AN AZALEOS WHITE PAPER

Monitoring and Managing Microsoft® Office SharePoint® Server

By **Christopher Mayer** and **Christina Hesse**
Denali Advanced Integration (www.denaliai.com)

May 15, 2008

azaleos™

An Alternative to Hosted Exchange

Azaleos Corporation 1938 Fairview Avenue East, Suite 100, Seattle, WA 98102 USA
tel 206.926.2000 / www.azaleos.com

Abstract

Microsoft Office SharePoint Server 2007 ("MOSS") is one of the fastest growing server products in the history of Microsoft. MOSS is a portal product that provides a full spectrum of collaboration and content management functionality. As powerful and popular as the solution offerings have become, however, the technology for the most part is still misunderstood and its complexity underestimated. This paper will discuss the MOSS technologies and the challenges and failed considerations in deployment and management. The paper will identify some key best practices with respect to monitoring and management of SharePoint and will identify gaps and market needs that the proven set of Azaleos remote monitoring and management service solutions can effectively bridge.

SharePoint Overview

Microsoft Office SharePoint Server Technologies

Microsoft Office SharePoint Server 2007 is best described as a collection of enterprise collaboration applications and features. Architecturally, the MOSS Stack is collectively made up of BackOffice and .NET technologies (Figure 1). As such, MOSS is reliant on Windows SharePoint Services 3.0 ("WSS"), a subset of the SharePoint technologies, ASP.NET and Windows Server 2003.

Figure 1

MOSS additionally requires a data repository. It can use Microsoft SQL Server® Desktop Engine ("MSDE") for development and experimental applications, and requires a full Microsoft SQL Server instance for production deployments.

Windows SharePoint Services 3.0

In the MOSS stack, WSS exists as a service providing layer. It is, however, often used as a standalone collaboration solution. The abundance of functionalities, while taken for granted within MOSS, is somewhat limited within WSS. Capabilities within WSS are restricted to very basic functionality and are lacking the core of the SharePoint platform capabilities around Content

Management, Search, Business Process and Forms, and Business Intelligence. WSS is the foundation of all SharePoint Services.

Microsoft Office SharePoint Server

MOSS is the full suite of Collaboration functionality. In addition to the features WSS provides, MOSS has been extended in such a way that it is beneficial to corporate, enterprise deployments and portal scenarios. MOSS includes all features provided by WSS and *additionally* provides the following functionality:

- **Portal**: includes Enterprise Portal templates, Site Directories, My Sites, social networking and privacy control.
- **Search**: incorporates Enterprise scalability, contextual relevance, rich people and business data search.
- **Content Management**: aligning disparate data sources, unified content includes integrated document management, records management, and Web content management with policies and workflow.
- **Business Forms**: leveraging Forms Server and InfoPath, with the MOSS platform to configure Rich and Web forms, LOB actions, and enterprise Single Sign On ("SSO").
- **Business Intelligence**: reporting and information roll-ups can be disseminated with Server-based Excel spreadsheets and data visualization, Report Center, BI Web Parts, and KPIs/Dashboards.

Deployment

As MOSS gains popularity and installed base share, the product's functionality, diversity, and capabilities are becoming quite apparent. However, for all its strengths, the MOSS weakness is a deceptive simplicity that coerces even the most seasoned IT professional to deploy a solution without sufficient background and planning. Deployed correctly MOSS will provide a true secure portal platform that will scale with an organization and extend to meet its application needs. Deployed incorrectly, SharePoint can quickly digress into an unmanageable paradigm akin to that of distributed shared folders. Any successfully deployed MOSS solution is one that has been planned to match the needs of the organization, the ability of the infrastructure to absorb the platforms, and the propensity of the users to adopt.

When planning for a deployment of any initial scale, it is imperative to consider:

- Portal Architecture: carefully considering the intended uses of the organization's portal environment will dictate how many use-specific portals will be part of a deployment. A best practice here is to match a portal to both a usage intent and security model. For example, an organization may deploy a publishing portal, a collaboration portal, a project management portal, and a shared services portal.

- Portal Topology: selecting a hardware foot print that will scale, as shown in Figure 2, is equally important as selecting one that works WITH an existing infrastructure. For example, TechNet may seem to recommend a standard medium farm configuration for a specific need, but what is not taken into account are various firewall layers and split Active Directory forests that will alter farm configurations.

- Taxonomy: deciding on how to name and organize a company's site structure based on organizational divisions is only one challenge at this stage of the deployment. The others are tagging the sites, listings and documents so that they are easy to classify, find and maintain.

