200808211-UG	01:12:10 01/04/80	Update to the tg3 Driver
ESX350-200808212-UG	01:12:10 01/04/80	Update to the MegaRAID SAS Driver
ESX350-200808215-UG	01:12:10 01/04/80	Update to the Emulex SCSI Driver
ESX350-200808218-UG	01:12:11 01/04/80	Security Update to Samba
ESX350-200808405-SG	01:12:11 01/04/80	Security Update to Net-SNMP
ESX350-200808406-SG	01:12:11 01/04/80	Security Update to Perl
ESX350-200808407-BG	01:12:12 01/04/80	Updates Software QLogic FC Driver
ESX350-200808409-SG	01:12:12 01/04/80	Security Update to BIND
ESX350-200808412-BG	01:12:12 01/04/80	Updates Inxcfg
ESX350-200810201-UG	01:12:13 01/04/80	Updates VMkernel, Service Console, hostd
ESX350-200810202-UG	01:12:13 01/04/80	Updates ESX Scripts
ESX350-200810203-UG	01:12:13 01/04/80	Updates MPT SCSI Driver
ESX350-200810204-UG	01:12:14 01/04/80	Updates bnx2x Driver for Broadcom
ESX350-200810205-UG	01:12:14 01/04/80	Updates CIM and Pegasus
ESX350-200810206-UG	01:12:14 01/04/80	Updates ATA PIIX SCSI Driver
ESX350-200810207-UG	01:12:15 01/04/80	Updates SCSI Driver for QLogic FC HBAs
ESX350-200810208-UG	01:12:15 01/04/80	Updates esxupdate documentation
ESX350-200810209-UG	01:12:15 01/04/80	Updates bnx2 Driver for Broadcom
ESX350-200810210-UG	01:12:16 01/04/80	Updates HP Storage Component Drivers
ESX350-200810212-UG	01:12:16 01/04/80	Updates VMkernel iSCSI Driver
ESX350-200810214-UG	01:12:16 01/04/80	Updated Time Zone Rules
ESX350-200810215-UG	01:12:17 01/04/80	Updates Web Access
ESX350-Update03	01:12:17 01/04/80	ESX Server 3.5.0 Update 3

For a differential list of rpms, use the -l/--listrpms option.

#

5.3. INSTALACIÓN DE VMWARE ESX

54. Las siguientes recomendaciones complementan el proceso de instalación estándar de VMware ESX [Ref.- 6] desde el punto de vista de seguridad.
55. **BIOS:** es recomendable establecer una contraseña para la BIOS del sistema, con el objetivo de mitigar ataques basados en el acceso físico al equipo, que podrían manipular la secuencia de arranque del sistema y otros parámetros de configuración de la BIOS.
56. Adicionalmente, conviene establecer en la BIOS la secuencia de arranque del sistema y la lista de dispositivos de arranque permitidos. Si no se restringe dicha secuencia, sería posible la realización de ataques mediante acceso físico basados en forzar el arranque del sistema desde un medio no autorizado (dispositivo externo removible, como CD-ROM, DVD, disco USB, etc) y un sistema operativo distinto, que permitirían el acceso a la información almacenada en el disco del servidor de virtualización.
57. **Particiones de disco:** durante el proceso de instalación se debe seleccionar un esquema de particionado del disco adecuado al propósito del sistema y a la capacidad de almacenamiento disponible.

58. Se crearán particiones independientes para los sistemas de ficheros correspondientes a /, /boot, /var, /tmp y /home, con el objetivo de evitar que éstos se llenen y se produzca una condición de denegación de servicio. El esquema de particionado recomendado por defecto no crea particiones independientes para /tmp y /home. Todas las particiones deberían tener un tamaño mínimo de 5GB, excepto /boot, que puede tener un tamaño de 300 MB.
59. **Red por defecto:** durante el proceso de instalación no debe seleccionarse la opción que permite crear una red por defecto para las máquinas virtuales (opción seleccionada por defecto), “Create a default network for virtual machines”.
60. La creación de una red por defecto para las máquinas virtuales puede permitir el acceso por red a la consola de servicio (o administración), ya que ésta reside en esa red disponible por defecto. La consola de servicio debe residir siempre en una red separada y privada.
61. Se procederá a segmentar la red adecuadamente, y crear los switches y puertos de red necesarios para el entorno virtual a través de los interfaces de gestión de VMware ESX.
62. **Grub:** se establecerá una contraseña para grub, el gestor de arranque estándar de RedHat Enterprise Linux, y por tanto del servidor VMware ESX.
63. El fichero de configuración de grub, “/boot/grub/grub.conf”, permite establecer una contraseña para el acceso al gestor de arranque.
64. La contraseña se especifica mediante la siguiente directiva, que debe situarse tras la línea que contiene el “timeout=” en la sección principal del fichero:

```
password --md5 <valor_MD5_de_la_clave>
```

65. El valor MD5 de la clave se obtiene mediante la ejecución del siguiente comando:

```
# grub-md5-crypt  
Password:  
Retype password:
```

Tras introducir la contraseña dos veces se generará el hash MD5 de la misma, por ejemplo, \$1\$hAHEw\$QnUNBzFKDhz2p6/yuixU10. Este valor es el que se debe copiar en el fichero “grub.conf”.

66. Tras establecer la contraseña de grub, y arrancar el sistema, el acceso a cualquier modificación del gestor de arranque (grub) solicitará el uso de la contraseña mediante la tecla “p”.
67. **Modo mono usuario (single user):** se recomienda establecer un mecanismo de autenticación para el arranque en modo mono usuario (single user), donde se solicite la contraseña se root, complementando las medidas de seguridad establecidas para grub previamente.

68. Es posible arrancar en modo mono usuario desde grub, tras introducir la clave de grub con la opción “p”, editando la entrada de arranque (opción “e”), editando la línea que comienza por “kernel” (opción “e”), y añadiendo “ single” (con un espacio en blanco delante) al final de la línea. La opción “b” permite realizar el arranque con la entrada seleccionada.
69. Añadir la siguiente línea en el fichero “/etc/inittab” para activar la autenticación en este modo:

```
~~:S:wait:/sbin/sulogin
```

70. **Dispositivos USB:** se recomienda deshabilitar que cualquier dispositivo USB pueda ser conectado al servidor VMware ESX, para evitar la ejecución de código malicioso desde el mismo.
71. Para deshabilitar los dispositivos USB (disponibles por defecto) es necesario editar el fichero “/etc/modules.conf” y comentar las líneas que contengan el término USB, añadiendo el símbolo “#” al comienzo de las mismas:

```
# alias usb-controller uhci  
  
# alias usb-controller1 ehci-hcd
```

72. Tras realizar los cambios, es necesario reiniciar el sistema VMware ESX para que se aplique la nueva configuración.

6. RECOMENDACIONES DE CONFIGURACIÓN DE VMWARE ESX

73. Se recomienda como requisito previo a la configuración segura de un entorno VMware ESX disponer de una copia de seguridad completa del sistema, y asegurarse de que previamente el sistema no presenta problemas de configuración o inestabilidad.
74. Adicionalmente, se debe realizar una copia de seguridad de cada fichero de configuración antes de realizar ninguna modificación sobre el mismo. La copia de seguridad puede llamarse como el fichero original, y finalizar en “.backup”.
75. Las recomendaciones de la presente guía indican los cambios necesarios a realizar respecto a los ficheros de configuración existentes por defecto en VMware ESX, por lo que se recomienda disponer siempre de una copia de seguridad de los ficheros por defecto a modo de referencia.

76. Como sugerencia general, se recomienda documentar todos los cambios y configuraciones particulares llevadas a cabo en el entorno de VMware ESX, tanto durante el proceso de instalación como de configuración posterior.
77. Con respecto a la documentación, es importante documentar el cambio, quién lo ha realizado, el motivo o propósito del mismo, detallando tanto el valor previo como el nuevo valor del parámetro modificado. Esto es especialmente importante para los elementos más complejos del entorno, como la configuración de red, de almacenamiento o la política de seguridad del firewall del servidor de gestión.

6.1. ACCESO AL ENTORNO VMWARE ESX

78. VMware ESX proporciona diferentes métodos de administración del entorno virtual, tal y como se detalla en el apartado “MECANISMOS DE GESTIÓN Y ADMINISTRACIÓN DE VMWARE ESX”.
79. Se recomienda hacer uso de mecanismos de administración que permitan disponer de información y auditar los accesos al sistema, como por ejemplo el interfaz web, el cliente VI y vCenter.

6.1.1. RESTRICCIONES DE ACCESO: BLOQUEO DE CUENTAS

80. Con el objetivo de gestionar, restringir y monitorizar el acceso al servidor de VMware ESX se recomienda llevar a cabo las siguientes medidas o configuraciones especiales.
81. Se recomienda fijar el número máximo de intentos de acceso no válidos antes de bloquear una cuenta de usuario [Ref.- 15]. Esta configuración puede aplicarse a todas las cuentas excepto al usuario root para evitar ataques de denegación de servicio sobre su acceso al sistema.
82. Para habilitar y establecer el número de intentos fallidos antes del bloqueo de cuentas debe modificarse el fichero “/etc/pam.d/system-auth”, y en concreto:

Añadir una nueva línea de configuración que emplea “pam_tally.so” (para bloquear las cuentas tras cinco accesos de login o su fallidos), tras la siguiente línea:

```
account    required    /lib/security/$ISA/pam_unix.so
```

```
account      required          /lib/security/$ISA/pam_tally.so per_user deny=5  
no_magic_root reset
```

Añadir una nueva línea de configuración que emplea “pam_tally.so” (para contabilizar acceso fallidos de login y su), tras la siguiente línea:

```
auth      required    /lib/security/$ISA/pam_env.so
```

```
auth      required    /lib/security/$ISA/pam_tally.so onerr=fail no_magic_root
```

83. Una vez se ha activado el uso de “pam_tally.so”, y tras reiniciar el sistema, se dispondrá del fichero “/var/log/faillog”, dónde se registran los accesos fallidos y permite la gestión de cuentas tal y como se describe a continuación.
84. El uso de “per_user” en la configuración permite evitar el bloqueo para cuentas críticas, dónde se haya fijado explícitamente que no se desea habilitar el bloqueo. Por ejemplo, para evitar que se aplique a la cuenta del usuario root, ejecutar:

```
# faillog -u root -m -l
```

85. Es posible visualizar el número de intentos de acceso fallidos y desbloquear una cuenta con los siguientes comandos, respectivamente:

```
# faillog  
  
# faillog -u root -r
```

86. Es importante enfatizar que el bloqueo de cuentas permanente puede dar lugar a situaciones de denegación de servicio, por lo que se recomienda evaluar su uso en cada entorno, y no aplicarlo a cuentas críticas del sistema, como root.

6.1.2. RESTRICCIONES DE ACCESO CON EL USUARIO ROOT

87. Se limitarán los interfaces de administración desde los que es posible acceder directamente como el usuario root al sistema.
88. Se deshabilitará la posibilidad de acceso directo como el usuario root a través de SSH (este acceso no está habilitado por defecto en la versión VMware ESX 3.5 U3, por lo que no es necesario efectuar este cambio). Para ello es necesario verificar que el fichero “/etc/ssh/sshd_config” dispone de la siguiente línea:

```
PermitRootLogin no
```

89. Para poder acceder al sistema mediante SSH es necesario disponer de un usuario no privilegiado. Este usuario debe ser creado mediante el comando “useradd” desde el CLI o mediante el cliente VI (pestaña “Users & Groups” de “Inventory”, especificando la opción “Grant Shell Access to this user”); ver siguiente figura.
90. Es necesario asegurarse que la contraseña fijada para este usuario, así como para cualquier otro usuario creado con permiso de acceso a la línea de comandos (*shell*), es suficientemente robusta y compleja.

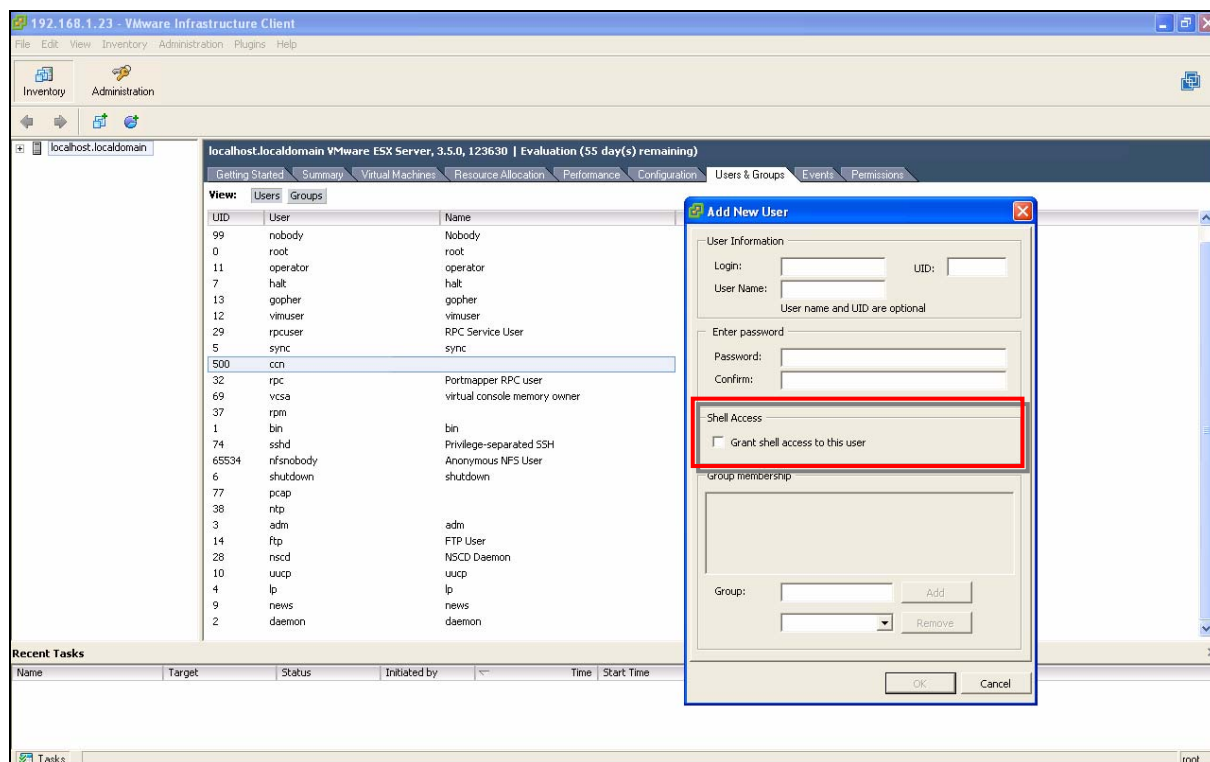


Figura 1.- Creación de un usuario en el cliente VI con acceso a shell

91. En el caso de habilitar el uso de “sudo”, se deshabilitará la posibilidad de acceso directo como el usuario root mediante el comando “su” en el CLI (habilitado por defecto) [Ref.- 16].
92. Se restringirá qué usuarios podrán hacer uso del comando “su”. Por ejemplo, para permitir únicamente a los usuarios pertenecientes al grupo “wheel” el uso de “su”, debe eliminarse el comentario (símbolo “#”) al comienzo de la siguiente línea en el fichero “/etc/pam.d/su”, quedando como sigue:

```
# Uncomment the following line to require a user to be in the "wheel" group.
auth    required    /lib/security/$ISA/pam_wheel.so use_uid
```

93. Se debe añadir al grupo “wheel” a todos y cada uno de los usuarios que se desee que puedan hacer uso de las capacidades de “su” mediante el siguiente comando:

```
# usermod -G wheel ccn
```

El comando previo añade el usuario “ccn” al grupo “wheel” (en el fichero “/etc/group”).

94. Adicionalmente, es necesario verificar qué usuarios pertenecen al grupo “wheel”, mediante los siguientes comandos (se muestra la configuración por defecto, más el cambio asociado al comando previo):

```
# cat /etc/group | grep wheel

wheel:x:10:root,ccn

# cat /etc/passwd | grep wheel

#
```

95. En lugar de hacer uso del comando “su” para la ejecución de tareas que requieren privilegios de administración, se recomienda emplear el comando “sudo” (ver el apartado “CONFIGURACIÓN DE SUDO”), ya que éste sólo proporciona privilegios de “root” para ciertas tareas y además con “sudo” se generan logs de todas las acciones realizadas.
96. Es posible comprobar los accesos directos (desde consola) que se han realizado como root en el sistema a través del CLI mediante el siguiente comando. La primera entrada corresponde a un intento exitoso, y la segunda a uno fallido:

```
# less /var/log/messages

...

Feb 24 15:22:12 localhost login(pam_unix)[1506]: session opened for user root by
LOGIN(uid=0)
Feb 24 15:22:12 localhost -- root[1506]: ROOT LOGIN ON tty1

Feb 24 15:31:57 localhost login(pam_unix)[2329]: authentication failure;
logname=LOGIN uid=0 euid=0 tty=tty1 ruser= rhost= user=root
Feb 24 15:31:59 localhost login[2329]: FAILED LOGIN 1 FROM (null) FOR root,
Authentication failure
```

97. Es posible comprobar los accesos mediante “su” que se han realizado como root en el sistema mediante el siguiente comando, ya que se registran en el fichero general de logs. La primera entrada corresponde a un intento exitoso, y la segunda a uno fallido:

```
# less /var/log/messages

...

Feb 24 15:28:10 localhost su(pam_unix)[2268]: session opened for user root by
ccn(uid=500)

Feb 24 15:30:45 localhost su(pam_unix)[2310]: authentication failure; logname=ccn
uid=500 euid=0 tty= ruser=ccn rhost= user=root
```

98. Es posible comprobar los accesos directos que se han realizado como root en el sistema a través de SSH (en el caso de permitirse el acceso tras cambiar la configuración por defecto, opción no recomendada) mediante el siguiente comando, ya que el servidor “sshd” registra tanto los accesos fallidos (segunda entrada) como exitosos (primera entrada) en el fichero general de logs:

```
# less /var/log/messages

...

Feb 24 15:24:25 localhost sshd[2207]: Accepted password for root from
192.168.1.250 port 1421 ssh2
Feb 24 15:24:25 localhost sshd(pam_unix)[2207]: session opened for user root by
(uid=0)

Feb 24 15:33:11 localhost sshd(pam_unix)[2331]: authentication failure; logname=
uid=0 euid=0 tty=NODEVssh ruser= rhost=192.168.1.250 user=root
Feb 24 15:33:13 localhost sshd[2331]: Failed none for root from 192.168.1.250 port
1440 ssh2
```

99. Como medida adicional de seguridad para entornos dónde la seguridad física sea un elemento relevante, se limitará el acceso directo del usuario root a través de la consola, forzando a que se realice la autenticación como otro usuario, para posteriormente acceder como root mediante el comando “su”.
100. Para ello es necesario ejecutar el siguiente comando:

```
# cat /dev/null > /etc/securetty
```

101. En el caso de habilitar esta restricción, es necesario tener en cuenta que no deben aplicarse las políticas de bloqueo de cuenta al usuario local no privilegiado con el que se pretende disponer de acceso a través de consola, con el objetivo de evitar una denegación de servicio en la que no sea posible acceder a través de la consola con ningún usuario.
102. La restricción aplica tanto a la consola local como a las consolas hardware remotas, tales como iLO, DRAC, MM o RSAII.

