ÍNDEX

Versió	Redactat / revisat per	Aprovat per	Data aprovació	Data publicació
1.0.	CTTI – Qualitat i Seguretat	Comitè de Direcció del CTTI	26/05/2006	01/06/2006
2.0	CTTI – QSRaP	CTTI - QSRaP	4/5/2009	18/5/2009

Estàndard signat digitalment pel:

Generalitat de Catalunya

Centre de Telecomunicacions i Tecnologies de la Informacio
Estàndard aprovat
Barcelona
2009.05.18 09:54:50 +02'00'

RESPONSABLE DEL DOCUMENT: CTTI – Qualitat, Seguretat i Relació amb Proveïdors

RESUM

OBJECTIU

Definir els controls a aplicar per a la protecció d'entorns de virtualització de servidors amb *VMware*, amb l'objectiu de garantir la confidencialitat, integritat i disponibilitat de la informació i serveis suportats per aquests sistemes.

ÀMBIT

Sistemes virtuals *VMware* de la Generalitat de Catalunya.

A més d'aquesta guia, s'hauria de complir allò que estigui establert a qualsevol altra guia d'administració de sistemes en general i de Windows en particular, ja que en aquesta guia s'identifiquen els controls específics per garantir un mínim de seguretat en els equips amb sistema operatiu Windows.

DESCRIPCIÓ

Es recullen els controls de seguretat orientats a garantir la confidencialitat, privacitat, integritat i disponibilitat de la informació de sistemes virtualització *VMWare*.

Cal remarcar que les configuracions de seguretat indicades en aquesta guia, caldrà provar-les en un entorn de proves abans d'aplicar-les en servidors que estiguin en explotació.

1 OBJECTIU

L'ús de sistemes virtuals és una tècnica cada vegada més utilitzada en els entorns de processament de la informació. Per tant, es requereix que aquests entorns es configurin i s'operin seguint uns criteris de seguretat que garanteixin la integritat, confidencialitat i disponibilitat de la informació i dels serveis que proporcionen.

Des del punt de vista de la seguretat, els sistemes virtuals ofereixen avantatges en diferents aspectes:

- Definir diferents entorns aïllats tant en l'aspecte de programari com de maquinari. Una fallada en un dels sistemes no afecta a la resta.
- Possibilitat de disposar d'una manera ràpida d'un nou entorn operatiu per assegurar la continuïtat d'un servei en explotació.
- Possibilitat de construir entorns de proves d'una manera ràpida i fàcil on provar actualitzacions de seguretat de diferents programaris.

L'objectiu d'aquesta guia és el de proporcionar uns controls de seguretat a implantar en la configuració i explotació dels sistemes virtuals. No és l'objectiu contemplar les tasques pròpies d'administració d'aquests sistemes ni tampoc els sistemes que contenen les diferents *màquines virtuals*.

S'anomena *màquina virtual* al sistema que s'instal·la sobre una plataforma que ofereix els recursos necessaris (processador, memòria, disc, xarxa) per l'execució d'aquest sistema sobre un mateix entorn físic (maquinari). D'aquesta manera, és possible tenir vàries *màquines virtuals* sobre un mateix maquinari. Això permet optimitzar els recursos de maquinari i adaptar-se a les necessitats de sistemes de processament de la informació de cada moment.

Els mateixos controls de seguretat aplicats als sistemes físics han de ser aplicats als sistemes virtuals (programari antivirus, permisos, etc.). És erroni pensar que els sistemes virtuals no requereixen d'establir controls de seguretat.

Aquesta guia està basada amb l'ús d'un programari comercial de sistemes virtuals anomenat *VMware* (www.vmware.com) utilitzat en els Serveis Centrals de la Generalitat de Catalunya. Entre tota la gamma de productes, en aquesta guia es fa referència a dos d'ells:

ESX Server

Programari que realitza l'abstracció de la capa de maquinari d'un sistema, possibilitant la creació de diferents entorns virtuals per sobre d'aquesta capa. No requereix de sistema operatiu, ja que està inclòs. S'utilitza en entorns grans de processament d'informació. Disposa d'una consola de servei per l'administració en Linux, basada amb una distribució RedHat protegida (servidor web *Apache* protegit, serveis innecessaris o insegurs inhabilitats, etc.).

