|  |  |  |
| --- | --- | --- |
| C:\Users\User\Downloads\Telegram Desktop\photo_2018-01-15_16-09-10.jpgphoto_2018-01-15_16-09-10  **BAHAGIAN PENDIDIKAN TEKNIK DAN VOKASIONAL**  **KEMENTERIAN PENDIDIKAN MALAYSIA**  **ARAS 5 & 6, BLOK E14, KOMPLEKS E,**  **PUSAT PENTADBIRAN KERAJAAN PERSEKUTUAN**  **KERTAS PENERANGAN**  ***(INFORMATION SHEET)*** | | |
| **KOD DAN NAMA NOSS** | IT-010-3:2016 APPLICATION MODULE DEVELOPMENT | |
| **KOD DAN NAMA CU/WA** | C03 – APPLICATION MODULE INTEGRATION | |
| **NAMA PROGRAM** | TEKNOLOGI SISTEM PENGURUSAN PANGKALAN DATA DAN APLIKASI WEB | |
| **TAHAP DAN SEMESTER** | 3 (SEMESTER 2) | |
| **KOD DAN TAJUK KURSUS** | KPD2042 BACKUP STRATEGIES MANAGEMENT | |
| **NO.DAN TAJUK KOMPETENSI** | K4 PRODUCE REPORT | |
| **NO. KOD KSKV** | KPD2042/ P(7/7) | Muka Surat : 1  Drp : 6 |
| **NO. KOD NOSS** | IT-010-3:2016-C03/ P(7/7) |

TAJUK/ TITLE:

MENGHASILKAN LAPORAN

TUJUAN/ PURPOSE:

Kertas penerangan ini adalah bertujuan menerangkan mengenai:

* Menghasilkan laporan sandaran (*backup*)
* Menerangkan isu-isu penyelenggaraan

**4.1 MENGHASILKAN LAPORAN SANDARAN**

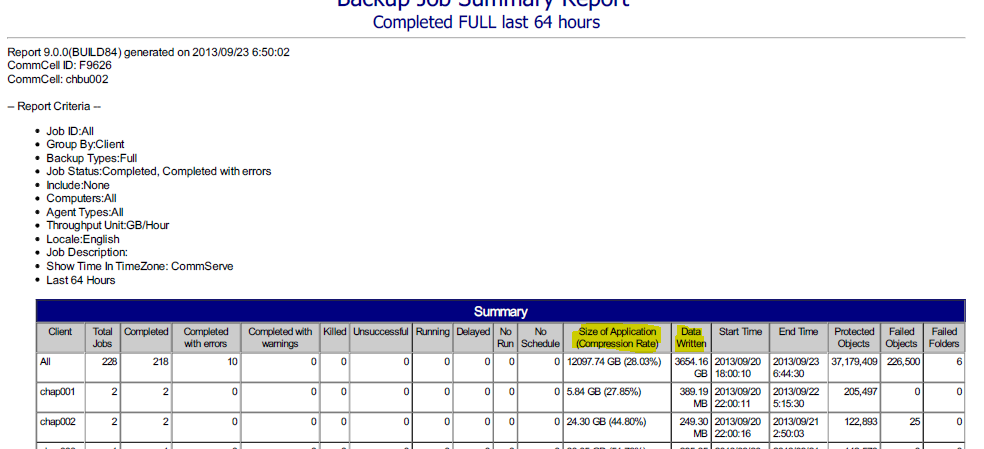
Laporan status sandaran menyediakan maklumat tentang masa lalu setiap kerja sandaran *(backup)* yang telah dilaksanakan dalam tempoh masa yang ditentukan, dan menunjukkan berapa jumlah data yang disandarkan.

Laporan status sandaran (*backup*) tidak mempunyai format yang khusus, bergantung kepada *Standard Operation Procedure (SOP*) yang telah ditetapkan oleh sesebuah syarikat.

Jadual 4.1 menyenaraikan dan menerangkan data yang tersedia dalam Laporan status sandaran (*backup*), dan menunjukkan sama ada setiap lajur diperlukan atau pilihan.

| **Backup Status Report Data Column** | **Description** | **Required** | **Optional** |
| --- | --- | --- | --- |
| Vault | Name of the vault where the backup data is saved |  | ✓ |
| Site | Site of the backup |  | ✓ |
| Computer | Computer or environment that was backed up | ✓ |  |
| Job | Name of the backup job | ✓ |  |
| OS Version | Operating system of the computer or environment that was backed up |  | ✓ |
| Agent Type | Type of Agent that ran the backup |  | ✓ |
| Backup Date | Date and time when the backup started |  | ✓ |
| Deleted At | If the backup data has been deleted, date and time when the safeset was deleted from the vault |  | ✓ |
| Backup Duration | Length of time that the backup ran |  | ✓ |
| Last Backup Original Size (GB) | Amount of data that was backed up from the computer or environment, in gigabytes |  | ✓ |
| Delta Size (MB) | Amount of changed data extracted during the backup, before compression, in megabytes |  | ✓ |
| Result | Outcome of the backup session: Successful or Failed | ✓ |  |

Jadual 4.1

Rajah 4.1 menunjukkan contoh laporan bagi proses sandaran yang telah dijalankan .

Rajah 4.1

**4.2 ISU-ISU PENYELENGGARAAN**

1. Sandaran (***Backup*) anda tidak berfungsi.**

Sebelum membuat sebarang perubahan pada sistem pengeluaran (*production system*) anda, pastikan (*backup*) anda berfungsi. Menjalankan beberapa pemulihan ujian jika ingin memadam data kritikal. Sebelum proses sandaran (*backup*), anda mungkin ingin memastikan anda telah memilih [lokasi sandaran yang betul](http://www_ms_5b44717b2a1a6b1501da5371_pipe.bablic.com/blog/selecting-a-backup-location/).

