ÍNDEX

Versió	Redactat / revisat per	Aprovat per	Data aprovació	Data publicació
1.0.	CTTI – QSRaP, Arquitectura	Comitè Direcció CTTI	6/4/2010	7/4/2010

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

RESUM

OBJECTIU

Definir els controls a aplicar per a la protecció d'instal·lacions del programari SAP Netweaver Application Server (AS) ABAP amb l'objectiu de garantir la confidencialitat, integritat i disponibilitat de la informació i serveis suportats per aquesta plataforma.

ÀMBIT

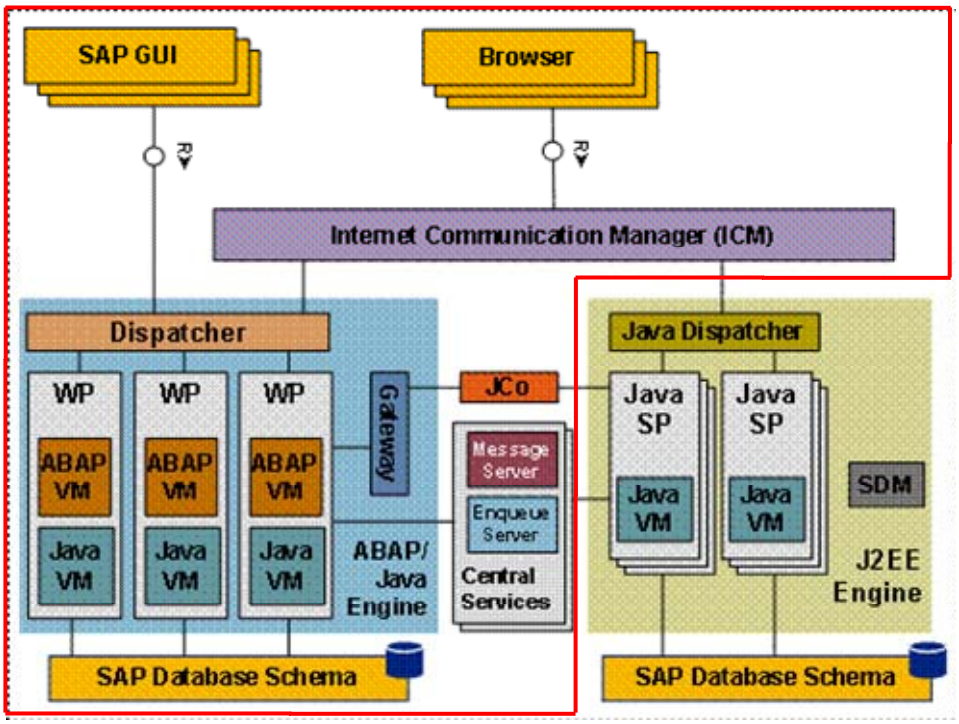
Instal·lacions de SAP Netweaver AS ABAP de la Generalitat de Catalunya.

1 OBJECTIU

Definir els controls per administrar i gestionar la seguretat en els equips que tenen instal·lat SAP Netweaver AS ABAP. No contempla la versió sobre Java que queda fora de l'àmbit d'aquest document.

SAP NetWeaver AS és la base de la instal·lació d'un sistema SAP. Proveeix la plataforma per altres components Netweaver (Portal, XI, etc.), tant per aplicacions ABAP com Java.

El següent esquema mostra gràficament els diferents components. El requadre en línia vermella indica els components que recauen en aquesta guia:



Font: SAP

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 i manteniment dels servidors SAP Netweaver AS ABAP de la Generalitat de Catalunya en la versió 7.0 (Netweaver 2004S).

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

En el cas que el manteniment dels equips estigui externalitzat, caldrà exigir per contracte l'aplicació dels controls de seguretat.

Entrarà en vigor el dia 7 d'abril de 2010.

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. Aquests s'agrupen per grups d'accions o procediments operatius orientats a combatre les amenaces a les quals un equip amb *SAP* està exposat. L'aplicació d'un conjunt ampli dels controls d'una manera lògica, ordenada i planificada reduirà progressivament les vulnerabilitats del sistema i, per tant, l'exposició als riscos. Sota la columna "categoria", s'especifiquen els aspectes de seguretat que cada control reforça (confidencialitat– C, integritat– I, disponibilitat– D).

NOTA: Aquests controls han de ser desplegats en cada instància del sistema.

