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	5/10/2009	6/10/2009

Estàndard signat digitalment pel:
Generalitat de Catalunya

Centre de Telecomunicacions i Tecnologies de la Informacio
Estàndard aprovat
Barcelona
2009.10.06 12:20:36 +02'00'

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

RESUM

OBJECTIU

Definir els controls a aplicar per a la protecció d'equips instal·lats amb el servidor d'aplicacions *Weblogic*, amb l'objectiu de garantir la confidencialitat, integritat i disponibilitat de la informació i serveis suportats per aquesta plataforma.

ÀMBIT

Servidors d'aplicacions *Weblogic* de la Generalitat de Catalunya.

DESCRIPCIÓ

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

1 OBJECTIU

Definir els controls per a instal·lar, configurar, mantenir i explotar el servidor d'aplicacions *WebLogic Server* d'una manera segura, que garanteixi la confidencialitat, integritat i disponibilitat dels serveis web implantats amb aquesta plataforma a la Generalitat de Catalunya.

No és l'objectiu d'aquesta guia, la definició i programació d'aplicacions en l'entorn *J2EE* de forma segura.

Weblogic Server proporciona un mecanisme de seguretat per a protegir els recursos anomenat *security realm*. Cada domini de seguretat consisteix en un conjunt de proveïdors de seguretat (*security providers*), usuaris, grups, rols de seguretat i polítiques de seguretat. Un usuari cal que estigui definit en un domini de seguretat per a poder accedir als recursos de *WebLogic Server* associats a un domini. Quan un usuari intenta accedir a un recurs en particular, *WebLogic Server* intenta d'autenticar i autoritzar a l'usuari contra el rol de seguretat definit en el domini de seguretat i la política de seguretat del recurs en particular.

No entra en l'objectiu d'aquesta guia, la suite de productes orientada a la gestió de serveis *SOA* (*Service-Oriented Architecture*) que conté un component específic per la gestió de la seguretat en els serveis anomenat *Oracle Entitlement Server*.

Tots els canvis proposats en aquesta guia han de ser primer instal·lats en un entorn de desenvolupament i s'ha fer un test exhaustiu de les aplicacions per tal d'assegurar que tot continua funcionant normalment.

2 ÀMBIT I VIGÈNCIA

Aquesta guia va destinada als administradors i responsables d'instal·lació, explotació i manteniment dels servidors d'aplicacions *WebLogic Server* de la Generalitat de Catalunya, contemplant les opcions de seguretat pròpiament.

La versió actual entrarà en vigor el dia 6 d'octubre de 2009.

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

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
- 9.2.1 Ubicació i protecció dels equips
- 10.10.1 Registres d'auditoria (logging)
- 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 controls de seguretat orientats a garantir la confidencialitat, privacitat, integritat i disponibilitat de la informació en els servidors d'aplicacions *WebLogic Server*. Sota la columna "categoria", s'especifiquen els aspectes de seguretat que cada control reforça (confidencialitat– C, integritat– I, disponibilitat– D).

4.1 IN – Instal·lació i manteniment

OBJECTIUS
Requisits en la instal·lació, actualització i manteniment del servidor d'aplicacions *WebLogic Server*. Els controls apliquen a entorns de producció.
CARACTERÍSTIQUES