6.1.3. RESTRICCIONES DE ACCESO CON USUARIOS REGULARES

103. Mediante el cliente VI, y en concreto desde la pestaña “Users & Groups” de la sección “Inventory”, es posible realizar la gestión y creación de usuarios en VMware ESX.

104. Es obligatorio no habilitar la opción “Grant Shell Access to this user” (deshabilitada por defecto) para usuarios no privilegiados, con el objetivo de que puedan realizar sus tareas en VMware ESX a través del cliente VI, y no directamente mediante la consola o los mecanismos de acceso de terminal remoto, como SSH.
105. La única excepción a esta obligación es aquellos usuarios para los que se necesita de disponer de acceso mediante terminal, como por ejemplo el usuario mencionado previamente, necesario para acceder mediante SSH y posteriormente realizar tareas como “root”, ya que el acceso directo como “root” en SSH no está permitido por defecto (y no se recomienda habilitarlo).

6.1.4. CONFIGURACIÓN DE SSH

106. Se recomienda permitir únicamente la versión 2.0 de SSH para el acceso mediante este servicio al sistema, tanto en el cliente como en el servidor SSH, deshabilitando el acceso mediante SSH v1. Esta es la configuración por defecto en VMware ESX, tanto para el cliente como para el servidor SSH.
107. La configuración por defecto de SSH en VMware ESX es suficientemente restrictiva desde el punto de vista de seguridad, por lo que se recomienda no modificarla.
108. Se recomienda la creación de un mensaje (o *banner*) asociado al servicio SSH que refleje el carácter privado del sistema, que se monitoriza su uso y que no se permite un uso no autorizado, antes de cualquier intento de acceso. El mensaje puede ser almacenado en el fichero “/etc/issue.net”.
109. Para ello se debe modificar el fichero “/etc/ssh/sshd_config” y sustituir las siguientes líneas comentadas (#) por la mostrada a continuación:

<pre># no default banner path #Banner /some/path Banner /etc/issue.net</pre>

110. El fichero “/etc/issue.net” existe por defecto con el siguiente contenido:

<pre>VMware ESX Server 3 Kernel \r on an \m</pre>

111. El contenido de ese fichero, así como el de los ficheros “/etc/issue”, “/etc/issue.emergency” y “/etc/motd” (vacío por defecto), refleja que el sistema es un VMware ESX Server 3. Se modificarán todos los ficheros para no proporcionar ninguna información y en su lugar incluir el mensaje de restricción de acceso personalizado.

6.1.5. CONFIGURACIÓN DEL SERVIDOR WEB DE VMWARE ESX

112. Se recomienda la creación de un mensaje asociado al servicio web de VMware ESX que refleje el carácter privado del sistema, que se monitoriza su uso y que no se permite un uso no autorizado, antes de cualquier intento de acceso.

113. Para ello es necesario incluir el mensaje en el fichero que contiene la página web por defecto de administración de VMware ESX, es decir, “/usr/lib/vmware/hostd/docroot/index.html”, por ejemplo antes de la sección “Getting Started” de la columna de la izquierda de la página web principal.

114. Para introducir el mensaje se recomienda realizar las siguientes acciones:

- Todas las referencias a ficheros se encuentran dentro de “/usr/lib/vmware/hostd/docroot”.
- Modificar el fichero “en/welcomeRes.js” y crear el título del mensaje y el mensaje con las etiquetas “ID_Message” y “ID_Message_Text”.

```
var ID_GettingStarted = "Getting Started";  
  
var ID_Message = "Acceso Restringido";  
  
var ID_Message_Text = "Prohibido el uso no autorizado del sistema";
```

NOTA: modificar el texto del mensaje para cumplir los requisitos legales y de restricción de acceso de la organización.

- Modificar el fichero “index.html” e incluir las referencias a las etiquetas “ID_Message” y “ID_Message_Text”.

```
<div id="body">  
  
<div id="content">  
  
<h3><script  
type="text/javascript">document.write(ID_Message);</script></h3>  
  
<p><script  
type="text/javascript">document.write(ID_Message_Text);</script></p>  
  
<h3><script  
type="text/javascript">document.write(ID_GettingStarted);</script></h3>
```

115. El resultado del nuevo mensaje es similar al de la siguiente figura:



Figura 2.- Creación de un mensaje (o banner) en el acceso web

116.

117. Siguiendo un procedimiento similar al mostrado para la modificación de la página web, se recomienda cambiar la página web por completo para no proporcionar información de la existencia de un entorno VMware ESX.

118. Es posible comentar partes de la página mediante las directivas de comienzo (<!--) y fin (-->) de comentario en HTML, o incluso redirigir a la página de login directamente: "/ui/". El siguiente código HTML, situado en la cabecera de la página (entre las directivas <HEAD> y </HEAD>) ejecuta la redirección:

```
<meta HTTP-EQUIV="REFRESH" content="0; url=http://<direccion_IP>/ui/">
```

6.1.6. GESTIÓN DE CONTRASEÑAS: COMPLEJIDAD Y CADUCIDAD

119. Se recomienda aplicar una política de gestión de contraseñas segura para todos los usuarios definidos en VMware ESX. Para ello se recomienda el uso de frases de acceso (passphrases) en lugar de palabras de acceso (passwords), dónde se enfatiza el uso de contraseñas de mayor longitud.

120. VMware ESX permite la creación de contraseñas de un máximo de 255 caracteres (empleando hashes MD5 estándar de Linux).

121. Adicionalmente es posible añadir requisitos de complejidad a las contraseñas, siendo necesario emplear diferentes conjuntos de caracteres: letras minúsculas, letras mayúsculas, números o símbolos de puntuación.

122. La política definida debe seguir, al menos, los principios de generación de contraseñas existentes para el resto de sistemas de información de la organización.

123. La política de contraseñas actual puede ser verificada mediante el siguiente comando:

```
# esxcfg-auth -p
```

124. Por defecto VMware ESX utiliza la librería pam_cracklib.so para la verificación de la política de contraseñas. El principal inconveniente de esta librería es que no verifica ni establece la política de contraseñas para la cuenta del usuario “root”. Para aplicar la política a todas las cuentas de usuario, incluido “root”, se recomienda utilizar la librería pam_passwdqc.so. Para ello debe emplearse el comando mostrado posteriormente, “esxcfg-auth”, con la opción “--usepamqc”.

125. La política por defecto de la librería pam_cracklib.so establece una longitud de contraseña mínima de 9, es decir, 8 caracteres si son todos del mismo tipo. Las contraseñas pueden ser de menor longitud si se combinan diferentes conjuntos (o tipos) de caracteres.

126. Se dispone de más información detallada de las comprobaciones y sistemas de gestión de contraseñas disponibles en VMware ESX en la guía de configuración [Ref.- 11](capítulo 12).

127. Por defecto la librería pam_cracklib.so no establece una regla de restricción respecto a la reutilización de contraseñas.

128. Se recomienda habilitar un histórico de contraseñas. Para ello es necesario modificar el fichero “/etc/pam.d/system-auth”, y añadir el parámetro “remember=10” al final de la línea “password sufficient /lib/security/\$ISA/pam_unix.so”, dejando un espacio en blanco antes. Esto permitirá recordar 10 contraseñas por usuario.

```
password          sufficient      /lib/security/$ISA/pam_unix.so      nullok
use_authtok md5 shadow remember=10
```

129. Adicionalmente es necesario ejecutar los siguientes comandos para crear el fichero dónde se almacenará el histórico de contraseñas:

```
# cd /etc/security
# touch opasswd
# chmod 0600 opasswd
# chown root:root /etc/security/opasswd
# ls -l opasswd
-rw----- 1 root  root    0 Feb 25 00:03 opasswd
```

130. Se establecerá el nivel de complejidad de las contraseñas para la librería pam_passwdqc.so mediante el siguiente comando:

```
# esxcfg-auth --usepamqc=-1 -1 -1 12 8 -1
```

Dónde el significado de cada parámetro es el siguiente:

```
# esxcfg-auth --usepamqc=<N0> <N1> <N2> <N3> <N4> <match>
```

Las clases o conjuntos de caracteres son letras minúsculas, mayúsculas, números y caracteres especiales.

N0 = Número de caracteres para una contraseña que sólo hace uso de una clase de caracteres.

N1 = Número de caracteres para una contraseña que hace uso de dos clases de caracteres.

N2 = Empleado para passphrases. VMware ESX requiere tres palabras al menos.

N3 = Número de caracteres para una contraseña que hace uso de tres clases de caracteres.

N4 = Número de caracteres para una contraseña que hace uso de las cuatro clases de caracteres.

match = Máximo número de caracteres para la nueva contraseña que pueden ser reutilizados de la contraseña previa.

Si cualquiera de los valores es “-1” implica que el requisito será ignorado.

Por tanto, el ejemplo superior sólo permite claves que combinen tres clases y de 12 caracteres de longitud, o que combinen las cuatro clases y de 8 caracteres de longitud.

131. Adicionalmente es obligatorio definir la caducidad de las contraseñas, es decir, el número máximo de días antes de forzar a los usuarios a realizar un cambio de contraseña. La configuración seleccionada se debe regir por los principios definidos en la política de seguridad de gestión de cuentas y contraseñas de la organización.

132. El objetivo es forzar a los usuarios a cambiar, y por tanto renovar, sus contraseñas, de forma que se minimice en el tiempo el uso de las mismas en el caso de haber sido robadas por un atacante.

133. El tiempo máximo en el que un usuario puede mantener su contraseña puede fijarse mediante el siguiente comando, que en este ejemplo, establece el tiempo de renovación en 60 días ó 2 meses (el valor por defecto es indefinido, 99999):

```
# esxcfg-auth --passmaxdays=60
```

134. Por defecto, la cuenta de “root” y otras cuentas de servicio no están afectadas por la restricción de días.

135. En el caso de querer aplicar una configuración especial sólo a determinadas cuentas de usuario, es posible emplear el siguiente comando, que establece el límite en 120 días únicamente para el usuario “operador”:

```
# chage -M 120 operador
```

136. Complementando el número máximo de días antes del cambio de contraseña, se recomienda establecer también el número mínimo de días antes de permitir un nuevo cambio de contraseña.
137. El objetivo es limitar que los usuarios puedan cambiar su clave múltiples veces en un corto espacio de tiempo y volver a fijar una clave utilizada previamente (la anterior, o una del histórico de claves usadas recientemente).
138. El tiempo mínimo de cambio de contraseña puede fijarse mediante el siguiente comando, que en este ejemplo, establece el tiempo de renovación en 10 días (el valor por defecto es 0, indicando que puede modificarse en cualquier momento):

```
# esxcfg-auth --passmindays=10
```

139. En el caso de querer aplicar una configuración especial sólo a determinadas cuentas de usuario, es posible emplear el siguiente comando, que establece el límite mínimo en 30 días únicamente para el usuario “operador”:

```
# chage -m 30 operador
```

140. Es posible configurar el número de días previos a la expiración en los que el usuario recibe una notificación de que su clave va a caducar. El valor por defecto es 7 días, y el mensaje sólo se muestra al autenticarse directamente a través de la consola o mediante SSH.
141. Es posible tanto establecer un valor general, como valores específicos para ciertos usuarios:

```
# esxcfg-auth --passwarnage=14
```

```
# chage -W 20 operador
```

6.1.7. CONFIGURACIÓN DE SUDO

142. El comando “sudo” permite la ejecución de tareas que requieren privilegios de administración por parte de cualquier usuario (con los permisos adecuados en “sudo”) sin requerir las credenciales del administrador (usuario “root”). El usuario únicamente deberá proporcionar sus credenciales para llevar a cabo la tarea privilegiada una vez autorizado a ello. El propósito principal de “sudo” es la delegación de tareas de administración por parte de “root” a otros usuarios.
143. Sudo debe ser configurado mediante el comando “visudo”, que permite editar de forma adecuada el fichero de configuración de “sudo”: “/etc/sudoers”. Para ello emplea el editor “vi” (u otro especificado en la variable de entorno EDITOR) y adicionalmente realiza verificaciones de sintaxis del fichero de configuración.

144. Como ejemplo de configuración de “sudo” se muestra el siguiente fichero “sudoers”. Es necesario definir y crear la política completa de ejecución mediante “sudo” para los distintos usuarios existentes en el sistema en función de los requisitos y necesidades del entorno:

```
%wheel  ALL=    /*bin/*,/usr/*bin/*,!/bin/*sh,!/bin/vi  /etc/sudoers,!/usr/bin/nano
/etc/sudoers

%admins  ALL=    /usr/sbin/esxcfg-*,    /usr/*bin/vmware-*,    /usr/*bin/vmfs*,
/usr/*bin/vmk*, /usr/lib/vmware/bin/vmk*

%backup  ALL=    /usr/*bin/vcb*
```

145. En el ejemplo superior, los usuarios pertenecientes al grupo “wheel” pueden ejecutar cualquier comando excepto disponer de acceso mediante shell o editar el fichero “/etc/sudoers”. Los usuarios pertenecientes al grupo “admins” (VMware Infrastructure administrators) pueden ejecutar cualquier comando de VMware ESX y los usuarios pertenecientes al grupo “backup” pueden ejecutar cualquier comando de copia de seguridad.
146. Se recomienda crear un grupo específico para los administradores, por ejemplo “admins”, y sólo permitir a usuarios de ese grupo la ejecución de “sudo”.
147. Para la configuración adecuada de “sudo” se debería aplicar el principio de mínimo privilegio, y otorgar a otros usuarios única y exclusivamente las capacidades privilegiadas para completar las tareas que necesitan llevar a cabo.
148. Por defecto, todas las acciones realizadas a través de “sudo” son registradas en el fichero de log “/var/log/secure”, tal como se especifica en el fichero “/etc/syslog.conf”. Se recomienda habilitar el envío de dichos mensajes a un servidor de syslog remoto (ver sección “LOGGING Y REGISTRO DE EVENTOS”).
149. Se recomienda consultar documentación externa para conocer todas las capacidades de “sudo” (al tratarse de un comando estándar en entornos Unix y Linux) y llevar a cabo su correcta configuración.

6.1.8. ACCESO SEGURO MEDIANTE SSL O TLS

150. VMware ESX emplea SSLv3 o TLSv1 para las comunicaciones de sus diferentes componentes: cliente VI, VirtualCenter y accesos web.
151. VMware ESX hace uso de certificados digitales para las comunicaciones basadas en SSL y TLS, pero emplea certificados creados por defecto por VMware, Inc. (autofirmados) que no pueden ser validados y verificados. Éstos han sido generados para el sistema “localhost.localdomain”.

152. Se recomienda reemplazar los certificados existentes por defecto por nuevos certificados válidos y verificables, empleando firma basada en SHA1 (en lugar de MD5), y habilitar las capacidades de verificación de certificados de VMware ESX [Ref.- 11](capítulo 11).
153. Para habilitar la verificación es necesario conectarse a VirtualCenter con el cliente VI, seleccionar el menú “Administration” y la opción “VirtualCenter Management Server Configuration.”. Seleccionar la opción “SSL Settings” y habilitar “Check host certificates” (ver siguientes figuras).

