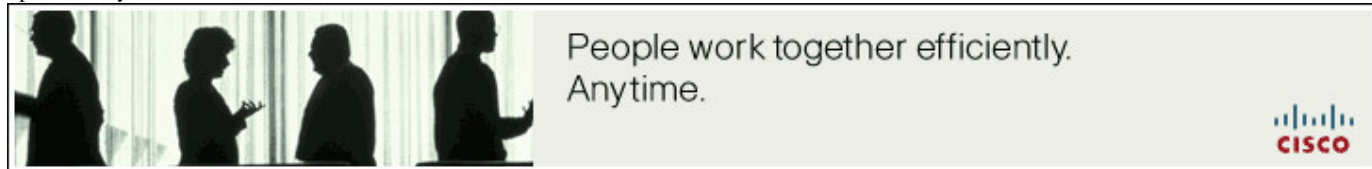


Sponsored by:



NETWORKWORLD

This story appeared on Network World at

<http://www.networkworld.com/news/2007/100807-5-it-projects-need-attention.html>

5 IT projects that need your attention right now

By Dustin Puryear , CIO, 10/08/07

There's always too much to do. If you had an infinite budget

and project schedule, or at least more resources than you have now, you could accomplish impressive things for your company. Performing triage means you need to pick IT projects that can deliver the most bang for the buck.

Accordingly, we discuss five projects that deserve a CIO's immediate attention. We chose these projects because they have a measurable impact, contain elements with a relatively fast ROI, and enhance both network security and manageability.

To start with, we discuss identity and access management, to ensure that the right people can get to the right resources. Next is Linux integration. Linux is here to stay, and it's time that you integrate it into your infrastructure. We follow with discussions on patch and change management, both integral pieces in terms of reliability and security for your network. Finally, we talk about incident management, a hot topic for any organization wishing to control costs and keep users content, whether they're behind a desktop or are business partners.

Manage identities

Account management has been IT's forgotten stepchild, but today's network complexity highlights its importance. IT managers are now faced with an incredibly varied mix of directory services, platforms and applications. Ensuring that accounts are properly provisioned and, when needed, terminated, has become an onerous task.

For example, a small network can have several Windows servers running in Active Directory (AD), several Linux servers using local accounts, and one or two network applications that maintain accounts in an Oracle database. In even this small setting, managing accounts, password resets and access rights is a significant task in itself. Now imagine an enterprise environment, particularly one with legacy applications and Big Iron. Ensuring that users have accounts and the required access in this environment can be both a security and a support nightmare—that is, unless there is a well-defined solution for managing those accounts and access rights.

The solution

Commit to an identity and access management (IAM) process, which manages account provisioning, password resets, and access rights for accounts on the network and within applications.

Where to start

There are several approaches to implementing IAM. Some focus on using enterprise directories to house accounts and access rights, but, frankly, this is a very limited approach that does not reach far enough into the enterprise, particularly in terms of legacy applications. Even Microsoft, which touts AD as an identity solution, understands the limitations of an enterprise directory; the company released Microsoft Identity Integration Service (MIIS) to support the broader IAM needs of the enterprise. Keep in mind, however, that an enterprise directory is still a critical element of IAM.

Sponsored by:

An advertisement for Cisco's integrated services network. It features a photograph of three people from behind, looking out over a city skyline. The text reads: "Expand your network as your needs expand with Cisco integrated services network. Meld voice, video, security, wired, and wireless. All managed from one place. → Learn more" and "welcome to the human network. CISCO" with the Cisco logo.

That said, begin by implementing an IAM product, such as those offered by CA, IBM, Novell, Microsoft or Sun, and use it first to manage your enterprise directory. This will give you a very quick win, and it will also give you time to learn both the complexities of the IAM product as well as the overall IAM process. Next, build and implement connectors to specific platforms and applications within your network. Fortunately, many IAM products come with built-in connectors for enterprise applications (for example, PeopleSoft, Exchange), which allow you to progress from simpler to more complex implementations over time.

Manage Linux

Linux. To many, the word itself evokes thoughts of a wild, untamed force in IT. And, all too often, this is indeed the case. Many Linux servers are deployed as is and with little integration, with systems administrators simply loading critical applications on the server and assuming that their job is done. Only later do systems administrators find that it is difficult, if not impossible, to allow others access to the servers and the applications. Yet, as a critical element in your infrastructure, Linux is here to stay and must be managed with that in mind.

The solution

There are several issues involved in managing Linux, with one of the most important being how to integrate it into Active Directory (AD). In many ways, this problem is part of the larger IAM issue discussed earlier, but there are very powerful, effective and fast ways to integrate Linux into your existing network without having to wait for your IAM process to take hold.

Where to start

Once you determine which Linux servers should be integrated (often, this is all of them), you can move forward with determining how to implement that integration. The open-source and widely used Samba package allows Linux and Unix to integrate into either a Windows NT domain or AD. With AD, the Linux server relies on Kerberos and LDAP to communicate with AD, just as if it were any Windows system. Also, once integrated, you can access and assign permissions to any AD user or group on the Linux server; this is very powerful for Linux-based file servers or if you wish to allow users to log in to the Linux server to access an application.

Commercial products also can make your job easier. For example, products from vendors such as NetIQ, Quest, Centrify and Centeris can make integration a snap, often with just a few clicks of a mouse. There are other value-adds as well. For example, Centrify allows you to support Group Policy Objects (GPOs) on Linux, while Centeris provides a point-and-click configuration capability for Linux services (such as Apache).

