Features

// New Spin on Workloads
Novell Open Enterprise Server 2 Workload Protection and Migration with PlateSpin

// Evolving Efficiency
Moving from Novell ZENworks 7 Desktop Management to Novell ZENworks 11 for Greater IT Efficiency

// The Real Challenge of Virtual Desktops
Create a real-time, end-to-end view of virtual desktop health, performance and cost drivers with Novell Operations Center

// Retail is Taking Off, But From What Launch Pad
SUSE Linux Enterprise Point of Service Provides the Foundation for Innovative Services

Departments

Proof Point
// You Don’t Need to Build Identity Management Policies from Nuts and Bolts

Trend Talk
// Vodacom and Novell Are Changing the Rules

Training Talk
// Putting Intelligent Workloads on the Path to Wisdom
Optimal workload execution and asset use requires the ability to easily move your different workloads as needed—whether from physical to physical, or physical to virtual environments. And to ensure continuous operation and the safety of your valuable data, you also need to provide the proper levels of protection for those workloads. To enhance your capabilities in these areas, PlateSpin Migrate, PlateSpin Protect and PlateSpin Forge from Novell will soon extend their migration and protection capabilities (currently supported on Windows, SUSE Linux, and RedHat Linux) to include workloads running Novell Open Enterprise Server 2.

Migrate Novell Open Enterprise Server Workloads
In the past, if you wanted to move a Novell Open Enterprise Server workload to a virtual environment, you would essentially have to rebuild that workload from scratch. The new platform support in PlateSpin Migrate eliminates that rebuild work, giving you an industry-proven tool for testing, migrating and rebalancing all your workloads on your different host environments.

As a workload portability solution, PlateSpin Migrate automates the movement of your Novell Open Enterprise Server workloads between physical servers, and virtual hosts. The major strength of PlateSpin Migrate is its ability to completely decouple a workload from its underlying server hardware. This enables seamless movement from physical to virtual hosts—as well as between physical hosts with different hardware, even to new, bare metal servers.

PlateSpin Migrate delivers hardware-independent migrations by automatically configuring a server’s workload on the fly with driver, kernel and other necessary changes that allow it to operate properly on its target environment. It leverages a driver database of over 55,000 hardware drivers and also gives you the ability to add your own custom drivers. This wide array of hardware and platform support, combined with the addition of Novell Open Enterprise Server 2 to its broad multi-OS support, ensures you can perform workload migrations from anywhere to anywhere, whether for physical to virtual server consolidations, virtual to virtual workload migrations, virtual to physical workload de-virtualizations, or physical to physical hardware migrations.

To migrate a Novell Open Enterprise Server workload, you must first discover the source and target of your migration from within the Novell PlateSpin Migrate console. This requires that you provide either a host name or IP address for your source and target hosts. Once discovered, you simply click Move Workload, and the migration wizard will guide you through the process of migrating your workloads. This process includes the following core steps:

As a workload portability solution, PlateSpin Migrate automates the movement of your Novell Open Enterprise Server workloads between physical servers, and virtual hosts.
New Spin on Workloads // Novell Connection Magazine

1. Select your source and target servers and click Start Wizard. (See Figure 1.)

![Source and target server selections](source_target_selections.png)

**Source and target server selections**

_Figure 1:_ PlateSpin Migrate enables seamless movement from physical to virtual hosts—as well as between physical hosts with different hardware, even to new, bare metal servers.

2. Provide administrator-level account credentials for both the source and target servers. If desired, you can click the Test button to make sure the credentials you supply work.

3. Mark the appropriate transfer method. For Novell Open Enterprise Server workload migrations, the method should be Take Control, which is a cold migration process.

4. If cloning a workload for a provisioning operation rather than simply migrating a workload, you can next select the Host Name option and change the host name of your workload to be cloned.

5. Next, you’ll be presented with the Networking configuration page, which lets you examine the workload’s existing network settings, such IP address and DNS.

6. For virtual targets, pre-configure the virtual machine on the VM Configuration page with the name of your target virtual machine as well as its CPU, storage and memory settings.

7. Select which drives will be part of your migration on the Volume page. You also have the option on this page to increase or decrease the drive size the workload will use on the target host after being migrated.
New Spin on Workloads // Novell Connection Magazine

8. If desired, on the Post Conversion page you can add a script to perform an action you want included as part of the migration process.

9. For more granular control of your migration job, click the Advanced button. From the Advanced Job Configuration dialog you can select the Schedule tab to configure a job in advance and then schedule it to run at a later time. (See Figure 2.) From the Notifications tab you can configure it to e-mail you regarding the status or progress of a migration. With notifications turned on, it will also alert you to migration failures or completions. From the Advanced dialog you can also configure settings for your license keys and temporary network settings that you might want to use during the transfer.

10. Click Start to initiate the migration.

![Migration scheduler](image)

Migration scheduler

*Figure 2:* You can migrate your workloads immediately or schedule them to run at a later time.

> Protect Novell Open Enterprise Server Workloads

With the upcoming update to PlateSpin Protect and PlateSpin Forge, you’ll also gain the ability to safeguard your Novell Open Enterprise Server workloads—along with your Windows, and Linux workloads—all from a single point of control. PlateSpin Protect and PlateSpin Forge both replicate your server workloads in to warm standby virtual machines, so you can easily recover their data, applications and operating systems in the event of an outage or some other disaster. In minutes, the replicated workloads can temporarily be powered on in a virtual environment, allowing the workloads to provide their normal services and operations until your production environment is restored.
PlateSpin Migrate delivers hardware-independent migrations by automatically configuring a server’s workload on the fly with driver, kernel and other necessary changes that allow it to operate properly on its target environment.

PlateSpin Protect and PlateSpin Forge leverage the same underlying code, allowing them to provide the same capabilities, use the same administration console and be managed in the same manner. Essentially, they are like two versions of the same product. However, PlateSpin Forge is packaged as an all-in-one hardware appliance that can protect up to 25 workloads with built-in storage, replication software, remote management capabilities and a hypervisor. It can be easily plugged into your data center and is ideal for mid-size enterprises and branch offices.

PlateSpin Protect has provided the added flexibility and scalability needed for larger and more complex enterprise networks. It includes the replication software and management interface, which you install in your own virtual infrastructure connected to your own storage system. And for maximum flexibility, you can purchase as many workload licenses as you need.