Figure 2

Scale Planning and Considerations

Planning for an initial MOSS environment or the expansion of an existing one can be a daunting task for any organization. Many questions will need to be answered before beginning:

- How many physical servers will be needed in the portal server farm?
- What are the capacity limits on those servers?
- When the organization grows, how hard will it be to add additional hardware to the existing server configuration, and how does it need to be added?
- What will performance look like if a smaller configuration is considered?
- Is there a need for load balancing between two servers?
- How many licenses will need to be purchased to run software on those servers?
- How long will it be until an upgrade is necessary?
- Does the portal set up need 64-bit machines?
- How will existing hardware be leveraged to avoid the overhead of a completely new system?
- When will the Systems Engineers find time to research all of this and implement it?
- Will a company's current number of systems engineers cover the planned server expansion and increased maintenance that is sure to follow?

- Hardware: Once the portal topology that the solution will scale towards has been determined, the initial hardware procurement has to consider 32bit or 64bit, physical or virtual. Figure 3 speaks to some of the considerations of using VMWare®.

Figure 3

MOSS and VMware

Organizations are starting to take advantage of the benefits gained by running their MOSS environment on VMware. VMware will let an organization run several "Guest" servers on a "Host" machine, thereby saving storage, network and computing resources.

MOSS is fully compatible with VMware; however there are some MOSS components that can behave differently on VMware than if they were to run on physical servers. For example, if a MOSS Portal Architecture is distributed across two virtual machines, a duplicate site name will be created and the content databases will not be correctly linked, thereby causing the sites to not restore correctly. Also, if not configured correctly, VMware could impact MOSS components that are dependent on time, such as Kerberos. If the time is not synchronized between the virtual machines, this could cause problems with user access or timer jobs performing tasks.

Organizations who leverage VMware will realize a powerful, cost effective solution. In order to most effectively realize these benefits, organizations are advised to consult with systems integrators or services organizations such as Azaleos in order to leverage their expertise and experience with virtualization.

- Environments: companies tend to plan for one production environment. This often isn't enough, and what isn't obvious is when one environment, leveraging the MOSS publishing capabilities, is sufficient and when ancillary environments, such as Staging, Testing, or Development are needed. In addition to how a company structures their MOSS environment, it also has options as to where it deploys its environments and how it is managed or monitored.
  - On Premise – owned and managed in the company building
  - Hosted – cloud service; data, hardware (server and storage) and software located at a remote server farm and managed by a 3rd party

- Hybrid – the company owns the software/hardware/data on premise, but outsources monitoring and management to a 3rd party via remote services [the Azaleos solution]

- Training: if an organization is not planning for training, then it should slow planning. A successful deployment requires specific training for developers, administrators, trainers and users. Training is something that should be ongoing or even made available from within the portal itself.

- Supportability: last, but definitely not least, what will be required to support the implementation, and is the organization prepared for it? Some areas of supportability include ongoing training, administration, user support, monitoring, backups and recoveries.

Significant planning and consideration is necessary to successfully deploy a MOSS solution. There are numerous online resources that can guide an organization in the right direction – but they will not consider its specific environment and deployment needs. There is no replacement for the experience that comes with having performed farm build outs before and having learned about all the possible pitfalls first hand.

Monitoring & Management

Once a company has a robust MOSS solution successfully deployed, as with any enterprise scale solution, there is a certain level of management required to ensure continued success.

Monitoring

Problems occurring in MOSS components often times go undetected until a user complains or until the system fails noticeably. These sometimes embarrassing issues can be easily prevented by implementing real time monitoring within the MOSS 2007 environment. Implemented correctly, a monitoring system will give companies real time information about their system's functionality, performance and behavior, so when something goes wrong, it can be controlled and corrected immediately or sometimes even predicted in advance and prevented from occurring at all.

Routine Systems Management

Routine systems management is essential for the smooth and efficient operation of a MOSS server farm. Most companies often underestimated, or even fail to considered, the elements and time necessary to maintain a MOSS Server Farm. This may place unrealistic time demands on Network Administrators who are being taken away from other, perhaps more important tasks. This can be particularly burdensome for companies who are used to maintaining a WSS site and have upgraded to a MOSS Portal environment. Additionally, MOSS has matured into such a vast application with numerous, rich features that it is difficult, if not impossible for just one person alone to be an expert in all of the functionality available. Consequently from an IT maintenance standpoint, there are several avenues to consider when working with MOSS 2007:

- **Administrative staffing requirements**: One fact that very few organizations realize is the extensive staffing need that can arise with a MOSS Server farm. The Microsoft recommended staffing for MOSS Server Farms are listed as follows in Figure 4:

Figure 4

Suggested Staffing Recommendations

Staff position	Small farm	Medium farm	Large farm	Multiple farms
System administrator	F	F	F F	F F
Search administrator	P	F	F P	F F F
Site designer	P	F	F F	F F F
Software developer	N/A	P F	F F	F F F
Software tester	N/A	P	F	F F
SQL DBA	P	F	F	F F

*F – Full time Employee *P – Part time Employee

- Back Up: The MOSS interface provides access to standard database backup and recovery capabilities. This often does not meet specific recovery needs, however. For example, the backup processes cannot be automated and as a result consume additional IT hours to execute on a regular manual basis. Other options that must be considered include site collection backups, individual site backups, profile and personalization backups and Recycle bin management. An organization's back up strategy will be a permutation of these options, dependant on its portal usage and design characteristics.

