

Connection

Novell Connection Magazine // JUN_2010

ARTICLES

PUBLISHED FOR
NOVELL CONNECTION
MAGAZINE.

NOTE: All content © 2010 by Novell, Inc. All rights reserved. For more information about Novell Connection Magazine or to obtain approval for bulk reprints, contact editor@novell.com

Features

// **Steps to Security Success**

One Step at a Time: Take a look at a phased approach to security management that enables you to ensure success every step along the way.

// **Higher Levels of Collaboration**

Higher Thinking: Novell Data Synchronizer enables your disparate collaboration solutions, business-critical applications and mobile devices to seamlessly synchronize events and information.

Departments

Trend Talk

// **Ending the Tug-of-War Between Agility and Compliance**

Proof Point

// **Von Par**

Trend Talk

// **Sprawl Killer**

Steps to Security Success

A Best-Practice Approach to Security Management

Policies

by Ken Baker

You're worried about data breaches or maybe you're working toward PCI-DSS, FISMA or HIPAA compliance, but you're not sure what more you need to do or where to start. You likely have some combination of firewalls, intrusion prevention systems, vulnerability scanners and AV software in place, but these systems generate more information than you can act on, and are completely siloed from each other. You know you need to address your compliance requirements for log collection, but how do you turn all that information from all your different systems' logs into usable information? Also, from that information, you want to be able to easily investigate and quickly respond to suspicious incidents that occur on your network. On top of that, you don't want to spend a lot of time and money on products that don't end up addressing your needs.

In a recent discussion with Brian Singer, Solutions Marketing Manager for Novell Security Management, he outlined a security management model that addresses these concerns with a phased approach comprised of the following three main security management aspects:

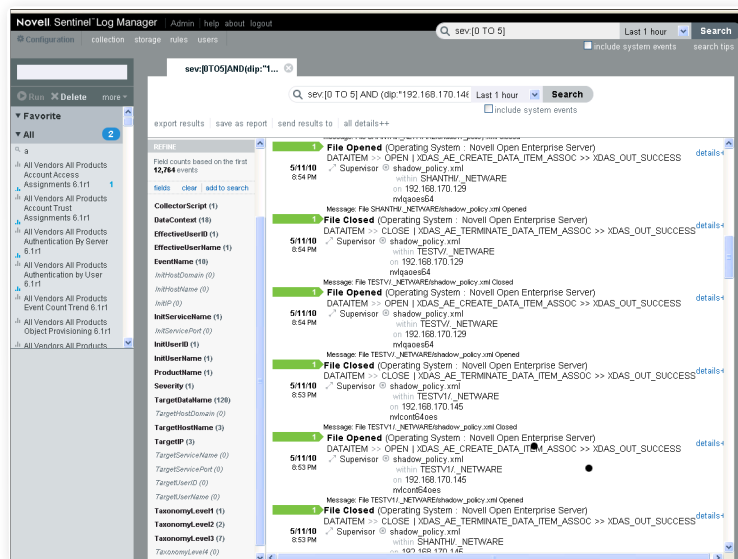
- 1. Log Management**
- 2. Security Information and Event Management**
- 3. Integration of Identity and Access Management**

This phased approach is designed to help you immediately get more value out of your existing investments, and also allows you to grow and add more capabilities as you're ready.

If an organization simply looks at its log data, it can often spot breach warning signs and stop breaches before they ever occur.

> Start with Log Management

With any undertaking like this, the first question is where do you start? One way is to get started by determining and prioritizing your high-risk assets and your low-risk assets. Once that's accomplished, you can bring in a log management product to collect information from all those you deem as high risk, which will likely include your firewalls, servers and mission critical applications.



Event search

Figure 1: Novell Sentinel Log Manager helps you spot suspicious activities, changes, or trends, as well as respond to audits or compliance requirements.

The typical log management product collects data from different system logs and then stores that data for a specified period of time to give you a historical account of events that have occurred. With this data you should be able to get reports on what's happening in your environment to help you spot suspicious activities, changes, or trends, as well as to respond to audits or compliance requirements. (See Figure 1.)

According to industry analysts, about 80 percent of the time the steps that hackers take leading up to a data breach are recorded in the target organization's logs prior to the breach. In other words, if an organization simply looks at its log data, it can often spot breach warning signs and stop breaches before they ever occur. This is why log management is a great place to start. It doesn't require complex configuration and provides a fast return on investment.

However, there are some things you need to watch for when choosing a log management product. Cost is always an issue. Some products are simply too expensive and too complex. Some use proprietary data storage solutions that are difficult and costly to deploy and manage. And since you might need to store certain information for short periods of time and other information for longer periods, make sure your log management product supports multiple data retention policies.

For example, PCI-DSS requires the storage of log data for your systems for 90 days online and two years offline. While it's critical to retain this data, you might not want to retain all your data for two years. This means you need a log management product with flexible policy management to handle different types of retention scenarios.

You should also be wary of products that claim to do everything at once. The reality is that it will take time to implement all the features in such products. And if you end up biting off more than you can chew, your project might not ever get off the ground. That's another reason why a phased approach is best. You can implement what you need to demonstrate success at each phase.

Another major evaluation point is that your log management product not only needs to be able to collect log data from all your different systems, but it needs to be able to parse, normalize and

consolidate those different data sets into cohesive reports that are easy to generate, interpret and use. Without this function, making sense of your log data from a collective enterprise perspective will be nearly impossible.

While log management is a great place to start for security management, you need to make sure you don't choose a dead-end product. Taking a phased approach to security management requires that you can build on top of your existing log management product. Beware of products that store data in proprietary formats, can't forward events, lack the ability to integrate or don't have a peer in the area of real-time event monitoring. Your log management choice needs to give you room to grow by providing a path to security information and event management. Novell Sentinel Log Manager (www.novell.com/products/sentinel-log-manager/) provides this path, as well as addresses the other critical evaluation points you need to consider when choosing a log management product.

While log management is a great place to start for security management, you need to make sure you don't choose a dead-end product. Taking a phased approach to security management requires that you can build on top of your existing log management product.

> Add Security Information and Event Management

Once you've deployed your log management product, how do you know when it's time to add the near real-time monitoring and management capabilities provided by a security information and event management (SIEM) product? In his white paper, *The Complete Guide to Log and Event Management* (www.novell.com/docrep/2010/03/Log_Event_Mgmt_WP_DrAntonChuvakin_March2010_Single_en.pdf), Dr. Anton Chuvakin, a recognized security expert in the field of log management and PCI DSS compliance, offers the following three criteria that can serve as a guide to when you're ready to graduate from log management to SIEM:

Response capability: You have the ability to respond to alerts soon after they are generated.