2. **Penggunaan cakera tidak mencukupi atau tidak sesuai.**

Jangan gunakan sistem pengeluaran anda sebagai sistem arkib. Padam log lama, e-mel, dan versi perisian tidak digunakan lagi supaya isu keselamatan yang disebabkan oleh pengisian versi lama dapat dielakkan. Jejak data yang lebih kecil membolehkan pemulihan yang lebih pantas. Jika penggunaan anda melebihi 90% daripada kapasiti cakera, sama ada mengurangkan penggunaan atau menambah lebih banyak storan. Jika *partition* anda mencapai 100%, pelayan anda mungkin berhenti bertindak balas, jadual pangkalan data boleh rosak dan data mungkin hilang.

3. **Kurang pemantauan terhadap**RAID**.**

Semua pelayan pengeluaran (*production server*) harus menggunakan RAID. Adalah penting untuk mengawasi status RAID. Kegagalan pelayan yang lengkap dapat menjadikan proses penggantian drive mudah ke dalam senario pemulihan yang lama.

4. Tidak mengemaskini **OS dengan kerap.**

Kemas kini untuk sistem Linux sering dikeluarkan. Jika menggunakan sistem pengoperasian (OS) boleh mendatangkan risiko. Itulah sebabnya perlu menggunakan alat pengurusan *patch* automatik dan memantau status sistem untuk memaklumkan apabila sistem pengoperasian sudah lama tidak dikemaskini. Sekiranya anda mengemas kini pelayan anda secara manual (atau jarang), anda mungkin terlepas kemas kini keselamatan (*security updates*) yang penting. *Hackers* sering mengimbas sistem yang mempunyai kelemahan atau tidak kemaskini dalam masa beberapa jam setelah isu didedahkan.

5. Tidak mengemaskini **Panel Kawalan (*control panel*) dengan kerap.**

Jika anda menggunakan panel kawalan atau pelayan kawalan, pastikan anda mengemas kini juga. Ini bukan sahaja mengemaskini panel kawalan itu sendiri, tetapi juga mengemaskini perisian yang dikendalikannya.

6.  **Tidak mengemasikini aplikasi dengan kerap.**

Merujuk kepada penyelidikan, aplikasi web menyumbang lebih daripada 95% dari semua pelanggaran keselamatan. Pastikan anda mengemaskini aplikasi web anda, terutamanya *platform* popular seperti WordPress.

7.A**lat pengurusan jauh tidak berfungsi.**

Sekiranya pelayan diletakkan bersama atau dengan pembekal pelayan, anda perlu memastikan alat pengurusan jauh anda berfungsi. Kawalan jauh, *reboot* jauh dan mod menyelamat merupakan tiga [alat yang penting untuk pengurusan pelayan (*server*) jauh](https://www_ms_5b44717b2a1a6b1501da5371_pipe.bablic.com/blog/3-essential-server-management-tools-for-your-dedicated-server/).

8.  **Perkakasan mempunyai ralat.**

Menyemak log untuk sebarang tanda masalah perkakasan. *Notification* yang terlalu panas, kesilapan membaca cakera dan kegagalan rangkaian boleh menjadi penunjuk awal terhadap kegagalan perkakasan. Ralat ini jarang berlaku tetapi perlu dititiberatkan, terutamanya jika sistem tidak berfungsi dalam keadaan normal.

9. **Penggunaan pelayan yang yang terhad .**

Sentiasa semak cakera pelayan, CPU , RAM dan penggunaan rangkaian. Jika anda mencapai had atau melebihi kapasiti, anda hendaklah merancang untuk menambah sumber ke pelayan (*server*) atau berpindah kepada pelayan yang baru.

10. **Akaun pengguna tidak dikemaskini.**

Sekira berlakunya pertukaran kakitangan, pembatalan pelanggan atau perubahan pengguna lain, mengeluarkan maklumat dan rekod daripada sistem adalah perlu agar tidak berlaku pertindihan data. Menyimpan akaun pengguna lama melibatkan keselamatan dan risiko undang-undang. Bergantung pada kontrak perkhidmatan, sesebuah organisasi atau syarikat mungkin tidak mempunyai hak untuk mengekalkan data pelanggan setelah mereka menamatkan perkhidmatan.

11. **Kata laluan tidak dikemaskini.**

Kata laluan hendaklah ditukar atau dikemaskini setiap 6 hingga 12 bulan, terutamanya jika anda telah memberikan kata laluan kepada orang lain untuk penyelenggaraan.

12. **Pemeriksa keselamatan sistem tidak berfungsi.**

Pemeriksaan berkala keselamatan pelayan (*server*) anda menggunakan alat pengauditan jauh seperti Nessus. Pemeriksaan keselamatan tetap berfungsi sebagai pemeriksaan konfigurasi sistem, kemas kini OS dan risiko keselamatan yang berpotensi. Pemeriksaan ini hendaklah dilakukan sekurang-kurangnya 4 kali setahun dan lebih baik pada setiap bulan. Selain itu, mengkaji semula [10 undang-undang pentadbiran keselamatan yang tidak berubah](http://www_ms_5b44717b2a1a6b1501da5371_pipe.bablic.com/blog/10-immutable-laws-of-security-administration-revisited/).

**SOALAN** / *QUESTION* :

1. Terangkan lapan jenis isu-isu penyelenggaraan.
2. Berikan definisi laporan sandaran secara ringkas.