



Respaldos de Solución de Trazabilidad

Servicios Tecnológicos
versión 1

Histórico de revisiones			
Fecha	Versión	Descripción	Autor
28/4/2016	1	Documento realizado en base a la planilla entregada por el equipo Backups de HG (SSI 64375)	Elena Viojo

1 Introducción.-

En este documento se describirá la implementación de la solución de respaldos utilizadas para trazabilidad, en función de la herramienta de IBM, Tivoli Storage Manager (TSM), que es utilizada para esta solución de respaldos actualmente.

2 Detalle de implementación de respaldos.-

La instanciación de un respaldo está compuesto de los siguientes puntos.

Fecha Alta-TSM.-

Fecha en la que se le dio de alta y empezó a ejecutarse y monitorearse formalmente el respaldo.

Host.-

Nombre del equipo que se está respaldando

TSM/Clientes.-

Nombre del nodo con el que se le identifica el respaldo en el servidor de TSM

Instancia.-

Instancia de TSM a la cual pertenece el nodo y donde se encuentran sus respaldos

Política.-

Política de retención que se usa para dicho respaldo.

Retención.-

Es la cantidad de tiempo que los archivos respaldados permanecen en cinta, una vez que son borrados del origen, en este caso 30 días para los backups de tipo incrementales y 60 días para los archives (full).

Proceso.-

Nombre del script que realiza el respaldo y que forma parte del proceso de respaldos

Contenido.-

Directorio o base de datos que se respalda

Tipo de Respaldo.-

Forma en la que opera el respaldo, *Incremental* es cuando el backup solo respalda los cambios realizados luego de la última vez que se ejecutó, *Archive* (Full) cuando se respalda el contenido total de un directorio cada vez que se es ejecutado.

Frecuencia.-

Indica la frecuencia con la que el respaldo se ejecuta, esta puede ser más de una vez en el día como en el caso de los archivedlogs de las bases de datos, o diaria y/o semanalmente. Por lo general la frecuencia se asocia al tipo de respaldo en el caso de una frecuencia diaria el tipo de respaldo es incremental, y en el caso de una frecuencia semanal el respaldo es de tipo archive.

Sistema operativo.-

Sistema Operativo del equipo a respaldar.

IP(SERV/BCKP).-

Muestra la IP de Servicios y Respaldo

Activo/Pasivo.-

Muestra el estado del respaldo, este es Activo cuando el equipo se está respaldando y Pasivo cuando está configurado pero se usa solo como contingencia y configurado cuando está configurado e instalado en el equipo pero no se está usando.

3 Respaldos

Fecha- Alta-TSM	Host	TSM /Clientes	Instancia	Política	Proceso	contenido	Tipo respaldo	Frecuencia	Sistema operativo	IP(SERV/BCKP)	Activo/Pasivo	
15/3/16	prod-trazabilidad-bd01.gestion.red.uy	prodtrazabilidadbd01_DB	AGESIC-TSM01	PD-PGE-GEN	30 dias - 60 dias	Bckp_online 2tsm Bckp_archive d2tsm.sh	/srv/pgdata/data/* /srv/pgdata/archivelogs/archives/* /srv/pgdata/archivelogs/archives/*	incremental	Diario	CentOSrele ase 6.7	192.168.20.10 / 192.168.15.10	Activo
15/3/16	prod-trazabilidad-bd02.gestion.red.uy	prodtrazabilidadbd02_DB	AGESIC-TSM01	PD-PGE-GEN	30 dias - 60 dias	respaldo_ts m.sh		incremental	Diario	CentOSrele ase 6.7	192.168.20.11/ 192.168.15.11	Pasivo
15/3/16	prod-trazabilidad-app01.nube.red.uy	PRODTRAZABILIDADAPP01_FS_DIARIO	AGESIC-TSM01	PD-PGE-GEN	30 dias - 60 dias	respaldo_ts m.sh	/opt/trazabilidad/wildfly/*	incremental	Diario	CentOSrele ase 6.7	192.168.5.10 / 192.168.10.10	Activo
15/3/16	prod-trazabilidad-app02.nube.red.uy	PRODTRAZABILIDADAPP02_FS_DIARIO	AGESIC-TSM01	PD-PGE-GEN	30 dias - 60 dias	respaldo_ts m.sh	/opt/trazabilidad/wildfly/*	incremental	Diario	CentOSrele ase 6.7	192.168.5.11 / 192.168.10.11	Activo
15/3/16	prod-trazabilidad-app03.nube.red.uy	PRODTRAZABILIDADAPP03_FS_DIARIO	AGESIC-TSM01	PD-PGE-GEN	30 dias - 60 dias	respaldo_ts m.sh	/opt/trazabilidad/wildfly/*	incremental	Diario	CentOSrele ase 6.7	192.168.5.12 / 192.168.10.12	Configurado

4 Datos y operativa de monitoreo.-

Cada proceso de respaldo genera un informe con el estado de finalización del respaldo que es enviado a un centro de monitoreo y seguimiento de incidentes, cuando este estado es de error o bien no es recibido por el centro de monitoreo, se genera un ticket que es asignado a un técnico apropiado, quien documenta lo realizado en el ticket para dar solución al incidente.