Monitoring capability: You already have or have started to build security monitoring capability through the creation of a security operation center or a team dedicated to ongoing periodic monitoring.

Tuning and customization ability: Your organization is willing to accept the responsibility to tune and customize your SIEM product once it's deployed. This is a necessity since so-called out-of-the-box SIEM deployment rarely succeed or manage to reach their full potential.

In talking about adding SIEM to your log management foundation, Dr. Chuvakin says, "Organizations that graduate too soon will waste time and effort, and won't realize any increased efficiency in their security operation. However, waiting too long also means that the organization will never develop the necessary capabilities to secure themselves."

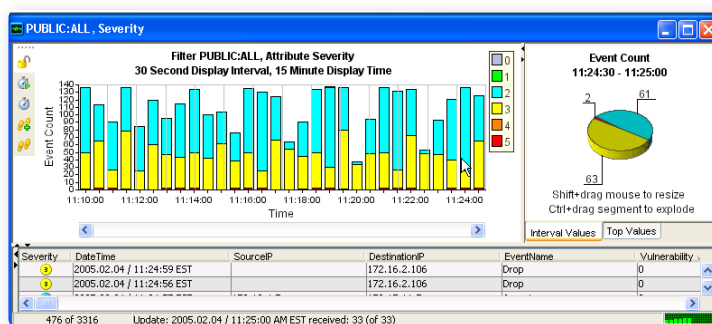
When you're ready to deploy a SIEM product, you want to choose a product that lets you build on and leverage your log management investment. This reinforces the need to also choose a log management product that can integrate or at least forward events to a SIEM product. This integration lets you naturally evolve your capabilities from reviewing periodic reports on log events to looking at those logged events in real time and even receiving immediate alerts on suspicious activity.

One of the features that you want to look for in your SIEM selection is true real-time correlation. Some products might claim to provide real-time correlation, when in reality they're just providing an event stream that shows events as they come in with some rudimentary alerting. True real-time correlation uses correlation rules to look for similarities between individual events that should raise warning flags.

For example, a user logging into one of your systems from an IP address in California probably won't draw your attention. However, if a few minutes later that same user logs in from an IP address originating in Europe you should have cause for concern. But it's unlikely you'll ever notice that event if your SIEM product only streams individual events across a dashboard without spotting the correlation between these seemingly innocuous events. Correlation rules in your SIEM product should be able to determine that such activity is not normal, and then automatically take appropriate action such as blocking the login attempt, notifying you of the activity, or putting that user or IP address on a watch list.

[Novell Sentinel](#) has a correlation engine that lets you create and customize rules that can identify such events and then take the appropriate action to mitigate the situation. This adds intelligence to your security event management by automating the analysis of incoming event streams to find patterns of interest, identify critical threats and complex attack patterns, prioritize events and initiate effective incident management and response.

Novell Sentinel also has a graphical control center interface that provides a real-time, holistic view of security and compliance activities across your IT environment. (See [Figure 2](#).) Novell Sentinel also leverages the same architectural foundation and technologies as Novell Sentinel Log Manager, including its communication bus, log connectors, data log collectors and event management system. Not only does this facilitate communication between all Sentinel Log Manager components and Novell Sentinel, but it provides you an efficient, streamlined solution that can scale to meet your needs.



Control center interface

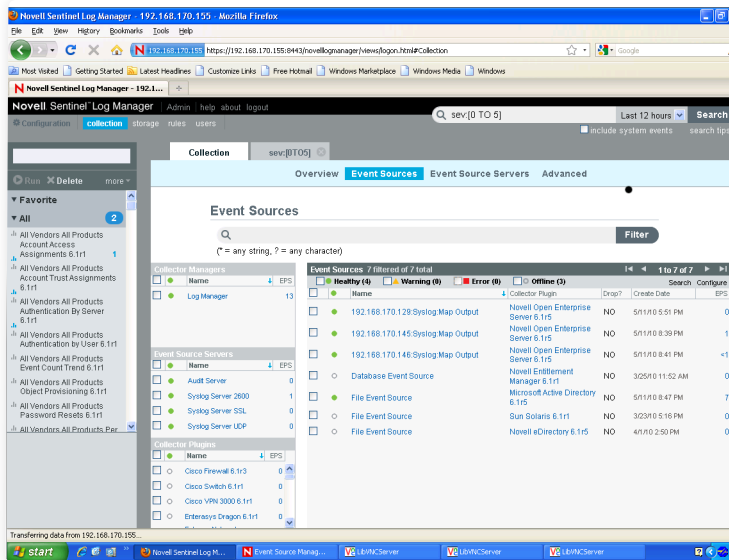
Figure 2: The graphical control center interface in Novell Sentinel provides a real-time, holistic view of security and compliance activities across your IT environment.

> Integrate Identity and Access Management

Once deployed, your goal should be to continually improve the depth and breadth of your SIEM capabilities. Part of this depth and breadth improvement can come from growing the number of systems in your environment that you proactively monitor and report. Novell Sentinel has data collectors for nearly a hundred different systems from vendors including Apache, Checkpoint, Cisco, HP, IBM, McAfee, Microsoft, Nortel, Novell, Oracle, Red Hat, SAP, Sun and more, as well as generic connectors that can be customized to work with nearly any other system. (See [Figure 3](#).)

While it's important to extend your security management reach through further integration of your SIEM with your various systems, one of the most powerful and important integration points for SIEM is with identity and access management systems. Integrating identity and access management into your SIEM environment lets you tie specific events back to specific users. This enables proactive user activity monitoring across multiple systems, as well as monitoring individual users with different user names and accounts. It also makes it significantly easier to differentiate between authorized, legitimate login attempts and unauthorized logins through a backdoor.

Achieving active user monitoring can be difficult and expensive if your SIEM product doesn't inherently support this level of identity and access management integration. However, Novell has already done the work for you by providing this integration in Novell Sentinel. If you already have Novell Identity Manager, it's as simple as flipping a switch to have it start feeding the necessary fine-grained identity information into the Novell Sentinel framework.



Log sources

Figure 3: Novell Sentinel and Novell Sentinel Log Manager let you log, monitor and respond to events in hundreds of different systems, including operating systems, applications, firewalls, routers and more.