4.1. IN – Instal·lació i manteniment

OBJECTIUS	
Identificar les mesures de seguretat a tenir en compte durant el procés d'instal·lació de SAP.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C1. Instal·lar la instància de SAP en una partició o unitat de disc diferent a on resideix el sistema operatiu.	D
C2. En cas d'instal·lar el gestor de base de dades, ubicar-lo en una partició o unitat de disc dedicada.	D
C3. Donar compliment als requeriments d'arquitectura definits pel CTTI en el *Manual d'arquitectura de SAP*.	C I D
C4. Protegir el sistema operatiu, controlant els serveis de xarxa que té habilitats. Cal mantenir el sistema operatiu al dia dels pegats de seguretat.	C I D
C5. Mantenir el sistema (tant el propi sistema SAP com el servidor o client de la Base de Dades) actualitzat amb els pegats de seguretat i els paquets de programari adequats. Pels sistemes ubicats en l'àmbit dels Serveis TIC Centrals, cal donar compliment a la *Norma de gestió de vulnerabilitats de programari base*.	C I D
C6. Netejar els usuaris i grups per defecte creats 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. Donar compliment a la *Norma de còpies de seguretat* per a garantir que es realitza còpia de seguretat dels sistemes.	C I D
C8. Donar compliment a la *Norma de creació de DMZ* per a segmentar els diferents entorns de la instal·lació de SAP.	C I
C9. Eliminar els fitxers del directori <user_home>/.sdtgui/. un cop finalitzada la instal·lació.	C I D

4.2. CN - Configuració

OBJECTIUS	
Identificar les mesures de seguretat a aplicar després de la instal·lació inicial del sistema o durant la utilització del mateix, per tal de configurar-lo adequadament.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C10. Donar compliment a la *Guia de gestió de comptes d'administració de sistemes* per a garantir la correcta definició i gestió dels comptes amb privilegis d'administració.	C I
C11. En entorns Windows, inhabilitar els privilegis de "Log on locally" a l'usuari SAPService<SID>.	C I D
C12. Per entorns Unix, bloquejar l'usuari <*db*><*sid*> en els servidors d'aplicació.	C I
C13. Donar compliment a la *Guia de contrasenyes* per a garantir la correcta definició i gestió dels comptes d'usuaris de SAP. A nivell informatiu en l'annex A es pot trobar el detall dels diferents paràmetres de configuració.	C I
C14. Inhabilitar tots aquells serveis de sistema operatiu que no siguin necessaris o insegurs.	C I D
C15. Canviar el paràmetre d'instància *login/no_automatic_user_sapstar* a 1. Evita que si el registre mestre de SAP* es esborrat o danyat, al reiniciar el sistema es regeneri automàticament amb el password PASS.	C
C16. Per l'accés dels usuaris finals des d'Internet al sistema SAP, implementar els requeriments d'arquitectura definits pel CTTI en la *Guia d'arquitectura de SAP*.	C I D
C17. En cas d'utilitzar *SAP Web Dispatcher* com a frontal d'accés al sistema SAP, configurar l'accés fins a aquest xifrant el tràfic (https) i redirigir el tràfic cap al servidor sense necessitat de xifrar (http).	C
C18. Per l'accés via *SAProuter* des de l'exterior, donar compliment als requeriments d'arquitectura definits pel CTTI en el *Manual d'arquitectura de SAProuter*.	C I D
C19. En cas d'utilitzar la funcionalitat *SSF* (*Secure Store and Forward*) s'ha de modificar una sèrie de variables als front-end dels servidors de l'aplicació mitjançant l'edició del fitxer *ssfrfc.ini* en cadascun dels equips configurant els paràmetres mitjançant la següent sintaxi: <*SSF parameter*>=<*parameter value*> • SSF_MD_ALG=SHA1 • SSF_SYMENCR_ALG=TRIPLE-DES • SSF_TRACE_LEVEL=0 La mateixa configuració ha de ser aplicada al servidor d'aplicacions.	C I
C20. El paràmetre d'instància **Auth/system_access_check_off** (inhabilita la verificació d'autoritzacions sobre alguns elements particulars del llenguatge ABAP) ha d'estar informat a 0.	C I
C21. Configurar el paràmetre d'instància **Auth/rfc_authority_check** amb valor 1 per a comprovar l'autorització dels objectes a les crides RFC.	C I
C22. Limitar l'accés als serveis del sistema que no siguin publicats per a tots els usuaris.	C I

Recomanacions

R1. Provar les configuracions de seguretat en un entorn de proves abans d'aplicar-les en servidors que estiguin en explotació.

