Data Centre Management

A newsletter for IT Professionals

Issue 8

I. Background of Data Centre Management

Data center management is a holistic process to oversee the operational and technical issues within a data centre or server room. It covers environmental control, physical security, hardware server operations and management of the services and applications used for data processing.

Through implementing a series of operational procedures and deploying specialised hardware and software, data centre management provides IT operational staff a clear picture of universities' data centre operating status, including real-time information on health, connectivity and resource utilisation, to effectively manage the data centers. A comprehensive data centre management solution also integrates information technology and facility / infrastructure management disciplines to provide necessary security control to protect universities' information assets from various threats.

Some basic components of data centre management are:

Environmental Control

The physical environment of a data centre, including temperature, humidity, power supply, is rigorously controlled since system hardware can only operate normally within defined ranges of temperature, humidity and voltage. Environmental control devices usually include air conditioning, ventilation system, temperature / humidity sensors, power surge suppressors and UPS.

In addition, current data centre management practice also aims at protecting IT assets from environmental hazards, such as fire and floods, by deploying fire suppression systems and raised floor.

Physical Security

Data centre security is becoming an integral part of robust and thriving data centre management solutions. Systems and devices hosted within data centres store sensitive information and support mission critical services of universities. With the increasing reliance on IT services in universities daily operations, data centres have become high-value targets and should be adequately protected from being compromised, both logically and physically.

Reference:
http://www.datacentresols.com/pdf/An-Introduction-to-Data-Center-Infrastructure-Management-English.pdf
http://www.assetgen.com/knowledgebase/Data%20Center%20Visualization%20with%20Visio.pdf

I. Background of Data Centre Management (cont’d)

Centralised Asset Inventory or Repository

A centralised asset inventory or repository is an accurate and authoritative database that records all data centre assets of a university, including application servers, network devices, power equipments (e.g. Uninterrupted Power Supply), and Heating, Ventilating & Air Conditioning (“HVAC”) devices. By implementing IT asset discover and tracking function, the IT management is able to accurately record data centre assets’ details, such as hardware / software specifications, supported IT services, target user groups and interdependences with other universities’ information systems or operations. For large scale data centres, automated asset inventory or repository software is installed to achieve efficiency and avoid human errors.

Capacity Planning

Capacity planning is performed by data centre IT staff to estimate the amount of information resources required to support the desired levels of services. The estimation leverages the data collected during the capacity monitoring process and requirements gathered from various academic or administrative departments. Effective capacity planning improves the overall performance and availability of the information systems hosted within the data centres through identifying underutilised resources and future capacity needs.

Operations

Batch job processing plays a vital role in sustaining the universities’ daily operations. IT staff working within Data Centre follow defined operational procedures or ad-hoc user requests to execute batch jobs manually or automatically through the use of job schedulers. Completion status of those batch jobs are closely monitored to ensure that any job failures are timely followed up and resolved.

Real-Time Data Collection and Monitoring

Various system information, hardware status and environmental data are collected through manual monitoring process or by automated tools. With such information, data centre IT staff can perform real-time capacity monitoring, effective usage trend analysis and immediate data centre incident response. Monitoring and control is a critical element of maintaining desired availability for universities’ critical IT services. Sophisticated monitoring software can provide proactive surveillance on the status of data centre assets, enable quick assessment of present situation and notify the appropriate IT staff should there be any threats that affect the availability of any information systems hosted within the data centres.

Reporting and Communication

A data centre management solution establishes specific responsibilities for each functional teams or IT staff, and determines clear reporting lines to enable timely exchange of operational status, incidents and management decisions. Right IT staff members are located for handling routine batch tasks, ad-hoc maintenance requests, installation jobs or urgent problems. A regular reporting function with the data centre management team also feeds IT management with up-to-date information for better data centre planning and administration.

Reference:
http://www.teamquest.com/pdfs/whitepaper/tqeb01.pdf
http://www.ciscosystems.net/en/US/solutions/collateral/ns170/ns896/ns1095/aag_c45-647419.pdf

I. Background of Data Centre Management (cont'd)

Key Benefits Achieved through Effective Data Centre Management

- **Cost and Energy Saving** – Idle servers or devices do not contribute any value to universities yet they still consume energy. With a centralised asset inventory or repository, universities are able to detect unused equipments and decide whether they should be turned off or re-commissioned for other services.