> One Step at a Time

In truth, you might never need to reach the level of fine-grained security management provided by the integration of SIEM and identity access management. In fact, the whole concept might seem

a bit overwhelming. That's okay. If you follow this phased approach to security management, you can start small with the simple-to-deploy, easy-to-use and fast ROI log management provided in Sentinel Log Manager. And as your security management needs and capacity increase, you can easily grow your capabilities and reach with the real-time monitoring of Novell Sentinel, and then if desired you can move up to active user monitoring with Novell Identity Manager integration when you're ready.

While it's important to extend your security management reach through further integration of your SIEM with your various systems, one of the most powerful and important integration points for SIEM is with identity and access management systems.

By taking this phased approach, you can ensure your success every step along the way while making small incremental investments that improve your security and decrease your compliance costs and complexity. To find out more about Novell Security Management solutions visit www.novell.com/solutions/security-management. If you want to see firsthand how easy it is to use and deploy Novell Sentinel Log Manager as your first step toward security management, you can download a free 90-day evaluation version of it at download.novell.com/Download?buildid=woGGwp3Mab4~.

Learn More about Novell Security

- [Novell Sentinel Log Manager](#)
- [Novell Sentinel](#)
- [Guide to Log and Event Management](#)
- [Evaluation of Novell Sentinel Log Manager \(90-Day\)](#)

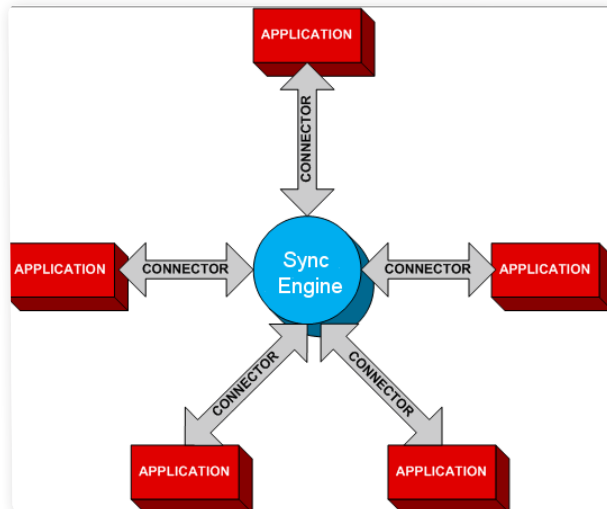
Higher Levels of Collaboration

Novell Data Synchronizer: Connecting Disparate Systems

by Ken Baker

With interoperability at the core of everything that Novell does, it's no wonder that a key architectural component of the Novell collaboration vision is a new technology that enables your disparate collaboration solutions, business-critical applications and mobile devices to seamlessly synchronize events and information. Available soon, Novell Data Synchronizer is a bi-directional, many-to-many synchronization engine that provides back-end synchronization of e-mail, calendar items, contacts and tasks to multiple systems.

Since Novell Data Synchronizer is a multi-source, multi-target synchronization engine, it's not tied to any specific collaboration solution. As a result, it will enable the synchronization of data and events between traditional collaboration systems as well as mission-critical enterprise applications such as CRM, ERP and other business solutions. Whenever a change occurs in one of these connected systems, the product will store the changes in real time to allow other connected systems to access them. (See [Figure 1](#).)



Synchronization hub and spoke model

Figure 1: Novell Data Synchronizer enables seamless back-end synchronization of data and events between traditional collaboration systems as well as mission-critical enterprise applications.

> Making Mobile Connections

Following a hub and spoke model—with the synchronization engine as the hub and connectors as the spokes—Novell Data Synchronizer will first provide connectors for mobile devices, Novell GroupWise, Microsoft SharePoint, SugarCRM and salesforce.com. In the future, a variety of other connectors—for Novell Teaming, Documentum, SAP, Exchange and more—will also be made available.

One of the most anticipated connectors for Novell Data Synchronizer is the Mobility connector. This connector will provide the mobile support foundation for Novell GroupWise and Novell Teaming. Through the Mobility connector, your users will enjoy even more functions, performance and device flexibility than they have with Novell GroupWise Mobile Server. In fact, all GroupWise Mobile Server customers will have access to the Novell Data Synchronizer Mobility Pack, which includes Novell Data Synchronizer, the Mobility connector, and the GroupWise connector. (See Move Up and Go Mobile.) Additionally, Novell will provide them with resources to simplify the move from GroupWise Mobile Server to the Novell Data Synchronizer Mobility Pack. (Novell will continue to support GroupWise Mobile Server until December 2010).

The Mobility connector will synchronize e-mail, contact and calendar data, and should be able to work with most mobile devices that use the iPhone (2.0, 2.0. 3.1 or later), Windows Mobile (6.0, 6.1 and 6.5), Palm, Symbian (Series 60 3rd Edition, 4th Edition, or 5th Edition), and Android (2.0) operating systems. To deliver stellar synchronization between BlackBerry devices and Novell GroupWise, we are continuing our long-time partnership with Research In Motion. (See BlackBerry Support.)

When you install the Novell Data Synchronizer Mobility Pack, the Mobility connector will automatically be installed. As you prepare for the installation, the Novell documentation provides a Mobility Pack Installation Summary Sheet to help you gather needed details such as LDAP server information, LDAP credentials, LDAP containers, GroupWise post office agents and mobile device ports.

Once you have the Novell Data Synchronizer engine and the Mobility Pack installed, you will need to set up an account on the users' mobile devices in order to allow them to synchronize using the Mobility connector. While the actual configuration will vary based on device type, the account will typically need to be configured with the user's GroupWise e-mail address, GroupWise mailbox password, e-mail account type, Novell Data Synchronizer server IP address or hostname, and a secure connection certificate. Once the mobile device connects to the Novell Data Synchronizer system (depending on GroupWise administration settings), the user's GroupWise personal address books, past e-mail messages (3 days or newer), past calendar items (14 days or newer), and all future e-mail and calendar items will be synchronized to the mobile device.

Since Novell Data Synchronizer is a multi-source, multi-target synchronization engine, it's not tied to any specific collaboration solution.

> More Connections

The GroupWise connector for Novell Data Synchronizer will be provided as part of Novell GroupWise and will leverage the SOAP interface to synchronize e-mail, tasks, calendar data and contact information across other collaboration systems. In order to get full functionality from the GroupWise connector, you'll need to be running Novell GroupWise 8.0.2, which will be available when

Novell Data Synchronizer ships. Additionally, SUSE Linux Enterprise Server 11 64-bit (using the Python database) is the only initially supported platform for the Novell Data Synchronizer engine. Additionally, Novell Data Synchronizer customers will automatically receive SUSE Linux Enterprise Server entitlements for as many servers as are required to run Data Synchronizer. In the future, Novell plans to expand platform support for Novell Data Synchronizer to include Windows, as well as other data bases.