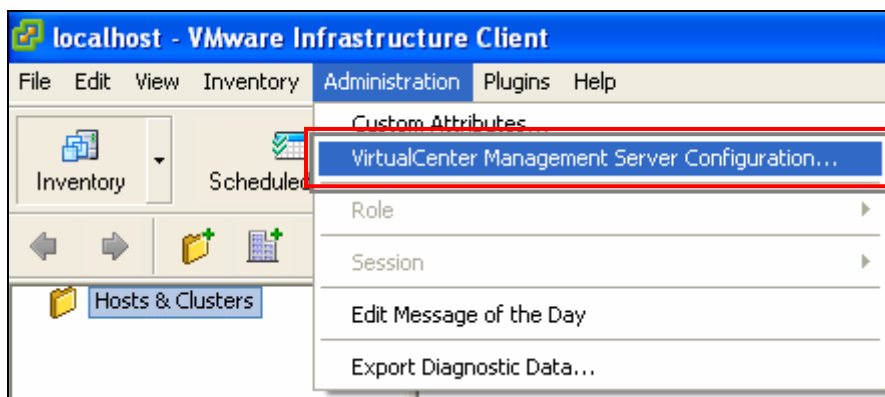


Figura 3.- Acceso a la configuración de gestión de vCenter

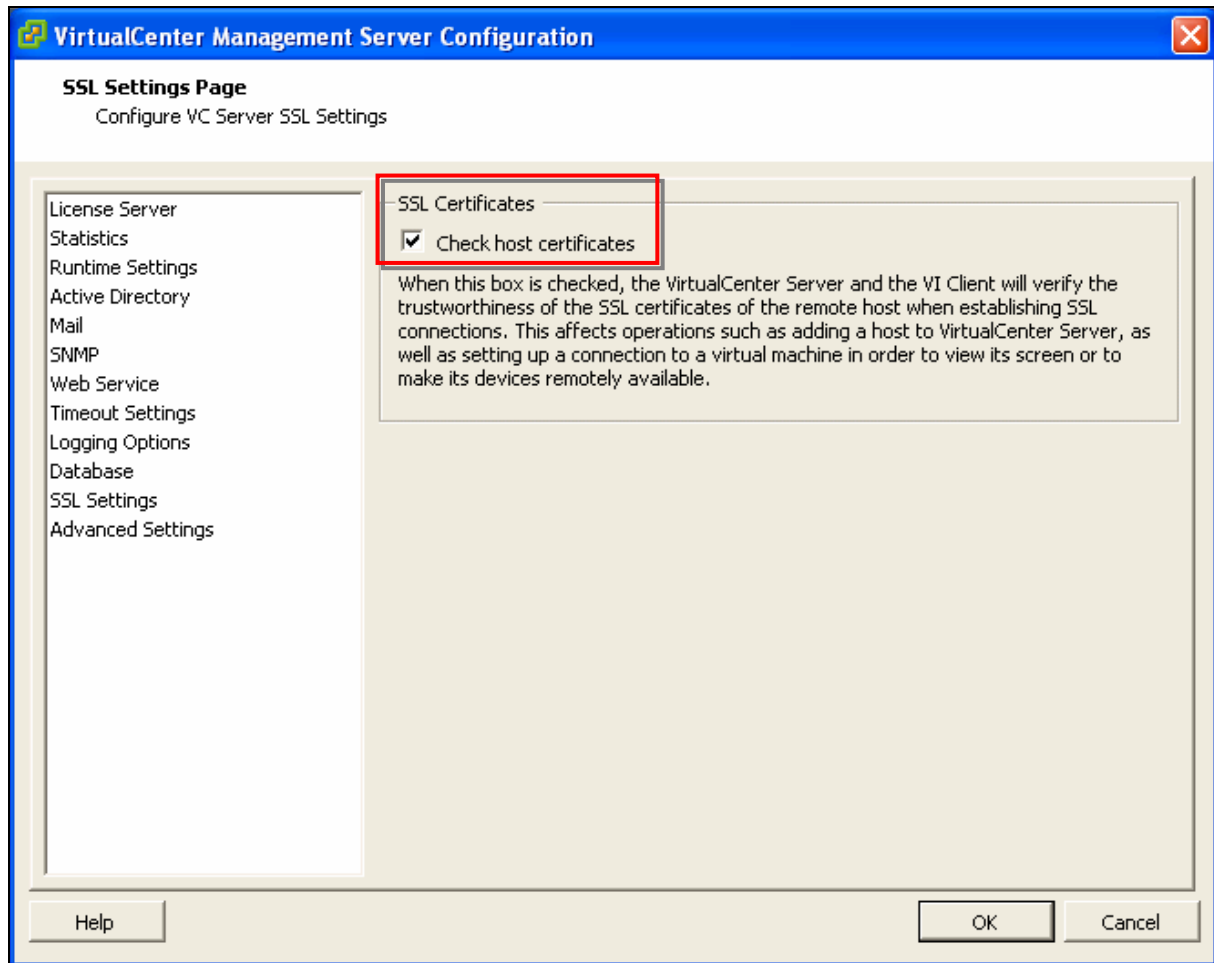


Figura 4.- Comprobación de los certificados digitales de SSL en vCenter

154. Los nuevos certificados deben instalarse en el directorio “/etc/vmware/ssl/” y consisten en dos ficheros: “rui.crt” (certificado digital) y “rui.key” (clave privada). La ubicación se define en el fichero “/etc/vmware/hostd/config.xml”.
155. Se recomienda hacer copia de seguridad de los ficheros existentes por defecto y reemplazarlos por los dos ficheros asociados al nuevo certificado. Adicionalmente los permisos de ambos ficheros deberían ser los adecuados:

```
# cd /etc/vmware/ssl/  
# mv rui.crt rui.crt.backup  
# mv rui.key rui.key.backup
```

Tras copiar los dos nuevos ficheros, ejecutar:

```
# chmod 0644 rui.crt  
# chmod 0400 rui.key  
# chown root:root rui.*
```

156. Los certificados a instalar deben haber sido generados por una autoridad certificadora (CA, Certification Authority) reconocida, ya sea externa o interna a la organización.
157. VMware ESX no soporta certificados X.509 protegidos por contraseña, por lo que este requisito debe tenerse en cuenta a la hora de generar los nuevos certificados.
158. La guía de configuración de VMware ESX [Ref.- 11] (capítulo 11) proporciona todos los detalles sobre la gestión de certificados digitales.

6.2. CONFIGURACIÓN DE SEGURIDAD DE LAS COMUNICACIONES EN VMWARE ESX

159. Adicionalmente a las configuraciones de seguridad del propio sistema VMware ESX y su servidor de gestión, se recomienda aplicar recomendaciones de seguridad específicas para el entorno de comunicaciones y redes de VMware ESX.

6.2.1. CREACIÓN DE UNA RED DE GESTIÓN DEDICADA

160. Se recomienda aislar y segmentar la red de gestión, a la que se conecta el servidor de gestión de VMware ESX y los diferentes interfaces y mecanismos de administración, del resto de redes empleadas por las máquinas virtuales y/o el host.
161. Existen diferentes alternativas para diseñar e implementar la segmentación de la red de gestión, como por ejemplo:
- Usar una VLAN privada para la red de gestión.
 - Usar una VLAN privada para la red de gestión junto a un vSwitch dedicado asociado a uno o varios puertos de conexión.
 - Usar una VLAN privada para la red de gestión junto a un vSwitch dedicado asociado a un interfaz de red físico independiente (opción recomendada). Este interfaz de red físico sólo debería estar conectado a una red real dedicada a tareas de gestión.
162. La red de gestión de VMware ESX se emplea para múltiples comunicaciones, como por ejemplo las conexiones a los servidores VMware ESX desde el cliente VI o VirtualCenter, o mediante SSH, las comunicaciones de alta disponibilidad entre servidores ESX, para las comunicaciones de los servicios auxiliares (DNS, NTP, syslog, etc), etc.

6.2.2. MODO PROMISCOUO

163. Los interfaces de red en VMware ESX pueden ser configurados en modo promiscuo, es decir, aceptarán todo el tráfico de red, tanto el destinado a su dirección MAC como a cualquier otra.

164. El modo promiscuo puede ser habilitado para los switches de red virtuales (o vSwitches) asociados a un interfaz de red físico, denominados “vmnic”, o para los vSwitches virtuales (sin relación con un interfaz de red físico), denominados “vmnet”.
165. Cuando se habilita este modo en un vSwitch asociado a un interfaz de red (vmnic), cualquier máquina virtual conectada al vSwitch puede capturar el tráfico enviado a través de ese vSwitch o a través de la red física donde reside el interfaz de red asociado al “vmnic”.
166. Cuando se habilita este modo en un vSwitch no asociado a un interfaz de red (vmnet), cualquier máquina virtual conectada al vSwitch puede capturar el tráfico enviado por cualquier otra máquina virtual conectada al mismo.
167. Mediante el cliente VI (“Inventory”), en concreto a través de la pestaña “Configuration”, opción “Networking”, es posible gestionar la configuración de los vSwitches. Seleccionando “Properties” para el vSwitch a configurar, es posible modificar los diferentes puertos y conexiones de red.

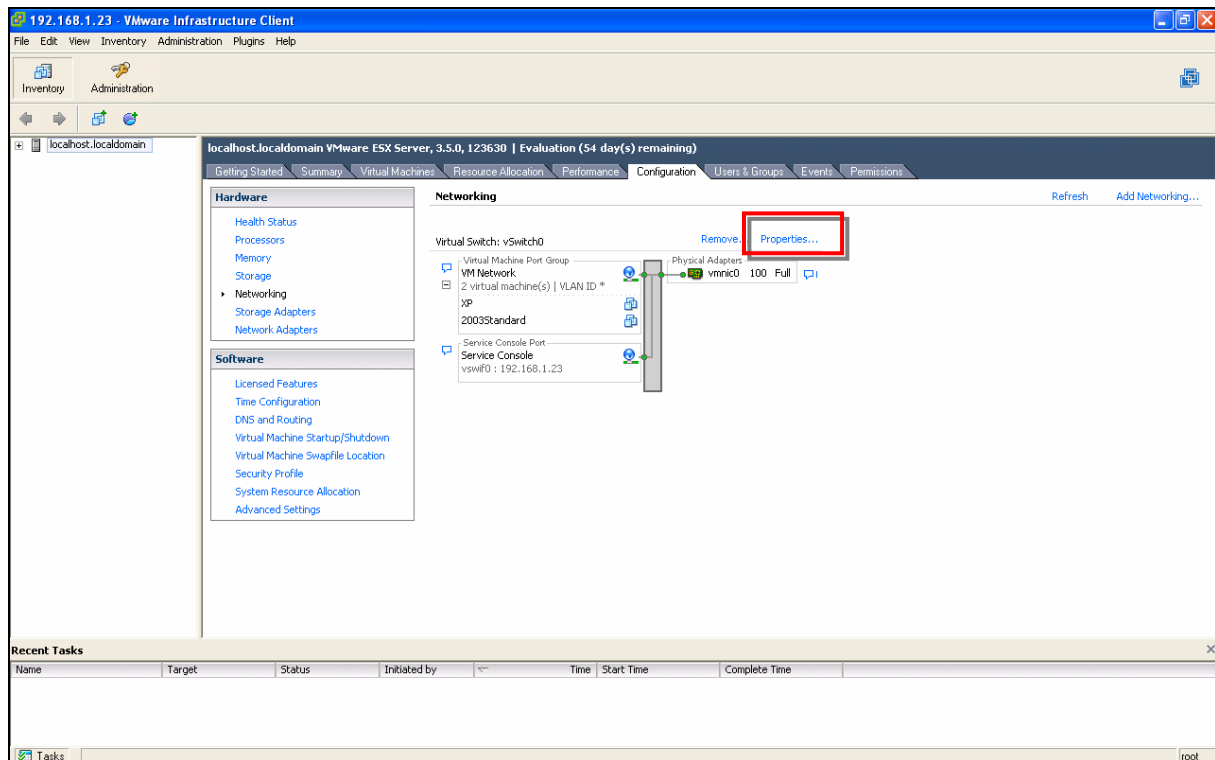


Figura 5.- Propiedades de los switches de red virtuales

168. Una vez seleccionado el puerto, con el botón “Edit...” y a través de la pestaña “Security”, se recomienda verificar y/o modificar el siguiente parámetro (teniendo en cuenta que su valor por defecto es “Reject”) para deshabilitar el modo promiscuo:
- Promiscuous Mode: Reject

169. Los cambios en la configuración de seguridad deben aplicarse en los vSwitches, de forma que afecten a todos los puertos o grupos de puertos definidos en el vSwitch. No deben aplicarse configuraciones de seguridad específicas en los puertos, ya que éstas reemplazarían la configuración general del vSwitch.

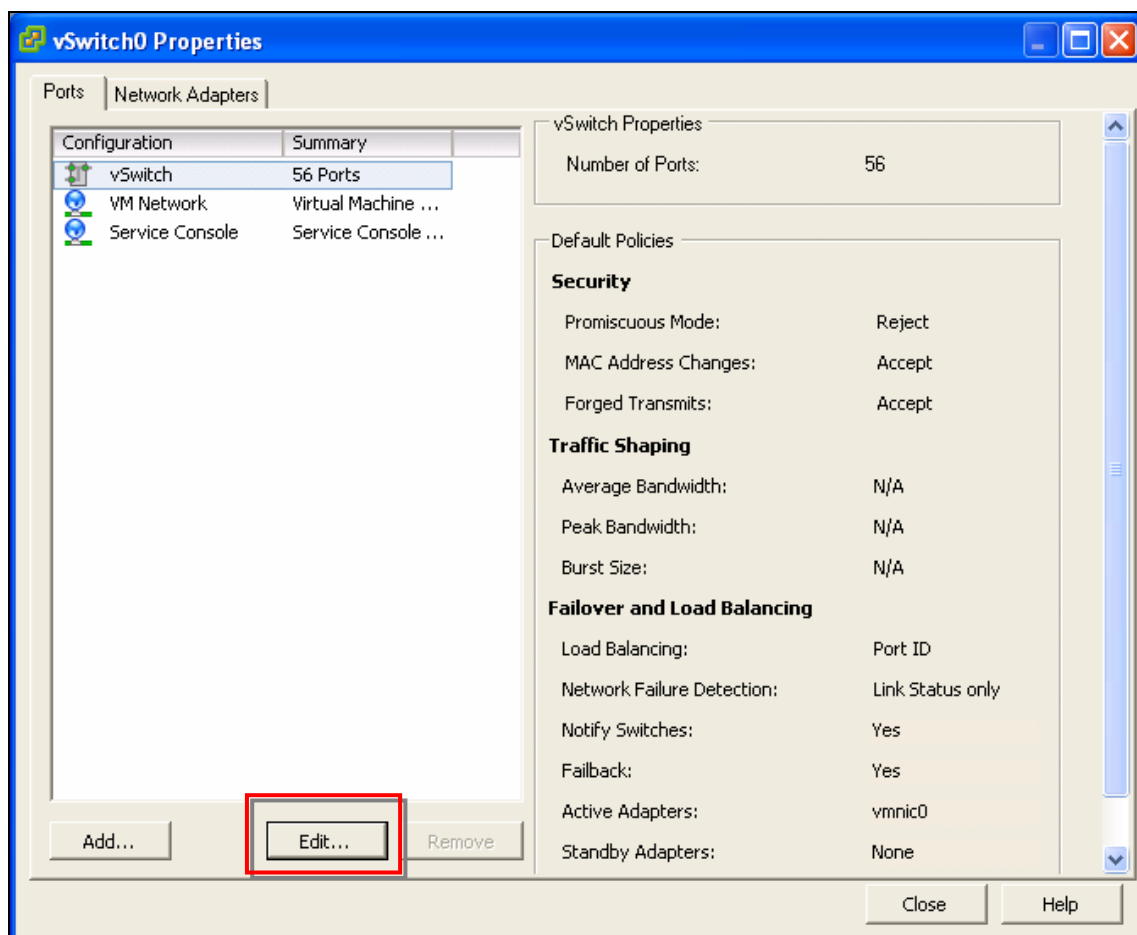


Figura 6.- Configuración de los parámetros de los switches de red virtuales

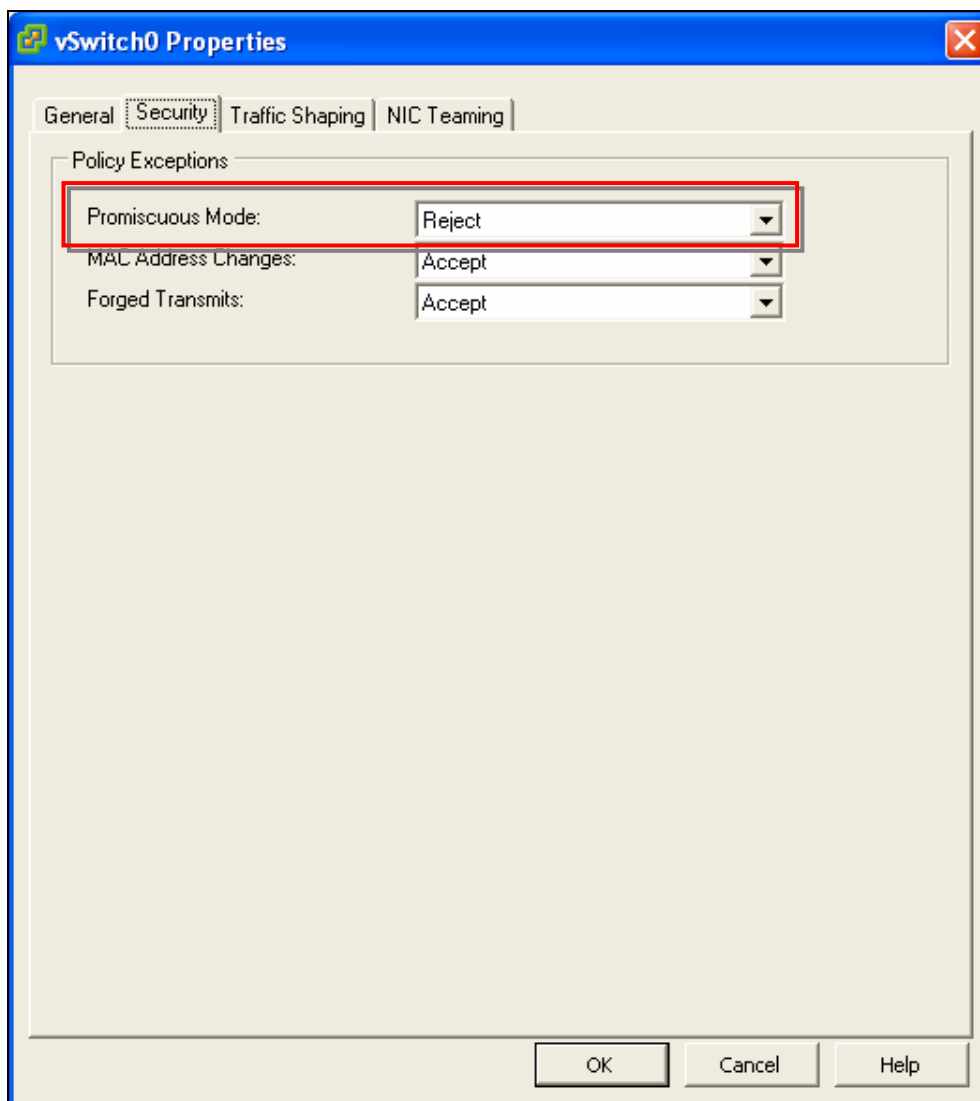


Figura 7.- Configuración del modo promiscuo en los switches de red virtuales

6.2.3. PROTECCIÓN FRENTE A ATAQUES DE SUPLANTACIÓN DE MAC

170. VMware ESX permite aplicar mecanismos de seguridad a nivel 2 sobre los vSwitches, protegiendo así tanto el servidor ESX (*host*) como las máquinas virtuales (*guests*).
171. Los mecanismos de seguridad pueden aplicarse de forma individual a cada puerto, o a grupos de puertos, que comparten la misma política de seguridad.
172. VMware ESX asigna una dirección MAC a cada interfaz de red virtual de cada máquina virtual en el momento de su creación. Adicionalmente, se asigna una dirección MAC efectiva que puede ser empleada para filtrar tráfico. Inicialmente ambas direcciones tienen el mismo valor.