  Meanwhile, with proper capacity planning, universities can determine the exact requirements for the support of daily operations and level of services. It helps to identify underutilised resources so that they can be consolidated or re-purposed, instead of unilaterally increasing the IT operational expenditure for acquiring additional assets.

- **Reduced Server Downtime** – Server downtime impacts on the availability of universities' information systems and reduces the level of services provided to their students, staff or other related parties. A service interruption may be caused by physical sabotage, malfunctioned server, software bugs, environmental hazards or scheduled installation / upgrade / reconfiguration. Well-established physical security controls over the data centres can effectively prevent unauthorised physical access attempts. Comprehensive HAVC equipments enable fast detection or recovery from environmental hazards. Regular monitoring assists IT management in identifying malfunctioned hardware or software timely and initiate the incident response procedure. Capacity planning allows better anticipation of future resource needs and prevents forced addition or hot-swapping of resources due to overload.

- **Increased Productivity** – A comprehensive data centre management solution brings efficiency in resource usage and allocation. Underutilised or unused equipments are re-commissioned for other resource-demanding services. Overloaded systems are timely detected and allocated with additional capacity. Therefore, higher productivity is gained through efficient provisioning of information resources, including processing, storing and networking.

- **Improved Security** – Information security of data centres are enhanced when most known vulnerabilities or weakness are considered during a comprehensive data centre planning phase. The mitigating strategies are then incorporated into the data centre management solutions and continuously enforced by IT management.

- **Compliance** – Universities are required to maintain compliance with regulatory mandates (e.g. Personal Data (Privacy) Ordinance), information security standards (e.g. ISO 27001) or other internal IT governance policies. A data centre management solution can incorporate compliance requirements into its operational procedures and assign specific responsibilities to IT staff members with proper qualifications.

Reference:
http://www.teamquest.com/pdfs/whitepaper/tqeb01.pdf

II. Risk Factors in Data Centre Management in Universities

While data centre management is a cost-saving approach and brings a lot benefits including increased productivity, higher reliability, improved security and compliance, however, there are risks that may make the universities vulnerable to attack. Some common factors that increase the risk exposure of data centres are:

- **System and Technology Complexity**

  Universities' IT environments are growing more complex that may result in the proliferation of servers, systems and devices. Different operating systems and management tools make IT management difficult to integrate with existing data centre management framework and create interoperation problems. Through the expansion of universities' IT services, additional devices and / or protocols in the data centres also cause more complexity, increasing the need for more management effort and skilled IT staff.

  Without properly designed data centre management solution that addresses the complexity within universities' data centres, issues such as inappropriate operational procedures, incompetent IT staff and gaps in communication may arise. Eventually, these issues will lead to greater risks of service interruptions, security flaws and system damages due to human errors or incompatibilities.

- **Virtualisation**

  One popular strategy for data centre management field is virtualisation that can effectively increases the utilisation of data centre resources and achieve the cost / energy saving objective. However, the flip side of this technology is the increased channels for attacks (i.e. hosting multiple virtual machines on a single physical machine increases the attack surface in the virtual environment), increased difficulty in change management controls of information system residing in virtualised platform, more complicated IT asset discovery and tracking process, and data confidentiality problem due to the sharing of physical server infrastructures.

- **Disaster Recovery and Business Continuity**

  In the event of a disaster or major service interruption, data centres require consistent and reliable replication of IT equipments to sustain universities' IT operations and services, which usually consumes costly resources.

  Without efficient allocation and management of the resources required for disaster recovery and business continuity, the reliability and availability of universities' information systems cannot be guaranteed within a cost constraint. Additionally, unavailability of resources will render the disaster recovery or business continuity plans ineffective, of which universities may not be aware.

Reference:
http://www.cxo.eu.com/article/Data-centre-design-improved-performance--efficiency/

III. Risk Factors in Data Centre Management in Universities (cont'd)

- **Growing Size**

  Generally speaking, growth of universities' information infrastructures will result in physical space crunch in the data centres as well as increases the consumption of energy. More networking, more servers and more storage continue to occupy costly floor space and consume higher power. On the other hand, such growth often indicates additional management effort and IT staff resources to perform routine operational jobs, monitoring, security checks and maintenance. A data centre management solution with poorly segregated functional teams and inefficient management utilities may be incapable of handling the increased data centre sizes.