4.3. MN - Monitoratge

OBJECTIUS	
Identificar quines accions i activitats dels usuaris que es realitzen en el sistema cal registrar.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C23. Donar compliment als requeriments de la *Norma de gestió de traces* per a garantir la traçabilitat i custòdia dels esdeveniments dels sistemes. A nivell informatiu en l'annex B es pot trobar el detall dels diferents paràmetres de configuració.	C I
C24. Pels sistemes d'àmbit departament / ens, es connectaran a eines de correlació de traces pròpies quan existeixin o a l'eina de Serveis Centrals; 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
C25. 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 D

Recomanacions

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

4.4. CA - Control d'accés

OBJECTIUS	
Proveir als usuaris i grups, de privilegis o drets d'accés als sistemes *SAP* aplicant sempre el principi de mínims privilegis	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C26. Els usuaris interactius tipus *Dialog* quedaran reservats només per l'accés d'usuaris finals i administradors que requereixin l'execució de transaccions de forma interactiva via GUI o via web.	C I
C27. Els processos batch faran servir usuaris tipus *System* que no permeten la connexió interactiva de l'usuari.	C I
C28. La connectivitat des d'altres serveis es realitzarà mitjançant usuaris tipus *Service* o *Communication*, el accés via GUI dels quals no és permès. Aquests usuaris hauran de disposar dels mínims privilegis possibles.	C
C29. Limitar la concessió dels perfils *SAP_ALL* i *SAP_NEW* només als administradors del sistema.	C I
C30. Canviar la contrasenya per defecte dels usuaris especials predefinits: • *SAP** • *DDIC* • *EarlyWatch* • *SAPCPIC*	C I D
C31. En entorns de producció, només els usuaris administradors han de tenir l'objecte d'autorització **S_DEVELOP** (desenvolupament de programes), **S_PROGRAM** (manteniment, crides i execució de programes) o **S_DATASET** (per a les funcions **OPEN DATASET**, **READ DATASET**, **TRANSFER** o **DELETE**).	C I D
C32. En entorns de producció, limitar l'accés dels usuaris a *l'ABAP Workbench*, des d'on es poden crear i executar scripts i crear o destruir autoritzacions a través d'objectes (també accessibles des de les transaccions **SU21** i **SU03**).	C I D

C33. Restringir l'accés a les transaccions que permeten l'execució de codi **SA38** y **SE38** a l'entorn de desenvolupament ABAP i les que ofereixen la possibilitat d'executar-les en segon pla (**SM36** y **SM37**).	C I D
C34. Limitar els accessos al sistema de transport TMS de forma que només els administradors puguin importar els canvis provinents d'altres entorns.	C I D
C35. Limitar els accessos als directoris d'intercanvi només als usuaris autoritzats.	C I D
C36. Els usuaris només han de tenir accés a la seva cua d'impressió.	C
C37. Només els administradors han de tenir accés les transaccions de: • Gestió de traces. • Activitat del sistema. • Tasques planificades. • Gestió de programes. • Accés a taules. • Crides a funcions remotes • Gestió de transports. • Gestió d'impressores. • Gestió d'usuaris i autoritzacions. • Gestió de modes d'operació. • Gestió de base de dades. • Gestió de perfils d'instància. • Rendiment. • Gestió de mandants. • Gestió de Support Packages i Kernel A l'annex D es pot trobar el detall de les transaccions més rellevants de les diferents àrees recollides en aquest control.	C I D

4.5. ID – Intercanvi de dades

OBJECTIUS	
Garantir que l' intercanvi de dades es realitza de forma segura.	
CARACTERÍSTIQUES	
C38. El transport de dades reals de l'entorn productiu a entorns no productius ha d'estar controlat i autoritzat. S'ha d'analitzar i disposar de tècniques de dissociació o xifrat de dades per a garantir les mateixes mesures de seguretat que a l'entorn productiu.	C I
C39. En cas de necessitar xifrar la transmissió de dades (requeriments legals o de seguretat), implementar *SNC* per a xifrar la comunicació entre els clients i el servidor, donat que la informació viatja en clar.	C I