In addition to the GroupWise connector, Novell will soon provide a Teaming connector as part of Novell Teaming. The initial Teaming connector will synchronize personal calendar and task information. Subsequent versions of the Teaming connector will also synchronize information related to teams, contacts and groups.

As mentioned before, Novell will also provide some non-Novell connectors. For example, its SharePoint connector will synchronize e-mail data, calendar items, tasks and contacts between SharePoint and other connected systems. The SugarCRM and salesforce.com connectors will synchronize the same collaboration data between these products and other connected systems.

It's important to note that connectors won't be limited to what Novell provides. By leveraging the Novell Data Synchronizer software development kit and its open API, organizations and Novell partners will be able to create custom connectors for their own systems as well as third-party solutions. The open nature of Novell Data Synchronizer creates limitless opportunities for you to create highly productive environments where your users can share relevant content from a wide array of collaboration and enterprise systems, such as CRM, ECM and document management systems; cloud-based social applications; and even solutions that compete with Novell collaboration offerings.

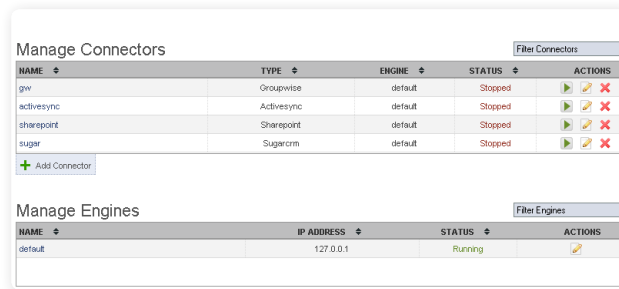
By leveraging the Novell Data Synchronizer software development kit and its open API, organizations and Novell partners will be able to create custom connectors for their own systems as well as third-party solutions.

> Configuring Connections

While a single synchronization engine will be able to host multiple connectors, Novell Data Synchronizer allows you to deploy multiple synchronization engines to give you the flexibility and scalability to manage the product's workload. After you install a synchronization engine, you can manage it and its connectors through the product's centralized Web interface by entering the server's IP address or domain name, and port 8080 (e.g. mydomainname.com:8080). While the management interface defaults to port 8080, you can change it as needed to avoid any conflicts that you might have with other products using that port.

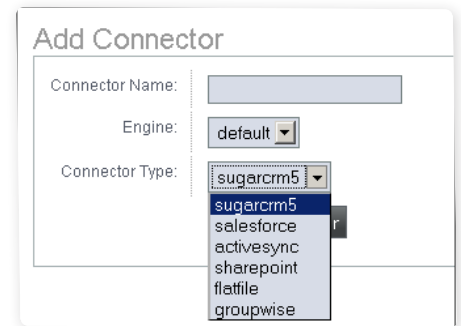
After you log into the Web interface using the admin user name and password that you established during the install, you'll be presented with the main management screen that gives you the option to manage your synchronization connectors or manage your synchronization engines. (See Figure 2.) To add a connector, simply click the Add Connector button and you'll be presented with three options: give your connector a name, assign it to a specific engine and choose the type of connector. (See Figure 3.)

Once you add a connector, you'll be prompted to configure its settings. While the settings dia-



Manage Connectors dialog

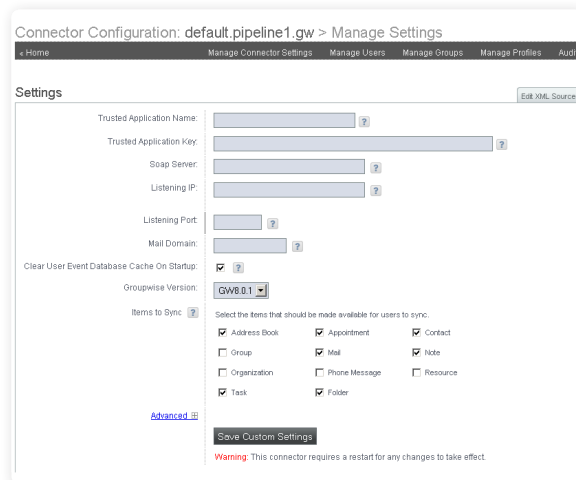
Figure 2: You can easily manage your synchronization engines and connectors through the centralized Web interface in Novell Data Synchronizer.



Add Connector dialog

Figure 3: Novell Data Synchronizer makes it easy to add different connectors to your synchronization engine.

log will vary for each connector type, the first settings you'll configure for the GroupWise connector will be its trusted application name and trusted application key. This trusted name and key are crucial for providing the necessary authentication credentials to access your GroupWise system. If you're running GroupWise 8 SP1 or later, you can easily create this trusted name and key in ConsoleOne. (See Figure 4.)



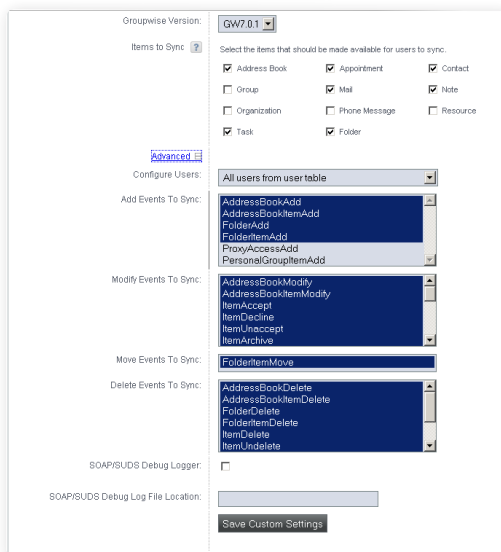
Manage Settings dialog

Figure 4: Each type of synchronization connector will have its own set of configurable settings.

The next setting you'll need to configure is the SOAP server, which is essentially the IP address of your GroupWise POA. You have to have SOAP enabled on your POA since the GroupWise connector relies on the GroupWise SOAP interface. You'll also need to enter the port number that you want the GroupWise connector to listen, meaning that you or your administrator will need to know what ports are available.

The settings page is also where you indicate the general type of GroupWise items you want the connector to synchronize. This can include address books, groups, organizations, tasks, appointments, mail, phone messages, folders, contacts, notes and resources.

