Seguretat de base de dades Versió Sprint 3.0

(Infraestructures)

VIA – Vilanova Intelligent Airport

Equip 1

Index

Introducció:

Aquest informe especifica els requeriments de seguretat aplicables a la base de dades del projecte VIA – Vilanova Intelligent Airport (PTIN 19-2020) referent a la part d'infraestructures. Queda obert a millores i suggerències per part del client empresarial, client tècnic, assessor metodològic i qualsevol altre membre dels equips del terminal 1

Actual: sprint 3.0 (/04/2020)
Anteriors: sprint 2.0
Actualitzacions: - Backups tipus snapshot i en màquina remota

Consensuat:

- ❏ Política de les còpies de seguretat BackUps
- ❏ Infraestructura requerida
- ❏ Pla de contingència de BackUp
- ❏ Punts a revisar al realitzar el Pla de Contingència de Backup

Validat:

- ➢ Política de les còpies de seguretat BackUps [pendent d'implementar]
- ➢ Infraestructura requerida [pendent d'implementar]
- ➢ Pla de contingència de BackUp [pendent d'implementar]
- ➢ Punts a revisar al realitzar el Pla de Contingència de Backup [pendent d'implementar]

Política de les còpies de seguretat BackUps:
Quinzenal: còpia incremental inversa Snapshot en màquina remota
Diàries: còpia incremental inversa Snapshot en màquina remota

Cada 6 mesos: còpia local en màquina remota
⋆*Tipus snapshot i en màquina remota explícitament demanat per el client*

Infraestructura requerida:

Recolzament de nodes:

Sempre hi haurà un segon node que pot entrar en calent per substituir al principal en cas de fallada és a dir, per tenir un recolzament immediat en cas de fallada del principal. També hi haurà un tercer node net que farà el rol d'auxiliar

Pla de contingència de BackUp:

Immediatament tras succeir un "desastre".
- Entrarà en funcionament el node secundari o de recolzament.

Durant la resolució de la situació.
- Mentres estigui el node de recolzament funcionant es buscarà la recuperació del principal i la posada en marxa d'un tercer, l'auxiliar, amb una restauració com a mirall del node secundari.

Després d'haver-se restablert el servei
- En cas de recuperació del node primari, aquést tornaria a ser el principal i el node secundari tornaria a ser de recolzament
- En cas de que no s'hagi recuperat el node primari, el node secundari passaria a convertir-se en el node primari i l'auxiliar en el secondari de recolzament. Alhora, es farà un enviament d'un missatge d'avís al responsable designat d'infraestructures amb aquests camps:

Destinatari: responsable@email.org
Tema: Node principal caigut
Body:
Data - hh/mm/ss
Prioritari, creació d'un node auxiliar net i preparat per la connexió
Guardat per a posterior revisió del node principal caigut i recuperació, si es pot, de la base de dades

També, es farà un enviament d'un missatge d'avís al responsable designat per l'aeroport en termes de privacitat amb aquests camps:

Destinatari: responsable@email.org
Tema: Caiguda del node principal
Body:
Data - hh/mm/ss
Descripció de la incidència així com de la localització de la base de dades. També s'informarà si està corrompuda i si hi ha hagut pèrdues i/o filtracions de dades personals.

Freqüència de realització del Pla de Contingència de BackUp:

Recomanat fer un simulacre de restauració del Backup cada 6 mesos per donar compliment a la LOPD, verificar la funcionalitat del sistema i poder comparar resultats amb pròximes restauracions.

Punts a revisar al realitzar el Pla de Contingència de Backup:

Revisió del repositori de Backup:
Revisió de forma periòdica de l'estat dels discos durs
Revisió de forma periòdica de l'espai disponible

Revisió de les tarees de BackUp:
Control de forma periòdica del tamany dels arxius de Backup
El.liminar còpies antigues per alliberar espai en cas de ser necessaris: còpies assegurades i prèviament autoritzades per el responsable designat per l'aeroport
Actualització de versions estables del software de BackUp
Notificacions: tenir actualitzats les adreces de mails dels corresponents responsables

Restauració de BackUps:
Crear un entorn de TEST per restauració: Creació d'un servidor bessó a l'original independent per fer tests de restauració
Comprovar la integritat dels arxius de restauració
Restaurar arxius individuals i apuntar temps de restauració.
Si la restauració fos fallida, resoldre el problema i, si no fos possible, s'el.liminaria i es faria un enviament d'un missatge d'avís al responsable designat per l'aeroport en termes de privacitat amb aquests camps:

Destinatari: responsable@email.org
Tema: Restauració fallida
Body:
Data - hh/mm/ss
Descripció de la incidència així com de la localització de l'arxiu de restauració.També s'informarà de l'el.liminació de l'arxiu corromput