A potential use case for PlateSpin Forge might consist of you running a variety of Novell business services (i.e., Novell GroupWise and Novell iFolder) across eight different physical servers running on top of Novell Open Enterprise Server. PlateSpin Forge can create a disaster recovery duplicate of all eight servers, but by leveraging virtualization they can all reside on and be launched from a single PlateSpin Forge appliance. PlateSpin Protect can do the same thing, but it gives you the flexibility to customize that virtual infrastructure the way you see fit.

Not only do PlateSpin Protect and PlateSpin Forge create virtual machine copies of all your Novell Open Enterprise Server workloads, but they keep them constantly up to date. So, when disaster strikes, rather than having to go through the pain and stress of traditional backup and recovery processes, you simply identify the workload to be failed over and click Run Failover. Then, once you repair or replace your server hardware, you can easily migrate the workload back to the production server. And since PlateSpin Protect and PlateSpin Forge use the same workload migration technology as PlateSpin Migrate, you can restore a workload to completely new production hardware to complete the trip back to business as usual.

With the upcoming update to PlateSpin Protect and PlateSpin Forge, you’ll also gain the ability to safeguard your Novell Open Enterprise Server workloads.
Once you have either PlateSpin Protect or PlateSpin Forge installed and running, the first thing you’ll see is its dashboard, which gives you an overall view of the workloads that are being protected. (See Figure 3.) The left side of the dashboard gives you a graphical representation of your protected workloads, such as how many workloads are protected, whether any have failed and how many workloads are not protected. The right-hand side of the dashboard gives you a view of past, present and upcoming events.

The console also provides tabs for configuring protection and replication settings, tasks and reports. The Reports tab gives you reports on how well your workloads have been protected, workload replication history, current protection status and more.

To configure a workload to be protected, you simply do the following:

1. Click the Add Workload button on the dashboard.

2. Provide the host name or IP address of the workload to be protected. (See Figure 4.)

3. Enter the administrator-level credentials to allow the product to interact with the workload as needed.

4. Configure the workload replication method you want. You can choose between full replication and incremental replication, depending on how often the workload’s data changes and how much network bandwidth you want to use for replication.

5. Configure additional workload protection details, including SMTP and e-mail notification methods when a workload failure is detected.

PlateSpin Forge dashboard

Figure 3: The dashboard in PlateSpin Protect and PlateSpin Forge present you an overall view of the workloads being protected and their status.
Once a workload has been added to be protected, it will be displayed on the Workloads tab. This tab is the control center for PlateSpin Protect and PlateSpin Forge. It provides a full inventory of the workloads being protected, including their protection status, replication status, replication schedule, date and time of last replication, and more.

If a workload or server fails, you can choose to have it immediately fail over to its virtual replica or prepare it for a failover. If you immediately fail over, the virtual machine will boot up, load the workload replica based on the latest snapshot and start providing services to the applicable users. If you think the workload failure might be a false alarm caused by temporary interruption to network communications or some other event, you might want to prepare for a failover instead. This allows PlateSpin Protect or PlateSpin Forge to stage the failover by readying the virtual machine to take over for the failed workload. However, it doesn’t actually fail over until you give it the final failover command. If you determine that it is, indeed, a false alarm, you can easily cancel the failover.

As mentioned before, in the event that you do failover, PlateSpin Protect and PlateSpin Forge make it easy to restore your workload to a repaired server, a new bare metal server, or even into a new virtual server environment. However, before you ever encounter a workload failure, it’s best to test your disaster recovery setup. Both of these PlateSpin disaster recovery products give you the ability to test your configured failover functionality and the integrity of the recovery workload. If you click the Test Failover button, the products will boot the recovery workload in a restricted network environment and apply the Test Failover Settings that you configured in the workload’s protection details.

> Simplify Workload Migration and Protection
Extending the PlateSpin workload protection and migration capabilities to Novell Open Enterprise Server not only enhances your ability to manage your Novell Open Enterprise Server environment, but it simplifies the management of your entire workload infrastructure. With PlateSpin, now you have a unified workload management solution for protecting and migrating all your workloads regardless if they’re running on Windows, Linux, or Open Enterprise Server.
New Spin on Workloads // Novell Connection Magazine

Online Resources // Novell Connection Magazine
Learn More

- PlateSpin Migrate
- PlateSpin Protect
- PlateSpin Forge
- Novell Open Enterprise Server
Evolving Efficiency
Moving from Novell ZENworks 7 Desktop Management to Novell ZENworks 11 for Greater IT Efficiency

by Jason Blackett

Every product has a natural lifecycle, and for Novell ZENworks 7 Desktop Management, that lifecycle will soon enter the next phase of its six-year evolution. On June 30, 2011, ZENworks 7 Desktop Management will move from the general support phase of its support lifecycle to the extended support lifecycle phase. (See Extended Support.) The extended support phase is designed to provide an interim solution if you need more time to make the transition to Novell ZENworks Configuration Management 11. And if you’re current on maintenance for the ZENworks 7 Suite, you are entitled to upgrade to Novell ZENworks Configuration Management 11 for free.

> Reasons to Transition
Beyond the fact that general support for Novell ZENworks 7 Desktop Management is ending and that moving to Novell ZENworks Configuration Management 11 is free if you’re current on maintenance, there are a number of compelling reasons for making the move. Chief among these additional reasons is productivity: simply put, ZENworks Configuration Management 11 will increase the efficiency of your IT department and the productivity of your users. That’s because not only does this latest ZENworks version feature most of what you’ve come to love about ZENworks 7 Desktop Management, but it delivers a host of new capabilities designed to significantly reduce the effort it takes for you and your IT team to manage, maintain and deploy your IT resources.

The following are just a few of the new capabilities you’ll find in Novell ZENworks Configuration Management 11:

• **Bundle management**—The next generation of application management allows you much more control over how software is delivered to devices.

• **Single pane of glass for lifecycle management and endpoint security**—Provides a unified, browser-based interface that features system dashboards, hot lists and other tools and shortcuts that provide quick, easy access to important tasks and device information.

• **Web-based architecture**—Enables administrators to access the system from anywhere using a simple browser interface, without installing an additional management console.

• **Location awareness**—Uses location to let you easily determine the closest Windows and Linux servers, as well as facilitate the control of bandwidth throttling.