Descripció	Categoria
C1. Quan calgui instal·lar un nou servidor *Weblogic Server* s'ha d'optar per una versió que tingui suport per part del fabricant i actualitzada amb els corresponents pegats de seguretat. 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
C2. Instal·lar WebLogic Server en un equip dedicat exclusivament. No és aconsellable que doni suport a altres aplicacions com bases de dades. En cap cas, s'instal·larà el servidor WebLogic en un equip que sigui controlador de domini.	C I D
C3. Col·locar el servidor d'aplicacions en una *DMZ*.	C I D
C4. No instal·lar els codis d'exemple ni utilitats com *XML Spy*. Cal inhabilitar aquestes opcions durant el procés d'instal·lació de *Weblogic Server*.	I D
C5. Quan s'utilitzi el *JRockit*, esborrar els components de programari del *JDK* de *Java* que no estiguin en el *JRockit*.	I D
C6. Eliminar les eines de desenvolupament com *Configuration Wizard*, *Weblogic Builder* i les eines *JCOM*.	I D
C7. Esborrar la base de dades per defecte *Pointbase* que està inclosa només per motius d'avaluació i proves i que no és necessària per entorns de producció.	I D
C8. Esborrar el fitxer *MedRec.jar* que conté un exemple d'aplicació. S'instal·la igualment encara que s'inhabiliti l'opció d'instal·lar els exemples.	I D
C9. Protegir el sistema operatiu, controlant els serveis de xarxa que té habilitats. Cal mantenir el sistema operatiu al dia dels pegats de seguretat. (Veure *Guia protecció entorns Linux, Solaris, AIX, HP-UX, Windows 2003*).	C I D
C10. Crear un usuari en el sistema per a l'execució del servidor *WebLogic Server* amb els següents requisits: • Privilegis d'accés a la carpeta on està instal·lat *WebLogic Server*. • Permisos de lectura, escriptura i execució a la carpeta *BEA home*, a l'arbre de directoris de *WebLogic Server* i els directoris de domini on resideixen les aplicacions i fitxers de configuració. • No ha de tenir privilegis d'administració sobre el sistema operatiu.	I D
C11. Prevenir que els següents fitxers de configuració puguin ser modificats per usuaris que no tinguin privilegis sobre *WebLogic Server*: • *boot.properties* • *config.xml* • *fileRealm.properties* (només s'utilitza en versions 6.x) • *web.xml*	C I D
C12. Si s'instal·la el servidor d'aplicacions com a servei perquè s'iniciï automàticament durant el procés d'arrencada del servidor, configurar el servei perquè ho faci amb l'usuari definit per a l'execució de *WebLogic Server*.	C I D
C13. No executar *WebLogic Server* en mode de desenvolupament en entorns de producció.	I D
C14. Protegir serveis externs que utilitzi *WebLogic Server* (bases de dades, etc.) per evitar que causin incidències en el funcionament del servidor d'aplicacions.	C I D
C15. Caldrà donar compliment a la *Norma de còpies de seguretat* per a garantir que es realitza còpia de seguretat dels sistemes	C I D

4.2 CN – Configuració

OBJECTIUS	
Configurar la instal·lació del servidor d'aplicacions *WebLogic Server* per a garantir la seguretat dels serveis web que presten.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C16. Utilitzar els filtres de connexió (*WebLogic Server connection filters*) per a controlar i limitar el trànsit amb el servidor d'aplicacions. Per exemple, limitar el nombre de IPs	C I D

amb accés, el tipus de trànsit, etc.	
C17. Utilitzar el port d'administració (*Administration Port*) per a tot el trànsit d'administració. Permet separar el trànsit d'administració del de servei de les peticions web. D'aquesta manera s'aconsegueix tenir un canal d'administració independent del de servei, i poder accedir al servidor davant de problemes de no respondre peticions web. Utilitzar-lo junt amb els filtres de connexió, per a controlar que només es puguin acceptar peticions administratives d'un conjunt de màquines o xarxes. A part, tota comunicació d'administració pel port d'administració es fa xifrada amb *SSL*.	C I D
C18. Habilitar canals d'administració (*Administration Channel*) per assegurar que la comunicació administrativa entre servidors *WebLogic Server* es realitza de forma segura. Sense usar el canal d'administració, es transfereixen els missatges administratius en clar, amb el conseqüent perill de captura, modificació, eliminació i resposta dels missatges.	C I D
C19. Protegir el port *LDAP* contra atacs de força bruta. Utilitzar filtres de connexió per a controlar que només es tingui accés al port des d'equips coneguts i de confiança. Es pot plantejar canviar el port d'accés a *LDAP*.	I D
C20. *WebLogic Server* disposa d'un *LDAP* incorporat, així com la possibilitat de connectar amb *LDAP* exteriors. Cal esborrar totes les comptes de *LDAP* que no es requereixen explícitament.	I D
C21. Quan es creï un nou domini, assegurar que l'opció *Anonymous Admin Lookup Enabled* no està seleccionada.	C I D
C22. No utilitzar certificats *SSL* de proves en entorns de producció. Cal utilitzar certificats que estiguin expedits per entitats certificadores reconegudes.	C I D
C23. Configurar el mòdul *SSL mod_ssl* per a poder utilitzar *HTTPS* per accedir al servidor web si és necessari. Utilitzar protocols robustos SSL v3 i TLS v1 i claus de com a mínim 128 bits.	C I
C24. Protegir l'emmagatzemament dels certificats en el *WebLogic Server* de manera que no puguin ser accedits ni revelats a tercers.	C I D
C25. Habilitar la verificació del nom del servidor. D'aquesta manera es prevenen atacs "*man-in-the-middle*" en les comunicacions *SSL*.	C I D
C26. Per cada aplicació, configurar els ports *SSL*, habilitant l'opció *SSL Listen Port Enabled* i informant del número de port.	C I D
C27. Restringir la longitud i el temps límit de les peticions web contra el servidor d'aplicacions per a evitar atacs de denegació de servei. Es pot configurar mitjançant el paràmetre `ServerMBean.StuckThreadMaxTime`	I D
C28. Limitar el número de connexions obertes permeses en el servidor. D'aquesta manera es protegeixen atacs de denegació de servei intentant esgotar els recursos de processament de peticions del servidor. Es pot configurar mitjançant el paràmetre `ServerMBean.MaxOpenSockCount`	I D
C29. Evitar que en les respostes *HTTP* als clients s'informi de la versió de servidor d'aplicacions.	C I D
C30. No utilitzar el *servlet Servlet* en entorns de producció. En el seu lloc, fer un mapatge[1] dels *servlets* que siguin necessaris per l'aplicació a *URI* específiques, evitant així també utilitzar el *servlet* per defecte.	I D
C31. Si s'utilitza *Active Directory* cal tenir en compte les següents consideracions de seguretat: • Inhabilitar els drets d'accés local al servidor (*Deny Logon Locally*) al compte que s'utilitzi per arrancar el servidor d'aplicacions. • Crear un grup global pel compte d'arrencada de *WebLogic Server* i afegir l'usuari d'arrencar WebLogic Server a aquest grup, eliminant-lo del grup d'usuaris del domini (*Domain Users*). L'objectiu és prevenir que el compte d'arrencada de *WebLogic Server* obtingui permisos i privilegis assignat als usuaris del domini. • Quan s'utilitzi el *Active Directory Authenticator* per defecte, utilitzar *IPSEC* per a	C I D

