ITIL: Microsoft and Open Source

White Paper

Microsoft Corporation
Published: October 26, 2007

Contents

ITIL: Microsoft and Open Source

Organizations live and die based on the efficiency, reliability, and security of Information Technology (IT). Because of this, IT must be fully aligned to the needs of all customers, internal and external. The Information Technology Infrastructure Library (ITIL) provides a strategy to define, implement, and monitor that alignment across the full spectrum of IT processes, ranging from Incident and Problem Management to Security Management.

While ITIL focuses on the strategy and process of IT management, in the end much of ITIL must be implemented in software systems. And the scope of ITIL does not guarantee that a single solution exists, nor should it. Instead, each element of ITIL involves a microcosm of vendors and software products. This gives organizations many choices in how to implement ITIL.

In this paper, we focus specifically on the choices available from Microsoft and the open source community. Both offer solutions which can assist critical elements of ITIL. Some solutions are similar, while others are distinctive. Indeed, throughout the paper we find examples of different approaches to the issues which ITIL raises.

Ultimately, our analysis found that:

- No single source wholly addresses the needs of ITIL.
- Microsoft offers several relatively complete products, but their Windows-centric approach may not address all enterprise ITIL activities.
- The open source community often focuses on particular technical ITIL activities at the expense of providing more inclusive support across an entire ITIL process.

Introduction to ITIL

The Information Technology Infrastructure Library (ITIL) describes strategies for implementing a cohesive management approach to address business and technology drivers. ITIL is not a procedure manual, nor does it provide solutions to specific technical problems. Instead, it provides an organization with a set of broad tools and a mindset for how to address IT management.

A key element of ITIL is that it is both vendor- and solution-agnostic. That is, the practices encouraged by ITIL can be applied across the board regardless of the underlying operating system (OS), middleware choice, or client toolset. Indeed, this is one of the most important ideas behind ITIL—it's not the technology, but the management strategy that makes IT successful.

To support this viewpoint, we analyze solutions by comparing product features against the relevant activities for the discussed ITIL processes. Furthermore, we organize the paper around the Service Support and Service Delivery sets included in ITIL v2.(Although

ITIL v3 was released in 2007, ITIL v2 is widely supported and is standard for most organizations.)

Service Support

This set revolves around the on-the-ground needs of an IT organization such as how to manage incidents, changes to the environment, and deploying new services. This paper begins by covering the actual support requirements for an IT organization:

- **Incident Management**
  Solving incidents and restoring services quickly.
- **Problem Management**
  Solving root cause problems to prevent future incidents.
- **Configuration Management**
  Maintaining all necessary information about services, service components, and relationships.
- **Change Management**
  Controlling the implementation of changes in the infrastructure.
- **Release Management**
  Controlling the rollout of new releases in the infrastructure.

Service Delivery

The ITIL Service Delivery Set involves the management of IT services and management practices which ensure that IT services are provided as agreed between a Provider and Customer. The set includes:

- **Service Level Management**
  Defining and implementing clear agreements for service delivery between an IT organization and its customers.
- **Financial Management for IT Services**
  Ensuring the proper management, maintenance, and financial operation of IT.
- **Capacity Management**
  Optimizing capacity to meet service requirements at an acceptable cost.
- **Availability Management**
  Ensuring the availability of IT resources to meet agreed upon service levels.
- **IT Service Continuity Management**
  Defining and maintaining appropriate Disaster Recovery plans for IT.
- **Security Management**
  Ensuring the proper access to services as defined by agreements and industry best practices.

History of ITIL

ITIL began life in the early 1980s stemming from the British government's need to promote quality IT initiatives and service. Originally, ITIL was written by the British Central Computer and Telecommunications Agency (CCTA), now part of the Office of Government Commerce (OGC). The CCTA was given the job of providing an underlying framework on which to build quality-driven IT organizations both within the government and in the private sector. It's important to note that while ITIL was originally developed in Europe, it has reached a truly global status, and is implemented both in the European and US markets.

During the 1990s, ITIL was rapidly adopted because of its emphasis on business driven needs, which met well with the financial and quality requirements of both government and business. In 2000, Microsoft looked to ITIL while developing the Microsoft Operations Framework (MOF). MOF was Microsoft's drive to help IT better manage and deploy their assets and to be enable the meeting of business drivers within the organization. 2001 saw the release of ITIL v2, while 2007 saw the release of v3.

Benefits of ITIL

At first, an organization must ask itself why an ITIL mindset is beneficial. As such an integrated and far-reaching approach, ITIL can be a considerable endeavor to undertake. Fortunately, ITIL brings many benefits to organizations of all sizes, even if not all processes are implemented. Some of these benefits include:

- faster incident resolution for customers;
- significantly fewer repeated IT problems and errors;
- better understanding of issues, performance, and security affecting IT services;
- increased utilization of existing resources;
- ability to cost justify IT expenditures;
- customer-driven service levels;
- improved reliability and availability;
- and, the ability to track and audit configuration and changes to ensure regulatory compliance.

IT Service Support: Incident Management

Definition

All organizations must deal with incidents affecting their IT services and customers. When an incident occurs, it's imperative that it be handled using a standardized process which ensures any incident reports are properly categorized, prioritized, and resolved. In this way an organization can reduce the impact and cost of the incident in the fastest manner possible. Incident Management aims to provide that mechanism, and it focuses on ensuring that incidents are resolved quickly.

There are several activities associated with Incident Management, including:

- **Detect and Record Incident.** Detecting an incident or accept a report of the incident from a user.
- **Classify.** Classifying and prioritizing an incident based on the needs of the business.
- **Initial Support.** Providing initial support to the user, e.g., immediate assistance from a help desk technician.
- **Investigate and Resolve.** Researching and determining a resolution for an issue if the initial support is unable to.
- **Track, Monitor, and Communicate.** Providing ongoing tracking of the incident and communicate with the user on the status of the resolution process.

Product Comparison

Traditionally, products that address the needs of Incident Management provide Help Desk capabilities. These capabilities include the following:

- Providing users the ability to submit reports containing incident information. Once submitted, these are often referred to as "tickets."
- Allowing help desk technicians to categorize the ticket based on business needs. For example, assigning a higher priority to tickets from a revenue generating department.
- Tracking progress notes and communication between users and the help desk.
- Determining key metrics such as the average time required for a technician to resolve a ticket.

The products listed in Table 1 provide some or all of these capabilities.

Table 1 - Incident Management Software

Solution	Vendor	Platforms	License	First release	Latest release
RT	Best Practical	UNIX	GPL	1996	7/5/2007
OTRS	OTRS	UNIX, Linux, Windows	GPL	4-9-2002	9-18-2007
Bugzilla	Mozilla	Linux	Mozilla Public License	9-19-1998	8/23/2007
Double Choco Latte	DCL	UNIX, Linux, Windows	GPL	1/17/2000	3/23/2005
Liberum	Liberum	Windows	GPL	6/25/2000	8/28/2002
Savane	Savane	UNIX	GPL	2/6/2004	12/9/2006
Microsoft System Center: Service Manager	Microsoft	Windows	Proprietary	Unreleased	4/2007 (beta)
dotProject	dotProject	UNIX, Windows	GPL	3/31/2005	5/21/2007

Table 2 provides a review of each product's capability to address the ITIL activities for Incident Management. We provide further analysis in the following sections titled "Open Source" and "Microsoft."