Virtual Center

Es el programari que permet via web la gestió centralitzada dels diferents sistemes virtuals que estiguin desplegats, mitjançant un sol punt de control. El canal de gestió del *VirtualCenter* és xifrat usant una contrasenya generada pseudo-aleatòriament que és única per cada *ESX Server*.

2 ÀMBIT I VIGÈNCIA

Aquesta guia va destinada als administradors i responsables de planificació, manteniment i explotació dels sistemes virtuals *VMware* de la Generalitat de Catalunya.

Entrarà en vigor el dia 18 de maig de 2009.

Aquesta guia romandrà vigent fins la propera versió aprovada de la mateixa.

És d'obligat compliment en l'àmbit dels *Serveis TIC Centrals*.

3 COMPLIMENT AMB ELS REQUISITS LEGALS I ESTÀNDARDS DE SEGURETAT

La present guia proporciona cobertura a aspectes recollits en els següents controls de la ISO 27002:2005:

- 6.2.3 Requeriments de seguretat en els acords amb les terceres parts
- 10.10.1 Registres d'auditoria (logging)
- 10.10.6 Sincronització de rellotges
- 11.4.4 Protecció dels ports de configuració i diagnòstic remot
- 11.5.1 Processos de connexió segurs

- 11.5.3 Sistema de gestió de les contrasenyes
- 11.6.1 Restricció d'accés a la informació
- 11.6.2 Aïllament de sistemes sensibles
- 12.5.3 Restriccions en els canvis als paquets de programari
- 13.1.1 Notificar dels esdeveniments de seguretat

4 DESCRIPCIÓ DELS CONTROLS

Es presenten a continuació els possibles controls de seguretat orientats a garantir la confidencialitat, privacitat, integritat i disponibilitat de la informació en els entorns implantats amb sistemes virtuals *VMware*. Sota la columna "categoria", s'especifiquen els aspectes de seguretat que cada control reforça (confidencialitat– C, integritat– I, disponibilitat– D).

En diferents controls es parla de commutadors virtuals. Fa referència a la pròpia infraestructura de xarxa virtual que proporciona *VMware* per a la definició de xarxes virtuals que permeten segregar entorns de comunicació.

4.1. IN- Instal·lació i manteniment

OBJECTIUS	
Definir els controls a tenir en compte a l'hora d'instal·lar un nou sistema *VMware* i el seu posterior manteniment.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C1. Es minimitzarà la instal·lació de programari a la consola de servei per a reduir el risc d'obrir forats de seguretat. Si cal instal·lar nou programari, es comprovarà que no s'hagi causat cap problema de seguretat una vegada finalitzada la instal·lació.	I D
C2. Es mantindran els sistemes actualitzats amb els pegats de seguretat que publiqui *VMware* per a corregir vulnerabilitats. Pels sistemes ubicats en l'àmbit dels *Serveis TIC Centrals*, cal donar compliment a la *Norma de gestió de vulnerabilitats de programari base*.	I D
C3. No s'aplicaran pegats de terceres parts a la instal·lació del servidor *ESX Service* (per exemple versions del servidor web *Apache*). Només s'utilitzaran els pegats proporcionats per *VMware*.	I D
C4. S'inhabilitaran els dispositius de CD / DVD / disquetera / USB que no s'utilitzin.	I D
C5. Caldrà donar compliment a la *Norma de còpies de seguretat* per a garantir que es realitza còpia de seguretat dels sistemes.	C I D
C6. Netejar els usuaris i grups per defecte que es creen durant la instal·lació. Si no són necessaris pels diferents serveis que s'hagin d'instal·lar, cal eliminar-los o bé inhabilitar-los per evitar forats de seguretat.	C
C7. Esborrar fitxers associats a un usuari quan aquest sigui eliminat del sistema, ja que sinó queden sense propietari assignat	C I
C8. S'utilitzarà el protocol *NTP* per la sincronització de rellotges de les *màquines virtuals* per assegurar que els rellotges dels diferents sistemes virtuals estan sincronitzats. És essencial tenir els rellotges sincronitzats per poder obtenir traces vàlides en un anàlisi d'un incident. D'aquesta manera s'evitaran problemes amb certes *màquines virtuals* com controladors de domini Windows, que poden presentar problemes si existeix desincronització dels rellotges. Per exemple, Kerberos falla si existeix una diferència de més de 5 minuts entre el client i el servidor.	I

Recomanacions

R1. El ESX server és instal·lat per omissió amb una configuració alta de seguretat, és a dir tots els ports de sortida estan tancats i els ports d'entrades que estan oberts són només els requerits per a interactuar amb clients. Es recomana conservar aquesta configuració fins que la Consola de Servei sigui connectada a una xarxa confiable.