4.6. AU - Auditoria

OBJECTIUS	
Recollir les tasques i activitats d'auditoria dels sistemes.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C40. Caldrà facilitar les tasques d'auditoria per part de l'Oficina de Seguretat davant la revisió del compliment dels requeriments de seguretat marcats pel CTTI.	C I D

4.7. 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 l'administració de sistemes *SAP*.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C41. Es recollirà contractualment el compliment de les normes i guies que el CTTI tingui per *SAP* així com qualsevol altra norma de gestió o administració que sigui d'aplicació.	C I D
C42. Es garantirà el compliment de la *Norma de contractació de tercers*.	C I D
C43. 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 Centrals de la Generalitat de Catalunya, 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 Centrals de la Generalitat de Catalunya, 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

El CTTI publicarà aquesta guia a la seva intranet.

Quan apliqui, l'Oficina de Seguretat serà responsable de la distribució d'aquesta guia en l'entorn de Serveis Centrals de la Generalitat de Catalunya.

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

ABAP Workbench: És un entorn de desenvolupament d'ABAP, que és un llenguatge de programació de quarta generació creat per SAP.

Mandant: Separació lògica dins d'una instància que recull una agrupació d'unitats organitzatives, administratives i/o empresarials amb un únic objectiu comú. Cada mandant gestiona les seves pròpies dades i fitxers de taules mestres.

SAProuter: SAProuter fa el paper d'un proxy per a SAP, permet fins i tot fer connexions a través de VPN.

SNC (Secure Network Communication): Funcionalitat de SAP Netweaver per a xifrar la informació a nivell de transport.

SSF (Secure Store and Forward): És una funcionalitat que s'utilitza quan es vol utilitzar un producte extern de seguretat per a proporcionar signatures digitals i suport de xifrat als sistemes SAP.
Per a més informació: https://cw.sdn.sap.com/cw/docs/DOC-27307

Usuaris Tipus Dialog: Tipus d'usuari per usuaris nominals (persones) del sistema.

Usuaris Tipus System: Tipus d'usuari utilitzat per a tasques de procés desassistit i comunicació amb el sistema (crides RFC internes) i entre múltiples sistemes (crides RFC externes).

10 DOCUMENTACIÓ REFERENCIADA

- Manual_Arquitectura_SAP_CSTSAP v2.0
- Manual_Arquitectura_SAProuter_CSTSAP v1.0
- NOR-GSEG-070308-v1.0 Norma de gestió de vulnerabilitats de programari base.
- 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
- GE-NOR14-01 Norma de creació de DMZ.
- CT-NOR03 Norma de contractació de tercers
- Pla d'auditories de seguretat.

Protecció entorns SAP sobre Windows:
http://www.microsoft.com/Downloads/details.aspx?familyid=63D54A72-BC62-43CF-8EAE-444935E08B40&displaylang=en

11 PARAULES CLAU

SAP Netweaver, ABAP, SAPRouter, hardening, protecció.

12 HISTÒRIC DEL DOCUMENT

Versió 1.0
Versió inicial del document

13 ANNEX A – Configuració d'usuaris

A continuació s'indica a nivell informatiu els paràmetres més rellevants per a la configuració dels usuaris en els sistemes SAP.