Table 2 - Incident Management Activities Review

Solution	Detect and Record Incident	Classify	Initial Support	Investigate and Resolve	Track, Monitor, and Communicate
RT	●	●	◑		●
OTRS	●	●	◑		●
Bugzilla	●	●	○		●
Double Choco Latte	●	●	◑		◑
Liberum	●	◑	◑		●
Savane	●	◑	◑		●
Microsoft System Center: Service Manager					
dotProject	●	●	○		◑

Chart legend - ● = strong, ◑ = weak, ○= none

Open Source

The open source community is well represented in this market, with several mature products available. In this comparison we concentrate on two well-established open source products: RT and OTRS.

Both RT and OTRS provide users with several means of submitting incident reports. For example, OTRS allows a user to submit a report via email or a web-based form. Both methods are now commonly implemented for all help desk packages.

The two products also offer the ability to classify incidents, including the capability to customize the classification system to include site specific information specific. For example, a ticket within RT can be classified by multiple custom fields.

As far as Initial Support, both RT and OTRS provide help desk technicians with a template-based response capability, which allows technicians to quickly assist users experiencing common problems.

Finally, both RT and OTRS provide a detailed history of comments and communication associated with an incident, which can provide crucial information if the incident occurs again or if the solution is being reviewed by another technician and management.

Notably, these and other open source tools do not provide the same comprehensive reports as many commercial products. For example, while RT provides reports to list

currently open tickets, it does not natively provide detailed management reporting on technician performance metrics.

Microsoft

Microsoft does not currently offer an Incident Management product; however, Microsoft System Center: Service Manager is planned for release in 2008. This product is currently in beta, and was not reviewed for this paper.

There are many commercial products within the Microsoft ecosystem which provide Incident Management capabilities. Some of these products plug into Microsoft Customer Relationship Manager (CRM), while others are stand-alone. Examples include LiveTime, Altiris Helpdesk Solution, and Parature.

Incident Management Conclusions

Overall, Incident Management is a mature and well-served ITIL process. There are several open source products available to implement the required ITIL activities, and many, such as OTRS and RT, are configurable. They provide for categorization and workflow, and offer reporting capabilities, allowing for the control and monitoring of the Incident Management process. The soon-to-be-released Microsoft System Center: Service Manager will add another potential solution for Incident Management.

IT Service Support: Problem Management

Definition

Incidents cost organizations time and money, and incidents that reoccur cost even more. Users become frustrated and IT funds are wasted because the same problem must be investigated and resolved repeatedly. A better approach is to determine which incidents reoccur, investigate the cause of these incidents, and address the root causes rather than the symptoms. This is the realm of Problem Management.

There are several activities associated with Problem Management, including:

- **Problem and Error Control.** Identifying and investigating problems and errors within the environment.
- **Proactive Management.** Identifying problems and errors before they occur.
- **Report.** Providing management information about Problem Management quality and operations.

Problem Management is directly related to Incident Management. In general, most problems addressed by Problem Management are initially generated within Incident Management. The two processes differ in that Incident Management is more concerned with a fast resolution process–even if only the symptom is addressed–while Problem

Management focuses on root cause analysis of the underlying issue. This type of resolution may require a considerable amount of time.

Product Comparison

Because of the close relationship between Incident Management and Problem Management, both tend rely on the same products, as we can see in Table 3. There are in fact few differentiators between a product that is deployed for Incident Management and one for Problem Management. However, some features can make a product more useful, such as the ability to define an incident type as a Known Problem to assist help desk technicians during incident resolution.

Table 3 – Problem Management Software

Solution	Vendor	Platforms	License	First release	Latest release
RT	Best Practical	UNIX, Linux	GPL	1996	7/5/2007
OTRS	OTRS	UNIX, Linux, Windows	GPL	4-9-2002	9-18-2007
Bugzilla	Mozilla	UNIX, Linux	Mozilla Public License	9-19-1998	8/23/2007
Double Choco Latte	DCL	UNIX, Linux, Windows	GPL	1/17/2000	3/23/2005
Liberum Help Desk	Liberum	Windows	GPL	6/25/2000	8/28/2002
Savane	Savane	UNIX, Linux	GPL	2/6/2004	12/9/2006
Microsoft System Center: Service Manager	Microsoft	Windows	Proprietary	Unreleased	4/2007 (beta)
dotProject	dotProject	UNIX, Linux, Windows	GPL	3/31/2005	5/21/2007

Table 4 provides a review of the capabilities of each product to address the ITIL activities for Problem Management. We provide further analysis in the following sections titled “Open Source” and “Microsoft.”

Table 4 – Problem Management Activities Review

Solution	Problem and Error Control	Proactive Management	Report
RT	●	◑	●
OTRS	●	◑	●
Bugzilla	●	◑	◑
Double Choco Latte	◑	◑	◑
Liberum Help Desk	◑	◑	◑
Savane	●	◑	○
Microsoft System Center: Service Manager			
dotProject	○	◑	◑

Chart legend - ● = strong, ◑ = weak, ○= none

Open Source

Problem and Error Control refer to the capability to find, investigate, and resolve problems within the environment. Open source products such as RT, OTRS, and Bugzilla offer technicians the tools needed to properly implement this process such as the ability to submit a problem report, to classify and priority it, the ability to track notes and communication regarding the report, and any follow-up reporting.

One important feature that can be used within Problem Management is the ability to tie related incidents together using a relationship. A common method is to assign a parent/child or sibling relationship between tickets to show the relationship. This allows help desk technicians and system administrators to more easily find patterns between incidents, to determine which incidents require root cause analysis, and to better organize their efforts. This, along with Capacity and Availability Management, provide a Proactive Management capability.

Microsoft

As with Incident Management, Microsoft is currently working to release the initial version of their Service Manager product in 2008. Once released, this product will be capable of assisting with both Incident and Problem Management activities.

The Microsoft ecosystem also offers products which can be used within Problem Management. For example, Parature, which was mentioned in the section on Incident Management, offers many features of a help desk in addition to services written to address some of the needs of Service Level Management and Asset Management.

Problem Management Conclusions

Overall, Problem Management is an underserved area of ITIL. It would be better served if the available open source tools were able to automatically trend and identify potential problems. Microsoft's soon-to-be-released Service Manager may have an impact on Problem Management in Microsoft-centric sites, although the Microsoft ecosystem

already currently offers products which are suitable for use in Problem Management (as with Incident Management).

IT Service Support: Configuration Management

Definition

Configuration Management provides an organization with the ability to identify, record, and report configuration information and relationships. In ITIL, configuration data is known as Configuration Items (CIs) and is stored in a database known as the Configuration Management Database (CMDB).

Configuration Management is actually a superset of Asset Management in that it not only tracks the hardware and software being used within an organization, but the configuration and relationships of those assets as well. Notably, Configuration Management can play a crucial role in adhering to regulations such as the Sarbanes-Oxley Act (SOX) in the United States because it allows an organization to track and audit changes.