• **Power management**—Leverages Intel vPro technology to allow you to create policies that control power management settings and perform out-of-band power-management tasks.
Evolving Efficiency // Novell Connection Magazine

If you’re current on maintenance for the Novell ZENworks 7 Suite, you are entitled to upgrade to Novell ZENworks Configuration Management 11 for free.

- **Bundle and policy change management**—Helps ensure that changes are only deployed to your production network when you’re ready to publish them.

- **64-bit support**—Employs a 64-bit JVM that allows you to make the most of today’s 64-bit hardware and operating systems.

- **Web-based reporting server**—Delivers actionable information about your IT environment with an enhanced reporting service that lets you run a wide range of canned reports and build custom reports as needed.

- **Integrated Windows and Linux device management**—Unifies your desktop environments by letting you manage all your Windows and Linux endpoints through a single unified, Web-based console, including the ability to discover Linux and Windows devices, enforce configuration policies, roll out new software, and deploy Windows and Linux operating systems.

You can take advantage of even more new features and capabilities if you choose to upgrade to Novell Endpoint Lifecycle Management Suite, which includes ZENworks Configuration Management, ZENworks Asset Management, ZENworks Patch Management and ZENworks Application Virtualization. This gives customers a proven set of ZENworks products at a significant discount over their combined stand-alone price.

This unified approach allows you to transform your IT specialists into IT generalists without compromising quality or performance. It eliminates the need to have people specialize in a single area. With a common, intuitive tool and a single management agent (ZENworks Adaptive Agent) for configuration management, endpoint security, asset management, and patch management, your people can easily acquire the knowledge and expertise needed to be proficient in all these areas. (See Figure 1.) The end result is that you can remove service bottlenecks without increasing headcount, eliminate unintended expenses associated with risk, and more efficiently and cost effectively meet your SLAs.

> **How to Transition**

Although there are architectural differences between the product versions, the ZENworks 11 platform has been designed with ZENworks 7 customers in mind. In fact, ZENworks 11 includes a migration utility that simplifies and streamlines the process. For best results, you should install your ZENworks Configuration Management 11 servers in a separate environment, while moving your ZENworks 7 Desktop Management application objects and managed devices in stages.
This gives you more control over the process and helps you to better decide which systems to move and when. With full control of the process, you can upgrade your environment as slowly or as aggressively as needed.

At a high level, the following represents the main steps you’ll take to upgrade from ZENworks 7 Desktop Management to ZENworks Configuration Management 11:

- Perform pre-migration tasks
- Move your data
- Test and publish your data

**> Perform Pre-Migration Tasks**

Before you begin the actual move, there are few tasks you’ll need to complete. The first of these is to install and set up a [Novell ZENworks Configuration Management 11](https://www.novell.com/zencm) server. ZENworks 11 will need to be installed on a different server than your ZENworks 7 server. The installation process will initialize the ZENworks Configuration Management database and create a primary server with a basic zone structure. You’ll be able to verify the success of your installation by accessing the ZENworks Control Center.

---

**Info // Novell Connection Magazine**

**EXTENDED SUPPORT**

The extended support phase gives you an interim solution if you want to move to Novell ZENworks 11, but need additional time to make the transition. During the extended support phase, you’ll continue to pay maintenance on the most current version of the product while purchasing an Extended Support Service Request pack for installation and configuration technical support on a 12x5 basis. Extended support will be available for Novell ZENworks 7 until August 2012. During this phase, you’ll be able to continue to receive critical security updates from Novell. Non-security related software patches and fixes will be provided as Novell deems appropriate and strategic.
To allow you to migrate the associations in your existing eDirectory tree for your ZENworks 7 environment, you’ll need to configure a user source that points to that tree. This user source will allow the ZENworks Migration Utility to read the GUIDs in the existing tree and assign them to the ZENworks 7 bundles and policies that you plan to move to ZENworks 11.

To help you identify the objects and data that need to be moved, as well as ensure the upgrade process runs as smoothly as possible, you should run pre-migration reports to identify the following:

- **Group policies** and the objects they reference.

- **Application objects that might need to be converted** to individual actions or MSIs for the move, since these applications might need extra testing to ensure success.

- **Applications that use Remote Alternate Applications** and the applications they reference so you can properly configure them after the move. ZENworks 11 does not support the remote alternate application attribute since the ZENworks 11 Adaptive Agent runs the same inside or outside your firewall and doesn’t need to make this distinction.

- **Image objects that might need to be modified** after the move or that might not migrate properly, such as image objects with scripts that reference other files that also need to be moved.

- **Applications that have non-applicable assigned attributes**, such as fault tolerance and load balancing. Since the content system in ZENworks 11 provides this functionality automatically on a whole zone basis, these settings will not be moved since they are no longer needed.

- **Devices that won’t be migrated**, such as Windows 9x devices.

The above reports can be created by leveraging the eDirectory ODBC driver to run queries against eDirectory using reporting tools such as the ODBC query tool, OpenOffice Base, Crystal Reports or Microsoft Access. You can also use an eDirectory reporting tool such as BindView.

> **Simply put, Novell ZENworks Configuration Management 11 will increase the efficiency of your IT department and the productivity of your users.**

> **Move Your Data**

The Novell ZENworks Migration Utility will allow you to move most of the configuration data stored in your Novell ZENworks 7 eDirectory tree to the new Novell ZENworks Configuration Management zone. (See **Figure 2**.) The utility will guide you through the migration of the following data types:
Application objects of all application types
This includes thin client, Web, AOT/AXT, MSI and simple. Application objects are migrated as Windows bundle objects with the same name as the original application. In most cases, the utility simply copies the existing data to the new bundle. Objects with distribution information will be automatically converted to individual actions or MSIs. Files associated with applications are uploaded to the content repository on the primary server.

Image objects and their associated image files
This includes scripted image objects, simple image objects and server-based image multicast sessions. The utility migrates the image object content to an image bundle of the same name in the zone, and updates the paths to the images referenced by simple or server multicast session objects. After the migration, you’ll need to copy any image files referenced by image scripts to the repository images directory, update scripts to reflect the new location, create images for add-on applications in the console and update their references, and clean up any image files that are no longer needed.