If you click the Advanced button on the settings page, the interface presents you with additional configuration options. One of the advanced options allows you to indicate events that you want to synchronize—in addition to the default events. These additional non-default events would include items such as the addition of proxy accesses, folder modifications or personal group item additions. The Advanced button also allows you to delete or modify the events being synchronized. (See [Figure 5](#).)



Advanced settings

Figure 5: The GroupWise Connector Advanced settings lets you add, delete and modify the events you want synchronized.

> Customizing User Synchronization Needs

In addition to configuring a connector's settings, you can specify which users and groups will use that connector, and how they will be able to use it. Through the interface, you can perform an LDAP query to pull all or a subset of your users and groups from your GroupWise system. It also provides a convention called application name that allows you to specify an alternate name for users that might be referenced in other systems by a different user name than they use for GroupWise.

Additionally, Novell Data Synchronizer lets you create profiles for your users and groups that allow detailed customization on how and what will be synchronized for different sets of users. For example, even though most of your users might want to synchronize all the events you specified in the general connector settings, you might have a group of users that only need to synchronize a subset of those events. Additionally, you might not want bi-directional synchronization for all events. As an example, you can specify that if you add an appointment to your mobile device, you want it synchronized with GroupWise, but when you add an appointment to GroupWise, you don't want it synchronized with your device. (See [Figure 6.](#))

	Direction Of Syncable Items	
	Engine To Connector	Connector To Engine
AddressBookItem:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Appointment:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CalendarItem:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Contact:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DocumentRef:	<input type="checkbox"/>	<input type="checkbox"/>
Group:	<input type="checkbox"/>	<input type="checkbox"/>
Mail:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Note:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Organization:	<input type="checkbox"/>	<input type="checkbox"/>
PhoneMessage:	<input type="checkbox"/>	<input type="checkbox"/>
Resource:	<input type="checkbox"/>	<input type="checkbox"/>
Task:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Folder:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

User profile

Figure 6: You can create user profiles that give you granular customization over how your synchronization connector for GroupWise will synchronize events.

> Bringing Together People, Tools and Interactions

One of the fundamental beliefs at Novell is that the formula for success within any organization is rooted in the ability to bring people, tools and interactions together in simple and secure ways. By bringing these three elements together successfully, you can drive new innovation and new levels of productivity in your organization. That's the whole point of the Novell Data Synchronizer offering: to raise your collaboration efforts to even greater heights by connecting your disparate collaboration software, business-critical applications and mobile devices. Furthermore, Novell Data Synchronizer plays a key role in the overall Novell collaboration vision to bring together people, tools and interactions in a way that empowers you to collaborate as one and achieve the highest levels of innovation, productivity and success.

Learn More about Novell Data Synchronizer

- [Novell Data Synchronizer Mobility Pack Technology Preview](#)
- [Novell Data Synchronizer Overview Presentation](#)
- [Novell Collaboration Strategy Presentation](#)

Ending the Tug-of-War Between Agility and Compliance

Building a GRC Foundation that Connects IT Controls to Business Policies

by Todd Swensen

Businesses have always faced an underlying tension between agility and control. On the one hand, you need an infrastructure that can respond quickly to competitive threats and new business opportunities. On the other hand, expanding regulations make new processes and controls nearly unavoidable, which all too often leads to a slower, less responsive enterprise. So which option do you choose? Do you grudgingly accept a higher level of regulatory risk to make your organization more agile? Or do you err on the side of caution with more restrictive controls and processes that can slow your business down and take away your competitive edge? Finding the right balance between agility and compliance presents a difficult dilemma—especially when different factions and interests inside your organization are constantly tugging on opposite ends of the rope.

> Rethinking Compliance

Fortunately, a new approach is emerging—one that focuses on connecting compliance controls directly to your overall business objectives. At the highest level, this means turning your infrastructure into a strategic asset that can simultaneously keep you compliant and drive business results. And of course, it's a significant departure from the siloed, tactical approach many businesses depend on today, where teams are assembled to address specific compliance needs and the only goal is passing the next audit. This new, more proactive model requires the kind of infrastructure that can provide deeper visibility into business objectives—and then clearly show how all the controls and processes you put in place affect those objectives across the whole enterprise. In other words, moving beyond the agility/control tug-of-war means taking governance, risk and compliance (GRC) solutions to the next level—by finding a way to map everything that's happening in your enterprise directly to the business results you're working to achieve.

Info // Novell Connection Magazine

THREE INDUSTRY LEADERS. ONE SOLUTION

Novell, SAP and Greenlight each contribute key capabilities to a new kind of continuous compliance foundation:

- **Novell:** Provides integrated identity and access, as well as security event management and monitoring
 - **SAP:** Embeds risk analysis and compliance into the provisioning process
 - **Greenlight:** Adds a deeper level of risk analysis and compliance to specific applications
-

> Connecting the Dots

So what does this new strategic infrastructure look like? And exactly what will it take to get there? The good news is that most organizations already have at least some of the necessary pieces in place. For example, some enterprises have already integrated their identity management systems and access control tools to create a more automated compliance framework. Others have added automated, real-time security capabilities to their identity infrastructures, which allows them to automatically test the controls that protect the organization. And most organizations already have some kind of solution in place to manage and enforce business policies. Although every organization is at a different point along this path to GRC maturity, most are in a position to leverage their existing investments as they move toward a framework that connects compliance efforts to business results. It's simply a matter of extending those investments, adding additional pieces, and then enabling all the components to interact and work together in new ways. Of course, this is much easier said than done. Forming all of the necessary connections and interactions among various IT controls, business policies, systems and applications demands a great deal of careful thought and planning. It also requires vendors that understand the big picture and are working actively together to close the traditional gaps between IT controls and business policies.

Example // Novell Connection Magazine

A JOINT SOLUTION IN ACTION

Here's one quick real-world example of how the Novell Compliance Management Platform works with the SAP BusinessObjects GRC solution to unify business processes and IT controls:

1. Bill, a new sales contractor, logs on to the SAP portal for the first time to review recent customer purchases
2. When he clicks to review the reports, the SAP system informs him that he does not have access to the CRM database and provides a link to a "request access" form.
3. Bill completes and submits the form.
4. Behind the scenes, the Novell Compliance Management Platform sees Bill's access request and sends it to SAP Access Control. SAP checks to see if providing Bill with access to the CRM system represents a separation of duties (SoD) violation. Bill's boss sees the results of the SoD check (no violation) and approves his access request.
5. The Novell Compliance Management Platform received the approval and automatically grants Bill access to the CRM system.
6. Bill receives an automated e-mail, logs in, and successfully accesses the reports he needs.