There are several activities associated with Configuration Management, including:

- **Planning.** Planning and defining the scope, objectives, policy and processes of the CMDB.
- **Identification.** Selecting and identifying the configuration structures and items within your IT infrastructure, including owners, attributes, dependencies, and relationships.
- **Configuration Control.** Ensuring that only authorized and identifiable CIs are accepted and recorded in the CMDB.
- **Status Accounting.** Keeping track of the status of components throughout the entire lifecycle of configuration items.
- **Verification and Audit.** Manual and scheduled auditing to verify that the correct information is recorded in the CMDB.

Product Comparison

Configuration Management aims to provide a knowledge base of the configuration of the hardware and software being used by an organization. In order to implement this, products must be able to perform functions such as the following:

- Discover devices on a network.
- Determine the host OS.
- Determine OS version and patch levels.
- Determine which applications are installed on the system.
- Detect any changes to the configuration.

Both Microsoft and open source offer products, shown in Table 5, which meet many of these demands. However, it should be noted that no single product addresses the full range of Configuration Management activities.

Table 5 - Configuration Management Software

Solution	Vendor	Platforms	License	First release	Latest release
CMDBuild	CMDBuild (Italy)	Linux, UNIX	GPL	4/28/2006	6/25/2007 – 0.60
Systems Management Server	Microsoft	Windows	Proprietary	1994 — Microsoft Systems Management Server 1.0	May 2007 — Microsoft System Center Configuration Manager 2007
Zenoss	Zenoss	Linux, UNIX, Windows	GPL, with EULA	3/2006	6/20/2007 – 2.0
OneCMDB	Lokomo Systems	Linux, Windows	GPL	11/16/2006	6/1/2007

Table 6 provides a review of the capabilities of each product to address the ITIL activities for Configuration Management. We provide further analysis in the section “Open Source” and “Microsoft.”

Table 6 - Configuration Management Activities Review

Solution	Identification	Configuration Control	Status Accounting	Verification and Audit
CMDBuild	●	○	◑	◑
Systems Management Server	●	●	●	●
Zenoss	●	○	◑	◑
OneCMDB	●	○	○	○

Chart legend - ● = strong, ◑ = weak, ○= none

Open Source

The open source community offers a wide range of solutions for Configuration Management.

Zenoss provides a good example of an open source product (Zenoss provides a free, open source "Core" application and then uses a commercial license for additional feature packs). Zenoss, as an infrastructure monitoring and management application, utilizes a CMDB to maintain information about the components in a network. However, Zenoss Core, the open source and free version, has limited support for enterprise

applications such as SQL Server, which limits its capabilities for activities such as Verification and Audit.

OneCMDB supports features such as discovery and modeling, and in fact has a significant set of features. However, it lacks an automated audit capability. CMDBuild, while an interesting open source CMDB project, is not broadly deployed and also lacks substantial English language documentation, restricting its audience.

Microsoft

Microsoft Systems Management Server (SMS), while not a complete CMDB per se, can discover and scan target systems for extensive configuration information, including hardware, operating system and version, and installed applications. And because of SMS's attention to the Windows platform and applications, it is able to perform a very detailed analysis that allows SMS to store a variety of information on managed systems.

In conjunction with various tools available in the Microsoft ecosystem, SMS is also able to provide a robust auditing capability.

Configuration Manager Conclusions

In many ways, Configuration Management and CMDBs can be a costly and complicated systems to design, build, deploy, and manage. In order to be effective, tools must be able to discover various types of devices, scan and understand configuration information, provide modeling capabilities, and be extensible.

The open source community has made strides to address the needs of Configuration Management and CMDBs in the enterprise, but still has a way to go. For example, the relatively weak support for automated reporting and auditing in the open source tools limits their effectiveness in an ITIL environment, even though they are all capable of gathering the needed information.

Microsoft SMS, for its part, is very effective at creating a platform-specific CMDB around services and applications. However, as an enterprise player, SMS is limited because of its restricted platform support.

IT Service Support: Change Management

Definition

Unless change is controlled within an organization, IT services will be at the mercy of ad hoc modifications to routers, servers, and software. Ad hoc changes can and will cost organizations revenue, and create unnecessary frustration as users must wait for the completion of unannounced upgrade or the rollback of a failed patch.

Change Management ensures that any change that will affect an IT service must be done using a standardized methodology. It attempts to reduce or eliminate service interruptions or incidents related to these changes.

As a side note, a key underpinning of Change Management is its ability to alter how an organization thinks about changes. Specifically, rather than discussing an actual change, a Request for Change (RFC) is discussed. While a simple concept, this change in vocabulary reinforces the mindset in Change Management that all changes must be subject to critical analysis and testing prior to deployment.

There are several activities associated with Change Management, including:

- **Filtering Changes**. Reviewing submitted RFCs to determine validity and need.
- **Implementing Changes**. Managing and implementing changes to hardware and software and managing the change management process itself.
- **Review and Close**. Reviewing the status of RFCs and closing any that have been completed and validated.
- **Report**. Provide management information about Incident Management quality and operations.

Product Comparison

Products used to implement Change Management activities fall into one of two categories: Workflow or Deployment. Workflow software is used to define the review and approval process. When an RFC is issued, the workflow software routes it to the appropriate parties for review, testing, and, eventually, deployment. Many help desk products actually support workflow, allowing them to be used to monitor the actual change process. An example of open source software which supports workflow is RT.

The second category, deployment, concentrates on automating the implementation of a change to a target endpoint. Our review focuses on this aspect of Change Management.

The capabilities required for implementing changes include the ability to:

- Install software updates and configuration changes.
- Detect an error during the update process.
- Record and report who has initiated a given set of changes.

The products listed below in Table 7 provide some or all of these Change Management capabilities.

Table 7 - Change Management Software

Solution	Vendor	Platforms	License	First release	Latest release
Bcfg2	Bcfg2	Linux, UNIX	BSD	8/11/2004	6/25/2007
Cfengine	Cfengine	Linux, UNIX, Windows	GPL	1993	1/27/2007
Radmind	Radmind	Linux, UNIX, Windows	BSD	3/26/2006	7/5/2007
Webmin	Webmin	Linux, UNIX	GPL	12/13/1999	8/2/2007
Systems Management Server	Microsoft	Windows	Proprietary	1994 — Microsoft Systems Management Server 1.0	May 2007 — Microsoft System Center Configuration Manager 2007
Zenoss	Zenoss	Linux, UNIX, Windows	GPL with EULA	3/2006	6/20/2007 – 2.0
BPMspace	Continental Software	Linux, UNIX, Windows	LGPL	12/22/2006	3/14/2007
NetDirector	Emu Software	Linux, UNIX	MPL	2/21/2007 – 3.1.1	2/27/2007 – 3.1.2

Table 8 provides a review of the capabilities of each product to address the ITIL activities for Change Management. We provide further analysis in the following sections titled "Open Source" and "Microsoft."

Table 8 - Change Management Activities Review

Solution	Filtering Changes	Implementing Changes	Report
Bcfg2	○	●	●
Cfengine	○	●	●
Radmind	○	●	◑
Webmin	○	◑	◑
Systems Management Server	◑	●	●
Zenoss	◑	○	◑
BPMspace	○	○	◑
NetDirector	○	●	●

Chart legend - ● = strong, ◑ = weak, ○= none

Open Source

The open source community is home to a great deal of research, particularly in the academic community, on how to best implement changes across a large set of systems. And, indeed, some of the most advanced tools available are open source, such as bcfg2, cfengine, radmind, and Webmin. All of these provide for varying degrees of controlled deployment of changes, although tools such as Webmin require that users access a manual configuration screen, limiting their use in large environments. Those tools which center on automation, such as bcfg2 and cfengine, actually provide a means to ensure

that configurations are not changed - any unapproved change is automatically reverted back to the original by a local software agent.