Policies still supported by ZENworks Configuration Management 11
This includes Dynamic Local User (DLU), Group, Imaging Server, Imaging Workstation, iPrint, Remote Control, Roaming Profile, and SNMP Trap Target policies. For most policies, the migration utility can create a similar type of policy.
Evolving Efficiency // Novell Connection Magazine

Image server policy settings and workstation launcher configure settings (Management Zones)
These settings will be moved into the ZENworks 11 environment as management zone settings. The launcher configuration settings that can apply to a whole management zone will not be migrated since they can be more easily configured as a global management zone setting.

Workstation, folder and group objects
You need to make sure you move all folders and groups that have associations. You can skip the migration of workstations if you don’t have associations to workstations or workstation GUIDs that you need to preserve from Novell eDirectory. You can also skip this step if you want to set up your workstations as managed devices in a management zone by using the ZENworks Control Center to discover them and deploying the ZENworks Adaptive Agent to them. Currently, the utility only supports the migration of Windows 2000 Support Pack 4, Windows XP SP2, and Windows XP SP3 workstations.

Novell eDirectory object associations
Associations will be migrated as assignment objects in ZENworks 11, which establishes a one-to-one relationship between two objects, such as “App A is assigned to User 1.” So, to move an association to an assignment object, you have to include both the ZENworks object and its associated object. For user-associated policies or applications, you need to define a user source for the zone. For workstation-associated policies, applications and images, you need to move their associated folders, workstation groups and workstations.

Although there are architectural differences between the product versions, the Novell ZENworks 11 platform has been designed with Novell ZENworks 7 customers in mind.

> Test and Publish Your Data
Even though the migration tool simplifies the movement of your Novell ZENworks 7 data to your new Novell ZENworks 11 environment, you should still extensively test the migrated objects to confirm they work as expected. This is especially true for applications that the migration utility needs to convert from AOT format to MSI format. The sandbox feature in ZENworks 11 facilitates this testing. By default, the migration utility can move your bundles, policies and other data into a sandbox, such that they can only be seen by test workstations that you specify. This allows you to validate your move and make any needed changes in a non-production environment. Once you’re satisfied that your new ZENworks 11 environment is ready, you can begin to publish your data by deploying the ZENworks Adaptive Agent.
Evolving Efficiency // Novell Connection Magazine

When you push out the ZENworks Adaptive Agent to a device, the old ZENworks 7 Desktop Management agent will be removed, and the device will automatically begin to be managed by your new ZENworks Configuration Management 11 environment. You can push the agent out to only a few or all of your devices. If you want to further ensure the integrity of your move, you might want to move just a few devices at a time. The point is that you can make the move as slowly or as quickly as you like. The nice thing is that this parallel setup approach lets you execute the move without any downtime.

To learn more about how you can benefit by moving to ZENworks Configuration Management 11, visit www.novell.com/products/zenworks/configurationmanagement, or contact your Novell account manager or Novell partner.

Online Resources // Novell Connection Magazine
Learn More

- Novell ZENworks Configuration Management
The Real Challenge of Virtual Desktops

Create a real-time, end-to-end view of virtual desktop health, performance and cost drivers with Novell Operations Center.

by Bill Tobey and John Woodard

In concept, the virtual desktop is understandably attractive to the thrift-minded executive. Any sane manager faced with the high costs of provisioning, managing and maintaining a conventional fleet of thick-client desktops would be duty-bound to consider a practical, centralized alternative. Virtual desktop infrastructure (VDI) technologies have been aggressively promoted as exactly that alternative—more economical, manageable and defensible by nature—and pilot-scale results have been very promising.

Production deployments, though, have often failed to deliver the promised goods. Costs have been higher than expected. Storage requirements have grown uncontrollably. Performance has been underwhelming and the user experience uninspiring. Nevertheless, new deployments continue as organizations look past the challenges and reach for the short-term hardware savings. Needless to say, far better results can be achieved by baking in the management at the outset.

> The Challenge: Many Moving Parts, No Single Management View

The roots of VDI under performance lie in the complexity of most solution architectures. While there are several variations, a typical VDI environment includes a thin-client device on each user’s desktop, a desktop system image running on a virtual machine, associated storage in a central repository and all the connecting networks. Because data and execution resources are always remote, VDI performance is highly network dependent.

In short, a VDI is exactly the type of mission-critical business service that demands service-oriented management, beginning with an end-to-end view across all the infrastructure elements, components and systems that contribute to its delivery.

In addition to these core elements, a production-scale VDI requires support services from a variety of management tools, most of which will already be present in any enterprise environment. These include:

- A provisioning orchestration service to automate user provisioning in response to role and employment status events
- An identity management service to provide central user authentication and role-based access management
- A virtual systems management service to monitor VM health and performance
The Real Challenge of Virtual Desktops // Novell Connection Magazine

- Physical systems management services that provide the same health and performance monitoring functionality for the servers, storage and network resources that support the virtual environment
- A service desk system for reporting and troubleshooting service problems
- A user experience monitoring service to measure and track VDI performance from the end user’s perspective

All of these services are provided through separate, siloed management environments, each with its own data set, repository, administrative console and system view. Individually they provide little or no visibility into problems that may develop across and between the service layers, which is exactly where the problems that undermine VDI cost and performance typically arise.

> The Solution: Manage VDI as a Service with Novell Operations Center

In short, a VDI is exactly the type of mission-critical business service that demands service-oriented management, beginning with an end-to-end view across all the infrastructure elements, components and systems that contribute to its delivery. Creating those integrated views across multiple domains and management environments is precisely the purpose of Novell Operations Center, the business service management component of our WorkloadIQ solution stack.

As a Connection reader, you probably know that Novell Operations Center provides management, monitoring and measurement of key business services across physical, virtual and cloud environments. It monitors service performance and availability, maps the relationships between services and the underlying infrastructure, and provides automated real-time measurement. It integrates the outputs of existing management tools with business context, creating a business-centric view of the most complex IT environments.

By using Novell Operations Center to create a dedicated real-time management dashboard for your VDI, you can gain an integrated, correlated view of all significant events that affect its health and performance, prioritized by their business impacts, no matter where in your IT environment they occur. You’ll be able to identify and address emerging issues quickly and effectively, before they can inflate costs or degrade performance.

Create a model of your VDI service and its dependencies on the IT infrastructure, then build customized views of its health and performance that update automatically in real time.