173. Debe tenerse en cuenta que el sistema operativo de cualquier máquina virtual puede cambiar la dirección MAC efectiva y, como resultado, suplantar la dirección MAC de otro interfaz de red e interceptar o redirigir tráfico asociado al interfaz suplantado, ataques conocidos como *MAC spoofing*.
174. VMware ESX puede prevenir y detectar cambios en las direcciones MAC y filtrar el tráfico entrante cuando la dirección MAC destino de las tramas de red no corresponde con la dirección MAC (efectiva) asociada al interfaz de red por el que se recibe el tráfico.
175. Mediante el cliente VI (“Inventory”), en concreto a través de la pestaña “Configuration”, opción “Networking”, es posible gestionar la configuración de los vSwitches. Seleccionando “Properties” para el vSwitch a configurar, es posible modificar los diferentes puertos y conexiones de red.
176. Una vez seleccionado el vSwitch, con el botón “Edit...” y a través de la pestaña “Security” se recomienda modificar los siguientes parámetros (ya que su valor por defecto es “Accept”) para deshabilitarlos. El objetivo es evitar el cambio de dirección MAC (para evitar la recepción de tramas destinadas a otro equipo) y el envío de tramas con una dirección MAC suplantada, respectivamente:
- MAC Address Changes: Reject
 - Forged Transmits: Reject
177. Los cambios en la configuración de seguridad deben aplicarse en los vSwitches, de forma que afecten a todos los puertos o grupos de puertos definidos en el vSwitch. No deben aplicarse configuraciones de seguridad específicas en los puertos, ya que éstas reemplazarían la configuración general del vSwitch.

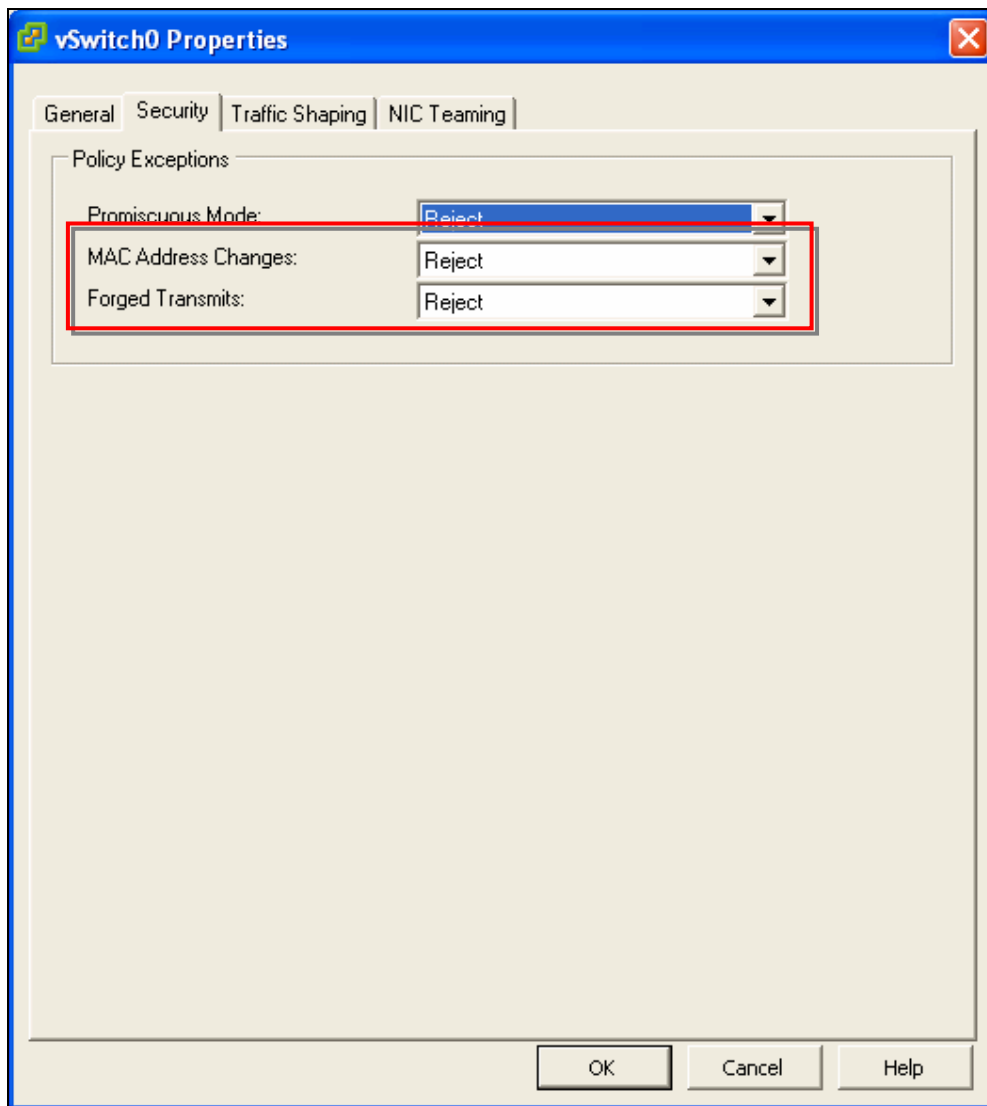


Figura 8.- Configuración del cambio de dirección MAC y el envío de tramas falsas en los switches de red virtuales

6.2.4. CONFIGURACIÓN DEL FIREWALL EN EL SERVIDOR DE GESTIÓN

178. VMware ESX proporciona mecanismos de filtrado mediante un firewall o cortafuegos para limitar el tráfico permitido a través de la red hacia el servidor de gestión y los diferentes mecanismos de administración existentes.
179. Con el objetivo de limitar el acceso no autorizado al servidor de gestión habilitado por defecto, se recomienda configurar el firewall. Este firewall se basa en el software “iptables” de Linux.
180. El firewall puede ser configurado a través del cliente VI (con ciertas limitaciones, ya que no muestra la política completa de tráfico permitido) o mediante los siguientes comandos del CLI (se recomienda el uso de “esxcfg-firewall”):

```
# esxcfg-firewall -q  
  
# iptables -nL
```

181. VMware ESX proporciona tres niveles de seguridad para el firewall: bajo, medio y alto (nivel por defecto). Es posible comprobar el nivel de seguridad actual mediante los siguientes comandos:

```
# esxcfg-firewall -q incoming  
  
Incoming ports blocked by default.  
  
# esxcfg-firewall -q outgoing  
  
Outgoing ports blocked by default.
```

Si tanto el tráfico entrante (incoming) como saliente (outgoing) está bloqueado, el nivel es alto. Si sólo el tráfico entrante está bloqueado, el nivel es medio. Si ninguno de los dos está bloqueado, el nivel es bajo.

182. Es posible establecer de nuevo el nivel alto de seguridad (opción recomendada) mediante el siguiente comando, tras el cual hay que reiniciar el proceso “vmware-hostd”:

```
# esxcfg-firewall --blockIncoming --blockOutgoing  
  
# service mgmt-vmware restart
```

183. Mediante el cliente VI, en concreto a través del menú “Configuration”, opción “Security Profile” y “Firewall”, es posible gestionar la configuración del firewall. Seleccionando “Properties” es posible modificar la política de filtrado del firewall.

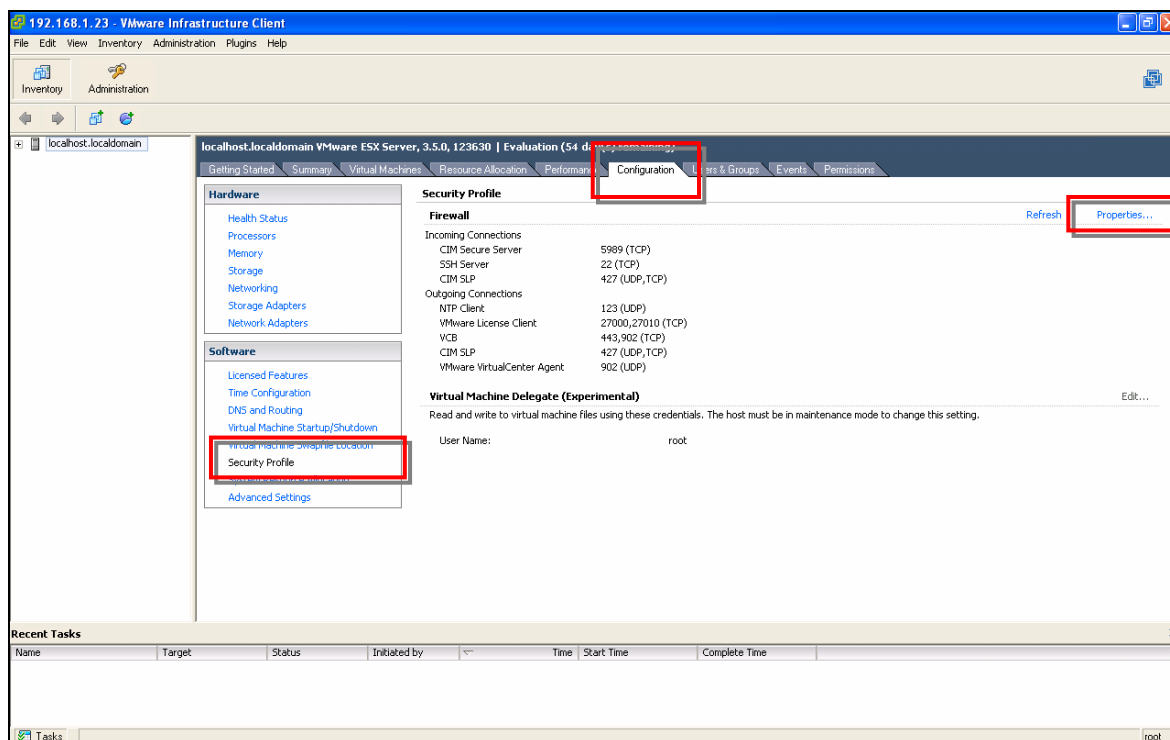


Figura 9.- Política de filtrado del firewall de VMware ESX en el cliente VI

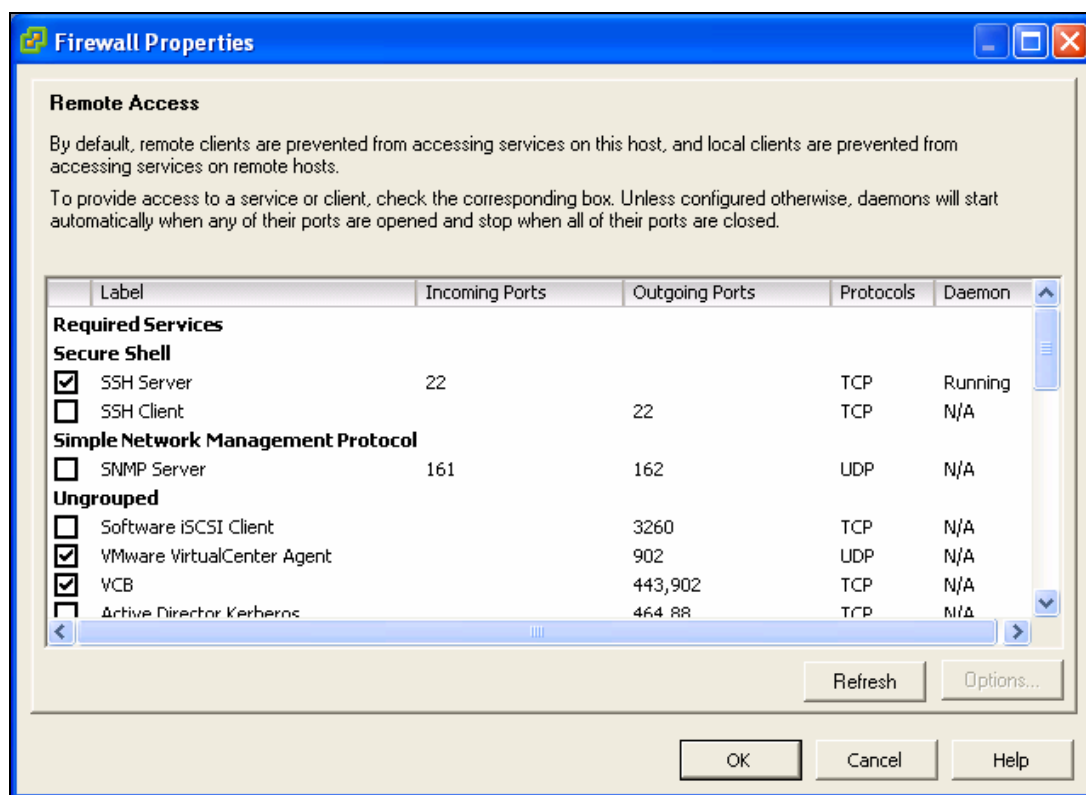


Figura 10.- Configuración de la política de filtrado del firewall de VMware ESX

184. También es posible modificar la política de filtrado mediante el comando “esxcfg-firewall --openPort” (o --closePort) [Ref.- 11](capítulo 12)

185. La política habilitada por defecto en el firewall (nivel alto) bloquea todo el tráfico entrante y saliente excepto para los puertos y servicios detallados en la siguiente tabla (considerados necesarios). La política detalla los puertos TCP y UDP (ordenados por número de puerto), y el tráfico ICMP, permitido desde y hacia los servicios del servidor de gestión (y su interfaz de red de gestión asociado).

NOTA: la tabla no detalla la política para el interfaz de red interno, o loopback, que acepta todo el tráfico de entrada (INPUT) y de salida (OUTPUT).

Protocolo	Dirección	Propósito
TCP/22	Entrante	Administración remota por SSH
TCP,UDP/53 (1)	Saliente	Resolución DNS
UDP/67,68 (1)	Entrante Saliente	DHCP (puertos fuente y destino 67 y 68)
TCP/80 (1)	Entrante	Administración remota por interfaz web (ver TCP/443)
TCP,UDP/427	Entrante	CIM (Common Information Model) SLP (Service Location Protocol)
TCP,UDP/427	Saliente	CIM SLP (puerto origen 427)
TCP/443 (1)	Entrante Saliente	Administración remota por interfaz web mediante HTTPS
TCP/902	Entrante Saliente	Autenticación y consola remota
UDP/902	Saliente	Autenticación y consola remota
TCP/5989	Entrante	Transacciones CIM XML sobre HTTPS
TCP/27000	Saliente	Transacciones de licencias de ESX al servidor de licencias (lmgrd.exe)
TCP/27010	Saliente	Transacciones de licencias de ESX al servidor de licencias (vmwarelm.exe)

NOTA: en todos los casos los puertos indican puerto destino, salvo que se indique lo contrario.

Tabla 1.- Política de filtrado por defecto del firewall del servidor de gestión.

NOTA (1): el tráfico marcado con (1) no puede ser gestionado desde el interfaz gráfico del cliente VI. En el caso de TCP/443 esta restricción sólo aplica al tráfico entrante. Esas reglas están configuradas directamente en el fichero “/usr/sbin/esxcfg-firewall”.

186. Adicionalmente la política por defecto definida en el fichero “/usr/sbin/esxcfg-firewall” permite el tráfico de conexiones ya establecidas y establece reglas anti-spoofing.

187. El fichero de configuración general de la política de filtrado del firewall se encuentra disponible en “/etc/vmware/firewall/services.xml”.

188. VMware proporciona información adicional sobre otros puertos que pueden ser necesarios para ciertas tareas opcionales o agentes software (backup, alta disponibilidad, gestión, etc) [Ref.- 11](capítulo 10).

6.2.5. EXCEPCIONES A LA POLÍTICA DE FILTRADO POR DEFECTO

189. Se recomienda deshabilitar el tráfico ICMP permitido por defecto: de entrada los tipos 0, 8 y 3 (código 4); de salida los tipos 0 y 8.
190. No es posible deshabilitar ICMP mediante el cliente VI. Es necesario editar directamente el fichero “/usr/sbin/esxcfg-firewall” y cambiar las siguientes líneas de configuración por el conjunto de directivas especificado a continuación:

```
# drops all outgoing icmp messages except ping
'icmp-out' => [
    '-p icmp --icmp-type echo-request -j ACCEPT',
    '-p icmp --icmp-type echo-reply -j ACCEPT',
    '-j DROP'],

# drops all incoming icmp messages except ping & frag-needed
'icmp-in' => [
    '-p icmp --icmp-type echo-reply -j ACCEPT',
    '-p icmp --icmp-type echo-request -j ACCEPT',
    '-p icmp --icmp-type fragmentation-needed -j ACCEPT',
    '-j DROP'],
```

Modificar la configuración para deshabilitar por completo el tráfico ICMP saliente, y sólo permitir como tráfico ICMP entrante las notificaciones de fragmentación:

```
# Deshabilitar el trafico ICMP de ping, tanto entrante como saliente

# drops all outgoing icmp messages
'icmp-out' => [
    '-p icmp',
    '-j DROP'],

# drops all incoming icmp messages except frag-needed
'icmp-in' => [
    '-p icmp --icmp-type fragmentation-needed -j ACCEPT',
    '-j DROP'],
```

191. Una vez realizados los cambios en el fichero de configuración, es necesario reiniciar el firewall:

```
# esxcfg-firewall -load
```


192. La gestión de la política del firewall de VMware ESX no permite restringir el tráfico sólo a ciertos equipos en función de la dirección IP origen. En caso de querer establecer ese tipo de restricciones, es necesario emplear un firewall externo o modificar a mano directamente el fichero “/usr/sbin/esxcfg-firewall”, añadiendo reglas de iptables propias.