As an example of their use, bcfg2 and cfengine - both well known and established within the UNIX community - rely on rule-based configuration for managed servers. In other words, both tools implement their own language definition which is then used to specify how a server should be configured. Any deviation from this definition is then corrected by the software. For example, if a server that is defined as web server is found to not have Apache software installed, both change management packages will correct this deviation by installing and configuring the Apache package.

This capability to define configuration rules and to enforce those rules allows both bcfg2 and cfengine to implement a potent mechanism for the Managing Changes activity.

However, as is often the case with open source, the reporting capabilities of these products are limited. While bcfg2 and cfengine provide reports on changes made to the system, there is no obvious way to determine which systems are currently out-of-sync other than allowing them to bring the systems back into sync. This limits their ability to audit for unauthorized changes to systems (however, this tends to be more important in Configuration Management.)

Unfortunately, the majority of open source change management products are UNIX specific, meaning that they do not support Windows, therefore they do not support a key server in enterprise environments.

Microsoft

Microsoft Systems Management Server (SMS) - called Microsoft System Center: Configuration Manager 2007 in its most recent release - is used within Microsoft environments to manage changes to target systems. It offers the following capabilities:

- **Deployment Planning.** Reports which provide information on hardware, software, and version information.
- **Deployment Based on Group.** Allows an administrator to distribute software to systems within groups, where a group can be defined using properties such as hardware, Active Directory (AD) organization units, and AD group membership.
- **Patch Updates.** Automates the deployment of patches to critical Windows servers and applications.

SMS is an effective tool which can be used in enterprise settings to automate most, if not all, of the needs of Change Management. However, SMS is specific to Windows environments, and is not suitable for managing UNIX and Linux servers and applications.

Change Management Conclusions

As discussed, there are viable solutions for Change Management in both open source and Microsoft environments. The open source community has provided robust technical solutions such as bcfg2 and cfengine, but often do not stress essential activities such as help in planning changes (e.g., the software does not easily allow an administrator to estimate the impact of a change). Microsoft's SMS offers a more comprehensive solution, but is limited in its reach because of its focus on Microsoft and Windows products. Thus, at this time any enterprise running Windows and UNIX must often run two change management products in parallel.

IT Service Support: Release Management

Definition

Enterprises are cautious in how, when, and where they deploy new hardware and software. Failed rollouts can result in downtime and potentially lost data—neither of which are good news for IT organizations trying to offer high uptimes and reliability.

Release Management provides organizations with a strategy for releasing software and hardware. It helps ensure the proper licensing, testing, and validation of new releases. An immediate benefit of Release Management is that it encourages an organization to view software and hardware rollouts strategically.

There are several activities associated with Release Management, including:

- **Build and Configure**. Build components in a controlled environment.
- **Test and Accept**. Test groups can test the hardware or software to ensure quality and reliability.
- **Schedule and Plan**. Schedule when a rollout occurs, and how it should occur. This part of the ITIL process also works closely with Configuration Management since Configuration Items (CIs) will be updated.
- **Communicate and Prepare**. Communicate the rollout plan to affected parties.
- **Distribute and Install**. Distribute and install the rollout to the existing infrastructure.

Product Comparison

Release Management is similar in some ways to Change Management, but is more concerned with the "big picture" of how a release will affect an organization's existing infrastructure. While specific changes to the infrastructure required by Release Management may then be issues as a Request for Change (RFC) within Change Management, Release Management is much more concerned with the broader process for testing, validation, and distribution.

Because of this, Release Management relies less extensively on technical solutions, and instead depends on software which promotes documentation, communication, and version control, as can be seen in the product selection shown in Table 9.

Table 9 - Release Management Software

Solution	Vendor	Platforms	License	First release	Latest release
RT	Best Practical	UNIX	GPL	1996	7/5/2007
OTRS	OTRS	UNIX, Linux, Windows	GPL	4-9-2002	9-18-2007
OpenOffice	OpenOffice.org	UNIX, Linux, Windows	GPL	-	-
Office	Microsoft	Windows	MS-EULA	-	-
Systems Management Server	Microsoft	Windows	Proprietary	1994 — Microsoft Systems Management Server 1.0	May 2007 — Microsoft System Center Configuration Manager 2007
Zenoss	Zenoss	Linux, UNIX, Windows	GPL with EULA	3/2006	6/20/2007 – 2.0
Cfengine	Cfengine	Linux, UNIX, Windows	GPL	1993	1/27/2007

Table 10 provides a review of the capabilities of each product to address the ITIL activities for Release Management. We provide further analysis in the following sections titled “Open Source” and “Microsoft.”

Table 10 - Release Management Activities Review

Solution	Plan	Communicate and Prepare	Distribute and Install
RT	○	●	○
OTRS	○	●	○
OpenOffice	○	○	○
Office	○	○	○
Systems Management Server	●	○	●
Zenoss	●	○	○
cfengine	◑	○	●

Chart legend - ● = strong, ◑ = weak, ○= none

Open Source

As shown in Table 10, Release Management is less technical than other processes (although it certainly contains technical elements ;) instead, it addresses the overall process of planning, testing, and communicating rollouts.

In terms of planning activities, Release Management requires that an IT organization be aware of how its infrastructure will be affected by a rollout. Generally, this capability requires an effective Configuration Management element to have been implemented within the organization. There are two open source products listed: Zenoss and cfengine. Zenoss provides a planning capability based on its ability to "model" the existing network infrastructure based on the knowledge maintained in its Configuration Management Database (CMDB). cfengine, which is used principally for Change Management, has no such capability.

Once a plan is created, it must then be communicated to the affected parties. Neither Zenoss nor cfengine provide this capability. Instead, this realm is based on workflow, project management, and ticketing systems which allow technicians to properly document, track, and communicate needs to other technicians and end-users. Thus, our comparison lists RT and OTRS, two open source help desk products.

Finally, there is a need to implement the actual rollout. How this is accomplished can vary based on the task at hand. For example, to deploy applications to the desktops of a new department, IT will have a relatively small software update burden once the initial patches have been loaded. However, if there is a mass rollout of a new operating system version, obviously the burden for managing the software is high. In this case, tools such as cfengine can prove valuable because most of the activities can be fully automated. Unfortunately, there are few cross-platform tools which can handle automated software rollouts to both Windows and UNIX environments.

Microsoft

System administrators working within Microsoft environments face the same issues as users of open source. Specifically, they must use different software for each need in Release Management. As with open source, managers in Windows environments must rely on workflow or ticketing systems to manage the planning process. In the Incident Management section of this paper we discussed AmberCat, an example of a help desk package from a Microsoft partner. There are of course many other help desk products, and those that allow for the definition of a workflow process tend to work best for Release Management.

Microsoft's Systems Management Server (SMS) again provides a significant capability for hardware and software management in Windows environments. For hardware rollouts, SMS is able to use its auto-discovery capabilities to locate the new devices and add them to its CMDB. Also, because SMS works with Windows Management Instrumentation (WMI), it is able to provide a detailed listing of the individual components of the new hardware. SMS is also well suited to software deployments - that is, for supported operating systems and applications.