4.2. CN - Configuració

OBJECTIUS	
Configuració del sistemes virtuals referent a aspectes de seguretat.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C9. Es crearà una xarxa de gestió dedicada on s'utilitzaran els *NIC* per restringir l'accés, proporcionar una connectivitat segura i minimitzar el risc d'atacs de *DoS* o *DDoS*.	C I D
C10. La consola de servei i les *màquines virtuals* es col·locaran en xarxes separades.	I D
C11. S'usaran certificats per SSL que estaran creats i emmagatzemats en el *ESX Server* amb la finalitat d'accedir la consola de gestió gràfica. És recomanable obtenir certificats emesos per una entitat certificadora de confiança i no usar certificats autosignats pel propi sistema.	C I
C12. Els noms de *DNS* seran correctes i coincidiran amb els dels certificats per a prevenir que apareguin missatges d'alerta en el navegador durant la fase d'autenticació contra el servidor.	I
C13. El *ESX Server* només suporta *SNMP* v1, en el qual les dades s'envien en text clar. Caldrà implementar un sistema que garanteixi la seguretat de les transaccions de *SNMP*. Els MIB de *VMware* són tots de només lectura, per tant no es poden establir parts de *SNMP* amb crides de gestió.	C
C14. No s'executarà el X Server de la consola de servei.	D
C15. S'ubicaran i protegiran els recursos d'emmagatzemament de forma apropiada, restringint-ne l'accés per part dels usuaris i dels sistemes.	C I D
C16. Es garantiran els permisos suficients d'accés a l'emmagatzemament per l'aplicació *VMotion*.	D
C17. S'analitzarà els requeriments d'espai de parts del sistema de fitxers com */home*, */var* i */vmimages*, en funció de l'ús de la consola de servei.	I D
C18. S'etiquetaran les xarxes virtuals a nivell de *Virtual Infraestructure Node* (*VIN*). Així es facilita la gestió d'aquestes xarxes i s'eviten confusions.	D
C19. S'evitarà que les *màquines virtuals* facin *spoofing* de l'adreça *MAC* virtual, mitjançant la configuració del *VirtualCenter*.	I
C20. No estarà permès configurar en mode promiscu els adaptadors de xarxa de les diferents màquines virtuals, així com els commutadors.	C
C21. S'inhabilitaran les accions de copiar i enganxar informació entre màquines virtuals.	C I
C22. Es segregarà la xarxa i l'emmagatzemament pels sistemes virtuals en zones segures.	C I D
C23. Els commutadors virtuals no transmetran tràfic entre dos *NIC* físics.	I
C24. S'habilitarà la capacitat de modelar el caudal en funció del tipus de paquets (packet shaping) per optimitzar el rendiment de les xarxes virtuals.	I D
C25. La transferència de la memòria activa de la màquina virtual *VMotion* es realitza de forma no xifrada. S'implantarà *VMotion* en una xarxa aïllada, ja sigui creant una *VLAN* o bé mitjançant una xarxa física separada.	C I D
C26. Caldrà disposar d'una xarxa de gestió per a l'accés a la consola. Si tècnicament no és possible, caldrà crear una VLAN separada o commutador virtual per a la comunicació entre eines de gestió i el servei de consola.	C I D
C27. Inhabilitar tots aquells serveis que no siguin necessaris o insegurs.	C I D
C28. Els únics ports del *ESX Server* que donaran servei seran el 22 (*SSH*), 80 (WEB), 443 (*HTTPS*), 902 (port d'administració remota *VMware*) i ports d'aplicacions de monitoratge. En cas de necessitar obrir nous ports, caldrà que siguin ports segurs.	I D
C29. Les connexions web es realitzaran amb el protocol segur *HTTPS*. El port 80 (*HTTP*) serà redirigit automàticament al port 443 (*HTTPS*).	C I
C30. Les contrasenyes s'han de guardar de forma xifrada i caldrà modificar els permisos per evitar que siguin de lectura per a tots els usuaris.	C I
C31. Restringir l'accés al directori de logs per a usuaris sense privilegis.	C
C32. El nombre d'aplicacions que usen la bandera *setuid* o *setgid* ha estat minimitzat. Cal deshabilitar qualsevol aplicació setuid o setgid que no sigui necessària per a l'operació del ESX server.	C I D