193. Puede ser necesario añadir reglas adicionales a la política para permitir el tráfico asociado a otros protocolos, como el cliente NTP (UDP/123 saliente) para la sincronización de tiempos:

```
# esxcfg-firewall --enableService ntpClient
```

194. Los clientes CIM (TCP,UDP/427) emplean el protocolo SLP (Service Location Protocol), versión 2, para localizar servidores CIM (Common Information Model). Si no se emplea software basado en CIM para la monitorización y gestión del entorno VMware ESX, se deben deshabilitar las reglas asociadas al puerto 427 y TCP/5989.

195. El puerto TCP,UDP/902 se emplea para tráfico de autenticación y de consola remota. VirtualCenter requiere mensajes UDP desde el servidor ESX (salientes), y el servidor ESX accede a otros servidores ESX para migraciones y aprovisionamiento. Algunos clientes VI (según la versión) lo emplean para acceder a las consolas de ESX. Si no se emplea VirtualCenter para la gestión de VMware ESX, puede deshabilitarse la regla asociada al puerto UDP/902 (saliente). Si no se emplea el mecanismo de VMware Consolidated Backup (VCB) para la realización de copias de seguridad, puede deshabilitarse la regla asociada al puerto TCP/902 (saliente).

196. Si se emplea el sistema de licencias interno del servidor VMware ESX, y no se dispone de un servidor de licencias, deben deshabilitarse las reglas asociadas a los puertos 27000 y 27010.

197. Si se emplea VirtualCenter o el cliente VI para la administración del entorno VMware ESX (y no SSH), es posible deshabilitar la regla de acceso mediante SSH (TCP/22).

6.3. CONFIGURACIÓN DE SERVICIOS EN VMWARE ESX

198. VMware ESX activa diferentes servicios durante el arranque del sistema. Es necesario gestionar estos servicios y emplear únicamente los mínimos necesarios.

6.3.1. ARRANQUE Y ACTIVACIÓN DE SERVICIOS

199. Se deberán reducir al mínimo todos los servicios no utilizados y que son activados durante el proceso de arranque, con el objetivo de minimizar la exposición del entorno y reducir el número potencial de vulnerabilidades en el sistema.

200. La lista por defecto de servicios en ejecución se puede obtener mediante el análisis de los servicios que arrancan en el nivel de arranque número 3 desde el CLI:

```
# ls -al /etc/rc3.d/S*
```

El apéndice A contiene la lista de los servicios mínimos recomendados en VMware ESX.

201. Adicionalmente, es posible contrastar la lista de servicios que se activan durante el proceso de arranque del sistema con la lista de procesos con puertos TCP o UDP activos actualmente.
202. La lista de puertos TCP y UDP activos en cualquier interfaz de red del sistema ESX se puede obtener mediante diferentes comandos desde el CLI:

```
# netstat -anp | egrep '0\.\0\.\0\.\0:.*'
```

Listado de puertos con servicios disponibles por defecto:

- tcp/5988, 5989 cimserver
- tcp/902 xinetd (vmware-authd)
- tcp/8009, 8080 webAccess
- tcp/80,443 vmware-hostd
- tcp/22 sshd
- udp/427 cimserver

203. Es posible verificar la lista de procesos que sólo escuchan en el interfaz de red local mediante los siguientes comandos:

```
# netstat -anp | grep "127.0.0.1" | grep LISTEN
```

Listado de puertos con servicios disponibles por defecto en localhost:

- tcp/32770 cimserver
- tcp/8005 webAccess
- tcp/8889 openwsmand

204. Se recomienda habilitar los siguientes servicios (y su configuración de red asociada):

sshd (TCP/22), ntpd (UDP/123), xinetd (TCP/902, vmware-authd), VMware webAccess (TCP/8005, 8009 y 8080), gestión de VMware ESX (TCP/80, 443, 8085, 8087, 9080, vmware-hostd), openvsmand (tcp/8889), y cimserver (TCP/32770, 5988, 5989 y UDP/427).

NOTA: Los puertos subrayados sólo escuchan en el interfaz de red local (localhost).

205. Para cada proceso es recomendable confirmar que no escucha adicionalmente en otros interfaces de red, empleando el comando “lsof” y el número de proceso (PID) obtenido del comando previo:

```
# lsof -i -p <PID>
```

6.3.2. NTP (NETWORK TIME PROTOCOL)

206. Se recomienda establecer la configuración de NTP (Network Time Protocol) con el objetivo de disponer de la misma referencia de tiempos en todo el entorno, de sistemas de información y evitar así discrepancias y anomalías en las marcas de tiempo de los logs y eventos generados por distintos equipos.

207. Para ello es necesario disponer de un servidor de tiempos propio con el que sincronizarse, u obtener acceso a un servidor NTP externo, por ejemplo el proporcionado por el proveedor de acceso a Internet.

208. La configuración de NTP se puede establecer a través del cliente VI, habilitando y configurando el servicio NTP (pestaña “Configuration” de “Inventory”, menú “Software – Time Configuration”, opción “Properties”).

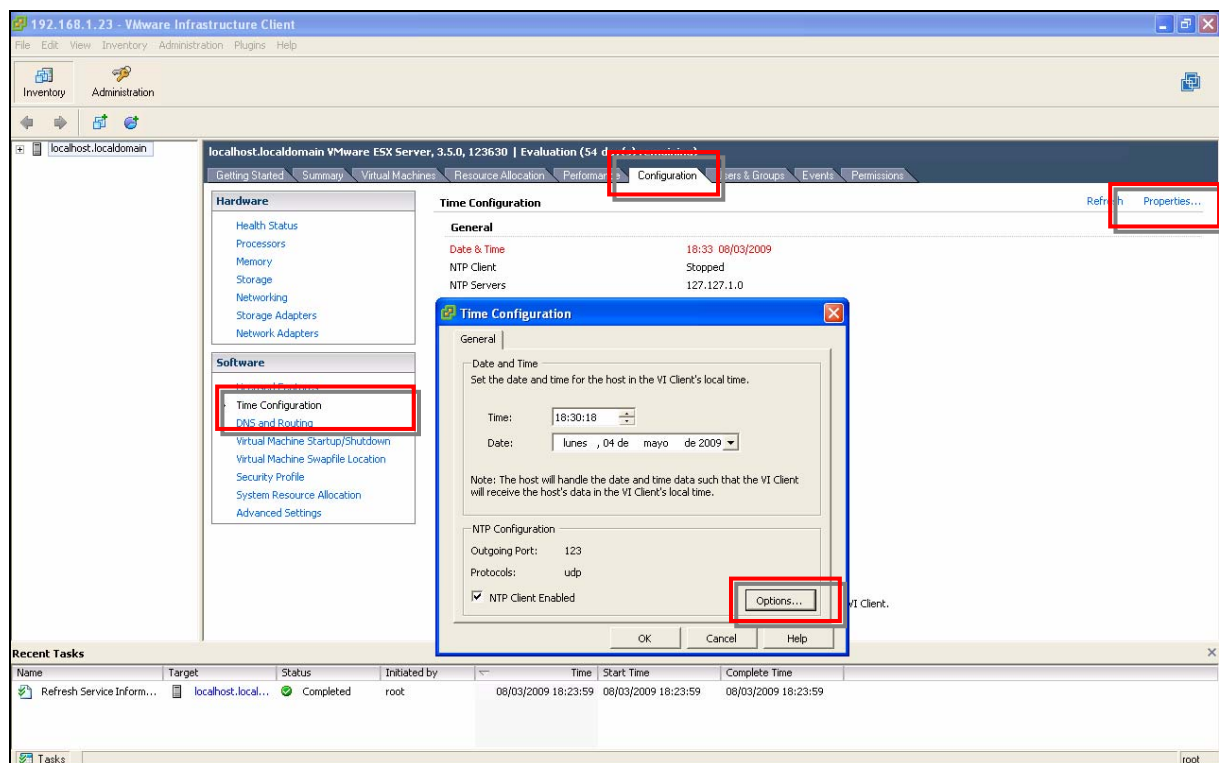


Figura 11.- Información del servicio NTP de VMware ESX

209. Mediante el botón “Options” es posible establecer cuando arrancará el cliente NTP y la configuración de NTP, en concreto, los servidores NTP a consultar. Se recomienda dejar la política por defecto para el arranque de NTP, es decir, cuando los puertos UDP necesarios estén abiertos en el firewall. Una vez configurado los servidores y la política, mediante el botón “Start” es posible iniciar el servicio. El cambio requiere disponer de acceso en modo mantenimiento temporalmente, estado en el que las máquinas virtuales no pueden funcionar ni ser gestionadas.

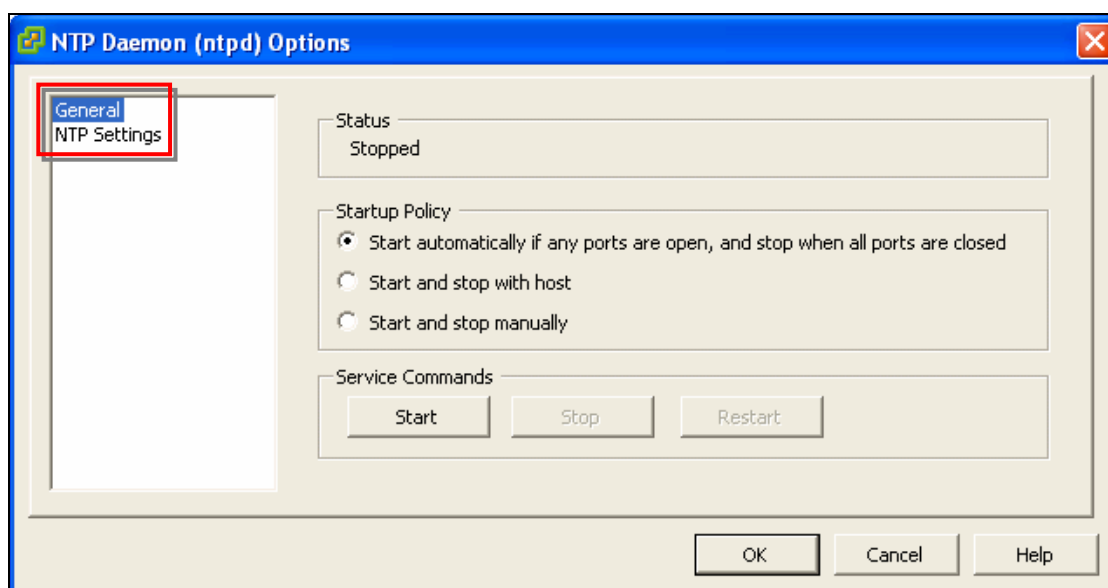


Figura 12.- Configuración del servicio NTP de VMware ESX

6.4. PERMISOS DE FICHEROS EN VMWARE ESX

210. Es necesario verificar y preservar la integridad de los sistemas de ficheros críticos de VMware ESX. Para ello es necesario asegurarse de que los permisos de los ficheros y directorios críticos del sistema son los adecuados, con el objetivo de limitar la lectura, modificación y/o ejecución de ficheros dentro de éstos por parte de un atacante o usuario no privilegiado.

6.4.1. FICHEROS DE CONFIGURACIÓN

211. La siguiente tabla detalla los permisos, propietario y grupo del sistema de ficheros “/etc” donde residen los principales ficheros de configuración. Se recomienda verificar que los permisos, propietario y grupo son los correctos de forma periódica.

Directorio o fichero	Permisos	Propietario	Grupo
/etc/	755	root	root
/etc/profile	644	root	root
/etc/ssh/sshd_config	600	root	root
/etc/pam.d/system_auth	644	root	root
/etc/grub.conf	600	root	root
/etc/krb.conf	644	root	root
/etc/krb5.conf	644	root	root
/etc/krb.realms	644	root	root
/etc/login.defs	644	root	root
/etc/openldap/ldap.conf	644	root	root
/etc/nscd.conf	644	root	root

/etc/resolv.conf	644	root	root
/etc/nsswitch.conf	644	root	root
/etc/ntp/	755	root	root
/etc/ntp.conf	644	root	root
/etc/passwd	644	root	root
/etc/group	644	root	root
/etc/sudoers	440	root	root
/etc/shadow	400	root	root
/etc/vmware/	755	root	root

Tabla 2.- Permisos de los principales ficheros de configuración en “/etc”

212. Es importante verificar adicionalmente los permisos de los ficheros de configuración de VMware ESX, disponibles en “/etc/vmware/*”. El Anexo B (“LISTADO DE PERMISOS DE LOS FICHEROS DE CONFIGURACIÓN DE VMWARE ESX (ETC/VMWARE)”) detalla dichos ficheros de configuración.

213. La idea de verificar los permisos de un conjunto de ficheros críticos puede ser extendida a todos los ficheros y directorios importantes del sistema.

214. Por ejemplo, en “/etc” existen directorios de configuración adicionales, como:

- initrdlogs, oldconf, vmksummary.d, etc.

215. Es posible obtener el listado de permisos de todos los ficheros disponibles bajo “/etc” mediante el siguiente comando:

```
# find /etc -type f -exec ls -l {} \; > /tmp/etc_permisos.txt
```

216. Se puede verificar la integridad de los ficheros mediante herramientas empresariales de verificación de integridad, como Tripwire o Configuresoft, o la integridad únicamente de su contenido mediante el siguiente comando, basado en “sha1sum”:

```
# find /etc -type f -exec sha1sum {} \; > /tmp/etc_sha1.sums
```

El comando almacena los hashes SHA1 de todos los ficheros existentes bajo “/etc” en el fichero “/tmp/etc_sha1.sums”.

217. Se recomienda ejecutar los comandos anteriores (verificación de permisos y contenidos) periódicamente y comparar los resultados obtenidos para detectar modificaciones en los ficheros de configuración. Adicionalmente se recomienda realizar una copia de seguridad periódica de dichos ficheros.

218. En “/usr/sbin” se dispone de todos los comandos de configuración de VMware ESX que comienzan por “esxcfg-*”. Todos deberían tener permisos 500 excepto “esxcfg-auth”, con permisos 544.

219. Todos los ficheros de log mencionados en la sección “LOGGING Y REGISTRO DE EVENTOS” posteriormente deberían tener permisos 600, excepto “/var/log/vmware/webAccess”, con permisos 755.

6.4.2. FICHEROS CON PERMISOS SETUID Y SETGID

220. VMware ESX minimiza el número de ficheros con permisos de setuid y setgid en el sistema. La guía de configuración de VMware proporciona un listado de ficheros opcionales y necesarios de este tipo [Ref.- 11](capítulo 12, sección “setuid and setgid Applications”).
221. Se recomienda deshabilitar los permisos setuid y setgid en todos aquellos ficheros listados como opcionales en la siguiente lista, extraída de la guía de VMware, que no vayan a ser utilizados por usuarios distintos a root:
- Setuid: /usr/bin/crontab y /bin/ping

chmod a-s <FICHERO>
 - Setgid: /usr/bin/wall y lockfile, salvo para Dell OM

chmod g-s <FICHERO>
222. La lista final de ficheros es dependiente del entorno y de las prácticas de administración y gestión de sistemas empleadas en el mismo.

6.5. LOGGING Y REGISTRO DE EVENTOS

223. Con el objetivo de preservar y monitorizar la seguridad del entorno VMware ESX, es necesario establecer mecanismos de registro de eventos y actividades adecuados.
224. Debe configurarse la funcionalidad de rotación de logs del sistema (logrotate) para evitar su pérdida o sobrescritura, y llevar a cabo su correcta gestión y almacenamiento.
225. El fichero “/etc/logrotate.conf” y los ficheros existentes en el directorio “/etc/logrotate.d” definen la configuración de gestión de logs. Es recomendable verificar que los siguientes parámetros de configuración están activos:
- Habilitar el mecanismo de compresión de los logs para ahorrar espacio en disco. Verificar que la directiva “compress” existe (comentada por defecto), y eliminar la directiva “nocompress” (caso de existir).
 - Incrementar el tamaño máximo de los ficheros de log mediante la directiva “size”. Por ejemplo, se puede fijar el tamaño a 8MB mediante “size 8192K”.
 - Las modificaciones de configuración de los ficheros de log se pueden aplicar de forma individualizada para distintos subsistemas y componentes del sistema operativo, definidos en “/etc/logrotate.d”, como por ejemplo “vmkernel”, “vmkwarning”, “vmksummary”, etc.

226. Se recomienda revisar periódicamente los logs del sistema VMware ESX y de las máquinas virtuales, donde cabe destacar:

- VMkernel: /var/log/vmkernel
- VMkernel warnings: /var/log/vmkwarning
- VMkernel summary: /var/log/vmksummary (más .html y .txt)
- ESX host agent log: /var/log/vmware/hostd.log
- Otros logs de VMware ESX: /var/log/vmware/*.log
- Web access: /var/log/vmware/webAccess/
- Service console: /var/log/messages
- Authentication log: /var/log/secure
- Storage Monitor: /var/log/storageMonitor
- Individual virtual machine logs: <path_a_la_máquina_virtual>/vmware.log. Normalmente las máquinas virtuales se encuentran disponibles en “/vmfs/volumes/storageN/<máquina_virtual>”.

227. Con el objetivo de evitar el riesgo de que un atacante pueda editar o eliminar los logs del sistema (que reflejan sus actividades) si éste ha sido comprometido, y con el objetivo de mejorar las capacidades de detección de ataques, se recomienda enviar los logs a un servidor remoto mediante Syslog.

228. La configuración del envío de logs a un servidor remoto pasa por la modificación del fichero “/etc/syslog.conf”, añadiendo la siguiente directiva al final del fichero, donde 192.168.1.250 es la dirección IP del servidor de syslog:

```
# Send all alerts to a remote syslog server  
*. * @192.168.1.250
```

229. Tras modificar el fichero de configuración de syslog es necesario activar la nueva configuración mediante los siguientes comandos, que rearrancan el servicio de syslog y abren los puertos necesarios en el firewall:

```
# esxcfg-firewall -o 514,udp,out,syslog  
# esxcfg-firewall -l  
# service syslog restart
```

Los cambios del nuevo puerto abierto (UDP/514, saliente) se reflejan en el fichero “/etc/vmware/esx.conf”.