> First Assess, Then Integrate

Before a service-oriented view of your VDI can tell you anything useful, a variety of management data feeds need to be available for integration. So your first order of business should be a high-level assessment of your environment and the issues you face. What management tools are already in place? Do you have everything in the service stack we discussed above? What data streams do those tools offer? What issues are you experiencing with the VDI? Are there gaps in the instrumentation you’ll need to understand them?
The Real Challenge of Virtual Desktops // Novell Connection Magazine

Once you’re satisfied the management stack is complete, use Novell Operations Center to integrate and correlate the data streams from your technology-specific tools. Create a model of your VDI service and its dependencies on the IT infrastructure, then build customized views of its health and performance that update automatically in real time. You’ll find a discussion of how to construct business views quickly and easily in the March 2010 issue of Connection here (http://www.novell.com/connectionmagazine/2010/03/building_a_business_view.html)

> Using an Integrated Service View to Manage VDI Performance
Here’s one example of how an end-to-end service view can help you manage the health and performance of your VDI.

In this illustration (See Figure 1.) we see a high-level summary of service health and performance information for two groups of VDI users, identified by role as Mechanics and Pilots, together with a summary of open service desk requests initiated by those user groups. It’s obvious at a glance that a major alarm condition is currently affecting the Pilot group, and that a major incident has been reported to the service desk.

An executive summary view of VDI health and performance data.

**Figure 1:** In this executive summary view of VDI health and performance data, a major alarm condition is seen to be affecting the end users who share the Pilot role.

In this illustration (See Figure 1.) we see a high-level summary of service health and performance information for two groups of VDI users, identified by role as Mechanics and Pilots, together with a summary of open service desk requests initiated by those user groups. It’s obvious at a glance that a major alarm condition is currently affecting the Pilot group, and that a major incident has been reported to the service desk.
A help desk view of VDI health and performance data.

**Figure 2**: This help desk view of VDI health and performance data shows key properties of the two user roles, and lists the configuration items associated with current alarm conditions.

Shifting to a Help Desk view of the same data streams (See Figure 2.) and selecting Roles at right brings up a list of user group properties, including the desktop VM template provisioned to each role. At lower right we also see a Root Cause display of the configuration items associated with the alarm conditions. These include the user AranP and the desktop VM PILOTS-V1-5.

Searching for the VDI user associated with an alarm.

**Figure 3**: This view of VDI health and performance data shows results of a CMDB search for the user associated with an alarm condition.
Searching the configuration management database (CMDB) for user AranP returns a table detailing the alarm conditions associated with him. (See Figure 3.) Clicking the link in his name brings up a list of the key properties and configuration details of his desktop VM, including the major alarm currently associated with it.

If we scroll down on this screen (See Figure 4.), we discover that the alarm associated with user AranP was triggered by the service desk request he called in at 1:45 p.m., reporting that his desktop connection had just seized. Immediately below we see that the alarm associated with his virtual desktop was triggered just six minutes earlier, when it failed an automated test of network latency.

So in just a few clicks these views that integrate virtual desktop service health information from multiple systems and management tools have alerted management to a potentially serious performance problem, and given service desk staff enough detailed information to expedite remediation.
> Using an Integrated Service View to Manage VDI Costs

Novell Operations Center can also help manage the costs that often escalate when VDI projects are scaled to production levels—software licenses, for instance. Opening the Executive Summary view of this VDI (See Figure 5.) we immediately see that there is a critical alarm condition affecting the Pilots user group.

An executive summary view of VDI alarms and service desk requests by user role.

Figure 5: This view of VDI summary view of VDI alarms shows a critical alarm associated with Pilots user role.
The Real Challenge of Virtual Desktops // Novell Connection Magazine

When we tab to the Help Desk view and select All Users at right (See Figure 6.), we can see in the Property Views display that all Pilot users seem to be affected. Meanwhile, the Root Cause display informs us that something [a configuration item] called Pilot Pro PilotHelper Course Track seems to be involved in each case.

A help desk view of VDI user properties and alarm condition root causes.

*Figure 6:* This view shows that all VDI users with the Pilot role are affected by the current critical alarm condition, and identifies a software configuration item associated with the alarm.

Since Pilot Pro is almost certainly a software package, we can tab to the Software Licensing Reports view via the navigation bar at the top of the screen. (See Figure 7.) Here we can see that despite the fact that only two paid Pilot Pro licenses are available, five copies of the application are currently in use. We now have all the information we need to either subscribe our way into compliance, or hold the line on costs and turn off the illegal users. The decision is ours.
The Real Challenge of Virtual Desktops // Novell Connection Magazine

A licensing report of VDI software products.

*Figure 7:* This licensing report on software components of a VDI shows that more copies of an application are in use than have been licensed.

> Get Real Control of Your Virtual Desktops

Virtual desktop infrastructure solutions promise real relief from the high costs, management headaches, security shortcomings and compliance challenges of conventional thick client desktop PCs, and it is now possible to hold them to their promises. No matter how large or complex your environment, Novell Operations Center can integrate and correlate the data streams from all your management tools and services, giving you real-time insight on the events that determine costs, health and performance. For more information visit [www.novell.com/products/operations-center](http://www.novell.com/products/operations-center).

Online Resources // Novell Connection Magazine

Learn More

- Novell Operations Center
- WorkloadIQ
Retail is recovering quickly from the dark days of the past few economic years. Holiday sales in the United States, for example, turned in numbers across all retail categories from apparel to electronics that rocketed past the predictions of even the preseason optimists. And that should be good news for retail IT departments. Well, relatively good news. Retail still has a number of hurdles to overcome.

Retail has traditionally lagged in technology, especially at the foundation level. And even though IT budgets are now beginning to increase, IT departments are saddled with outdated hodgepodge systems, licensing fees, maintenance and multiyear rollouts.

At the same time, retail customers are more technology savvy than ever, and they want to use their technology to shop. This presents a real dilemma for IT. How does it come from behind the curve, keep ahead of customers and do it on growing but still limited budgets?

One answer is to ensure retail systems from the data center to the point of service (POS) systems are built on a solid, secure, flexible and cost-efficient platform. Many retailers are turning to open source systems due to their security, dependability, scalability and lower costs. And because they aren’t locked into a hardware platform, they can scale on a moment’s notice.

> Enterprise-class Linux Operating System Tailored for Retail

SUSE Linux Enterprise Point of Service from Novell is the only enterprise-class Linux solution that is designed specifically for retail environments, including branch and POS devices.