> Novell, SAP and Greenlight: Forging New Connections

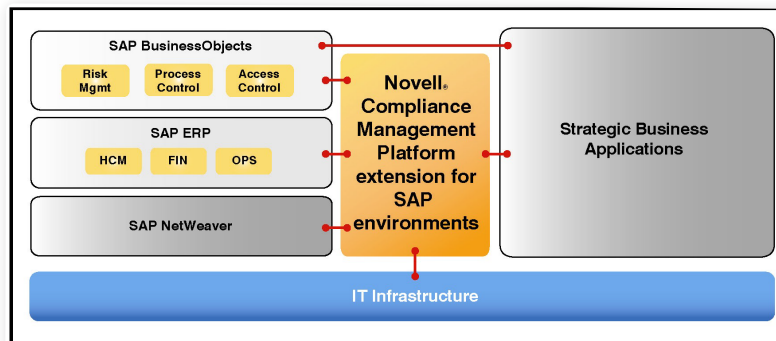
Novell, SAP and Greenlight are at the forefront of these efforts—with joint offerings that make it practical and affordable to create and extend these crucial connections across your enterprise. This starts with the Novell Compliance Management Platform, which integrates identity and access information with security information and event management technology to give you a real-time, enterprise-wide view of every network event. By creating a bridge between identity management (which defines who should have access to specific resources) and security event monitoring (which tracks who is actually accessing those resources), the Novell Compliance Management Platform provides important new integrated governance and risk management tools that deliver new levels of visibility and control. (See [Figure 1](#)).



Continuous compliance

Figure 1: Novell, SAP and Greenlight are ready to help you move toward continuous compliance and beyond.

Next, a Novell Compliance Management Platform extension for SAP environments connects all these integrated Novell identity, access and security management capabilities to the risk analysis features in SAP's GRC solutions. This creates a proactive infrastructure where IT controls and SAP access control tools work together to ensure authorized and appropriate access, avert threats and automatically shut down activities that could lead to policy violations. (See [Figure 2.](#))



Compliance management

Figure 2: The Novell Compliance Management Platform extension for SAP environments links crucial IT controls directly to SAP business policy and process management.

Finally, a partnership with Greenlight extends risk analysis and remediation within business applications. For example, Novell provisions users into specific applications and indicates when users have logged in, while Greenlight determines what users are allowed to do within the application based on SoD rules. This makes risk analysis and compliance an integral part of the end-user provisioning process enterprise wide, so you always know who is provisioned to what application and what they can do in that application.

> Building a Better GRC Foundation

This new infrastructure—where SAP business policies are integrated with Novell event management and monitoring and then extended across the whole enterprise—finally creates an environment where business objectives and compliance requirements can work in harmony. It makes a state of continuous, automated compliance a practical reality. And it finally puts a permanent end to that counterproductive tug-of-war between agility and control.

Online Resources // Novell Connection Magazine

Learn More about Novell and SAP

- Information about Novell and SAP on Novell's Web site www.novell.com/partners/sap
- Watch the product overview www.novell.com/products/compliancemanagementplatform/cmp_main.swf

Soda Pops

Vonpar

Following significant growth in its SAP ERP environment, Vonpar decided to implement a new hardware landscape and migrate from Microsoft Windows to SUSE Linux Enterprise Server, using Xen virtualization to simplify administration while reducing hardware and software licensing costs.

> Overview

Established in 1945, Vonpar is one of Brazil's largest Coca-Cola franchises. Operating in the states of Santa Catarina and Rio Grande do Sul, the company employs 2,500 people to manufacture and distribute approximately 67 million liters of product to more than 60,000 customers each month. The company enjoys a 56.4 percent market share in its region, and generates annual revenues of 1.2 billion Reais (US\$ 700 million).

> Challenge

To manage the manufacturing and distribution of Coca-Cola to thousands of businesses across southern Brazil, Vonpar relies on a suite of SAP ERP applications. When the company decided to introduce a number of new SAP modules, its computing requirements increased from 2,800 SAPs to 12,000. As a result, its existing Windows and Intel infrastructure was no longer able to deliver sufficient performance.

“We decided to go back to square one and redesign our IT architecture for SAP,” said Alexandre Leite, IT Infrastructure Manager at Vonpar. “We chose three new servers based on AMD Opteron 8000-series technology, each of which could hold up to eight six-core processors. We also began evaluating alternatives to Microsoft Windows, because we wanted to avoid having to install so many security updates and patches all the time.”

As a secondary objective, Vonpar was keen to reduce IT costs. The IT team saw virtualization as a good option, and decided to investigate the different technologies on the market.

> Solution

“For some time, we had been convinced that business-critical IT systems such as our core ERP databases ought to run in a Linux environment,” said Leite. “We had been using Linux in a number of smaller systems and were impressed with its resilience, security and performance—so we were ready to take the next step and move our main applications onto a Linux platform. [SUSE Linux Enterprise Server](#) was our preferred option, because of the enterprise-class support from Novell, and the fact that Xen virtualization is built in to the operating system.”

The Vonpar IT team migrated its SAP applications and data bases from Windows into eight virtualized SUSE Linux Enterprise Server environments on three of the new servers.

“The great advantage of using Xen virtualization is enhanced flexibility,” said Leite. “If we decide to add new hardware or move to a different type of server, we can easily migrate the virtual environments, without worrying too much about drivers and compatibility. In most cases, we can also expand our virtual servers without incurring additional software licensing costs, so we can grow more cost-effectively.”

Looking at Vonpar's entire infrastructure, the IT team now only needs to deal with 12 physical servers, instead of 18 separate machines.

“Even though we have expanded our SAP environment and introduced many new applications, we actually spend less time on hardware maintenance,” said Leite. “We only have one member of the team working on full-time infrastructure support, which means that the rest of our IT staff can focus on adding value in other areas.”

Vonpar is also using SUSE Linux Enterprise Server Priority Support for SAP applications, which gives the company a single source of support for both the operating system and the SAP applications themselves. In the event of a software-related problem, the company can quickly get access to the top experts at Novell and SAP via the SAP Solution Manager interface, and gain a swift resolution.

> Results

Migrating the SAP environment to [SUSE Linux Enterprise Server](#) has made a significant contribution to the performance, reliability and security of Vonpar's new IT infrastructure.