6.6. CONFIGURACIÓN DEL ALMACENAMIENTO EN RED

230. VMware ESX dispone de capacidades de acceso a almacenamiento a través de la red, ya sea a entornos iSCSI SAN (Storage Area Network) o a dispositivos NAS (Network Attached Storage) mediante protocolos de compartición de ficheros estándar (NFS, SMB, etc). Para estos últimos aplican las mejores prácticas de seguridad generales.
231. VMware proporciona recomendaciones de seguridad para el almacenamiento de las máquinas virtuales en discos NFS en el entorno VMware ESX [Ref.- 11](capítulo 11).

6.6.1. iSCSI

232. iSCSI es un protocolo de comunicaciones que permite la transmisión de datos de almacenamiento a través de redes de datos, como Ethernet y protocolos TCP/IP, en lugar de emplear redes de fibra óptica dedicadas.
233. Este tipo de redes de almacenamiento se denominan SAN, y son ampliamente utilizadas en entornos de centros de datos y en entornos virtuales para compartir dispositivos de almacenamiento entre múltiples sistemas, tanto reales como virtuales.
234. Desde el punto de vista de seguridad, es necesario emplear los mecanismos de autenticación y cifrado proporcionados por el estándar iSCSI, con las limitaciones descritas a continuación.
235. VMware ESX únicamente soporta autenticación en iSCSI mediante el protocolo CHAP (Challenge Handshake Authentication Protocol) en un único sentido (no bidireccional), y no otros mecanismos de autenticación más avanzados, como Kerberos, certificados digitales o SRP (Secure Remote Protocol). Se recomienda emplear CHAP para la autenticación del servidor VMware ESX en los dispositivos de almacenamiento iSCSI.
236. Para configurar CHAP mediante el cliente VI es necesario seleccionar el servidor del panel “Inventory”, seleccionar la pestaña “Configuration”, y en concreto la opción “Storage Adapters”. Tras seleccionar el adaptador iSCSI, es necesario seleccionar “Properties”. En la pestaña de “CHAP Authentication”, seleccionar “Configure” y definir las credenciales de CHAP: nombre (el propio del adaptador iSCSI (initiator) o uno propio) y la contraseña.

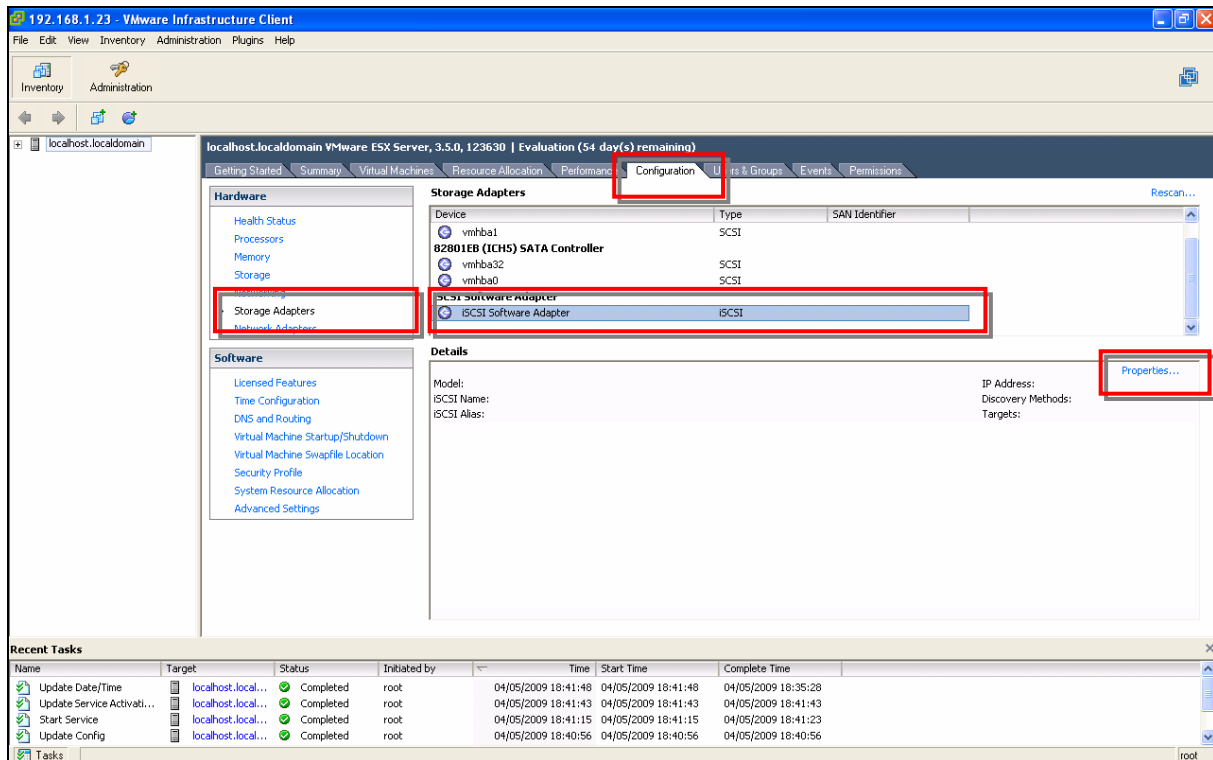


Figura 13.- Configuración de autenticación CHAP para iSCSI

237. La contraseña debe ser robusta, pero puede estar limitada por los requerimientos impuestos por el dispositivo de almacenamiento iSCSI. Se recomienda consultar la documentación del fabricante de los dispositivos de almacenamiento.
238. Las comunicaciones iSCSI en VMware ESX no están cifradas (al no soportarse IPsec), por lo que es necesario aislar la red de almacenamiento con el objetivo de evitar la interceptación de las mismas. Se recomienda crear una VLAN independiente para la red de almacenamiento y emplear un vSwitch dedicado e independiente.
239. VMware proporciona información detallada sobre la seguridad del almacenamiento con iSCSI en el entorno VMware ESX [Ref.- 11](capítulo 10).

7. RECOMENDACIONES DE CONFIGURACIÓN DE VIRTUALCENTER (VCENTER)

240. Las siguientes recomendaciones proporcionan información de seguridad complementaria para la protección de un entorno VMware ESX donde se emplea VirtualCenter (vCenter) para la gestión de los sistemas VMware ESX.
241. En primer lugar, es necesario proteger el servidor Windows donde será instalado VirtualCenter aplicando las mejores prácticas de seguridad para servidores Windows [Ref.- 4], bases de datos (empleada por VirtualCenter) y la red donde este servidor será ubicado.

242. Las recomendaciones de seguridad detalladas a continuación aplican a VMware VirtualCenter versión 2.5.0 (build 119598).
243. Se recomienda realizar un backup periódico de los ficheros de configuración más críticos de VirtualCenter y de los ficheros de log. Para ello puede emplearse la utilidad “Generate VirtualCenter Server log bundle”, disponible en el menú de “Inicio -> Programas -> VMware” del servidor de VirtualCenter.
244. Como resultado se genera un fichero .ZIP, llamado “vcsupport-FECHA-HORA.zip” y ubicado en el escritorio del usuario actual, con información relevante del entorno de VirtualCenter.

7.1. COMUNICACIONES DE RED DE VIRTUALCENTER

245. Con el objetivo de filtrar y gestionar las comunicaciones en un entorno virtual basado en VMware ESX, es necesario conocer el tráfico generado entre diferentes componentes y configurar adecuadamente las políticas de filtrado de los cortafuegos existentes en la arquitectura de red [Ref.- 11](capítulo 10).
246. Por defecto, el interfaz web de VirtualCenter emplea los puertos TCP 80 (HTTP) y 443 (HTTPS, SSL o TLS) para las comunicaciones de administración y gestión. Estos puertos son empleados tanto por el cliente VI al acceder a VirtualCenter, como por el acceso web directo mediante un navegador.
247. Se recomienda únicamente utilizar comunicaciones mediante HTTPS a través del puerto TCP/443.
248. Las comunicaciones entre VirtualCenter y los servidores ESX también se realizan a través del puerto TCP/443.
249. Adicionalmente, los servidores ESX pueden comunicarse a través del puerto UDP/902 con VirtualCenter y VirtualCenter puede comunicarse con el License Server en los puertos TCP/27000-27010.

7.2. CONFIGURACIÓN DEL SERVIDOR WEB DE VIRTUALCENTER

250. Al igual que se recomendaba modificar la página web por defecto del interfaz de administración de VMware ESX (ver sección “CONFIGURACIÓN DEL SERVIDOR WEB”), se recomienda llevar a cabo tareas similares en la página web de administración existente por defecto en VirtualCenter.
251. Se recomienda la creación de un mensaje asociado al servicio web de VirtualCenter que refleje el carácter privado del sistema, que se monitoriza su uso y que no se permite un uso no autorizado, antes de cualquier intento de acceso.

252. Para ello es necesario incluir el mensaje en el fichero que contiene la página web por defecto de administración de VirtualCenter en Windows, es decir, “C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\docRoot\index.html”, por ejemplo tras la sección “Getting Started” de la columna de la izquierda de la página web principal.
253. Siguiendo la recomendación de VMware ESX, es aconsejable modificar la página web al completo para limitar la información disponible sobre el entorno.

7.3. ACCESOS DE GESTIÓN MEDIANTE VIRTUALCENTER

254. El entorno VirtualCenter permite la gestión completa de toda la infraestructura virtual basada en VMware ESX, por lo que es fundamental restringir el acceso al mismo.
255. VirtualCenter (y en su defecto el cliente VI) permite la definición y configuración de usuarios, grupos, permisos y roles. Se recomienda establecer una política de acceso acorde a los requisitos de la organización siguiendo las pautas de la guía de configuración de VMware ESX [Ref.- 11](capítulo 11).
256. Al igual que se recomienda proporcionar un certificado digital válido para el acceso directo a VMware ESX (ver sección “ACCESO SEGURO MEDIANTE SSL O TLS”), se debe proporcionar un certificado digital válido y verificable para el acceso por SSL o TLS a VirtualCenter. La guía de VMware “Replacing VirtualCenter Server Certificates” [Ref.- 17] proporciona todos los detalles de configuración.
257. VirtualCenter emplea la cuenta de “root” para realizar la gestión inicial de un servidor ESX y añadirlo a su base de datos de equipos gestionados (Datacenter). Una vez realizada la configuración inicial, VirtualCenter crea una nueva cuenta de usuario para futuros accesos, llamada “vpxuser”. La cuenta “vimuser” es creada por defecto en la instalación de VMware ESX.
258. Opcionalmente, y únicamente para VMware ESX 3 (no ESX 3.5, que es la versión referenciada en esta guía), si sólo se pretende gestionar la infraestructura virtual mediante VirtualCenter, es posible seleccionar la opción “Enable Lockdown Mode”. Esta acción deshabilita el acceso remoto para “root” una vez que el equipo es gestionado por VirtualCenter.
259. Desde VirtualCenter, usando el menú “Inventory”, seleccionar el host VMware ESX en la columna de la izquierda. Mediante la pestaña “Configuration”, seleccionar la opción “Security Profile”. Utilizar la opción “Edit” existente junto a “Enable Lockdown Mode” (esta opción no está disponible en VMware ESX 3.5).

8. RECOMENDACIONES DE CONFIGURACIÓN DE LAS MÁQUINAS VIRTUALES (GUESTS) EN VMARE ESX

260. Se recomienda aplicar las mejores prácticas de seguridad para la creación e implementación de máquinas virtuales, independientemente del entorno virtual en el que sean desplegadas, como por ejemplo la instalación de un antivirus, firewall personal y aplicación del principio de mínimos privilegios.
261. El principio de diseño a seguir es que las máquinas virtuales, y su sistema operativo, deberían de ser protegidas con el mismo nivel de detalle que los sistemas reales.
262. Adicionalmente, se recomienda que todas las máquinas virtuales dispongan únicamente del hardware necesario para su funcionamiento y propósito.
263. Las amenazas y ataques a los que están expuestas las máquinas virtuales se detallan en la guía CCN-STIC-956 [Ref.-3].
264. Este apartado detalla recomendaciones de seguridad adicionales que deberían aplicarse en un entorno virtual basado en VMware ESX.
265. Para llevar a cabo cualquiera de los cambios de configuración detallados en las siguientes secciones es necesario que la máquina virtual a modificar esté apagada.
266. Se recomienda realizar una copia de seguridad del fichero de configuración de la máquina virtual (.vmx) antes de realizar ningún cambio.
267. La existencia y disponibilidad de los parámetros de configuración avanzados de VMware ESX [Ref.- 19] detallados en las siguientes secciones puede variar entre diferentes versiones.

8.1. DESHABILITAR OPERACIONES SOBRE EL HARDWARE DE LAS MÁQUINAS VIRTUALES

268. Los usuarios no privilegiados dentro de las máquinas virtuales pueden conectar o desconectar dispositivos hardware, como el CD-ROM o los adaptadores de red a través, por ejemplo, del *applet* de VMware Tools [Ref.- 20].
269. El impacto de que un usuario no privilegiado desconecte, por ejemplo, la tarjeta de red del sistema es muy elevado (denegación de servicio). Para evitar este tipo de acciones, se deberá limitar que se puedan llevar a cabo.
270. Mediante el cliente VI, acceder a cada máquina virtual desde “Inventory”, empleando la columna de la izquierda, y utilizando la pestaña de “Summary”, seleccionar “Edit Settings”. Seleccionar la pestaña “Options” y la opción “General Options” para identificar la ubicación en el sistema de ficheros del fichero de configuración de la máquina virtual.

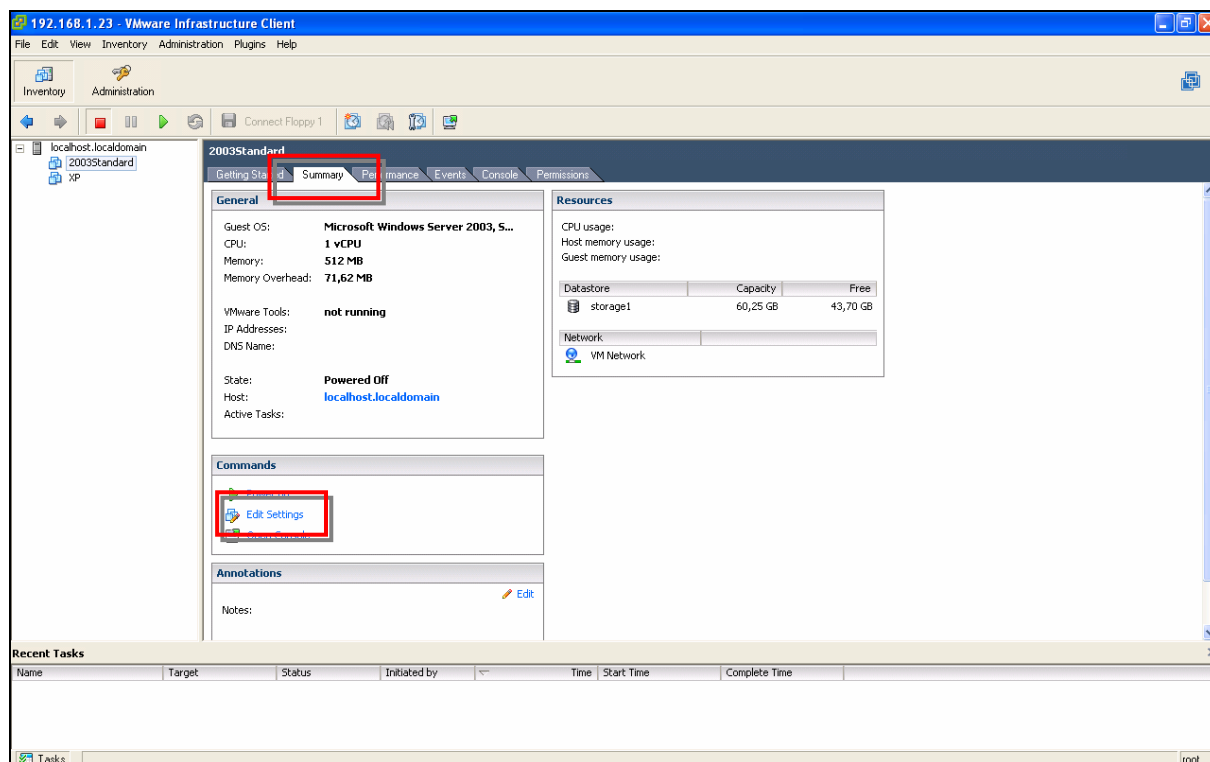


Figura 14.- Configuración de una máquina virtual en el cliente VI

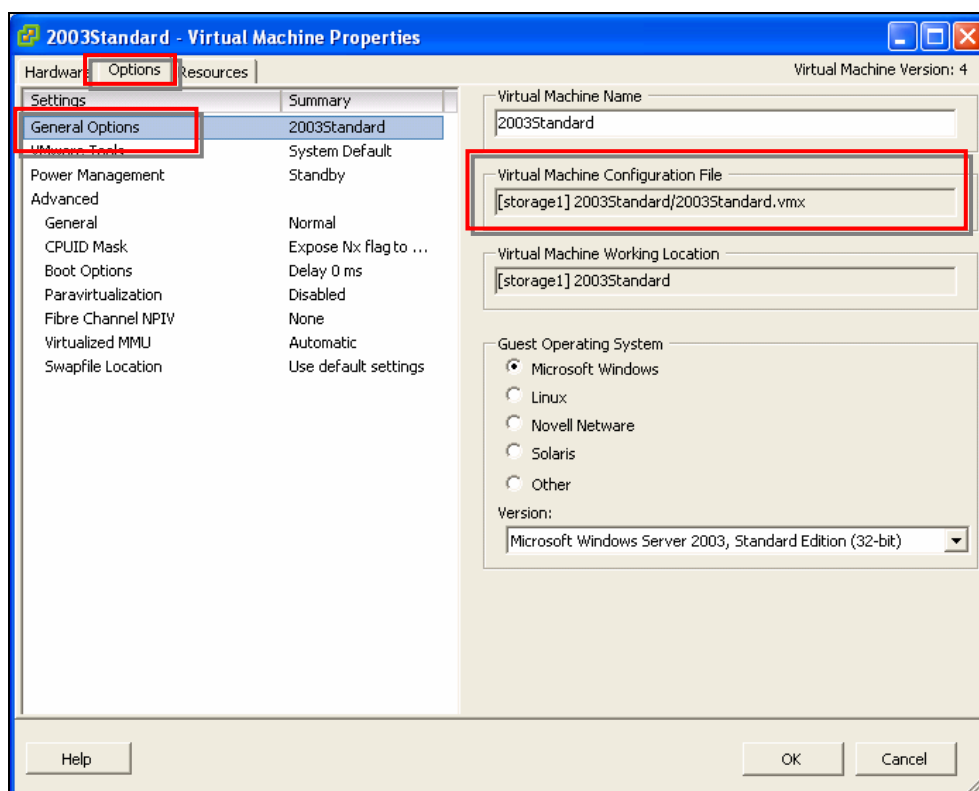


Figura 15.- Ubicación del fichero de configuración de una máquina virtual

271. Modificar el fichero de configuración (.vmx) identificado en el paso previo (dentro del directorio “/vmfs/volumes/...”), como “root” desde la consola de terminal, añadiendo las siguientes líneas para evitar la desconexión y la modificación de dispositivos respectivamente:
- isolation.tools.connectable.disable = “TRUE”
 - isolation.device.edit.disable = “TRUE”
272. Esta configuración es la recomendada cuando no se quiere eliminar un dispositivo hardware de forma permanente de la máquina virtual, porque, por ejemplo, va a ser usado en el futuro.
273. Los parámetros de restricción de operaciones a través de VMware Tools comienzan por “isolation.tools”.
274. En versiones previas de VMware ESX (y VMware GSX) para cada dispositivo hardware a deshabilitar en la máquina virtual (por ejemplo, donde “<dispositivo>” es “ethernet1”, “floppy0”, “serial0”, “parallel0”, etc), debía añadirse una línea como la siguiente:
- <dispositivo>.allowGuestConnectionControl = “FALSE”
275. La próxima vez que se reinicie la máquina virtual con el nuevo fichero de configuración no debería disponer de acceso a los dispositivos que han sido deshabilitados.
276. El método mostrado permite establecer los parámetros avanzados de configuración de VMware ESX directamente en el fichero de configuración (.vmx), lo que permite automatizar el proceso en múltiples máquinas virtuales. Posteriormente se mostrará un método similar, pero más sencillo desde el punto de vista de configuración, basado en el establecimiento de los parámetros de configuración a través del interfaz gráfico del cliente VI o de VirtualCenter.
277. Una vez realizados los cambios en el fichero de configuración, es muy importante verificar que éstos se reflejan en el cliente VI (ver siguiente sección).