SUSE Linux Enterprise Point of Service includes an operating system that runs on any x86-64 or x86 hardware. A typical architecture includes one central administrative server that communicates with branch servers. The branch servers are connected to POS terminals, which run retail applications or specialized cash registers and kiosks. (See Figure 1.)

> The Administration Sever Manages the Entire Infrastructure

The administration server hosts an LDAP database and creates the images that are sent to the branch offices and POS devices. The LDAP database stores the configuration of each POS client configuration.

The functions of the administration server include the following:

- Maintaining the master LDAP directory for each branch server system
- Providing the tools such as the YaST Image Creator, which is a graphical front end to the KIWI image building technology for building custom system images and holding the images for distribution
- Storing branch server configuration parameters
- Providing the infrastructure to distribute the system images and software updates
- Supporting the Network Time Protocol (NTP) for synchronizing the branch servers
- Consolidating the syslog output from the branch servers
You manage all administrative tasks for the branch and POS terminals at the administrative server, including building and distributing images. The branch servers may also automatically download images based on daemons you set up.

> **Branch Servers Boot POS Terminals**
The branch servers play several roles. They serve as the boot servers and provide the system management infrastructure for the POS terminals, and they may host store applications, databases and POS applications. The branch server functions include the following:

- Running domain name services (DNS) for the local network
- Running dynamic host configuration protocol (DHCP) services to control the boot process
- Providing a multicast boot infrastructure for POS terminals (PXE, tftp)
- Transferring system images from the administration server to the terminals

The branch server automatically pulls new system images from the administration server and downloads them to the POS terminals. You can also distribute images as delta files with only the changes between image versions.
Creating Images

To easily roll out SUSE Linux Enterprise Point of Service, you can build customized application images that graphical and non-graphical terminals automatically download from the branch servers when they boot.

Creating images is easy. To start, SUSE Linux Enterprise Point of Service ships with templates that are proven to work out of the box.

Each image file contains the Linux operating system, drivers, configuration settings and application files. Each terminal requires two images: a boot image that contains the kernel and a bootstrap image, and the system image.

You can build images using the KIWI command-line tool, but it’s much easier to use the YaST Image Creator, which is a front end for KIWI and ships with SUSE Linux Enterprise Point of Service. This YaST for building images is the same as YaST for building new systems.

When you start Image Creator, you’ll see the Configuration Overview dialog, which lists image configurations that have been saved in the /var/lib/SLEPOS/system directory. You can add, delete or edit configurations right in the dialog box. You can also build images from a newly added configuration or from the configuration opened in Edit.

To create a new image configuration from a template shipped with SUSE Linux Enterprise Point of Service, follow these steps:

1. In the YaST Control Center, click Miscellaneous followed by Image Creator.
2. In the Image Creator Configuration Overview dialog, press Add, which brings up the Image Preparation dialog. Enter the name of the new configuration in the Kiwi Configuration.
3. Select Base on Template and choose the template to use from the list. If you want to re-use previously created configurations, select Base on Existing Configuration and choose the directory with the configuration to use.
4. Select the Image Type you want to create. To create a bootable live CD with a system image, choose Live ISO Image. To create a bootable USB memory device with a system image, choose USB Stick Image. If you need to boot clients from the network using PXE/DHCP and then download a system image from the network, select Network Boot Image. The path in which the directory with the image will be created is set in the Output Directory. The default value is determined by the template, and you can leave it as it is.
5. Package repositories used for creating the image are listed in the Package Repository table. The templates include paths to the copies of the SUSE Linux Enterprise Server and SUSE Linux Enterprise Point of Service source media located in the default distribution directory, /var/lib/SLEPOS/dist/. These copies should be created using the POSCopyTool before creating images. (See Figure 2.)
6. To add a new repository, click Add, select the type of the repository and enter the required information. If the image-building server is on the same architecture as the terminals (i586), it is possible to use update repositories defined in the operating system. To add a system repository, configure the update repository according to the SUSE Linux Enterprise Server Administration Guide and use Add From System in Image Creator.

7. You can also add selected packages manually to the /var/lib/SLEPOS/system/image_name/repo/ directory.

8. Click Next to proceed with creating the image configuration. Image Creator now downloads the repository metadata, which may take some time. If the configured repositories are not valid, Image Creator will report that.

9. In the Image Configuration dialog, add root and other needed users. Otherwise, you can use the default values defined in the template.

10. Create the image by selecting Yes. If you choose No, the image configuration will be saved but no image will be built. A window showing logs opens. After successfully creating the image, click OK. The path to the directory containing the new image is shown. Click OK.

**The Package Repository**

*Figure 2:* You will use the packages in the repository to build images.
Retail Is Taking Off, But From What Launch Pad? // Novell Connection Magazine

> Managing POS Terminals Remotely and Securely
A daemon enables you to connect to POS terminals located in remote locations via the branch server to shut down terminals, reload configurations and restart applications. You manage remote POS terminals using easy command line options. You can also back up and restore all system information for each branch server and POS terminal from the administration server. All information is stored in an LDAP directory on the administration server.

Security comes via several barriers. First you should ensure that each server, administration and particularly each branch server, is physically secure. SUSE Linux Enterprise Point of Service then uses AppArmor to maintain profiles to restrict applications to accessing only files and directories they are authorized.

> A Dedicated Solution for a Recovering Industry
The retail industry’s unique use of POS devices connected through branch offices or stores requires unique technology solutions. This industry has traditionally lagged behind other industries in its investments in technology to provide solutions due to low margins and tight IT budgets. This has been compounded by the recent recession. But the retail industry is pulling back into the black and is boosting its IT budgets. SUSE Linux Enterprise Point of Service is a dedicated operating system solution for this industry and offers a secure, flexible and low-cost solution that lets retailers make use of their current hardware to manage their POS devices from a central location without vendor lock-in. It is an ideal foundation from which to launch a market recovery.

Online Resources // Novell Connection Magazine
Learn More

• SUSE Linux Enterprise Point of Service
You Don’t Need to Build Identity Management Policies from Nuts and Bolts
Using and Building Packaged Policies in Novell Identity Manager 4
by Michael Astle

Automobile manufacturers don’t build cars from nuts and bolts anymore. They haven’t for many years. They build them from components. The engines may come from Japan, transmissions from Mexico, bodies from Thailand and entertainment systems from Malaysia. Then the cars are assembled in Canada. So why do some IT departments still pay to have their identity management policies built from Java code?