C33. Emprar perfils de seguretat de commutador virtual en el ESX server hosts per a protegir els adaptadors de xarxa de l'atac de suplantació de la identitat de l'adaptador de xarxa. Aquests son: • *MAC address changes* -> canviar a rebutjar • *Forged transmissions* -> canviar a rebutjar • *Promiscuo mode operation* -> per defecte ja és rebutjar	C I D

Recomanacions

R2. Provar les configuracions de seguretat en un entorn de proves abans d'aplicar-les en servidors que estiguin en explotació.
R3. Eliminar dispositius de maquinari innecessaris.
R4. Canviar les comunitats *SNMP* per defecte (public, private).

4.3. IA - Identificació i Autenticació

OBJECTIUS	
Identificar i autenticar correctament als usuaris que requereixen accedir als sistemes *VMware*.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C34. S'utilitzarà l'autenticació de què disposa el *VirtualCenter*.	C
C35. Es configurarà la contrasenya del gestor d'arranc (*grub/lilo*) per prevenir que els usuaris amb accés al teclat puguin modificar les opcions d'arrencada del *kernel*.	C I D
C36. Es minimitzarà l'ús de *VMware Remote Console*, utilitzant serveis d'administració remota com *terminal server* o *SSH* per prevenir impactes en el rendiment de la consola de servei.	C I D
C37. S'habilitarà un missatge de benvinguda al accedir al sistema per a recordar la finalitat del sistema i advertir de les conseqüències d'un ús incorrecte del mateix.	D

4.4. CA - Control d'accés

OBJECTIUS	
Controlar l'accés dels usuaris als sistemes VMware.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C38. No es permetrà l'accés als usuaris al *VirtualCenter* en mode local. Caldrà utilitzar el client del *VirtualCenter* per accedir.	D
C39. L'accés mitjançant el superusuari (*root*) serà proporcionat usant l'eina *sudo* que està inclosa en el *ESX Server*. S'han d'utilitzar usuaris nominals per cada administrador.	C
C40. S'utilitzarà la funcionalitat de control d'accés del *VirtualCenter* que gestiona el control d'accés en funció basat en rols.	C
C41. S'utilitzarà el *VirtualCenter* per a protegir l'accés als *VIN* i les màquines virtuals.	C
C42. Durant la instal·lació del sistema gestor de base de dades pel *VirtualCenter* l'usuari administrador de la base de dades tindrà permisos d'accés al *VirtualCenter*. Per l'operació normal, caldrà controlar els permisos d'executar *stored procedures*, així com les sentències de seleccionar, sobreescriure, afegir i esborrar a la base de dades.	C I D
C43. Es complirà la *Norma de gestió de comptes d'administrador de sistemes* per a garantir el control dels comptes amb privilegis d'administració sobre *VMware*.	C
C44. Serà obligatori l'ús del protocol *SSH* per accedir a la línia de comandes dels sistemes i als fitxers, evitant l'ús de la versió 1 d'aquest protocol, per presentar vulnerabilitats de seguretat.	C I
C45. No utilitzar aplicacions de connexió remota en les quals la contrasenya viatgi en clar per la xarxa, com per exemple telnet, ftp, etc. Utilitzar les protocols segurs com sftp o ssh.	C I D
C46. Fer un ús adequat dels usuaris, grups, propietat dels fitxers i permisos dels usuaris i grups sobre els fitxers per tal de mantenir la confidencialitat i integritat de les dades que continguin aquests fitxers. Sempre caldrà garantir el principi de mínims privilegis.	C I
C47. Inhabilitar l'accés al compte d'invitat, si existeix.	C I D