One of the strengths of SMS is the ability to provide a "mass rollout" of OS updates, applications, patches, and configuration changes. And because SMS is able to restrict a

rollout to groups of systems based on properties such as hardware or AD group membership, it gives system administrators granular control of the rollout process.

Release Management Conclusions

Release Management, like Change Management, is impacted in many ways by the IT environment itself. While some Release Management activities, such as the Planning and Communication activities, are not platform specific, the more technical aspects, such as Distribute and Install, currently require that each type of platform environment maintain their own set of tools. Specifically, UNIX and open source environments rely on products such as cfengine to implement changes, while Windows environments will need to rely on SMS or other change management products available within the Microsoft ecosystem.

IT Service Delivery: Service Level Management

Definition

An enterprise succeeds or fails based on a number of factors, one of the most important of which is the IT service that powers computing and communications. Because of the mission-critical nature of IT services it is then critical to be able to quantify availability, reliability, and performance.

Service Level Management provides a way to manage, maintain, and improve the quality of IT services. Like many ITIL processes, Service Level Management is a continuous process which includes a cycle of agreeing, monitoring, and reporting IT service levels, allowing system administrators and managers to determine where IT is falling short of expectations. A critical aspect of Service Level Management is that it provides metrics for IT service performance and quality.

Service Level Management relies on three types of agreements:

- **Service Level Agreements (SLAs).** Agreements between an IT organization and its customers.
- **Operational Level Agreements (OLAs).** Agreements between units within the IT organization.
- **Underpinning Contracts (OCs).** Agreements between an IT organization and its suppliers and service providers.

Each of these agreements requires that an IT organization define its services (known as the Service Catalog) and gather key metrics on the quality of those cataloged services.

Knowing this, we can discuss the activities associated with Service Level Management, which include the following:

- **Define Service Catalog.** Defines the services either provided or supplied to an IT organization.
- **Define SLAs.** Defines and negotiates the agreements between an IT organization and its customers.
- **Define OLAs.** Defines and negotiates the agreements between internal units within an IT organization.
- **Define UCs.** Defines and negotiates the agreements between an IT organization and its suppliers.
- **Status Accounting.** Gathers metrics and monitors the performance of monitored services.

Product Comparison

Because of the emphasis on monitoring and historical reports, products which are geared for Service Level Management must be capable of not only providing point-in-time performance information for a service, but also be capable of supplying reports which can be used to determine when agreements were violated (For example, if a database service failed more than expected).

There are other features that are commonly found, such as:

- Sending an alert when a service first fails.
- Trending reports to determine if an agreement is in danger of being violated in the near-term.
- Allowing customers to view the levels of service being provided.

The products listed in Table 11 provide some or all of these capabilities.

Table 11 - Service Level Management Software

Solution	Vendor	Platforms	License	First release	Latest release
GroundWork Foundation Monitoring	Groundwork Foundation	Linux	GPL	9/5/2006	7/22/2207
ZABBIX	ZABBIX	UNIX, Linux, Windows	GPL	4/7/2001	8/21/2007
OTRS	OTRS	UNIX, Linux, Windows	GPL	4/9/2002	8/3/2007
Zenoss	Zenoss	UNIX, Linux	GPL	6/1/05	8/27/07
Microsoft System Center: Operations Manager	Microsoft	Windows	Proprietary	-	3/23/2007
Hyperic HQ	Hyperic	UNIX, Linux, Windows	GPL	7/18/07	8/9/07

Table 12 provides a review of the capabilities of each product to address the ITIL activities for Service Level Management. We provide further analysis in the following sections titled “Open Source” and “Microsoft.”

Table 12 - Service Level Management Activities Review

Solution	Define Service Catalog	Status Accounting
GroundWork Foundation Monitoring	○	●
ZABBIX	○	●
OTRS	◑	○
Zenoss	○	●
Microsoft System Center: Operations Manager	○	●
Hyperic HQ	○	●

Chart legend - ● = strong, ◑ = weak, ○= none

Open Source

The open source community offers several applications which can assist with Service Level Management. For example, GroundWork Foundation Monitoring, ZABBIX, Zenoss, and Hyperic HQ.

A viable project is ZABBIX, which is highly extensible and can be configured to monitor specific, granular parameters in both open source and Microsoft environments. For example, ZABBIX is able to monitor many of the same Exchange metrics as Microsoft System Center: Operations Manager (MOM); however, configuration of ZABBIX requires in-depth knowledge, and it does not use the simpler template systems of Microsoft System Center: Operations Manager (MOM), Zenoss, or Hyperic HQ.

Zenoss and Hyperic HQ also offer Service Level Management capabilities. For example, both can be used to measure specific whether a given IT service meets specific SLA requirements, e.g., whether a database service has an uptime of 99.9% or better.

OTRS is mentioned in passing because it offers a limited ability to define a Service Catalog for use in Incident Management, which can then be used to determine if SLAs related to that ITIL process are being met.

Completely free and open products, such as ZABBIX, can be used to monitor almost all of the elements of an SLA. However, they require intimate knowledge of both ZABBIX and the service being monitored (e.g., an Oracle database server). Products such as Zenoss, which offers a free and open source “Core” application, require the purchase of upgrades to monitor specific applications easily.

Microsoft

Microsoft Operations Manager (MOM) has an SLA monitoring capability. It is generally deployed in Windows-centric environments, but can in fact be extended by third-party add-on products to expand its reach. For example, Quest has an extension suite known as Quest Management Xtensions which allow MOM to be used to manage UNIX operating systems such as Solaris, AIX, and Linux.

Like Zenoss, MOM provides generic monitoring of network services out-of-the-box, including support for SNMP and UNIX Syslog. However, to monitor a client system with the full range of MOM capabilities, a license must be purchased and, preferably, an agent installed. In addition, to monitor applications or frameworks such as for Oracle or .NET requires the use of expansion packs.

For configurability, MOM leverages a point-and-click configuration and template system. For example, by using the Exchange SLA Template within MOM several key Exchange SLA parameters may be tracked, ranging from the availability of specific servers within an Exchange infrastructure (e.g., Bridgehead Server Availability) to counts of actual blocked and delivered email.

Service Level Management Conclusions

There are several products capable of assisting with Service Level Management from both Microsoft and the open source community. Each has its own strengths and weaknesses. For example, while MOM is relatively simple to implement and includes templates for Microsoft applications, it focuses on the Windows platform and requires third-party add-ons for additional platform support. Open source applications, such as ZABBIX, have a more diverse perspective but are also saddled with a more difficult implementation. In the end, a product decision will be based on whether your services tend to be Microsoft-specific or range across a broader spectrum of vendors.

IT Service Delivery: Capacity Management

Definition

Capacity Management is a proactive ITIL process of determining the capacity needs of current and future IT services. The goal of Capacity Management is to ensure that IT services are given sufficient resources to be effective, sustainable, and scalable. There are several benefits to Capacity Management, including the ability to determine where resources are under-allocated, over-allocated, and where additional capacity should be funded.