- Per evitar l'ús d'una determinada contrasenya pot incloure-la en la taula **USR40**, on a més d'especificar contrasenyes concretes pot introduir expressions usant els caràcters comodí interrogant de tancament (?) i/o asterisc (*). Així amb l'expressió '*2009' es prohibiria l'ús de contrasenyes que acabessin amb els números 2009.
- **Login/fails_to_session_end:** Defineix el número d'intents fallits d'inici de sessió permesos abans de cancel·lar l' inici de sessió pel sistema (3 per defecte).
- **Login/fails_to_user_lock:** Defineix el número de vegades que un usuari pot introduir una contrasenya errònia abans que el seu compte quedi bloquejat fins la mitjanit del dia en qüestió. Per defecte dotze.
- **Login/failed_user_auto_unlock:** Desbloca usuaris bloquejats per intentar iniciar sessió incorrectament. Si val 1 (per defecte) el sistema no bloqueja usuaris. *No s´ ha de mantenir aquest valor per defecte*.
- **Login/system_client:** Especifica el client per defecte i emplena les seves dades a la pantalla d'inici de sessió automàticament.
- **Login/ext_security**: Si aquest paràmetre està activat (amb una "X") es pot especificar identificació addicional per a cada usuari (a user maintenance). Això s'utilitza si hi ha sistemes de seguretat implantats al voltant de SAP, com Kerberos o Secude.
- **Login/disable_multi_gui_login:** amb valor "1" reconeix i prevé múltiples intents d'inici de sessió d'un únic usuari en un servidor SAP des de diferents clientes (front-ends).
- **Rdisp/gui_auto_logout:** Especifica el temps màxim que transcorre des que l'usuari va realitzar qualsevol activitat per **darrer** cop (introduint alguna dada des de la interfície gràfica o movent-se pel sistema) fins que el sistema automàticament dóna la sessió per terminada. El valor per defecte és "0", que significa que aquesta directiva no s'aplica. No es recomanable mantenir aquest valor per defecte.
- **Login/min_password_lng**: Especifica la longitud mínima en caràcters de la contrasenya, pot oscil·lar entre tres i vuit.
- **login/min_password_lowercase:** Número mínim de caràcters en minúscules.
- **login/min_password_uppercase:** Número mínim de caràcters en majúscules.
- **login/min_password_specials:** Número mínim de caràcters especials.
- **login/min_password_letters:** Número mínim de caràcters de l'alfabet en la contrasenya.
- **login/min_password_digits:** Número mínim de caràcters numèrics obligatoris en la contrasenya.
- **login/min_password_diff:** Número de caràcters que han de ser diferents entre la nova contrasenya i l'anterior (per canvis de contrasenya realitzats per l'usuari).
- **login/password_history_size:** Número de contrasenyes guardades com historial de manera que no puguin repetir-se (mínim 1 i màxim 100).
- **Login/password_expiration_time:** Defineix el número de dies de vida d'una contrasenya després dels quals haurà de ser canviada per l'usuari. Per evitar que una contrasenya caduqui s'utilitza el valor "0".
- **login/password_compliance_with_current_policy:** Determina que durant els nous logins es verifiqui si la contrasenya compleix amb l'estàndard definit. (0 no comprova, 1 comprova) D'aquesta manera, les modificacions de paràmetres de seguretat impactaran immediatament en els usuaris requerint que realitzin un canvi de contrasenyes en el proper login si no compleixen la política actual.
- **login/password_max_idle_initial:** Màxim número de dies que la contrasenya definida per l'administrador (inicial) pot estar habilitada per que l'usuari l'utilitzi (0 a 1000). És utilitzat per evitar

que els usuaris siguin donats d'alta amb contrasenyes inicials però mai es connecten al sistema deixant una porta semi-oberta en el mateix sistema (contrasenyes inicials dèbils)

- **login/system_client:** Defineix el mandant per defecte que apareixerà proposat.
- **Rec/client:** Gravar tots els canvis relacionats amb les taules del sistema. El valor per defecte és desactivat, i es recomana canviar-lo.
- En el cas d'accedir a un servidor web SAP mitjançant un navegador d' Internet, el ticket d'accés s'emmagatzema en la memòria del navegador, tenint així una duració determinada. Aquesta duració es pot modificar en el paràmetre del sistema **login/ticket_expiration_time**, que per defecte és de 8 hores.
- El generador de contrasenyes aleatòries de SAP s'ha de configurar per a què generi contrasenyes robustes. Es configura a la taula PRGN_CUST mitjançant els valors:
  - **GEN_PSW_MAX_LETTERS**
  - **GEN_PSW_MAX_DIGITS**
  - **GEN_PSW_MAX_SPECIALS**

  que indiquen respectivament el número màxim de lletres, números i caràcters especials que el generador automàtic de contrasenyes (SU01 o SU10) utilitzarà, sempre i quan no es contradiguin amb els paràmetres definits en el perfil del sistema. A vegades SAP utilitza caràcters especials difícils de teclejar.

14 ANNEX B – Configuració de traces

A continuació s'indica a nivell informatiu els paràmetres més rellevants per a la configuració de les traces en els sistemes SAP.

- La taula TPLOG (a la que s'accedeix a través de la transacció **SE16**) permet observar els moviments d' un usuari durant una franja de temps determinada.

- La transacció **ST03N** permet observar el rendiment i la càrrega computacional de les diferents instàncies, però en el seu mode expert es pot detallar aquesta informació fins al nivell d'usuaris i transaccions.