“SUSE Linux Enterprise Server is an excellent operating system in every respect,” said Leite. “Compared to our previous Windows solution, the performance is outstanding, and there is much less need to worry about whether the system is protected against viruses and malicious attacks.”

Looking at the total cost of ownership of the new solution, Vonpar's choice of Xen virtualization has proven its value.

“By allowing us to run numerous SAP application instances on each physical server, the Xen virtualization technology within SUSE Linux Enterprise Server has reduced our hardware costs by around 75 percent,” said Leite. “We also need fewer licenses, which has reduced software costs by 20 percent too. With fewer physical servers, our electricity bills are approximately 12.5 percent lower than before.”

With fewer servers to manage, Vonpar's IT team spends less time on hardware maintenance and administration.

“We haven't measured this precisely, but the perception in the department is that since migrating to SUSE Linux Enterprise Server, we are spending 10 or 20 percent less time on basic administration work,” said Leite. “The IT team is happy because they can now concentrate on more interesting and rewarding projects, and as a result, we estimate that productivity across the department has increased by around 30 percent.”

Learn More about the Offerings Featured in This Success Story

- [SUSE Linux Enterprise Server](#)

Sprawl Killer

Virtualizing Workloads with SUSE Linux Enterprise Server for System z Eliminates Server Sprawl

by Meike Chabowski

Virtualization in distributed computing environments is wildly popular—with good reason. It’s dramatically reducing the numbers of x86-based physical servers in IT environments everywhere. However, for many organizations with high-volume transaction and data-processing needs, there’s a smarter way to reduce physical server numbers and total cost of ownership while providing the highest levels of scalability, availability, energy efficiency and footprint reduction. The smarter way is virtualizing workloads using the z/VM hypervisor and [SUSE Linux Enterprise Server for System z](#).

> But Mainframes Are So 1960s!

Maybe, but so is virtualization. Virtual machine technologies were first developed by IBM for its System/360 mainframe in 1964.¹ What’s more, mainframes have never gone out of favor in many organizations. For banking, finance, health care, insurance, utilities, government, and a multitude of other public and private enterprises that need reliable and powerful data-processing capabilities, mainframes have been continuously on the job for decades. More than 95 percent of Fortune 500 companies use mainframes.

Today, in many organizations, mainframes are taking on more of the computing load than ever before, largely due to the benefits of SUSE Linux Enterprise Server for System z. Those benefits include cost reduction, access to hundreds of Linux applications and a global community of Linux experts, compatibility with other systems running Linux, and Novell support.

And there are other compelling benefits.

Server Sprawl Is Obliterated

Physical server numbers can be reduced by factors of 100-200:1. This compares to around a 10:1 reduction through virtualization in a homogeneous distributed computing environment.² When it comes to reducing space requirements, the mainframe wins hands down.

CPU Use Goes Way Up

On average, x86-64 platform CPU use rates of 10 to 15 percent are considered normal. With virtualization technologies, you can take those numbers up between 25 to 50 percent. But even in rare “high-use” cases, you are still stuck with the scale-out approach to workload

Today, in many organizations, mainframes are taking on more of the computing load than ever before, largely due to the benefits of SUSE Linux Enterprise Server for System z.

growth that drains power and hogs real estate. System z, on the other hand, normally operates at anywhere from 85 to 100 percent use and takes about as much floor space as a big refrigerator.

Licensing Costs Come Down

Consolidate software stacks and dramatically reduce CPU-based software licensing costs with the Integrated Facility for Linux (IFL), the specialty engine for Linux workloads on System z. An IBM System z10 Enterprise Class mainframe can reduce per-core licensing costs up to 30:1 compared to x86 environments⁴. This is because a single System z server can run multiple Linux applications on a single processor engine, and enterprise Linux software is usually priced on a per-engine basis.

Support Staff Requirements Level Off

Consolidating multiple servers onto a single System z mainframe running multiple virtual Linux servers can reduce the labor required for system management and maintenance. The centralized system management^[1] and autonomic computing features of SUSE Linux Enterprise Server for System z can also help cut down on the errors and workload-balancing tasks that can devour IT staff time.

Electric Bills Drop Like Rocks

Power and cooling cost reductions can exceed 80 percent. Distributed computing can't compete when it comes to cost per kilowatt. In fact, according to one analyst, the IBM System z platform can be configured to require 1/12th the electricity of a distributed server farm with equivalent processor capability.⁵

Data Center Footprints Shrink

Expect data center floor space reductions of up to 25:1. The System z10 Business Class (z10 BC) mainframe has the capacity of up to 232 x 86 servers with 83 percent smaller footprint.⁶ Basically, the difference comes down to one big box versus a full room of server racks (and all of the associated cables and switches).

Server Provisioning Accelerates

Provisioning an x86-based server can take weeks or months. Provisioning a server partition on a System z machine can be accomplished in just a few hours.

Security Becomes Less of an Issue

Securing virtual servers at the hypervisor level is an ongoing concern in any distributed computing environment. However, with the level of security inherent in the System z platform, it's not something that typically worries mainframers.

IT Environment Simplifies

Distributed server solutions can entail three to four times the number of servers that a mainframe production environment requires just to address workloads such as test/development/QA and D/R.⁷ All these workload requirements can reside within a single System z mainframe using existing virtualization techniques like z/VM and PR/SM LPAR, which are common to most System z configurations.

TCO Is a Pleasant Surprise

Combining the benefits of System z servers with those of SUSE Linux Enterprise Server for System z creates an entirely new TCO value proposition. This is due in part to Integrated Facility for Linux (IFL), which costs significantly less than typical central processors. Linux on mainframes gives organizations the opportunity to add more power to existing “Big Iron” infrastructure at a fraction of the cost of a non-Linux deployment. In a high-volume, high-transaction environment, TCO reductions range from 30 to 50 percent compared to distributed computing. Of course start-up costs for non-mainframe shops might seem high at first sight, but if planned right, substantial savings can kick in as the system grows in use.

> Here Comes the Cloud

Everyone has their own take on what the cloud is and what it can do for their organization. But regardless of what people hope to accomplish with cloud computing, the common denominators are agility and paying for what you need. On-demand compute power makes the cloud possible, and that’s been the foundation of [SUSE Linux Enterprise Server for System z](#) and the z/VM hypervisor from the start. The Linux/System z combination is a powerplant that is highly scalable, available and reliable by design. It’s a workhorse with costs that are fixed, manageable and predictable. What’s more, IBM mainframes have a mean time between failure (MTBF) that isn’t just measured in years, but decades.