Because Capacity Management is such a large field, there are three realms to consider:

- **Business Capacity Management (BCM).** Stakeholders evaluate business, financial, economic, and technology indicators with the goal of forecasting future business load.
- **Service Capacity Management (SCM).** Short-term needs are identified and addressed within the organization for service-level, end-to-end needs.
- **Resource Capacity Management (RCM).** Short-term needs for specific resources within the network are addressed.

While SCM/RCM is tactical in nature, BCM is a longer-term, strategic approach to Capacity Management, particularly for planning. All are important, but this paper emphasizes SCM/RCM toolsets since they gather information needed for both short- and long-term capacity planning.

There are several activities associated with Capacity Management, including:

- **Monitoring**. What can the product monitor out-of-the-box and what can it be adapted to monitor.
- **Analysis**. How well can the product assist with trending.
- **Demand Management**. How well does the combination of a product's Monitoring and Analysis capability assist with Demand Management.
- **Modeling**. The capability to provide a working model of both the existing environment as well a proposed environment.
- **Planning**. The ability to rely on models and existing capability and performance information to analyze and plan long-term changes to the environment.

Product Comparison

Capacity Management is designed to support the "optimum and cost effective" provisioning of IT services. For a product to meet the requirements of Capacity Management, it must be able to model the existing infrastructure and to track performance metrics to determine when that infrastructure must be altered to meet demand.

The products listed below in Table 13 provide some or all of these capabilities.

Table 13 - Capacity Management Software

Solution	Vendor	Platforms	License	First release	Latest release
Cacti	Cacti	UNIX, Linux	GPL	9/22/2001	1/17/2007
Zenoss	Zenoss	UNIX, Linux	GPL	6/1/05	8/27/07
Capacity Planner	Microsoft	Windows	Proprietary	4/2007	4/2007 (beta)
Microsoft System Center: Operations Manager	Microsoft	Windows	Proprietary	2000	3/2007
Hyperic HQ	Hyperic	UNIX, Linux, Windows	GPL	7/18/07	8/9/07
Zabbix	ZABBIX	UNIX, Linux, Windows	GPL	4/7/2001	8/21/2007

Table 14 provides a review of the capabilities of each product to address the ITIL activities for Service Management. We provide further analysis in the following sections titled “Open Source” and “Microsoft.”

Table 14 – Capacity Management Activities Review

Solution	Monitoring	Analysis	Demand Management[1]	Modeling	Planning
Cacti	●	○	◑	○	○
Zenoss	●	●	●	◑	●
Capacity Planner				●	
Microsoft System Center: Operations Manager	●	●	●	◑	●
Hyperic HQ	●	●	●	◑	●
Zabbix	●	●	◑	◑	●

Chart legend - ● = strong, ◑ = weak, ○= none

Open Source

Notice that the needs of Demand Management are closely tied with that of Monitoring and Analysis. Specifically, with Demand Management we want to know when and where to transfer demand based on utilization, both in the short- and long-term. Obviously, this requires that we have a performance baseline as well as current information on

[1] We rate Demand Management based on the combined rating of Monitoring and Analysis for a product.

used and available capacity. When thinking in these terms, it should be clear that Demand Management is closely aligned with the overall concept of Capacity Management. Specifically, how can we best direct the flow of demand across our infrastructure with an eye toward sustainable growth and availability?

Markedly, some open source products, such as Cacti, perform well in Monitoring, but do poorly during the Analysis phase. The reason: Cacti collects data, but does not provide any tools for trending and analysis. Indeed, with Cacti you must extract the data from the Cacti database with an external reporting tool to perform additional analysis.

Zenoss, Hyperic HQ, and Zabbix fare better. Rather than only collecting data for historical reporting, these products provide trending capabilities which can be used to easily compare baselines and current values and help estimate future performance and needs.

Microsoft

Microsoft System Center: Operations Manager (MOM) fills the Capacity Management niche in Microsoft environments. MOM is similar to both Zenoss and Hyperic HQ in the features it provides, including:

- **Monitoring**. MOM can provide extensive performance monitoring at the network-, OS-, and application-level. For example, it is capable of monitoring almost every detail of the performance characteristics of an Exchange or Microsoft SQL Server.
- **Analysis**. MOM provides system administrators with historical and trending information. Additionally, through the use of templates, it is able to help administrators determine when near-term capacity issues may occur.

MOM alone, however, does not fully satisfy the needs of Capacity Management in Microsoft settings. While Microsoft does not offer a generic modeling capability, the Microsoft Capacity Planner provides a way to model and plan for Exchange and MOM deployments. Conceivably, this, or tools like it, will be available in the future to help plan for the deployment of other Microsoft applications.

Capacity Management Conclusions

There is a lot of similarity in the tools used by managers dealing with both Capacity and Availability Management. The information gathered is critical to both. Thus, we see a lot of shared products between the two.

The open source community offers several compelling options. However, there are notable issues involved in the products. ZABBIX is a “pure” open source solution, and while powerful does require manual configuration, which can be troublesome in large environments. Zenoss and Hyperic HQ are both very powerful, but in order to access

advanced features for “supported” applications such as Oracle or SQL Server, commercial add-ons must be purchased, moving them outside the realm of open source.

Microsoft provides a purely commercial solution for both monitoring and reporting that has very robust features, but their focus is almost exclusively on Microsoft products, limiting reach. In addition, unlike software such as ZABBIX, MOM exposes less “under the hood” configuration options, meaning that users must often look to add-on software to extend its abilities.

IT Service Delivery: Availability Management

Definition

All organizations, especially those working under Service Level Agreements (SLAs), must ensure that downtime of any service is minimized. This is particularly the case where an IT service, such as a Local Area Network (LAN), is mission-critical to the operations of a customer.

Availability Management provides a strategy for detecting and responding to IT service faults. It results in a more reliable infrastructure, and can help to ensure that the services an organization depends upon are available when they are needed.

There are several activities associated with Availability Management, including:

- **Define Requirements.** Determine the IT service availability needs of customers; much of this information can be gathered from the agreements (e.g., SLAs) between an organization and its users.
- **Availability Planning.** Create plans for ensuring the availability of critical services based on the needs determined in the requirements definition activity.
- **Monitor Availability.** Track the availability of monitored services. Often, this activity includes generating alerts when a monitored service fails.
  Monitor Obligations. Compare availability reports and trending against the obligations an IT organization has with its customers.

Product Comparison

Because the term “IT service” can actually include non-technical operations such as how quickly a help desk returns a support call on average, there really is no single solution. However, we can narrow our focus to those products which monitor the availability of specific types of technical services, such as network capacity and the speed of a database.

Products that provide this level of assistance must be able to monitor service availability as well as to generate reports showing historical trends. In addition, in order to monitor obligations, products should be able to provide uptime reports for a given service.

The products listed in Table 15 provide some or all of these capabilities.

Table 15 - Availability Management Software

Solution	Vendor	Platforms	License	First release	Latest release
Nagios	Nagios	UNIX, Linux, Windows	GPL	5/10/2002	8/30/2007
BB	Quest Software	UNIX, Linux, Windows	GPL	12/31/1996	12/20/2005
Zabbix	Zabbix	UNIX, Linux, Windows	GPL	4/7/2001	8/21/2007
Zenoss	Zenoss	UNIX, Linux, Windows	GPL	6/1/05	8/27/07
Hyperic HQ	Hyperic	UNIX, Linux, Windows	GPL	7/18/07	8/9/07
Microsoft System Center: Operations Manager	Microsoft	Windows	Proprietary	2000	3/23/2007

Table 16 provides a review of the capabilities of each product to address the ITIL activities for Availability Management. We provide further analysis in the following sections titled “Open Source” and “Microsoft.”