4.5. MN - Monitoratge

OBJECTIUS	
Registrar totes les accions en els sistemes per tal de poder conduir futures investigacions en cas de necessitat i atribuir-ne responsabilitats.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C48. Caldrà donar compliment als requeriments de la *Norma de gestió de traces* per a garantir la traçabilitat i custòdia dels esdeveniments dels sistemes.	C I
C49. Pels sistemes d'àmbit departament / ens, es connectaran a eines de correlació de traces pròpies quan existeixin; de no ser així, caldrà guardar les traces durant un període mínim d'un any i revisar-les periòdicament per a detectar anomalies o incidències en el funcionament del sistema.	C I
C50. Qualsevol incident de seguretat haurà de ser comunicat en la major brevetat possible mitjançant el *Procediment de notificació d'incidents de seguretat.*	C I D

Recomanacions

R5. Es recomana, revisar periòdicament les traces per a detectar activitats anòmales que puguin comprometre la seguretat del sistema.

R6. Es controlarà que el sistema de fitxers no s'ompli. En cas de què passés podria afectar l'operació de la consola de servei sobre el ESX Server.

R7. Si s'envien les traces cap a un sistema remot (syslogd), cal tenir en compte que la comunicació no és xifrada. Caldrà garantir un canal segur per la transmissió de les traces (per exemple IPSec).

R8. Pels fitxers vmk*, es limitarà la capacitat a 4096k i s'habilitarà la compressió. Això permetrà registrar més traces causant un mínim impacte en el sistema d'emmagatzemament de fitxers.

4.6. AU - Auditoria

OBJECTIUS	
Controlar la configuració dels diferents sistemes i facilitar les traces del sistema a l'eina centralitzada de gestió de traces.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C51. Caldrà facilitar les tasques d'auditoria per part de l'Oficina de Seguretat davant a la revisió del compliment dels requeriments de seguretat marcats pel CTTI.	C I D

4.7. DS - Disponibilitat del servei

OBJECTIUS	
Garantir la disponibilitat i continuïtat de les infraestructures de sistemes virtuals.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C52. Abans de crear una nova *màquina virtual*, caldrà analitzar i documentar quins requeriments d'infraestructura (processador, memòria, etc.) necessita el nou servei de tractament de la informació.	D
C53. S'utilitzarà la tecnologia *VMotion* per a garantir la continuïtat i disponibilitat del servei en cas d'incident, traslladant el sistema virtual afectat a una altra unitat de processament.	I D
C54. Es realitzarà una còpia de seguretat de la configuració de la consola de servei.	I D
C55. Només es connectaran els sistemes que donin servei als usuaris (servidors web, *front-end*) a les connexions físiques amb l'exterior.	I D
C56. Els servidors d'aplicacions i bases de dades, estaran ubicats en xarxes virtuals internes, sense accés a l'exterior.	C I D
C57. Existirà una segregació d'entorns de les *màquines virtuals* en funció de les necessitats. Així mateix, se segregaran les xarxes amb infraestructura virtual.	C I D

4.8. OU - Outsourcing o subcontractació del servei

OBJECTIUS
Garantir l'acompliment de les mesures de seguretat i dels acords de nivell de servei en cas de subcontractació o externalització del servei de sistemes virtuals.

CARACTERÍSTIQUES	
Descripció	**Categoria**
C58. Es recollirà contractualment el compliment de les normes i guies que el CTTI tingui per entorns de virtualització així com qualsevol altra norma de gestió o administració que sigui d'aplicació.	C I D
C59. Es garantirà el compliment de la *Norma de contractació de Tercers*.	C I D
C60. Es garantirà la qualitat i el nivell de servei requerit a través d'acords de nivell de servei: • Procediments d'escalat d'incidències. • Temps de resolució d'incidències. • Temps de resposta per canvis / noves instal·lacions. • Compliment i actualització dels controls de seguretat. • Gestió de problemes. • Etc. L'incompliment d'acords de nivell de servei haurà de comportar penalitzacions econòmiques al proveïdor.	C I D

5 CONTROL

Per a l'àmbit dels *Serveis TIC Centrals*, el control del compliment d'aquesta guia es realitzarà mitjançant auditories periòdiques segons s'estableix en el *Pla d'auditories de seguretat*. Per altres àmbits, es recomana realitzar auditories cada 6 mesos.

En el cas de què no s'apliqui algun dels controls d'aquesta guia, caldrà justificar i documentar aquestes excepcions. Per a l'àmbit dels *Serveis TIC Centrals*, cada excepció a un control haurà de ser autoritzada prèviament per l'Oficina de Seguretat.