8.2. DESHABILITAR LA OPCIÓN DE COPIAR Y PEGAR ENTRE MÁQUINAS VIRTUALES Y EL HOST

278. La funcionalidad de copiar y pegar datos entre máquinas virtuales y el servidor (o host) es útil en entornos virtuales de cliente (como los basados en VMware Player o Workstation), pero no se recomienda su uso en entornos de servidor, como VMware ESX, donde el objetivo es obtener el mayor aislamiento posible entre máquinas virtuales.

279. Esta funcionalidad es un riesgo de seguridad, ya que habilita un canal de comunicación entre las máquinas virtuales y el servidor, y entre distintas máquinas virtuales, que potencialmente podría ser empleado para acciones maliciosas. Por ejemplo, se podría tener acceso a información confidencial disponible en el portapapeles de otro sistema.

280. Mediante el cliente VI, acceder a cada máquina virtual desde “Inventory”, empleando la columna de la izquierda, y utilizando la pestaña de “Summary”, seleccionar “Edit Settings”. Seleccionar “Options”, “General” dentro de la categoría “Advanced”, y el botón “Configuration Parameters”, para gestionar los parámetros de configuración de las máquinas virtuales.

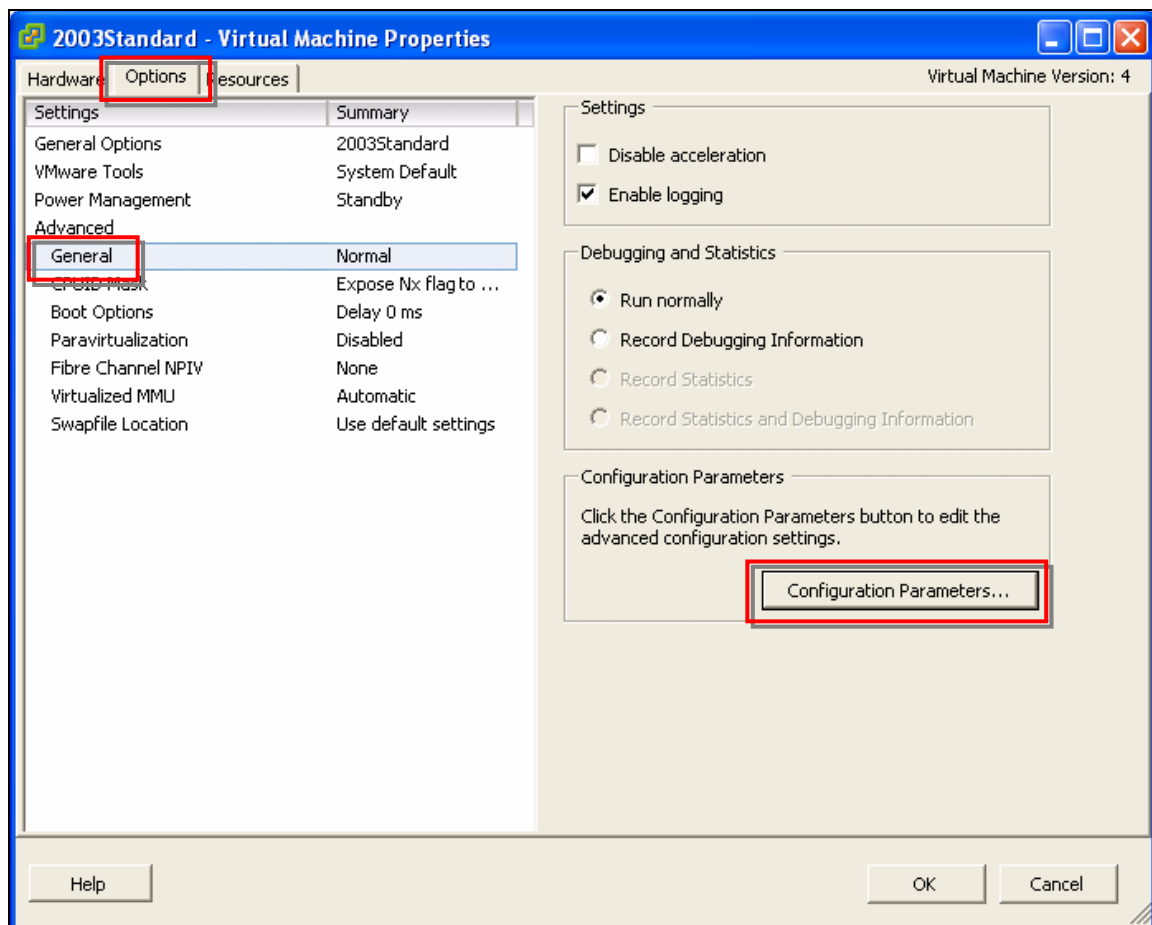


Figura 16.- Configuración de los parámetros de una máquina virtual desde el cliente VI

281. Añadir los tres parámetros siguientes (identificados como pares, nombre y valor) mediante el botón “Add Row”:

- isolation.tools.copy.disable: true
- isolation.tools.paste.disable: true
- isolation.tools.setGUIOptions.enable: false

282. El método mostrado permite establecer los parámetros avanzados de configuración de VMware ESX a través del interfaz gráfico del cliente VI o de VirtualCenter, simplificando el proceso de configuración. Previamente se ha mostrado un método similar, basado en el establecimiento de los parámetros de configuración directamente en el fichero de configuración (.vmx), mecanismo más complejo pero que permite automatizar el proceso en múltiples máquinas virtuales.

8.3. GESTIÓN Y ROTACIÓN DE LOS LOGS DE LAS MÁQUINAS VIRTUALES

283. Es necesario definir y establecer mecanismos de gestión y rotación de los logs generados por las máquinas virtuales para evitar que ocupen espacio innecesario en el sistema de almacenamiento del servidor del entorno de virtualización.
284. Por defecto, la rotación de ficheros de log en VMware ESX se realiza en las operaciones de encendido y apagado de las máquinas virtuales, y se conservan únicamente 6 ficheros de log (más el original). Es posible cambiar el criterio de rotación y basarlo en función del tamaño del fichero de log.
285. Mediante el cliente VI, acceder a cada máquina virtual desde “Inventory”, empleando la columna de la izquierda, y utilizando la pestaña de “Summary”, seleccionar “Edit Settings”. Seleccionar “Options”, “General” dentro de la categoría “Advanced”, y el botón “Configuration Parameters”, para gestionar los parámetros de configuración de las máquinas virtuales. Añadir los siguientes parámetros para establecer la rotación en función del tamaño del fichero de log y el número de ficheros de log a mantener respectivamente:

- log.rotateSize: <tamaño máximo del fichero de log>
- log.keepOld: <número de ficheros de log a mantener>

286. Por ejemplo, 10 ficheros de log (más el original, sin número) de 100KB cada uno:

- log.rotateSize: 100000
- log.keepOld: 10

8.4. EVITAR QUE LAS MÁQUINAS VIRTUALES DESBORDEN CON LOGS AL SERVIDOR VMWARE ESX

287. Las máquinas virtuales pueden enviar mensajes informativos al servidor VMware ESX a través de VMware Tools, denominados mensajes setinfo. El nivel de log “setinfo” puede generar excesivos mensajes de log desde las máquinas virtuales hacia el servidor VMware ESX, llegando a desbordar y saturar la memoria o disco del servidor.

288. Se recomienda fijar el tamaño máximo de memoria dedicada a este propósito, que por defecto es 1MB (valor más que suficiente). Esta acción no afecta al resto de logs de las máquinas virtuales, que seguirán almacenándose en el fichero “/vmfs/volume/storageN/<máquina_virtual>/vmware.log”.

289. Mediante el cliente VI, acceder a cada máquina virtual desde “Inventory”, empleando la columna de la izquierda, y utilizando la pestaña de “Summary”, seleccionar “Edit Settings”. Seleccionar “Options”, “General” dentro de la categoría “Advanced”, y el botón “Configuration Parameters”, para gestionar los parámetros de configuración de las máquinas virtuales. Añadir el siguiente parámetro:

- tools.setInfo.sizelimit: <número de bytes>

Por ejemplo, para fijar un tamaño de 1 MB:

- tools.setInfo.sizelimit: 1048576

290. Existe la posibilidad de deshabilitar por completo el nivel de log “setinfo” de VMware Tools mediante el siguiente parámetro:

- isolation.tools.setinfo.disable: true

291. Si se deshabilita por completo este canal de comunicación, la dirección IP y el nombre de la máquina virtual no se mostrarán en el cliente VI [Ref.- 20]. Por tanto, se recomienda limitar el tamaño de memoria asignada para este propósito, y no deshabilitar por completo la comunicación de mensajes “setinfo”.

292. Adicionalmente, VMware ESX permite la generación de logs por parte de un usuario no privilegiado hacia el host mediante el “backdoor” de comunicación implementado mediante el binario “VMwareService.exe” (por ejemplo, en máquinas virtuales Windows) [Ref.- 20].

293. Es posible deshabilitar el “backdoor” para la generación de logs, y no así los logs generales de la máquina virtual, mediante el siguiente parámetro:

- isolation.tools.log.disable: true

8.5. LIMITAR OPERACIONES DE MODIFICACIÓN DE LOS DISCOS VIRTUALES

294. Los usuarios no privilegiados de las máquinas virtuales pueden realizar operaciones de modificación de los discos virtuales a través del *applet* de VMware Tools. Por ejemplo la operación de *shrinking*, operación que permite liberar el espacio en disco en el host que está libre en el disco virtual.

295. Esta operación sobre los discos, invocada numerosas veces, puede dar lugar a una denegación de servicio, ya que hace un uso intensivo de la CPU del sistema. Para evitar este tipo de acciones, se recomienda limitar que esta operación se pueda llevar a cabo.

296. Mediante el cliente VI, acceder a cada máquina virtual desde “Inventory”, empleando la columna de la izquierda, y utilizando la pestaña de “Summary”, seleccionar “Edit Settings”. Seleccionar “Options”, “General” dentro de la categoría “Advanced”, y el botón “Configuration Parameters”, para gestionar los parámetros de configuración de las máquinas virtuales. Añadir los siguientes parámetros:

- isolation.tools.diskWiper.disable: true
- isolation.tools.diskShrink.disable: true

8.6. SINCRONIZACIÓN DE TIEMPO ENTRE LAS MÁQUINAS VIRTUALES Y EL HOST

297. Los usuarios no privilegiados de las máquinas virtuales pueden configurar si se sincroniza el tiempo entre la máquina virtual y el host, o no, a través del applet de VMware Tools, y concretamente la opción “Time synchronization between the virtual machine and the host operating system”.

298. La manipulación de la configuración de tiempo podría conllevar un desajuste del reloj entre la máquina virtual y el host al ser deshabilitada, lo que daría lugar a inconsistencias en la generación de registros de tiempo, por ejemplo, en los logs. Para evitar este tipo de acciones, se recomienda limitar que esta operación se pueda llevar a cabo.

299. Mediante el cliente VI, acceder a cada máquina virtual desde “Inventory”, empleando la columna de la izquierda, y utilizando la pestaña de “Summary”, seleccionar “Edit Settings”. Seleccionar “Options”, “General” dentro de la categoría “Advanced”, y el botón “Configuration Parameters”, para gestionar los parámetros de configuración de las máquinas virtuales. Añadir el siguiente parámetro:

- isolation.tools.setOption.disable: true

8.7. DESHABILITAR EL ARRANQUE MEDIANTE PXE

300. En el caso de máquinas virtuales almacenadas en discos en red, como por ejemplo en SAN iSCSI, existe una vulnerabilidad en el proceso de arranque si los discos iSCSI no están disponibles [Ref.- 20].

301. El fichero de configuración de la máquina virtual (.vmx) se almacena en el disco iSCSI, pero también en la memoria del servidor ESX. Si no se tiene acceso al disco, la máquina virtual no puede arrancar. En ese caso, recorre la lista de dispositivos de arranque, hasta llegar a la opción PXE, arranque a través de la red.

302. Un atacante podría lanzar una denegación de servicio en la red para hacer que los discos no estuvieran disponibles, y simultáneamente, proporcionar un servidor PXE para que las máquinas virtuales arrancaran de éste con las imágenes seleccionadas por el atacante, que podrían incluir herramientas para la realización de otros ataques. Para evitar este tipo de ataque, se deberá deshabilitar el arranque mediante PXE.
303. Mediante el cliente VI, acceder a cada máquina virtual desde “Inventory”, empleando la columna de la izquierda, y utilizando la pestaña de “Summary”, seleccionar “Edit Settings”. Seleccionar “Options”, “General” dentro de la categoría “Advanced”, y el botón “Configuration Parameters”, para gestionar los parámetros de configuración de las máquinas virtuales. Añadir los siguientes parámetros:
- vlance.noOprom: true
 - vmxnet.noOprom: true

8.8. RESUMEN DE LOS PARÁMETROS DE CONFIGURACIÓN AVANZADOS DE LAS MÁQUINAS VIRTUALES

304. La siguiente lista resume todos los parámetros de configuración avanzados que se recomienda aplicar sobre el fichero de configuración de cada máquina virtual:

```
isolation.tools.connectable.disable = "true"
isolation.device.edit.disable = "true"
isolation.tools.copy.disable = "true"
isolation.tools.paste.disable = "true"
isolation.tools.setGUIOptions.enable = "false"
log.rotateSize = "100000"
log.keepOld = "10"
tools.setInfo.sizelimit = "1048576"
isolation.tools.log.disable = "true"
isolation.tools.diskWiper.disable = "true"
isolation.tools.diskShrink.disable = "true"
isolation.tools.setOption.disable = "true"
vlance.noOprom = "true"
vmxnet.noOprom = "true"

vmware.tools.requiredversion = "7302"
```

8.9. PERMISOS DE LOS FICHEROS DE LAS MÁQUINAS VIRTUALES

305. Los ficheros de las máquinas virtuales deberían tener los siguientes permisos, propietario y grupo:

Directorio o fichero	Extensión	Permisos	Propietario	Grupo
Fichero de configuración	.vmx	755	root	root
Ficheros de discos virtuales	.vmdk	600	root	root
Ficheros de log	.log	644	root	root

Tabla 3.- Permisos de los ficheros de las máquinas virtuales

8.10.EVITAR EL USO DE DISCOS NO PERSISTENTES EN LAS MÁQUINAS VIRTUALES

306. Los discos no persistentes de una máquina virtual VMware no guardan los cambios asociados al disco tras el apagado o re arranque de la máquina virtual.
307. Desde el punto de vista de seguridad, el uso de discos no persistentes permitiría a un atacante eliminar todas las trazas y eventos maliciosos realizados y almacenados en el disco.
308. Se recomienda por tanto evitar el uso de discos no persistentes, de forma que cualquier acción llevada a cabo por el atacante quede registrada en los discos y pueda realizarse un análisis forense posterior a un incidente de seguridad en el caso de ser necesario.
309. Es posible configurar el modo de todos los discos de una máquina virtual a través del cliente VI. Seleccionar la máquina virtual de la columna de la izquierda en el panel “Inventory”, acceder a la opción “Edit Settings” y a la pestaña “Hardware”. Para cada disco, seleccionarlo y verificar (y en su caso cambiar) el modo de operación del mismo.