- Per a observar els temps computacionals i d'ús de memòria per a controlar el rendiment de SAP sobre l'equip en que s'executi, existeixen certes transaccions que li facilitaran una sèrie de dades útils:

  - **ST06**: On es mostra el temps de resposta del sistema operatiu; de CPU, memòria en disc, memòria d'intercanvi i de xarxa.
  - **ST02**: Estat dels buffers de memòria usats.
  - **ST04N**: Temps de resposta i estat de la Base de Dades.

- La grandària dels logs del sistema es governa amb las variables **rslg/max_diskspace/central** i **rslg/max_diskspace/local**, segons es tracti del log centralitzat o local. Aquests arxius son cíclics, és a dir que una vegada omplerts es sobreescriuen les dades més antigues. Per a configurar un node com a node de registre d'esdeveniments central s'ha de fer mitjançant les següents variables:

  - **rslg/collect_daemon/host:** Node on s'ubica el log central,
  - **rslg/collect_daemon/listen_port:** Port d'entrada per al procés de recol·lecció de dades del log. Per defecte 14## on les ## són el número de sistema SAP.
  - **rslg/collect_daemon/talk_port**: Port de sortida per al procés de recol·lecció de dades del log. Per defecte 15## on les ## són el número de sistema SAP.
  - **rslg/send_daemon/listen_port**: Port d'entrada per al procés d'enviament de dades del log. Per defecte 13## on les ## són el número de sistema SAP.
  - **rslg/send_daemon/talk_port:** Port de sortida per al procés d'enviament de dades del log. Per defecte 12## on les ## són el número de sistema SAP.
  - **rslg/send_daemon_autostart:** Amb valor "0" el procés comença automàticament a l'arrancar el sistema.

- Existeix un mode de visualització de les traces del sistema anomenat estadístic que consisteix en una ordenació segons usuari, transacció, ús de memòria o crides RFC. No es tracta de substituir el log del sistema sinó de complementar-lo. S'accedeix a través de la transacció **STAT** i es configura mitjançant els següents paràmetres:

  - **stat/level:** Activa o desactiva el registro estadístic. Per defecte està activat.
  - **stat/version:** Per defecte amb el valor "2" que permet estadístiques sobre crides RFC i d'ús de memòria. L'altre valor ("1") s'utilitza per compatibilitat amb les versions 2.2 i anteriors i no realitza estadístiques sobre crides RFA ni ús de memòria.
  - **stat/file:** Ubicació del fitxer de traces estadístiques dins del sistema d'arxius.

- Es poden especificar les accions a registrar (relacionades amb la seguretat de la informació com per exemple quan un usuari intenta un inici de sessió amb una contrasenya errònia o es modifica un registre d'usuaris) en la transacció **SM19**, el propi log es pot trobar en la transacció **SM20** o **SM20N** i es poden esborrar els més antics a través de la transacció **SM18.** Els següents paràmetres defineixen:

- **rsau/ensable**: Activa el registre d'auditoria en un servidor d'aplicacions, per defecte està desactivat**.**
- **rsau/local/file:** Especifica la ubicació del fitxer en el sistema d'arxius.
- **rsau/max_diskspace/local:** Capacitat màxima del fitxer de traces.
- **rsau/selection_slots:** número de filtres utilitzats (definits en **SM19**) en el procés de registre d'esdeveniments.
- Per a poder accedir a les estadístiques un usuari necessita permisos sobre l'objecte **S_TOOLS_EX**, en cas contrari només podrà veure les seves pròpies estadístiques i no les d'altres usuaris.

- Mitjançant la transacció SLG1, es pot obtenir el registre de l'execució de determinades aplicacions (que s'indiquen en la transacció SLG0), des d'on es pot utilitzar l'informe RSFKT100 per a veure quins usuaris han accedit a aquestes aplicacions.

- Segons les versions es pot accedir a **SU01** o a l'aplicació **Authorization Infosystem** per a veure els canvis registrats sobre usuaris, perfils i autoritzacions.

- En quant al registre d'esdeveniments del sistema de transport existeix una variable de sistema anomenada ***transport/tp_logging***, el valor de la qual per defecte ja és "ON" des del moment de la instal·lació.

- Com a administrador es pot consultar les connexions d'usuaris i des de quines direccions IP, mitjançant la transacció **OS01,** "Presentation Server" i després en "Change View".

15 ANNEX C – Control d'accés

A continuació s'indica a nivell informatiu els paràmetres més rellevants per a la configuració de control d'accés en els sistemes SAP.