[1] Traducció al català de *mapping*.

protegir la comunicació entre WebLogic Server i *Active Directory*. Una altra opció és utilitzar *TLS*/*SSL*. En aquest cas, informar el nom complet del servidor (*FQDN*) en el camp de host.	
C32. Només afegir al grup *Administrators* el mínim número d'usuaris que hagin de tenir privilegis d'administració sobre *WebLogic Server*.	I D

Recomanacions

R1. Configurar les pàgines a mostrar en cas d'error del servidor d'aplicacions, evitant que siguin per defecte les del servidor. Per a fer-ho cal configurar el paràmetre `<error-page>` en el descriptor d'aplicació *web.xml*.

4.3 MN – Monitoratge

OBJECTIUS	
Registrar totes les peticions que es realitzin en el servidor d'aplicacions. A part de detectar anomalies o possibles atacs, també serviran per a obtenir estadístiques d'ús dels llocs web.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C33. 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
C34. 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'1 any i revisar-les periòdicament per a detectar anomalies o incidències en el funcionament del sistema.	C I
C35. Qualsevol possible incident de seguretat haurà de ser comunicat en la major brevetat possible mitjançant el *Procediment de notificació d'incidents de seguretat*.	C I
C36. Si s'instal·la el servidor d'aplicacions com a servei de *Windows*, cal redirigir la sortida de la consola a un fitxer, ja que sinó no s'obtenen les traces del sistema.	I

C37. Redirigir les sortides estàndard i d'errors a fitxers:
`-Dweblogic.Stdout="stdout-filename"`
`-Dweblogic.Stderr="stderr-filename"`
	I

C38. Protegir els fitxers de traces que genera *WebLogic Server* contra modificacions d'usuaris o processos mal intencionats.	C I D
C39. Habilitar els mecanismes que proporciona *WebLogic Server* per a realitzar un seguiment dels canvis de configuració i que aquests quedin gravats en el registre de traces d'administració del servidor d'aplicacions: `-Dweblogic.domain.ConfigurationAuditType="logaudit"`	I D

Recomanacions

R2. Es recomana, revisar periòdicament les traces per a detectar activitats anòmales que puguin comprometre la seguretat del sistema

4.4 IA – Identificació i Autenticació

OBJECTIUS	
Especificar els mecanismes de que disposa *WebLogic Server* per a realitzar la identificació, autenticació i control d'accés als recursos del servidor d'aplicacions.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C40. Modificar la contrasenya per defecte dels usuaris d'administració de *WebLogic Server*. És preferible crear nous usuaris amb privilegis d'administració i esborrar els definits per defecte.	C I D
C41. Cal definir nous usuaris amb privilegis d'administració abans d'esborrar els definits	C I D

per defecte.	
C42. Complir la *Norma gestió de comptes d'administració de sistemes* per a la configuració de les contrasenyes dels comptes amb privilegis d'administració.	C I D
C43. Utilitzar la consola d'administració per a crear rols a usar en l'estratègia de control d'accés. És aconsellable no esborrar els grups i rols definits per defecte, amb les corresponents polítiques de seguretat.	I D
C44. Assegurar que els usuaris i grups s'han assignat correctament als rols de seguretat per defecte de *WebLogic Server*.	I D
C45. Existeix un *realm* per defecte de seguretat que és el *myrealm*. És aconsellable configurar aquest domini amb les necessitats de l'aplicació enlloc de crear un nou *realm*.	C I D