- Service Account and Security Management: Expert knowledge of the functions of all MOSS Service Accounts will be needed to set up the backup tasks over a multifaceted network, as within complex network set ups the permissions and different service account tasks can be quite confusing. The lack of knowledge could potentially result in long trial and error sessions.

- Database Maintenance: MOSS is a SQL Server based product. While the application is responsible for creation and general management of the required database, routine database maintenance is crucial to preserve the MOSS environment and to prevent corruption. Obviously, in order to implement regular SQL maintenance, it requires having SQL database experience and expertise on staff --- not always a given in all IT departments. It is recommended that SQL Server databases get treated to regular routine maintenance in order to run at optimum speed. Examples of database maintenance tasks that commonly are overlooked include:
    - Checking database integrity to ensure there is no corruption
    - Defragmenting indexes either via reorganization or a rebuild to fine tune database performance
    - Setting the fill factor for a server to create space for future database growth
    - Updating index statistics
    - Shrinking databases to recover unused disk space
    - Internal consistency checks and backups

As MOSS deployments become more advanced, companies may want to also consider the following:

- Archiving: Often overlooked in MOSS and WSS deployments, Archiving is used to streamline search results and simplify management such as backup and recovery. An effective Archiving

strategy should be considered in Portal Architecture planning. This involves creating a divide between disposable information - information that has terminal relevancy such as the length of a project, and dynamic information.

- Disaster Recovery: MOSS environments are typically distributed across a farm made up of various servers, including index (or query) servers, front-end Web servers, application and Microsoft SQL Server database servers. While actual content is stored in the diverse databases, other information such as application-specific configuration data, IIS configuration data and farm configuration databases may reside in several different locations. A sizable company will likely have multiple server farms, and the challenge of reliable application recoverability can become complex rather quickly and it may not always be clear what exactly needs to be included in the backup.

Deployment Maintenance

Assuming that there is still IT bandwidth available after dealing with the ongoing systems management issues for MOSS, there will also always be some inherent and ongoing customization and provisioning upkeep with an organization's SharePoint installation. Some of the most commonly overlooked deployment maintenance items include:

- Portal customization: Managing the deployment or propagation of custom Web Parts, custom site definitions, templates, graphics and styles, views, user profiles requires the utilization of basic .NET continuous integration. Management at this level includes versioning, propagating, staging and recovery.

- Security and Services: Features, such as workflows, need to be configured correctly with the correct service accounts – a complex domain structure may interfere with publishing flow if not set up correctly.

- Roles and Audiences: To maintain the proper content access and targeting, audiences, SharePoint Groups and inherent Active Directory Groups need to be managed through the proper policies or governance.

It is important to note, that management challenges of MOSS are compounded by the distributed nature of the implemented solution. If a deployed solution does not have unified monitoring and management protocols in place, then unified integrity cannot be guaranteed.

The Azaleos Solution

One distinct alternative solution for a company to take on a major portion of the MOSS puzzle is a relationship with the remote managed services provider, Azaleos. The Azaleos Remote Managed Services for SharePoint solution fits comfortably into the existing Azaleos portfolio of Exchange, Active Directory, Storage and SQL architecture services, and focuses on running MOSS 2007 on both physical machines and/or on the VMware virtualization infrastructure.

The unique Azaleos solution is hybrid which allows a company to keep all the SharePoint hardware, software, and, most importantly, mission critical data, on-premise behind the corporate firewall. Azaleos will then focus specifically on the routine systems management services while managing the solution remotely from the Azaleos Network Operations Center.

The Azaleos team expertise encompasses the entire Microsoft Unified Communications stack: SharePoint, Office Communications Server and especially Microsoft Exchange. Azaleos employs its patented ViewXchange technology to offer 7x24 monitoring of approximately 4800 data points

across SharePoint, IIS, Exchange, Active Directory, Storage, the Network topology and SQL Server. The benefit to the customer is the utmost in high reliability and availability for SharePoint systems.

A relationship with Azaleos will provide a company with the latest Azaleos and Microsoft best practices regarding comprehensive deployment consultation and assistance.

Additionally, utilizing the efficient Azaleos remote managed services will free up IT resources to allow companies to focus on the deployment maintenance issues for MOSS and especially on other strategic and revenue producing IT projects, while retaining control over their MOSS environments --- all data is secure behind the firewall and on premise.