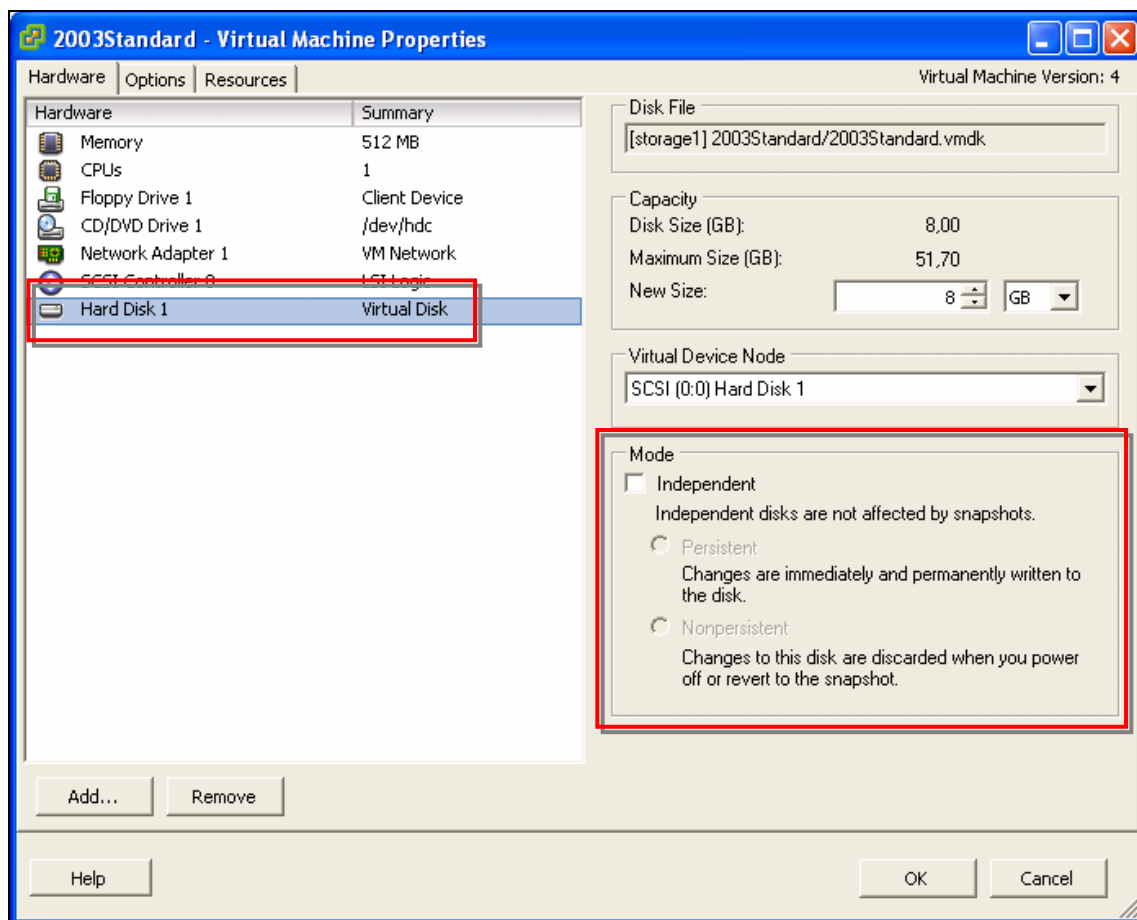


Figura 17.- Configuración de los discos virtuales en modo no persistente

ANEXO A. LISTA DE LOS SERVICIOS MÍNIMOS RECOMENDADOS EN VMWARE ESX

La siguiente lista detalla los servicios mínimos necesarios para el funcionamiento de VMware ESX (arrancados en los niveles 1, 2 y 3 de ejecución de Linux):

```
/etc/rc3.d/S00microcode_ctl
/etc/rc3.d/S00vmkstart
/etc/rc3.d/S01vmware
/etc/rc3.d/S02mptctlnd
/etc/rc3.d/S09firewall
/etc/rc3.d/S10network
/etc/rc3.d/S12syslog
/etc/rc3.d/S13irqbalance
/etc/rc3.d/S14ipmi
/etc/rc3.d/S20random
/etc/rc3.d/S55sshd
/etc/rc3.d/S55vmware-late
/etc/rc3.d/S56rawdevices
/etc/rc3.d/S56xinetd
/etc/rc3.d/S58ntpd (OPCIONAL)
/etc/rc3.d/S85gpm
/etc/rc3.d/S85vmware-webAccess
/etc/rc3.d/S90crond
/etc/rc3.d/S97vmware-vmkauthd
/etc/rc3.d/S98mgmt-vmware
/etc/rc3.d/S99local
/etc/rc3.d/S99pegasus
/etc/rc3.d/S99vmware-autostart
/etc/rc3.d/S99wsman
```

ANEXO B. LISTADO DE PERMISOS DE LOS FICHEROS DE CONFIGURACIÓN DE VMWARE ESX (/ETC/VMWARE)

La siguiente lista detalla los permisos, propietario y grupo de los ficheros de configuración de VMware ESX, disponibles en el directorio “/etc/vmware”:

Directorio o fichero	Permisos	Propietario	Grupo
/etc/vmware/backuptools.conf	-rw-----	root	root
/etc/vmware/config	-rw-r--r--	root	root
/etc/vmware/configrules	-rw-r--r--	root	root
/etc/vmware/esx_checksum.conf	-rw-r--r--	root	root
/etc/vmware/esx.conf	-rw-----	root	root
/etc/vmware/firewall	drwxr-xr-x	root	root
/etc/vmware/hostd	drwxr-xr-x	root	root
/etc/vmware/ima_plugin.conf	-rw-r--r--	root	root
/etc/vmware/ima_plugin.conf.ima-qla4xxx.rpmsave	-rw-r--r--	root	root
/etc/vmware/init	drwxr-xr-x	root	root
/etc/vmware/keying	drwxr-xr-x	root	root
/etc/vmware/license.cfg	-rw-r--r--	root	root
/etc/vmware/locations	-rw-r--r--	root	root
/etc/vmware/logfilters	-rw-r--r--	root	root
/etc/vmware/patchdb	drwxr-xr-x	root	root
/etc/vmware/pci.classlist	-rw-r--r--	root	root
/etc/vmware/pciid	drwxr-xr-x	root	root
/etc/vmware/pci.ids	-rw-r--r--	root	root
/etc/vmware/pcitable	-rw-r--r--	root	root
/etc/vmware/pcitable.Linux	-rw-r--r--	root	root
/etc/vmware/pci.xml	-rw-r--r--	root	root
/etc/vmware/pci.xml.merged	-rw-r--r--	root	root
/etc/vmware/service	drwxr-xr-x	root	root
/etc/vmware/shutdown	drwxr-xr-x	root	root
/etc/vmware/simple.map	-rw-r--r--	root	root
/etc/vmware/snmp.xml	-rw-r--r--	root	root
/etc/vmware/ssl	drwxr-xr-x	root	root
/etc/vmware/storageMonitor.conf	-rw-r--r--	root	root
/etc/vmware/UserWorldBinaries.txt	-rw-r--r--	root	root
/etc/vmware/vmfs3queue	-rw-r--r--	root	root
/etc/vmware/vmware-cim-config.xml	-rw-r--r--	root	root
/etc/vmware/vmware-devices.map	-rw-r--r--	root	root
/etc/vmware/webAccess	drwxr-xr-x	root	root

ANEXO C. CHECKLIST

La siguiente lista de comprobaciones o checklist resume las diferentes recomendaciones detalladas a lo largo de la presente guía:

1. DISEÑO Y ARQUITECTURA DEL ENTORNO DE VIRTUALIZACIÓN

- ☐ Selección de los mecanismos de administración y gestión de VMware ESX.
- ☐ Diseño y definición de la arquitectura de red del entorno VMware ESX:
 - ☐ Red de gestión.
 - ☐ Red de backup.
 - ☐ Red de migración de máquinas virtuales con VMotion.
 - ☐ Red(es) de servicio.
 - ☐ Red de almacenamiento (iSCSI).

2. INSTALACIÓN DE VMWARE ESX

- ☐ Contraseña en la BIOS.
- ☐ Definición en la BIOS de la secuencia de arranque.
- ☐ Limitación en la BIOS de los dispositivos de arranque.
- ☐ Definición de las particiones: tamaño de cada una y sistema de ficheros: (tamaño mínimo recomendado, 5GB, excepto para /boot, 300 MB)
 - ☐ Particiones de los usuarios aisladas (/home y /tmp).
 - ☐ Partición de arranque (/boot) en partición independiente.
 - ☐ Partición variable de logs aislada (/var).
 - ☐ Configuración final:

Partición en disco	Punto de Montaje	Tamaño	Sistema de Ficheros
	/		
	<swap>		
	/boot		
	/home		
	/tmp		
	/var		

- ☐ Configuración de la red por defecto de las máquinas virtuales (deshabilitada).
- ☐ Configuración de contraseña en el gestor de arranque GRUB.
- ☐ Configuración de autenticación para el arranque en modo mono usuario.
- ☐ Deshabilitar la conexión de dispositivos USB al servidor VMware ESX.

3. ACTUALIZACIÓN DE SOFTWARE DE VMWARE ESX

- ☐ Actualización completa del sistema VMware ESX.

4. ACCESO AL ENTORNO VMWARE ESX

- ☐ Establecimiento del mecanismo de bloqueo de cuentas de usuario.
- ☐ Evitar que el bloqueo de cuenta por intentos fallidos aplique al usuario root.

- ☐ Verificar que el acceso mediante SSH con el usuario root está deshabilitado.
- ☐ Crear un usuario no privilegiado (con acceso a shell) para el acceso mediante SSH.
- ☐ Permitir únicamente el uso de “su” a los usuarios del grupo “wheel”.
- ☐ Limitar el acceso directo del usuario root a través de la consola (OPCIONAL).
- ☐ Verificar que los usuarios no privilegiados no disponen de acceso a shell (1).

- ☐ Creación de un mensaje (o *banner*) de acceso al sistema mediante SSH.
- ☐ Creación y modificación de los diferentes ficheros de mensajes de acceso.
- ☐ Creación de un mensaje (o *banner*) de acceso al sistema mediante web.

- ☐ Creación de la política de contraseñas para todos los usuarios, incluido root.
- ☐ Creación de un mecanismo histórico de contraseñas.
- ☐ Creación de la política de caducidad y renovación de contraseñas.

- ☐ Configuración de sudo.

- ☐ Instalación de certificados digitales válidos para SSL en el servidor web.

NOTA (1): Salvo la excepción previa: usuario con acceso a shell para accesos como root.

5. SEGURIDAD DE LAS COMUNICACIONES EN VMWARE ESX

- ☐ Creación de una red de gestión dedicada.

- ☐ Deshabilitar el modo promiscuo en todos los switches de red virtuales.
- ☐ Deshabilitar cambios en la dirección MAC en todos los switches de red virtuales.
- ☐ Deshabilitar el envío de tramas falsas en todos los switches de red virtuales.

- ☐ Configuración del firewall (iptables) del servidor de gestión de VMware ESX.
 - ☐ Bloquear por defecto tráfico entrante.
 - ☐ Bloquear por defecto tráfico saliente.
 - ☐ Verificar y modificar la política de filtrado de tráfico.

6. SERVICIOS EN VMWARE ESX

- ☐ Verificación de la lista de servicios activos (ver apéndice A).
- ☐ Verificación de la lista de puertos activos y escuchando en todos los interfaces.
- ☐ Verificación de la lista de puertos activos y escuchando en localhost.
- ☐ Habilitar el servicio NTP (Network Time Protocol).

7. PERMISOS DE FICHEROS CRÍTICOS EN VMWARE ESX

- ☐ Verificación de los permisos de los ficheros de “/etc” (ver apartado “6.4.1”).
- ☐ Verificación de los permisos de los ficheros de “/etc/vmware” (ver apéndice B).
- ☐ Deshabilitar los bits setuid o setgid en ficheros dónde éstos son opcionales.

8. LOGGING Y REGISTRO DE EVENTOS

- ☐ Habilitar la compresión de los ficheros de log.
- ☐ Incrementar el tamaño máximo de los ficheros de log.
- ☐ Configuración de un servidor de syslog remoto.

9. CONFIGURACIÓN DEL ALMACENAMIENTO EN RED (ISCSI)

- ☐ Configuración de autenticación CHAP en iSCSI.
- ☐ Verificar que se dispone de una red de almacenamiento independiente.

10. VIRTUALCENTER (vCENTER)

- ☐ Configurar la política de filtrado de tráfico para el acceso a VirtualCenter.
- ☐ Configurar la política de filtrado de tráfico entre VirtualCenter y VMware ESX.
- ☐ Configurar la política de filtrado de tráfico entre VirtualCenter y License Server.
- ☐ Creación de un mensaje (o *banner*) de acceso a VirtualCenter mediante web.
- ☐ Definición de usuarios, grupos, permisos y roles para el acceso a VirtualCenter.
- ☐ Habilitar la opción de gestión exclusiva mediante VirtualCenter (OPCIONAL).

11. MÁQUINAS VIRTUALES (GUESTS) EN VMWARE ESX

- ☐ Aplicación de recomendaciones de seguridad generales según el sistema operativo.
- ☐ Deshabilitar dispositivos hardware no necesarios en las máquinas virtuales.

- ☐ Deshabilitar la opción de copiar y pegar entre máquinas virtuales y ESX.
- ☐ Establecer los mecanismos de gestión y rotación de logs de las máquinas virtuales.
- ☐ Limitar los mensajes informativos (setinfo) desde las máquinas virtuales al host.
- ☐ Deshabilitar los mensajes de log (backdoor) desde las máquinas virtuales al host.
- ☐ Limitar las operaciones de modificación de los discos virtuales.
- ☐ Sincronización de tiempo entre las máquinas virtuales y el host.
- ☐ Deshabilitar el arranque mediante PXE.
- ☐ Verificación de los permisos de los ficheros de las máquinas virtuales.
- ☐ Evitar el uso de discos no persistentes en las máquinas virtuales.

ANEXO D. REFERENCIAS

- [Ref.- 1] VMware.
URL: <http://www.vmware.com>
- [Ref.- 2] VMware ESX (o VMware Infrastructure). VMware.
URL: <http://www.vmware.com/products/vi/>
URL: <http://www.vmware.com/products/vi/esx/>
- [Ref.- 3] CCN-STIC-956. “Seguridad en Entornos de Computación Virtuales (Virtualización de Sistemas)”. CCN-CERT. (Acceso restringido).
URL: <https://www.ccn-cert.cni.es/privateDocs/protegido/ccn-stic/CCN-STIC-956.htm>
- [Ref.- 4] Guías de seguridad CCN-STIC. CCN-CERT. (Acceso restringido).
URL: https://www.ccn-cert.cni.es/index.php?option=com_passthru&task=read&filerequested=protegido/ccn-stic/index.htm&Itemid=134
- [Ref.- 5] VMware ESX Hardware Compatibility List (HCL) and Guide. VMware.
URL: <http://www.vmware.com/resources/compatibility/search.php>
URL: http://www.vmware.com/pdf/vi3_35/esx_3/r35/vi3_35_25_compat_matrix.pdf
- [Ref.- 6] “Quick Start Guide”. Update 2 and later for ESX Server 3.5 and VirtualCenter 2.5. VMware.
URL: http://www.vmware.com/pdf/vi3_35/esx_3/r35u2/vi3_35_25_u2_quickstart.pdf
URL: http://www.vmware.com/support/pubs/vi_pages/vi_pubs_35u2.html
URL: http://www.vmware.com/support/pubs/vi_pubs.html
- [Ref.- 7] CCN-STIC-614. “Seguridad RedHat Linux (FEDORA)”. CCN-CERT. (Acceso restringido).
URL: <https://www.ccn-cert.cni.es/privateDocs/protegido/ccn-stic/CCN-STIC-614.htm>
- [Ref.- 8] “VMware Infrastructure 3 Security Hardening (for ESX 3.5 & VC 2.5)”. VMware.
URL: <http://www.vmware.com/resources/techresources/726>
- [Ref.- 9] “VMware vCenter Update Manager”. VMware.
URL: <http://www.vmware.com/products/vi/updatemanager.html>
- [Ref.- 10] VMware ESX Server 3. “Best Practices for VMware ESX Server 3”. VMware.
URL: http://www.vmware.com/pdf/esx3_best_practices.pdf
- [Ref.- 11] “ESX Server 3 Configuration Guide”. Update 2 and later for ESX Server 3.5 and VirtualCenter 2.5. VMware.
URL: http://www.vmware.com/pdf/vi3_35/esx_3/r35u2/vi3_35_25_u2_3_server_config.pdf
- [Ref.- 12] VMware Security Portal.
URL: <http://www.vmware.com/security/>
- [Ref.- 13] “VMware Support: Download Patches”. VMware.
URL: <http://support.vmware.com/selfsupport/download/>
URL: http://www.vmware.com/download/vi/vi3_patches.html
- [Ref.- 14] “Patch Management for ESX Server 3”. VMware.
URL: http://www.vmware.com/pdf/esx3_esxupdate.pdf
- [Ref.- 15] “Securing and Hardening Red Hat Linux Production Systems”. “ Locking User Accounts After Too Many Login Failures”. Werner Puschitz.
URL: <http://www.puschitz.com/SecuringLinux.shtml#LockingUserAccountsAfterTooManyLoginFailures>

- [Ref.- 16] "Securing and Hardening Red Hat Linux Production Systems". " Restricting su Access to System and Shared Accounts". Werner Puschitz.
URL: <http://www.puschitz.com/SecuringLinux.shtml#RestrictingSuAccessToSystemAndSharedAccounts>
- [Ref.- 17] "Replacing VirtualCenter Server Certificates". VMware Infrastructure 3. VMware.
URL: http://www.vmware.com/pdf/vi_vcserver_certificates.pdf
- [Ref.- 18] "Networking Virtual Machines". Jon Hall. VMWorld 2006.
URL: <http://download3.VMware.com/vmworld/2006/TAC9689-A.pdf>
- [Ref.- 19] "VMX-file parameters". Ulli Hankeln.
URL: <http://www.sanbarrow.com/vmx.html>
- [Ref.- 20] "Hardening the VMX File: How Your Servers May Already be Owned by Your Users". Virtual Foundry. Robert Patton.
URL: <http://virtualfoundry.blogspot.com/2009/04/hardening-vmx-file.html>
URL: <http://virtualfoundry.blogspot.com/2009/04/hardening-vmx-file-redux.html>
- [Ref.- 21] "VMinform: Securing your virtual infrastructure".
URL: <http://www.vminformer.com>