Table 16 - Availability Management Activities Review

Solution	Monitor Availability	Monitor Obligations
Nagios	●	○
BB	●	○
Zabbix	●	●
Zenoss	●	◑
Hyperic HQ	●	○
Microsoft System Center: Operations Manager	●	●

Chart legend - ● = strong, ◑ = weak, ○= none

Open Source

Notably, all of the open source products listed provide for an extensive monitoring capability. However, the do-it-yourself history of open source comes through in this area. For example, products such as Nagios and Big Brother (BB) require hand configuration for much of the implementation, and can be very complicated to setup.

A good example of a widely used open source product in the Availability Management arena is BB. It is both extensible and widely deployed, and in fact has a significant following in Internet Service Provider (ISP) and collocation facilities because of its strength in network monitoring. It also supports a highly customizable platform for creating new service tests to detect for outages (e.g., disk space checks).

However, the open source Big Brother is almost entirely driven by a series of Bourne-shell scripts, which limits its scalability; also, arguably, the reliance on shell scripts can cause code maintenance issues. (Nagios, which is younger, provides a similar environment for extensions and, like Big Brother, provides a web and alert interface.) In addition, while BB can provide for both real-time and historical availability information, it cannot by itself monitor obligations, meaning that managers must perform manual analysis of service availability reports against obligations requirements.

Newer tools, such as Zenoss and Hyperic HQ, have expanded on the BB and Nagios models. Hyperic HQ specifically provides for an advanced Search/Discover capability, and can be extended to monitor almost any type of network service. In addition, both Zenoss and Hyperic HQ understand the concept of an SLA, and the monitoring can be mapped against SLA needs in a way that simplifies obligation monitoring.

Microsoft

Microsoft System Center: Operations Manager (MOM) product also provides Availability Monitoring features. It is capable of monitoring network-, server, and application-level availability (e.g., whether a Domain Controller is performing correctly). This information, along with its integrated performance monitoring, allows Operations Manager to play an important role in both Capacity Management and Availability Management.

MOM also supports alerting based on thresholds, allowing systems managers to use it for automated incident reporting, e.g., if a network link fails. In addition, the use of the Availability Management Pack, which is a free add-on to the base MOM installation from Microsoft, expands the capabilities of MOM in Availability Management scenarios. The Availability Management Pack is essential when using MOM to monitor obligations against SLAs. The Pack is designed for SQL Server, Exchange, IIS, AD, and Windows endpoints.

Availability Management Conclusions

Availability Management benefits from a diverse community of products, most of which can be used in heterogeneous environments where both open source and Microsoft technologies exists.

Open source products such as Nagios and BB provide a foundation for monitoring services, but reporting tends to be relatively week, especially for trending. Solutions such as Zenoss and Hyperic HQ add many more reporting features which are necessary

to large organizations, particularly those running mission-critical database and messaging systems, but require the purchase of commercial add-ons.

MOM remains an important element in Microsoft environments because of its intimate knowledge of and support for Microsoft products such as Exchange. MOM also crosses over into other ITIL processes, such as Capacity Management and Service Level Management, allowing it to provide a one-stop-solution for those processes, albeit with limited support for the diverse range of products in today's enterprise.

IT Service Delivery: Security Management

Definition

Regardless of how reliable the IT services being provided, an organization that doesn't actively manage the security of its networks and information is destined to experience downtime and, even worse, loss of data. When providing services to customers, an IT organization must ensure that it meets not only its own security standards, but those of the customers as well.

Security Management is the process of managing a defined level of security for IT services and information, and it relies heavily on the ability to implement security controls, to manage security incidents, to perform audits, and to report on the efficacy of the Security Management process. In ITIL, the activities associated with Security Management include:

- **Coordinate Security Management.** Define and coordinate the departments and policies which will govern Security Management.
- **Implement Controls.** Implement the controls required to implement the Security Management policies required by the organization.
- **Evaluate and Audit Controls.** Evaluate and audit the Security Management supporting infrastructure.
- **Maintain and Monitor.** Maintain Security Management people, processes and technical infrastructure.

Product Comparison

Security Management is a significant ITIL process that includes activities ranging from the creation of security policies and requirements to implementing and auditing the controls put into place to execute those policies. In this review, we focus on those products which can assist in implementing and auditing the security controls that are a critical element of Security Management.

The products listed in Table 17 provide some or all of these capabilities.

Table 17 - Security Management Software

Solution	Vendor	Platforms	License	First release	Latest release
-	Microsoft	-	-	-	-
OSSIM	OSSIM	Linux, UNIX	BSD	8/22/2003 0.1-alpha	8/8/2007 – 0.9.9rc5
Prelude-IDS	Prelude-IDS	Linux, UNIX	GPL	-	9/25/2007 – 0.9.0

Table 18 provides a review of the capabilities of each product to address the ITIL activities for Incident Management. We provide further analysis in the following sections titled “Open Source” and “Microsoft.”

Table 18 –Security Management Activities Review

Solution	Coordinate	Implement	Audit	Maintain
Microsoft				
OSSIM	○	●	●	○
Prelude-IDS	○	●	●	○

Chart legend - ● = strong, ◑ = weak, ○= none

Open Source

Unfortunately, while there are a great many open source projects which focus on the needs of security in the enterprise, there are few that focus on Security Management as a comprehensive process across an organization. Thus, during the research for this paper, we focused on products which are able to manage security information, rather than tools implementing specific network, platform, or application security controls.

The two most viable products available in the open source community are Open Source Security Information Management (OSSIM) and Prelude IDS.

The OSSIM project aims to integrate a full suite of intrusion detection and correlation facilities, all of which can prove effective in monitoring the security controls which implement policy. Specifically, OSSIM offers the following integration:

- **Arpwatch.** Used for anomaly detection.
- **P0f.** Used for passive OS detection and OS change analysis.
- **Pads.** Used for service anomaly detection.
- **Nessus.** Used for vulnerability assessment and for cross correlation.
- **Snort.** An IDS and also used for cross correlation with NESSUS.
- **Spade.** The statistical packet anomaly detection engine.
- **Tcptrack.** Used for session data information useful for attack correlation.
- **Ntop.** Builds a network information database used for anomaly detection.

- **Nagios.** Monitors host and service availability information.
- **Osiris.** A host-based intrusion detection system (HIDS).

A significant feature of OSSIM is that it can be used to implement not only monitoring of controls, but many of the actual controls as well. For example, Osiris is a HIDS which can be deployed across open source systems such as Linux to detect intrusions or unauthorized access.

OSSIM does suffer from scalability concerns. While it offers many features, there is a high implementation burden for networks with many devices because of the labor-intensive configuration process.