- **Remote Access**

  Continuous and uninterrupted information access services, such as e-learning, are provided by most universities today. The always-on and always ready service mode needs high system availability. Remote data centre management tools allow IT staff to instantly access to information systems without physically entering the data centres. However, the flexibility and convenience of remote access also raises security concerns. Successful attacks by exploiting the vulnerabilities of remote data centre management tools can grant hackers with privileged access to universities' critical information systems.

Related Article

Data Centre Security: A 10-point Checklist

Whether you are a hosting, co-locating, or running your own data centre, security issues seems to persist. Not only do you need to keep data safe and meet service-level agreements, but the cost of a breach is also high. That cost will vary depending on a number of factors, such as the type of breach or how you value your data.

According to the Ponemon Institute's Annual Cost of a Data Breach study, the cost of a breach in 2009 was US $202 per personal record, an amount made up of what the institute describes as "direct, indirect and opportunity costs from the loss or theft of personal information".

Yet securing a data centre is a huge task that includes physical as well as electronic and procedural issues. Here is a 10-point checklist to help you verify that your security arrangements cover the key areas.

See the article: (http://www.zdnet.co.uk/news/security-management/2010/04/19/datacentre-security-a-10-point-checklist-40088570/)

Reference:
http://www.cxo.eu.com/article/Data-centre-design-improved-performance--efficiency/
http://www.eepublishers.co.za/images/upload/Securing%20remote%20data.pdf

III. Exploitations on Data Centre Management

Vulnerabilities of data centres are found in their physical security, systems / devices hosted and management procedures implemented. Several common exploitation techniques are illustrated below:

1 Back Door

Data centre procedures developed by the IT staff that may have flaws that can create back door vulnerabilities. Exploitation on such weakness can inadvertently introduce security breaches and result in financial loss or repartition damage to universities.

A backup operation provides a good example of how data centre management can be exploited by insecure backup process. IT staff usually overlook the security of tape backup infrastructures, which may contain vulnerabilities and can be exploited to create disastrous consequences. Since the execution of the backup task that usually requires escalated system privileges at the operating systems, network, data repository and application system levels. Malicious parties can take advantage of this security weakness through penetrating flawed backup infrastructure to gain access to universities' sensitive data.

2 Attacks on Remote Access to Data Centre Management

Exploitations on remote access technologies used for data centre management are in many forms. Known attacking techniques include:

- Use of Virtual Private Network ("VPN") access of terminated staff to gain access to data centre systems or management tools
- Offline password cracking through decrypting the hash data received from VPN servers with Internet Key Exchange ("IKE") Aggressive Mode Shared Secret Hash Leakage Weakness
- Denial of Service ("DoS") attack on Secure Sockets Layer ("SSL") -based VPN can be achieved by using hidden attack packets, which was undetectable by Intruder Detection Systems ("IDS"). For example, disguise malformed Internet Security Association and Key Management Protocol ("ISAKMP") headers as standard IKE headers
- Login guess attack on Windows Remote Desktop by hackers

3 Social Engineering

As of today, social engineering still remains as the biggest cyber threats to information security. As opposed to DoS and other remote hacking techniques, social engineering involves obtaining physical or logical access to data centre assets via manipulating IT staff relevant to data centre management, rather than by breaking in or using technical cracking approaches. Some social engineering techniques frequently used by hackers include piggybacking, penetrating data centre by getting a job within the data centre management team, and disguising as vendor support personnel for performing maintenance services inside data centres.

Reference:
http://www.computereconomics.com/article.cfm?id=1112
http://www.ncp-e.com/fileadmin/pdf/techpapers/NCP-Attack-Vectors-WP.pdf
http://www.eepublishers.co.za/images/upload/Securing%20remote%20data.pdf
http://www.nta-monitor.com/posts/2005/01/VPN-Flaws-Whitepaper.pdf
http://www.pcworld.com/article/182180/top_5_social_engineering_exploit_techniques.html

IV. Hardening Steps for Data Centre Management

To ensure that data centres meet the reliability and performance needs of universities, and achieve the comprehensive protection from various security threats, a number of aspects should be taken into the consideration during the design and implementation of the data centre management solutions.

Environmental Control

- **Temperature and Humidity**

  The temperature of each computer room within the data centre is recommended to be controlled between 20 and 24 degrees celsius, and a humidity between 40 and 55%.

- **Fire Protection**

  Halon, FM-200 or other total flooding agent solution should be deployed in each computer room within the data centres. Fire extinguishers should be located strategically across the data centres. Wet pipe sprinkler systems must not be used. Emergency power off switches should be available inside each computer room of the data centres.

