Critical Components to Build a Data Center

Drew Mora, *Microsoft Government Solutions, Avum, Inc.*

Abstract—This paper introduces the necessary components to build a fully operational data center. This includes reviewing information at the core infrastructure layer, shared services layer, and application layer in order to correctly create a data center the first time that will not cost extra time and money later.

1 Introduction

This paper describes the various critical components to consider when building a data center. Because building a new data center is such an enormous undertaking, this paper will only cover the most important things to consider when building a new data center.

March 27, 2012

2 Problem

Often times data center planning teams overlook important items to save time and cost. While this can ensure a timely delivery, this oversight can cause very expensive problems within 1 or 2 years time.

3 Solution Objective

Rather than overlooking potentially expensive problems, it is best to consider all options beforehand and create a solution that works perfectly for specific needs. Considering all options and being confident in the right solution helps facilitate an easy transition process to a data center.

1) Core Infrastructure Layer
   a) Ensure the building has the proper power and low voltage conduit for cable growth. When performing an overhaul of older buildings many times the 4 inch telecom conduit does not allow for future growth. Also existing power distribution and layout may not be adequate for todays high density layouts.
   b) Layout: Blade servers will affect the design and require: under floor systems, ceiling plenum air, above ceiling ducted systems, and possibly water cooling. Rack placement and equipment layout is more important now than ever. Take steps to allow racks with blade chassis to maintain only 70% - 80% density. Strategically place equipment to allow for hot cold isles.
   c) Core network requirements will need to be addressed based on current capacity and estimated growth.
   d) IDS Intrusion Detection System: Having an IDS in place is crucial when running a secure datacenter. Below is a list of some popular IDS systems:
      i) Snort is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Combining the benefits of signature, protocol and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide.
      ii) OSSEC is an Open Source Host-based Intrusion Detection System. It performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response.
      iii) Fragroute intercepts, modifies, and rewrites egress traffic destined for a specified host, implementing most of the attacks described in the Secure Networks "Insertion, Evasion, and Denial of Service.
      iv) BASE is the Basic Analysis and Security Engine. It is based on the code from the Analysis Console for Intrusion Databases (ACID) project. This application provides a web front-end to query and analyze the alerts coming from a SNORT IDS system.
      v) Sguil (pronounced sgweel) is built by network security analysts for network security analysts. Sguil's main component is an intuitive GUI that provides access to realtime events, session data, and raw packet captures.
   e) Storage distribution: Consider implementing all of the following technologies:
      i) SAN: Fibre Channel SAN disks can produce the best performance at the highest cost. This is a great solution for highly transactional enterprise systems.
      ii) NAS: Network Attached Storage also known as iSCSI is cheaper and more flexible that FC (Fibre Channel) however the performance and reliability is not as great. This is a great solution for large volume, but non speed critical systems.
      iii) DAS: Direct Attached Storage can be very simple and easy to manage, however this solution does not scale out well, and does not allow for easy data transfer between systems.
      iv) HSM: Hierarchical Storage Management systems allow backups and other tier2 data to be stored on cheaper lower performing disks, saving cost to the datacenter.
2) Shared Services Layer
   a) Authentication (LDAP, FW): Athentication can be handled in many different ways, typically a hybrid implementation of all of these works well.
      i) IP whitelists: This is done at the router level and allows a specific external IP to communicate with a specific internal IP on a specific port.

- *hi*

Manuscript created March 27, 2012.

ii) Layer 7 or CSS switches: Most content switches can provide authentication as well as create server farms.
iii) Active Directory or OpenLDAP can provide one central place for user management. Most CSS and appliances can support LDAP authentication for single sign on.

b) Shared Messaging, internet and DBMS
i) Depending on the density and the requirements of the applications shared messaging can provide great service with a very low TCO to the application owner. This can be done with Microsoft Exchange or other open source messaging systems.
ii) Consolidating back end databases to 2 or more centralized instances can lower TCO to application owners, however this is usually best suited for mid-range or lower transaction applications.

3) Application Layer
a) Private Cloud: Private clouds are a good strategy to load balance resources and produce a high uptime application. The front end of an application is a very good candidate for cloud services. With a private cloud applications are not aware of the hardware below the cloud, so the application can function in a hardware agnostic environment.
b) Applications that share the same hardware requirements can usually also share physical servers creating a low TCO for the application owners.
c) Individual Applications that require specific hardware, will need to be installed on the vendor specific hardware and will consume rack space. Shared services and high density will not be available for the vendor specific hardware.

4 Our Method

Avum process is to review and analyze each application that transitions into a hosted data center to decide the best fit from a hardware, software and cost of ownership perspective. Avum always tries to produce the highest necessary uptime for the lowest cost of ownership. If cost savings can be leveraged from existing infrastructure Avum will always try to leverage the savings. The load varies per application and unless specifically requested, Avum always puts uptime above cost. These decisions are best made between Avum and the application owner. The hardware and infrastructure expertise from Avum is key to making informed decisions that provide the maximum uptime for the lowest cost.

5 Conclusion

Transitioning applications to a shared delivery point requires combining the business rules with infrastructure best practices and in the trenches lessons learned. This team effort in decision making is key to a successful transition.

Andrew Mora An experienced and forward thinking resource, Drew Mora manages the partnerships with AVUM customers, Microsoft and Dell for hardware solutions and software services. Working diligently to provide the best solution and value to AVUM customers, he oversees the design, staffing, architecture, planning and implementation of AVUM's Microsoft government solutions. Mr. Moras primary role is to ensure the best technical solution is implemented at the lowest possible cost within the time frame given by the customer. Current AVUM solutions focus on BI with MOSS 2007, server and data center migrations and High Availability (HA) solutions.