Informe de resultats:
Després de l'execució del Pla de Contingència, el responsable designat per l'aeroport rep un informe explicant la situació detallant:

- Tamanys dels fitxers de còpia
- Temps reals de restauració
- Percentatge d'èxit mensual de les tarees de restauració

Annex: documentació rebuda per part de l'equip responsable A2

Sprint 2:

--FeedBack de la versió 2:

Política de les còpies de seguretat BackUps:

Considerem que amb la còpia local quinzenal i la snapshot cada 24h ja és suficient. La còpia mirall entre nodes es considera excessiva. El tema de disk mirroring es queda pendent per desconeixement

Infraestructura requerida:

Recolzament de nodes:

Estem d'acord, ja s'està contemplant així des de l'inici, però actualment no és la nostra prioritat assegurar això

Encriptació de dades:

Punt pendent de consensuar

Privacitat(Informació confidencial de dades personals):

No en correspon, apartat pendent de realitzar

Pla de contingència de BackUp:

Immediatament tras succeir un "desastre"

Estem d'acord

Definició dels objectius de recuperació:

Pendent, es desconeix el que és

Freqüència de realització del Pla de Contingència de BackUp:

D'acord

Punts a revisar al realitzar el Pla de Contingència de Backup:

Revisió del repositorio de Backup:

Revisió de les tarees de Backup:

Restauració de BackUps:

Informe de resultats:

D'acord amb el punts presentats menys en el gràfic. Se'l considera excessiu. Usar una alternativa no gràfica per complir la mateixa funció ja és suficient.

SPRINT 2

Política de les còpies de seguretat BackUps:
A l'espera del sistema proposat per l'equip d'infraestructures
Mensual: còpia completa externa
Còpia de seguretat de tots els arxius i carpetes en un dispositiu extern (ubicat en altre ubicació física)
Quinzenal: còpia completa local
Còpia de seguretat de tots els arxius i carpetes en un dispositiu local en una partició diferenciada
Diari: còpia incremental inversa Snapshot cada 24 hores
Realització programada de backups incrementals inverses tipus Snapshot perquè la seva restauració és més ràpida i es manté la capacitat de tornar a les versions anteriors per debugar errors a posteriori
Constant: còpia mirall entre node principal i node secundari Actualització S3.0
Tipus específic RAID 1 (disk mirroring), commutació immediata en cas de failover amb una alta disponibilitat en temps de recuperació

Infraestructura requerida:
A l'espera del sistema proposat per l'equip d'infraestructures
Recolzament de nodes:

Sempre hi haurà un segon node que pot entrar en calent per substituir al principal en cas de fallada és a dir, per tenir un recolzament immediat en cas de fallada del principal. També hi haurà un tercer node net que farà el rol d'auxiliar

Encriptació de dades:

Es farà servir criptografia asimètrica (key-pairs) amb certificats, encara que l'ús d'algoritmes addicionals en les operacions de consultes pot fer disminuir el rendiment en l'accés a la base de dades, s'utilitzaran per reforçar la seguretat.
El servidor de CA (Certification Authority) serà independent del servidor de BBDD amb una generació de certificats de clau públicas originats per aquest servidor.
S'usaran algorismes d'encriptació RSA amb protocols TLS (Transport Layer Security).
El tamany de les claus públiques serà de 1024 bits que és el mínim amb el qual no es coneix un mètode eficient de factorització

Privacitat(Informació confidencial de dades personals):

-Tabla PASSATGERS
nombre: nombre
apellidos: apellidos
nació: fecha de nacimiento
género: hombre/mujer
nom: nom d'usuari
password: xifrat

-Protocol en cas de violació de dades personals:
En cas de violació de dades personals, segons l'article 33 de l'RGPD, *Notificació d'una violació de la seguretat de les dades personals a l'autoritat de control*, es farà un enviament d'un missatge d'avís al responsable designat en termes de privacitat per l'aeroport amb aquests camps:

Destinatari: responsable@email.org
Tema: Violació de dades personals
Body:
Data - hh/mm/ss
Descripció de la incidència així com el passatger/s i els seus camps afectats

Pla de contingència de BackUp:
A l'espera del sistema proposat per l'equip d'infraestructures

Immediatament tras succeir un "desastre".
- Entrarà en funcionament el node secundari o de recolzament.
Durant la resolució de la situació.
- Mentres estigui el node de recolzament funcionant es buscarà la recuperació del principal

i la posada en marxa d'un tercer, l'auxiliar, amb una restauració com a mirall del node secundari.
Després d'haver-se restablert el servei
- En cas de recuperació del node primari, aquést tornaria a ser el principal i el node secundari tornaria a ser de recolzament
- En cas de que no s'hagi recuperat el node primari, el node secundari passaria a convertir-se en el node primari i l'auxiliar en el secondari de recolzament. Alhora, es farà un enviament d'un missatge d'avís al responsable designat d'infraestructures amb aquests camps:

Destinatari: responsable@email.org
Tema: Node principal caigut
Body:
Data - hh/mm/ss
Prioritari, creació d'un node auxiliar net i preparat per la connexió
Guardat per a posterior revisió del node principal caigut i recuperació, si es pot, de la base de dades

També, es farà un enviament d'un missatge d'avís al responsable designat per l'aeroport en termes de privacitat amb aquests camps:

Destinatari: responsable@email.org
Tema: Caiguda del node principal
Body:
Data - hh/mm/ss
Descripció de la incidència així com de la localització de la base de dades. També s'informarà si està corrompuda i si hi ha hagut pèrdues i/o filtracions de dades personals.

Definició dels objectius de recuperació: Actualització S3.0

El RPO (Recovery Point Objective): Actualització S3.0

El RTO (Recovery Time Objective): Actualització S3.0

Freqüència de realització del Pla de Contingència de BackUp:

Recomanat fer un simulacre de restauració del Backup cada 6 mesos per donar compliment a la LOPD, verificar la funcionalitat del sistema i poder comparar resultats amb pròximes restauracions.

Plans de recuperació del BackUp de la base de dades: Actualització S3.0

Punts a revisar al realitzar el Pla de Contingència de Backup:
A l'espera del sistema proposat per l'equip d'infraestructures

Revisió del repositorio de Backup: Millores S3.0
Estat dels discos durs
Espai disponible

Revisió de les tarees de BackUp: Millores S3.0
Anotació del tamany dels arxius de Backup
El.liminar còpies antigues per alliberar espai: còpies assegurades i prèviament autoritzades per el responsable designat per l'aeroport
Encriptació de les dades en totes les tarees que afecten el BackUp
Actualització de versions del software de BackUp
Notificacions: tenir actualitzats les adreces de mails dels corresponents responsables

Restauració de BackUps: Millores S3.0
Crear un entorn de TEST per restauració: Creació d'un servidor bessó a l'original independent per fer tests de restauració
Comprovar integritat dels arxius de restauració
Restaurar arxius individuals i apuntar temps de restauració.
Si la restauració fos fallida, resoldre el problema i, si no fos possible, s'el.liminaria i es faria un enviament d'un missatge d'avís al responsable designat per l'aeroport en termes de privacitat amb aquests camps:

Destinatari: responsable@email.org
Tema: Restauració fallida
Body:
Data - hh/mm/ss
Descripció de la incidència així com de la localització de l'arxiu de restauració.També s'informarà de l'el.liminació de l'arxiu corromput

Informe de resultats: Millores S3.0
Després de l'execució del Pla de Contingència, el responsable designat per l'aeroport rep un informe explicant la situació detallant:

- Tamanys dels fitxers de còpia
- Temps reals de restauració
- Percentatge d'èxit mensual de les tarees de restauració
- Gràfic actualitzat de la situació dels BackUps.
- Propostes de millora (si s'escau)

Annex: documentació rebuda per part de l'equip responsable A4

Sprint 1:

--FeedBack de la versió 1:
Usuaris:

Administrador de la base de dades:Ok

Política de generació de contrasenyes:Ok
Rols-usuaris de la base de dades(inf. proporcionada per l'equip A4):

¿A que haceis referencia con "personal de alta autorización" o con "personal con autorización"?
Política general de la base de dades: Ok a tot
Política de les còpies de seguretat BackUps: Excesiva, si lo hacemos con AWS ya tiene amazon copias más que suficientes.
Infraestructura requerida: No es responsabilidad nuestra hablar acerca de la infraestructura.
Privacitat(Informació confidencial de dades personals): Nosotros teníamos planeado hacer las notificaciones a los usuarios, pero esto es una notificación a un responsable. ¿Podrías especificar más a que os referis con este apartado?
Pla de contingència de BackUp: No es responsabilidad nuestra hablar acerca de la infraestructura.
Punts a revisar al realitzar el Pla de Contingència de Backup: No es responsabilidad nuestra hablar acerca de la infraestructura.

-Resposta:
"Privacitat(Informació confidencial de dades personals): Nosotros teníamos planeado hacer las notificaciones a los usuarios, pero esto es una notificación a un responsable. ¿Podrías especificar más a que os referis con este apartado?"
Me refiero a las notificaciones requeridas a un hipotético responsable designado por la administración del aeropuerto, externo al equipo informático, experto en LOPD y responsable de todos estos asuntos. Esta figura es un requerimiento y una obligación por ley.
"¿A que haceis referencia con "personal de alta autorización" o con "personal con autorización"?"
Es la definición dada por vosotros mismos en el formulario del sprint 0 y confirmado en el formulario del sprint 1