So, SUSE Linux Enterprise Server for System z is a natural platform for delivering the next generation of utility computing services, whether in private or public cloud scenarios. The core requirements for these applications—massive resources coupled with intelligent workload management (IWM) features capable of supporting extremely dynamic workloads—map perfectly to the features of SUSE Linux Enterprise Server on System z.

It’s no wonder Linux on the mainframe is the foundation of IBM’s cloud strategy.

> Innovations in the SUSE Linux Enterprise Server Distribution

It has been ten years since Linux premiered on the mainframe. SUSE Linux Enterprise Server for System z has been available since the outset. Year after year, it has gained popularity—retaining 80 percent of the zLinux market. And Novell keeps adding functionality.

A critical tool for adding functionalities and innovation—a tool that is unique to Novell—is the Internal Build Service (formerly known as AutoBuild). It enables Novell to create a feature or capability once—or fix a problem once—and release it on all Linux platforms the company supports.

Key innovations include the SUSE Linux Enterprise Server for System z Starter System. It makes installing Linux on mainframes a lot more user-friendly by letting you transfer images to z/VM using FTP. Then, using z/VM commands and utilities, you can create a Linux guest that is a full-blown installation server that can be used to create other Linux guests under z/VM as necessary. The image can include a complete SUSE Linux Enterprise Server OS configured with FTP, HTTP, Samba and other servers. All you need to provide is an IP address and some disk space.

In addition, Novell is working with partner IBM to bring new workloads to the mainframe. Customers can now run .NET based applications on their mainframes thanks to the availability of SUSE Linux Enterprise Mono Extension for System z.

> Performance Basics

Nationwide Insurance IT management was looking for a way to dramatically reduce the total cost of ownership of their distributed server and Web hosting environment. They found it with SUSE

Linux Enterprise Server for System z—“it” being reduced complexity, shorter provisioning times, fewer staff requirements (no physical installation to perform), a smaller carbon footprint and much reduced floor space requirements.

The following performance basics are courtesy of Rick Barlow, Senior z/VM Systems Programmer, Nationwide Insurance. They are excerpted from his presentation at the SHARE IBM user group conference on March 17, 2010.

Basic Metrics to Watch: z/VM

- CPU use
 - System z runs fine at 100 percent, but Linux workload is much more demanding than traditional mainframe workloads.
- Significant impact of memory over-commit
- May need to keep peak periods at 85-90 percent
- Memory
 - Many Linux guests have huge working set sizes and many don't go idle
 - Keep memory over-commit less than 2:1: (ratio of combined working set sizes to real memory available)
- Paging
 - z/VM has no problem with high page rates: Keep expanded storage for high-speed page buffer
 - Guests may not be tolerant
 - Allocate enough VM page space for twice the total of the working set of expected guests; Use CP QUERY ALLOC PAGE to monitor and keep page space less than 50 per cent full

Basic Metrics to Watch: Linux Guests

- Don't wake guests to ask: Choose performance tools that understand that Linux is running on z/VM
- Pick one tool: Multiple monitoring tools adds a lot of overhead
- CPU measured inside guest is not very meaningful
- Avoid TOP—significant overhead: Use vmstat or nmon
- Memory
 - Don't over provision. Large virtual storage sizes drive up z/VM paging
 - Use a swap hierarchy—it is not a problem for Linux to do some swapping
 - Show all snapshot of memory/swap
 - Avoid multiple I/O caching in DB2
 - Default Linux memory management may not be optimal
- Paging
 - Prevent Linux from paging. z/VM paging is much more efficient.
 - Show Linux page-in/page-out
- Look at guest CPU demand from z/VM
- Watch for excessive paging on behalf of a guest this may indicate inefficient memory usage or excessive virtual storage allocation
- Watch for guests with poor I/O response: System z handles high I/O rates fine but bottle necks can occur
- Watch for percent of active time that guests spend in various queues

Basic Metrics to Watch: Linux Guests Internal Performance

- Tools to analyze guests functions vary greatly—pick the right one
- Application developers debugging skills may be limited: They might be accustomed to working with excessive capacity, but not accustomed to shared environment

Ideas that May Help

- Utilize Cryptographic hardware. This dramatically improves SSL calls for secure Web pages
- Minimize external network hops
- Reduce NTP frequency
- Minimize or stagger cron scheduling

> Linux on System z Is Extremely Attractive

Mainframes will continue to play a vital role in the enterprise for the foreseeable future. It's not an overstatement to say that System z is the ultimate virtualization resource—a massive data center consolidation platform capable of up to 60 logical partitions and the addition of hundreds of Linux virtual servers under the direction of z/VM technology. All in a single rack.

Moreover, SUSE Linux Enterprise Server for System z is a cost-effective open platform for development. In fact, mainframe growth is largely being driven by Linux developers using Linux with Apache, MySQL and PHP (the LAMP stack).

Through the years, IBM has consistently improved the price/performance ratio of System z mainframes, and IFLs are lowering licensing requirements and costs for SUSE Linux Enterprise Server in a big way. Many companies that conduct cost-per-transaction analyses find that [SUSE Linux Enterprise Server for System z](#) is unbeatable—in some cases as much as 50 percent lower than distributed environments. And, of course, Linux on mainframe environments are easier on the planet. In that context, upfront mainframe costs don't look so bad after all.

Online Resources // Novell Connection Magazine

Learn More about SUSE Linux Enterprise

- [SUSE Linux Enterprise Server](#)
- [SLES on System z](#)

Sources // Novell Connection Magazine

- 1 www.networkworld.com/news/2009/043009-ibm-virtualization.html
 - 2 www.vmware.com/solutions/consolidation/consolidate.html
 - 3 www-03.ibm.com/systems/z/os/linux/about/
 - 4 www-03.ibm.com/systems/z/advantages/energy/index.html and www-03.ibm.com/systems/z/os/linux/about/#foot6 <ftp://public.dhe.ibm.com/common/ssi/sa/wh/n/zsw03162usen/ZSW03162USEN.PDF>
 - 5 IBM System z: Platform Star for Linux and Open Source Software, Ptak, Noel & Associates, as cited at www-03.ibm.com/systems/z/advantages/energy/index.html
 - 6 www-03.ibm.com/systems/z/os/linux/about/#foot
 - 7 IBM System z, the Smarter Mainframe, IBM white paper (03/2010), <ftp://public.dhe.ibm.com/common/ssi/sa/wh/n/zsw03162usen/ZSW03162USEN.PDF>
-