Recomanacions

R3. Avaluar la necessitat d'usar el producte *Oracle Entitlement Server* per a la gestió del control d'accés als serveis que ofereixen les aplicacions

4.5 AU - Auditoria

OBJECTIUS	
Controlar la configuració de *WebLogic Server* i analitzar esdeveniments registrats que poguessin suposar una amenaça per la seguretat, identificant àrees vulnerables.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C46. 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

4.6 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 de serveis basats en servidors d'aplicacions *WebLogic*.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C47. Es recollirà contractualment el compliment de les normes i guies que el CTTI tingui per als servidors d'aplicacions *Weblogic* així com qualsevol altre norma de gestió o administració que sigui d'aplicació.	C I D
C48. Es garantirà el compliment de la *Norma de contractació de Tercers*.	C I D
C49. 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

DMZ: *DeMilitarized Zone*. Host o xarxa neutral entre la xarxa privada d'una organització i la xarxa pública.

HTTPS: *HTTP* sobre *SSL*. Protocol de transmissió segura de contingut web.

IPSEC: Internet Protocol Security. És un entorn per un conjunt de protocols per a proporcionar seguretat a la xarxa a nivell de processat de paquets.

J2EE: *Java 2 Platform Enterprise Edition*. Plataforma Java dissenyada per a entorns de processament d'informació de grans empreses. Enfocada al desenvolupament d'aplicacions per capes.

JAAS: *Java Authentication and Authorization Services*. Part de l'entorn J2EE que proveeix serveis d'autenticació i de control d'accés als usuaris de recursos web.

Java: Llenguatge de programació dissenyat per ser usat en entorns distribuïts a Internet.

JDK: *Java Development Kit*. Entorn de desenvolupament per escriure aplicacions en Java.

JRE: *Java Runtime Environment*. Entorn d'execució de programes en Java.

JSP: *Java Server Page*. Tecnologia per a controlar el contingut i aparença de les pàgines web usant servlets. Permeten que la pàgina sigui construïda dinàmicament abans de ser enviada al servidor.

LDAP: *Lightweight Directory Access Protocol*. Programari per possibilitar la localització de recursos com fitxers i dispositius en una xarxa, ja sigui sobre Internet o en una xarxa d'una organització.

NAT: *Network Address Translation*. Traduir adreces IP usades en una xarxa a unes altres adreces IP conegudes en una altra xarxa..

SDK: *Software Development Kit*. Conjunt de programes usats pels programadors per a desenvolupament de programes.

Serveis TIC Centrals: Serveis TIC Centrals de Caràcter Continuat de la Generalitat de Catalunya, gestionats pel Centre de Telecomunicacions i Tecnologies de la Informació (CTTI).

Servlet: Programa que s'executa en el servidor per realitzar accions que generalment generen una resposta per enviar al client web.

SSL: *Secure Socket Layer*. Protocol per a aportar seguretat en la transmissió de missatges per Internet.

Socket: Canal de comunicació amb un equip per a la prestació d'un servei a través d'un port.

URI: *Uniform Resource Identifier*. La manera d'identificar continguts i recursos a Internet.

10 DOCUMENTACIÓ REFERENCIADA

- GE-GUI07 Guia protecció entorns Linux
- GE-GUI08 Guia protecció entorns Solaris
- GE-GUI27 Guia de protecció entorns HP-UX
- GE-GUI32 Guia protecció entorns AIX
- GE-GUI10 Guia protecció entorns Windows 2003
- GE-GUI40 Guia de còpies de seguretat
- GE-PRO01 Procediment de notificació d'incidents de seguretat
- GE-GUI19 Guia de contrasenyes
- GE-GUI20 Guia de gestió de comptes d'administrador de sistemes
- CT-NOR03 Norma de contractació de tercers
- Pla d'auditories de seguretat
- Pàgina web de documentació del servidor d'aplicacions *WebLogic*: http://www.oracle.com/technology/documentation/index.html

11 PARAULES CLAU

Servidor d'aplicacions, WebLogic Server, realm, JSP, servlet, J2EE, Java, JDK, protecció, hardenning.

12 HISTÒRIC DEL DOCUMENT

Versió 1.0
Versió inicial.

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