- Es poden bloquejar transaccions per a tots els usuaris, independentment de les seves autoritzacions (sempre que no tinguin autorització per a desactivar el bloqueig), a través de la transacció **SM01**. En la mateixa es pot indicar el codi de transacció a bloquejar i a partir de confirmar el bloqueig no es permetrà l'execució d'aquesta transacció per a cap usuari fins que no es torni a desbloquejar. Aquesta opció és útil per a impedir l'execució de transaccions que es considerin crítiques o que calgui bloquejar temporalment.

- Existeix un *procediment* que pot ajudar a l'administrador per administrar rols i perfiles *sense privilegis administratius totals* o, per a delegar-los en altres administradors mitjançant el *Profile Generator (transacció **PFCG**).* Aquests administradors, posseeixen uns privilegis limitats segons unes plantilles predeterminades. El procediment segons les recomanacions de SAP és el següent:
  - Un usuari (Administrador de dades) crea els rols (transaccions permeses més les autoritzacions) però els emmagatzema en el *Profile Generator* enlloc del registre mestre d'usuaris. Aquest administrador utilitza la plantilla SAP_ADM_PR (Administrador de perfils d'autorització).
  - Un altre administrador (administrador de rols) comprova el rol creat i l'aprova o denega mitjançant la transacció **SUPC.** Aquest administrador utilitza la plantilla SAP_ADM_AU (Administrador de dades d'autorització – transaccions)
  - L'administrador d'usuaris assigna els roles als usuaris (transacció **SU01** o **CUA**). Aquest administrador utilitza la plantilla SAP_ADM_US (administrador d'usuaris).

SAP utilitza diferents ports TCP per a comunicar-se amb els clients. L'interfície gràfica (SAP GUI) usa els ports 32<nn> on nn correspon al número d'instància que pot anar del 00 a 98, mentre que la comunicació via RFC usen els ports 33<nn>. Si la comunicació es via grup de logon, es comunica directament amb el message server pel port 36<nn>. Per defecte aquesta comunicació està en text clar.

16 ANNEX D – Transaccions amb accés restringit a administradors

A continuació s'indiquen les transaccions més rellevants a les quals només ha de tenir-hi accés els administradors.

- Gestió de Logs
  - SM21 Transacció de Logs
  - ST22 Dumps
- Activitat al sistema
  - SM12 Entrades de bloqueig
  - SM13 Registres d'actualització
  - SM50 Processos
  - SM04 Usuaris connectats
- Tasques Planificades
  - SM37 Revisió de jobs
  - SM36 Creació de jobs
  - DB13 Tasques planificades
  - DB12 Gestió de backups
- Gestió de programes
  - SE38 Creació de reports
- Accés a taules
  - SE11 Creació i modificació de taules
  - SE12 Configuració de taules
  - SM30 Visualització de taules
- Crides a funcions remotes
  - SM59 Gestió d'RFCs
  - SM58 Logs RFCs
- Gestió de transports
  - STMS Transport management
  - SE01 Gestió d'ordres de transport
  - SE10 Gestió d'ordres de transport
- Gestió d'impressores
  - SPAD Creació i modificació
  - SP01 Logs d'impressió
- Gestió d'usuaris i autoritzacions
  - SU01 Creació y modificació
  - SU10 Tractament massiu
  - PFCG Gestió d'autoritzacions
  - SU53 Objectes d'autorització
  - SUIM Cerca de rols
- Gestió de modes d'operació
  - SM63 Planificació
  - RZ04 Modes d'operació
- Gestió de base de dades
  - DB02 Database performance

- Gestió de perfils d'instància
  - RZ10 Tratamiento de perfiles
  - RZ11 Actualització paràmetres

- Rendiment
  - ST02 Tune sumary
  - ST03n Càrrega de treball
  - ST06 Monitor SO

- Gestió de mandants
  - SCC4 Gestió de mandantes
  - SCC7 Import de mandants
  - SCC8 Export de mandants
  - SCCx …

- Gestió de Support Packages i Kernel
  - SPAM - Patches
  - SAINT- Add-ons
  - SPAU – Gestió de canvis

- Altres transaccions d'interès
  - SM02 - Enviament massiu de missatges a usuari
  - SM30 - Modificació de dades d'una taula
  - SMLT - Idiomes
  - SMLG - Grups de logon
  - OSS1 – Accés a la SAPNet
  - SNOTE – Download de notes OSS
  - SLICENSE – Gestió llicències