Manage patches

It was difficult enough five years ago to maintain patches for Windows. Today, patch management has to consider several versions of Windows, Linux, Unix and various mission-critical applications. This makes patch management one of the most time-consuming activities for IT, especially considering that many organizations liberally use the term "management."

The solution

Implement a patch management process, even if manually driven at first, to identify critical vulnerabilities and patches. Later on, implement a system for automating the process of patching systems, with the ability to roll back changes if necessary.

Where to start

Despite the complexity of patch management, you can make great strides quickly if you focus on key elements of the patch management lifecycle, which is shown below:

- Reach. Discover, identify, and categorize the servers, workstations and network equipment.
- Resolve. Access vulnerabilities and missing patches.
- Research. Maintain up-to-date knowledge of available vulnerabilities and patches.
- Repair. Prioritize, schedule and patch vulnerable systems.
- Report. Monitor the patching process.

Unfortunately, there is no one-size-fits-all patch management solution, especially for heterogeneous environments with several platforms and applications. The real need for most enterprises is to focus on the Reach, Resolve and Research phases so that your organization can maintain awareness of patching needs. Once this part of the process is being managed effectively, you can move on to finding ways to automate the patching process itself, which is, by far, the most complex task in patch management.

Several vendors are in the patch management space, including ANSA, BindView, GFI Software and Quest. Notably, some products, such as ANSA's Autonomic Software, can be used to patch non-Windows platforms.

Manage infrastructure change

All too often, a change made to a mission-critical server has devastating results on an enterprise. Even major companies experience downtime or data loss because of an ill-timed or poorly planned change. Take, for example, a DNS administrator who decides to clean up DNS, only to later find that critical services failed because they relied on an older server hostname. At another level, new regulations, such as Sarbanes-Oxley (Sox), place a much higher burden on IT to ensure control and the ability to audit changes within the network.

The solution

Initiate a program to formalize the change management process within your organization.

Where to start

Begin by identifying which elements within your IT infrastructure can best be served by change management. While it may be nice to say "everything," in reality, organizations generally restrict change management to critical infrastructure pieces, such as servers and network devices.

Next, create a process document that identifies how a change request should flow through your organization. For example, if a change is made to a critical healthcare application in a hospital, should the change be approved by the application's management committee? And how should this workflow be enforced?

To help automate change management, look for two types of applications: workflow and systems management.

The first, workflow, manages the approval, review and reporting process involved in change management. Workflow software can come in many forms, but most often it has the feel of a help desk ticketing system but with additional features. For example, Change Management Control from SLAM offers workflow for change management and provides for a good deal of control over the process. Even open-source products are capable of use within change management, including the RT help desk package.

The second, systems management, is software that can actually implement the change on a target system for you. These types of systems are available in both the Windows and Unix worlds. In Windows, a good example is Microsoft Systems Management Server (SMS), which allows you to implement changes for critical Windows-based operating systems and applications. However, SMS is limited in the scope of applications supported. For Linux and Unix, configuration engines such as cfengine provide a very powerful policy-driven mechanism for implementing change and also for ensuring that systems do not diverge from their expected state.

Manage incidents

Organizations around the world lose untold dollars in lost productivity and wasted IT efforts because incidents are not correctly handled. It's a simple fact. This can happen with something as simple as an end user losing access to a printer, to losing a T1 connection to a remote office. And, instead of the incident being quickly identified and resolved, all too often the incident is incorrectly prioritized or missed completely—that is, until the incident causes significant problems for the organization. Worse yet, patterns of incidents are often missed, meaning similar problems continue to crop up, even when the root problem could be resolved entirely.

The solution

Incident management requires more than just help desk software; it's a symbiosis between your staff and software. Knowing this, implement help desk software that allows you to categorize and prioritize incidents, and, optionally, allows for workflow so that you can enable peer or management review for critical incident resolution.

Where to start

Incident management revolves around the premise that an incident must be quickly identified and resolved. Thus, a project implementing an incident management process within your organization must begin with how you answer four questions:

- How do you learn about an incident?
- How is the incident categorized?
- How is the incident prioritized?

-- How can the incident be quickly resolved?

Boiling this down, you need to determine how users can best communicate with IT; how to categorize incidents, which is critical for identifying any patterns later on; how to prioritize an incident based on both a user's needs and the needs of the organization overall; and, finally, how to use the incident information, the category and the prioritization to best focus your resources for incident resolution.

Fortunately, incident management is a very mature and large market, meaning you have a large number of vendors from which to choose. For example, in the open-source community there are RT and OTRS, which both have very strong incident management/help desk systems. Commercial products, such as Remedy and Clarify, also have a very long, mature history in this space.

And what do you do after lunch?

Obviously, a lot of work must be done in the enterprise to keep it working efficiently and to ensure IT's budget is maximized. In this article, we addressed five very specific projects to make certain you do just that. These projects include identity and access management, Linux integration, patch management, change management and incident management. All together, these five areas can enable powerful and substantive gains in how well and in how cost-effectively you can manage your network and IT services.

*Dustin Puryear is president of Puryear IT, LLC, which provides expertise in identity management, directory services and Linux interoperability. He is also a public speaker and the author of *Integrate Linux Solutions into Your Windows Network and Best Practices for Managing Linux and UNIX Servers*.*

All contents copyright 1995-2007 Network World, Inc. <http://www.networkworld.com>