With a host of policies making up an identity management system, and nearly every organization in the world requiring complex security protection, the chances are that the very policies your programmers or integrators are building from code right now have already been created a thousand times by someone else.

Novell decided to take advantage of these potential resources in its Novell Identity Manager product, first by introducing a graphical means of building policies when it introduced Designer, and now with a large library of packaged policies. In this article we’ll discuss these packaged policies and look at how you can use them and even build your own packaged policies.

> What Is a Policy?

Before we go further, we need to define what we mean by policy. This word can refer to myriad concepts, from company policies specifying how employees treat customers to government regulations. In Novell Identity Manager, the term policy refers specifically to the set of configurations that define how the application functions. Novell Identity Manager policies are primarily security related and enforce the other kind of policies, the business policies companies create to safeguard their systems and data. For example, the company likely has a business policy specifying that only authorized people can access certain financial information. The company uses identities and strong passwords to enforce this business policy. To manage the identities and passwords, the IT department or its integrator create a policy in Novell Identity Manager that checks to ensure passwords are 12 characters and include nonalphanumeric characters. This is a password policy in Novell Identity Manager.

> Taking Two Steps Beyond Programming

If you’re still programming policies line by line in Java or some other programming code, you’re spending a lot of time and resources unnecessarily. When you program policies using raw code, you have to build, debug, test, stage, beta test and deploy the policy. Over time that code needs to be updated to keep up with changing business needs, and with each change it has to be rebuilt, debugged, tested and so on. With enough changes, the code may become so fragile that you can no longer make changes without breaking the whole system.
Novell Identity Manager came on the scene with its graphical drag-and-drop Designer a few years ago to save companies from this resource-draining programming merry-go-round. Designer gave policy builders a visual programming environment, where personnel could point and click on the components they needed to build policies.

Novell Identity Manager 4 Advanced Edition now includes another major step beyond programming with content libraries. These libraries contain packaged policies that Novell has built based on the experience of Novell and its thousands of customers over several years of building policies across industries and countless business needs. What’s especially nice about these policies is that they are all tested to work together. And when business needs change, you can unplug the existing policy and either modify it or select another policy from the library.

You can customize the packaged policies using Designer, and if the policy you need isn’t in the library, you can build the policy, package it and place it in the library. Novell is constantly adding to the library via an update website and encourages customers to contribute policy packages they build. You can also set policies to automatically update.

> Novell Identity Manager Designer and Drivers

The Designer in Novell Identity Manager is an Eclipse-based tool with which you can design, simulate, deploy and document your Novell Identity Manager system. You or your consultant use a graphical interface to drag and drop components that create the control between Novell Identity Manager and the applications for which you are adding control. You use Designer to configure policies and manipulate how data flows between connected applications. (See Figure 1.)

![Novell Identity Manager Policy Designer](image)

**Figure 1:** Novell Identity Manager Designer is a graphical drag-and-drop interface that lets you easily build identity policies.
Drivers connect the applications that hold the identity information. They have two responsibilities. First, they report event changes in the application to Novell Identity Manager, and second, they execute data change commands that the Novell Identity Manager engine submits to the applications. Packaged policies contain the drivers needed to control the applications.

In addition to controlling identity information, the new package management function of Designer notifies you if conflicts exist between policies and dependencies between policies, along with the prerequisite policies that must be installed.

> Installing Policies from Libraries

Novell Identity Manager 4 ships with dozens of policy packages already in its library, and more are available on the Identity Manager 4 Advanced Edition website. Locating the policy you need is a simple process. In the left-hand menu of Designer is a package library or catalog with a list of package categories, such as Directory, E-mail, Provisioning and so on. Look up the policies you need by opening a category folder and selecting the policy. The policy titles are descriptive and should tell you what you’re looking for.

If the policy package is just what you’re looking for, you can drag it to the Modeler in the center of the Designer screen and proceed with the process of simulating and deploying the policies. If you want to customize a policy package, you can do that, too.

---

**Copy Package Dialog**

*Figure 2:* Copy an existing package and begin modifying it by giving it a name and version number.
Customizing Policy Packages
Creating a new package or customizing a package, starts by your right clicking on the Package Catalog in the Designer left-hand menu and selecting New Category. You’ll name the category and click OK. Then right click on the new category you just created to create a new group. It’s in this group that you will place the packages you are creating. You could also place them in one of the existing groups and categories if they belong there.

Now select an existing package that you want to use as your template. For example, you may go to the Active Directory category and select the Active Directory Base. In here you’ll find one or more packages, and you’ll notice the package icons may have a little lock icon on them. This is to indicate that if you make changes to this package, you will not be able to save the changes back to the package. This is a safeguard Novell has included to prevent customers from modifying the library packages, which would then no longer be available if you need to revert to them. But you can make a copy of the package and change that. To make modifications, right click on the desired package and select Copy Package. This opens a dialog box, where you set the name, version number and so on. If you created a new category and group for this package, you can specify those here to save the package in the right place. (See Figure 2.)

Select Properties for the package by right clicking on the package. You can set the IDM compatibility, minimum and maximum application versions for compatibility, supported drivers, and vendor information for the vendor who is creating the package. You can also set the configuration wizard definitions, constraints, dependencies, initial settings, languages, licensing, linkages, the read-me, targets and the vendor. (See Figure 3.)
The new package now exists in your new category and group. If you right click on it there, you can open its properties to generate prompt resources, including driver names, initial settings, upgrade settings, remote loader and so on. You can also open the Resources folder and right click on the drivers to set or modify their settings.

You’re now ready to build the package. Right click on the package icon, and select Build. In the Build dialog box, you specify where to save the file and check Release Package. Checking this box locks the package, so no one can make further modifications, which will be indicated by the little lock icon on the package icon. (See Figure 4.)

And your package is complete. This was a simplified walk-through to show the highlights of how you can build or modify packages in Novell Identity Manager 4 Advanced Edition. The packaged-policy approach is a major advance from the nuts-and-bolts days of policy creation and management. This time-saving approach should save you a lot headache and resources if you build your own policies, or if you depend on an integrator, it should save a large portion of your IT budget. The best part is that you should end up with a much more stable environment that is easier to maintain and update as business needs evolve. For more information visit www.novell.com/identitymanager.