Prelude IDS is another open source product which aims to bring security under a single umbrella. Like OSSIM, Prelude IDS largely addresses Security Information Management (SIM) and Security Event Information Management (SEIM). The actual security controls and information gathering are based on other software, much of it open source, including software such as:

- **Snort.** An IDS and also used for cross correlation with NESSUS.
- **Nessus.** Used for vulnerability assessment and for cross correlation.
- **Nagios.** Monitors host and service availability information.
- **Argus.** Used for anomaly detection.
- **AIDE.** A host-based intrusion detection system (HIDS).
- **OSSEC.** A host-based intrusion detection system (HIDS).

Applications such as OSSIM and Prelude IDS allow managers to not only implement security controls, but to also manage them centrally rather than having to monitor many distinct elements within the network.

Microsoft

As with open source, there is no single tool provided by Microsoft to implement Security Management. However, Microsoft does offer a wide range of security-focused products which are used to implement security controls. Examples include:

- **ISA Server.** Firewall with the capability to control network access to network resources for both incoming and outgoing connections.
- **Rights Management Services.** Digital Rights Management (DRM) capabilities to help safeguard digital information from unauthorized use.
- **Microsoft Antigen.** Server-level anti-virus features for collaboration software such as Exchange and SharePoint.
- **Microsoft Anti-Spyware.** Workstation-level protection from spyware and malware.

In the open source community, OSSIM and Prelude IDSA provide not only controls, but also a central resource for security information management. Microsoft does not offer a similar product, but other vendors in the Microsoft ecosystem do. For example, CA offers CA Security Information Management (SIM), which provides for a similar "enterprise-wide" view of security information as OSSIM.

Security Management Conclusions

One of the most important ITIL processes, Security Management encompasses a wide set of processes and procedures, and there are many products which provide niche solutions.

Because of this, there are few solutions in the open source space that can be considered true "ITIL Security Management" solutions. Instead, open source products tend to focus on specific objectives, such as Network Intrusion Detection or Vulnerability Scanners. Only recently have projects such as OSSIM and Prelude-IDS begun to address this vacuum.

Microsoft also provides targeted solutions in the security space, such as the ISA Server firewall and Rights Management Services (RMS) for DRM. However, system administrator must rely on the Microsoft ecosystem to provide tools which address Security Management in a way similar to OSSIM and Prelude-IDS.

ITIL: Microsoft and Open Source - Conclusions

We've seen that the history of both open source and Microsoft have played a role in product implementations. Open source solutions often target specific, niche problem areas (often because the product addresses the needs of the original authors). Microsoft, on the other hand, typically addresses issues in a Windows-centric fashion. Both approaches have merit, and yet both also bring with them risks.

For open source, the risk has evolved from the traditional open source and UNIX perspective of "solve one problem, and solve it well." This mindse**t**, which tends to result in well thought out and implemented solutions for specific tasks, brings with it the danger of deep but narrow products which simply have too limited a scope. More integration across products can certainly mitigate this risk, but that level of integration is extremely rare.

Microsoft, on the other hand, has a history of tackling large problems with more comprehensive suites of applications and tools. Indeed, in many ways Microsoft has maintained their focus on solving Windows-centric issues, whether at the network-, server-, or application-level. The risk in this approach is whether or not these tools satisfy enterprise ITIL requirements. The risk inherent in not meeting the full needs of the enterprise is that administrators will opt to use products which offer support for non-Windows platforms and applications. This risk affects both Microsoft and its customers.

When viewed in this light, we see that no single solution exists which completely satisfies the needs of ITIL, often even within a single ITIL process. Instead, we must perform in-depth review and analysis of the needs of the customer, and then match those needs against products that target those needs. Perhaps some solutions will involve open source only, while others will be Microsoft-centric, but, in most cases, the solutions will involve both.

About the Author

Dustin Puryear is the author of *Integrate Linux Solutions into Your Windows Network* and *Best Practices for Managing Linux and UNIX Servers*, and he provides organizations with guidance on issues affecting interoperability, identity management, and directory services.

Appendix

Table A - Incident Management Product URLs

Software	Website
RT	http://bestpractical.com/rt/
OTRS	http://otrs.org
Bugzilla	http://www.bugzilla.org
Double Choco Latte	http://dcl.sourceforge.net/
Liberum Help Desk	http://www.liberum.org/
Savane	https://gna.org/projects/savane
Microsoft System Center: Service Manager	http://www.microsoft.com/systemcenter/svcmgr/default.mspx
dotProject	http://www.dotproject.com

Table B - Problem Management Product URLs

Solution	URL
RT	http://bestpractical.com/rt/
OTRS	http://otrs.org
Bugzilla	http://www.bugzilla.org
Double Choco Latte	http://dcl.sourceforge.net/
Liberum Help Desk	http://www.liberum.org/
Savane	https://gna.org/projects/savane
Microsoft System Center: Service Manager	http://www.microsoft.com/systemcenter/svcmgr/default.mspx
dotProject	http://www.dotproject.com

Table C - Configuration Management Product URLs

Solution	URL
CMDBuild	http://www.cmdbuild.org
Systems Management Server	http://www.microsoft.com/smserver/default.mspx
Zenoss	http://www.zenoss.com/
OneCMDB	http://www.onecmdb.org/wiki/index.php/Main_Page

Table D - Change Management Product URLs

Solution	URL
Bcfg2	http://trac.mcs.anl.gov/projects/bcfg2/
Cfengine	http://www.cfengine.com/
Radmind	http://webapps.itcs.umich.edu/radmind/index.php/Main_Page http://rsug.itd.umich.edu/software/radmind/windows.html
Systems Management Server	http://www.microsoft.com/smserver/default.mspx
Zenoss	http://www.zenoss.com/
BPMSpace	http://www.bpmspace.org/
NetDirector	http://www.netdirector.org/
Webmin	http://www.webmin.com/

Table E - Release Management Product URLs

Solution	URL
OpenOffice	http://www.openoffice.org/
Microsoft Visio	http://www.office2007.com/
Microsoft Project	http://www.office2007.com/
Microsoft Power Point	http://www.office2007.com/
Systems Management Server	http://www.microsoft.com/smserver/default.mspx
Cfengine	http://www.cfengine.com/
Zenoss	http://www.zenoss.com/

Table F - Service Level Management Product URLs

Solution	URL
GroundWork Foundation Monitoring	http://gwfoundation.sourceforge.net/
ZABBIX	http://www.ZABBIX.com/
OTRS	http://otrs.org/
Zenoss	http://www.zenoss.com
Microsoft System Center: Operations Manager	http://www.microsoft.com/systemcenter/opsmgr/default.mspx
Hyperic HQ	http://www.hyperic.com

Table G - Capacity Management Product URLs

Solution	URL
Cacti	www.cacti.net
Zenoss	www.zenoos.com
Microsoft System Center Capacity Planner	www.microsoft.com/systemcenter/
Microsoft System Center: Operations Manager	http://www.microsoft.com/systemcenter/opsmgr/default.mspx
Hyperic HQ	www.hyperic.com
Zabbix	www.zabbix.com

Table H - Availability Management Product URLs

Solution	URL
Nagios	www.nagios.org
BB	www.bb4.org
Zabbix	www.zabbix.com
Zenoss	www.zenoss.com
Hyperic HQ	www.hyperic.com
Microsoft System Center: Operations Manager	http://www.microsoft.com/systemcenter/opsmgr/default.mspx

Table I - Security Management Product URLs

Solution	URL
OSSIM	http://www.ossim.net/
Prelude-IDS	http://www.prelude-ids.org/