- **Flood Protection**

  Whenever possible, raised floors should be used in the data centres. Water detectors should be installed beneath the raised floors.

Physical Security

- **Location of Data Centre**

  The locations of data centres should be carefully selected to reduce the risk of accidental or deliberate trespass by the unauthorised parties. The data centres should not have obvious signs. It is best to have concrete walls without windows. If there are windows, universities should use those areas for administrative purposes only.

  Data centres are also recommended to be located where the risk of external threats, such as flooding, is low.

- **Surveillance**

  There should be Closed-Circuit Television (“CCTV”) cameras outside the data centre monitoring the entrance and inside the data centre. Security guards should be hired to monitor the perimeter of data centres and report any incidents to IT management on a timely basis.

Reference:
http://www.sans.org/reading_room/whitepapers/awareness/data-center-physical-security-checklist_416

IV. Hardening Steps for Data Centre Management (cont'd)

- **Physical Access Control Device**

  Lockers or key card access systems should be used to restrict the access to data centres to authorised personnel only. The best practice is to have two-factor authentication systems, such as key card access systems with individual personnel identification number ("PIN") for each access card holder. Other systems like biometric (e.g. fingerprint) access control products can also be implemented to achieve this objective.

- **Assignment of Physical Access Rights**

  The IT management of universities should ensure that physical access is restricted to personnel on an as-needed basis. Tiered approach can be deployed by granting IT staff with physical access to different segments of the data centres based on their job functions. Only the IT staff members who absolutely need to operate with information system servers or network devices directly should gain physical access to the room hosting the servers.

  The IT management should also review the authorised personnel with physical access to the data centres on a regular basis (e.g. quarterly or annually) to detect any discrepancies.

Disaster Recovery

- **Disaster Recovery Plan**

  Universities should develop disaster recovery plans for their data centres and ensure that the plans are regularly tested, reviewed and updated at least on an annual basis. IT management should ensure sufficient backup resources are available to support the disaster recovery plan.

- **Offsite Backup**

  Regular offsite backups of essential data should be performed by the IT department. The IT management should establish a set of operational procedure to define the scope, frequency, media and restoration of offsite backup process.

Remote Data Centre Management

- **Logical Security Requirement**

  A secure remote data centre management solution should support one or more of the following capabilities:

  - Remote authentication dial-in user service;
  - Lightweight directory access protocol;
  - Breach-prevention modes (programmable response to port scans, pings);
  - Internet protocol (IP) and Firewall packet filtering;

Reference:
http://www.sans.org/reading_room/whitepapers/awareness/data-center-physical-security-checklist_416
http://www.eepublishers.co.za/images/upload/Securing%20remote%20data.pdf

IV. Hardening Steps for Data Centre Management (cont'd)

- Dual-factor authentication;
- IP security tunnelling;
- Comprehensive data logging and event notification features; and
- Other features necessary to support your security policy.

Some popular data centre management products with remote access features available on the market are Microsoft System Centre, IBM System Director VMControl and Avocent.

Others

- **IT Staff Training**

  Sufficient training program should be provided to IT staff members so that they are adequately equipped with knowledge and skills to perform the monitoring, configuration, installation and maintain tasks for systems and devices hosted within the data centres.

  If data centre management software is used, IT management should ensure that comprehensive instruction manual and training courses are offered by vendors prior to deploying the software in production.

- **Operational Procedures**

  IT management should establish a set of operational procedures related to data centre management functions. For example, routine monitoring of system health, IT asset tracking, visitor logging and capacity planning. These operational procedures should include the detailed steps required for the performance of specific tasks and any necessary information such as prerequisite(s) of each step, expected system return code and explanations on error messages.

Reference:
http://indiasecure.in/sites/default/files/Best%20Practices_Data%20Center%20Security_0.pdf

V. Summary

To meet the challenges of higher-density information systems, dynamic processing workloads, and the need for more efficient energy consumption, it is necessary for universities to have a management solution that operates data centres at minimum cost and in a secure manner.

A holistic data centre management solution can maximise the universities’ capacity to control their data centre spending, to preserve desired IT service level and to utilise IT assets more effectively. Such solution should combine proper data centre planning, committed management involvement, competent IT staff and usage of sophisticated management tools. Various hardening steps should also be implemented at environmental, physical, logical and procedural levels to reinforce the data centre security.