Caldrà mantenir un registre on quedin recollides totes les excepcions, a disposició de les auditories.

6 PENALITZACIONS

Quan l'explotació / manteniment dels sistemes estigui subcontractat, en cas d'incompliment aplicaran les penalitzacions recollides en el contracte de la prestació del servei.

Si l'administració del sistema recau en personal intern de la Generalitat de Catalunya, l'incompliment d'aquesta guia pot determinar, si s'escau, l'aplicació del règim disciplinari corresponent.

7 DIVULGACIÓ

L'àrea de Qualitat, Seguretat i Relacions amb Proveïdors del CTTI publicarà aquesta guia al repositori d'estàndards de la intranet del CTTI.

8 REVISIÓ

Aquesta guia ha de ser revisada anualment.

En cas de produir-se una incidència de seguretat relacionada amb aquesta guia, caldrà fer una revisió de compliment i completesa.

9 GLOSSARI DE TERMES

DoS: *Denial of Service*. Atac malintencionat amb l'objectiu de col·lapsar un servei fins a provocar que quedi sense proporcionar resposta a les peticions de servei.

DDoS: *Distributed Denial of Service*. *DoS* realitzat des de diferents ubicacions a la vegada, amb l'objectiu d'incrementar l'efectivitat de l'atac.

DNS: *Domain Name Server*. Equips que traslladen el nom lògic d'un equip en la corresponent adreça lògica (IP).

HTTPS: Protocol de transmissió web segur que xifra la comunicació entre el navegador i el servidor web.

IDS: *Intrusion Detection System*. Sistema que analitza el tràfic per a detectar possibles atacs o tràfic anòmal que pugui causar incidències en els sistemes.

LAN: *Local Area Network*. Xarxa que permet la comunicació entre diferents sistemes en un entorn local.

NIC: *Network Interface Card*. Dispositiu que permet la comunicació d'un sistema a través d'una xarxa.

NIDS: *Network Intrusion Detection System*. *IDS* que analitza el tràfic de la xarxa.

SNMP: *Simple Network Management Protocol*. Protocol per a la gestió de xarxes així com el monitoratge dels dispositius i les seves funcions.

Spoofing: Falsificar la identitat de l'equip d'origen en una comunicació.

SSH: *Secure Shell*. Programari que permet establir una sessió amb un equip remot i administrar-lo mitjançant una línia de comandes. Xifra la comunicació entre el client i el servidor per evitar que sigui desxifrada si s'intercepta.

Stored procedure: Conjunt de sentències en SQL compilades que poden ser usades per diferents programes per a la gestió de la informació d'una base de dades.

VIN: *Virtual Infraestructure Node*. Infraestructura virtual (processador, disc, xarxa, memòria) que necessita per la seva execució cada màquina virtual.

VLAN: *Virtual Local Area Network*. Circuit de xarxa virtual construïda sobre una LAN física. Operativament funciona com una LAN completament autònoma. Utilitza l'etiquetatge dels diferents paquets que circulen per la mateixa xarxa física per identifica a quina VLAN pertanyen (estàndard 802.1q).

VMFS: *VMware File System*. Fitxers utilitzats pel programari de *VMware* per persistir a disc la informació dels diferents sistemes virtuals.

VMotion: Sistema de *VMware* que permet la transferència d'una màquina virtual en temps real entre dos contenidors. S'utilitza per situacions d'emergència o per tasques de manteniment.

Xinetd: Servei que gestiona els serveis de xarxa dels sistemes *Linux*.

10 DOCUMENTACIÓ REFERENCIADA

- GE-GUI20 Guia de gestió de comptes administrador sistemes
- CT-NOR03 Norma de contractació de tercers
- SC-NOR16 Norma de gestió de traces
- GE-PRO01-01 Procediment de Notificació d'Incidents de Seguretat
- Pla d'auditories de seguretat

http://www.vmware.com/pdf/vi3_301_201_server_config.pdf

11 PARAULES CLAU

Sistema virtual, protecció, ports, xarxa virtual, hardenning, VMWARE, ESX, protecció.

12 HISTÒRIC DEL DOCUMENT

Versió 1.0
Versió inicial.

Versió 2.0
Versió revisada de l'estandard. Veure la fitxa de l'estàndard per a més informació.