Online Resources // Novell Connection Magazine

Learn More

- Novell Identity Manager
Vodacom and Novell Are Changing the Rules

by Eric Harper

We've all heard the adage, “you can have it fast, good or cheap–pick two.” Cloud computing may be the one thing that turns that adage on its head with promises of all three. And no one is making that case better than Vodacom Hosted Services in South Africa using Novell technology.

First of all, let’s define what we’re talking about when we use the term Cloud Computing, because it can mean different things to different people. We use expressions like Software as a Service (SaaS), Storage as a Service (StaaS), Hardware as a Service (Haas), etc. You can describe just about any IT characteristic this way. So maybe the best way to look at Cloud Computing is to take our mind out of the idea of buying things to run IT and into the concept of buying the ability to do things.

With this approach, businesses can focus on getting the services they need without the worry of vendor lockdown and typical technology constraints. And Cloud Computing isn’t an all-or-nothing scenario for most companies. Most organizations that implement some sort of Cloud use a hybrid approach where workloads are split between the data center, a private Cloud and a public Cloud.

That is the type of infrastructure that Vodacom (part of the Vodafone family) set out to create when they launched Vodacom Business Services in 2008. And since the organization is so new, they didn’t have to worry about the shackles of a legacy infrastructure, hacked and patched together over the years. Now they are the only service provider in Africa to provide such an extended set of services.

> Fast

Richard Vester, executive head of hosted services at Vodacom Business Services said, “Customers in corporate South Africa want to know how they can address the challenges of the future. Vodacom Business Services addresses this today through Cloud Manager.” In fact, for the NOW-ology seminar at the Vodacom World event in South Africa last September. Vester, assisted by Markus J. Krauss, VP of service providers for Novell EMEA, added virtual servers on a live system operating in the Vodacom data center.

They configured the servers with the required operating systems, databases, and applications. In addition, they set the access rights, security levels, and compliance rules—all of that in less than ten minutes. In the physical world, such a feat would take at least eight hours. Not to mention the time required to procure the hardware and get it shipped to your location.

Business customers in South Africa want to know how they can address the challenges of the future. Vodacom Hosted Services addresses this today through Cloud Manager.
> Good

Clearly, working in the cloud is fast, but how does it perform once it’s set up? According to Vester, “Most global service providers sell virtual machines. Very few sell flexible workloads. Cloud Manager translates technology into business sense. It is changing the way that you have the ability to onboard more resources in a completely automated way.”

Cloud Manager lets customers take advantage of a wide range of business services. Using Workload IQ solutions from Novell, Vodacom supports their business customers IT environments through workload migration, virtual and physical data replication and protection to achieve a scalable Cloud, managed and controlled with Novell Cloud Manager. It’s a highly efficient way to do business.

With state-of-the-art data centers in Johannesburg, Cape Town, and Durban, Vodacom customers have complete flexibility in workload deployment. Risk is mitigated, as customers can spread the risk across multiple locations to ensure an appropriate disaster recovery solution.

Cloud Manager also extends the service level agreements (SLAs), allowing customers to choose whatever levels—gold or platinum—they require.

Cloud Manager translates technology into business sense. It is changing the way that you have the ability to onboard more resources in a completely automated way.

> And Cheap

So Vodacom and Novell provide services that save you time. And they’re full of features you can’t find anywhere else. But do these benefits come at a cost that only the very rich can afford? On the contrary. With Cloud Computing, you can actually save money over the traditional in-house data center. The flexibility it provides is the key.

Many customers today require greater infrastructure resources at different times of the month or year. Typically, an in-house data center must be built to handle those peaks, even if the extra resources stand idle during the valleys. With the shared resources provided in the Cloud, customers can increase service capabilities only when they need it. And, just as important, reduce them again when they don’t.

Remember, customers are buying the service—the capabilities—not the underlying technology. With these solutions provided by Vodacom and Novell, even SMB customers can take advantage of economies of scale. Running a modern data center is increasingly costly, as you most surely know. It makes a lot more sense to leverage shared resources in an external cloud.
Cloud computing means significant cost reductions when it comes to high availability and redundancy.

“Cloud computing means significant cost reductions when it comes to high availability and redundancy,” Vester said. Novell’s Krauss agrees, “The partnership between Novell and Vodacom is helping business customers achieve a more secure, scalable and cost-effective computing environment.”

> Conclusion
So, the adage, “Fast, good or cheap—pick two” may still apply to auto repair and home construction, but it doesn’t need to be that way for your IT infrastructure. Vodacom and Novell have proven that point. In South Africa, these two companies have worked together to give businesses significant cost savings through highly-efficient and flexible Cloud Computing services. It’s time CIOs start thinking in terms of these services so they can take advantage of a different strategy for 21st century computing.

Online Resources // Novell Connection Magazine
Learn More

- Novell Cloud Computing
- Novell Cloud Manager
- WorkloadIQ
- Vodacom World
Putting Intelligent Workloads on the Path to Wisdom

by Richard Whitehead

Caine: I will prepare myself, Master.
Master Po: That is wise, Grasshopper. That is wise.

Long before Yoda imparted his wisdom on Luke, Master Po was teaching Caine some of life’s most important lessons. It seems we’ve all found ourselves under someone’s mentorship at one time or another. Someone who tried to teach us right from wrong. Someone who showed us a different way of thinking. Someone to show us the path to wisdom. Why should intelligent workloads be any different?

The next evolution in intelligent workload management (IWM) is going to be what I’m terming “wise workloads.” Now there’s no hard and fast definition for these sage bits of software. IWM itself is still evolving. Wise workloads are simply where I see IWM ultimately headed.

Like intelligent workload management, wise workloads will be identity-enabled, secure and compliant. They will also traverse all physical, virtual and cloud computing environments—while remaining unscathed. IT staff are able to monitor and track them wherever they may be running—but they don’t really need to. That’s because wise workloads will be capable of monitoring themselves and their environments. In fact, and this is the “wise” part of the equation, the workloads have moved beyond simple intelligence and are able to learn from their experiences.

The Evolution of Man—and Workloads
Consider this: As humans, we have an innate desire to learn, but it’s not until we put our knowledge into practice that we can truly become wise. For example, say you’re walking to the neighborhood grocery store late one night. You’re about to take your favorite shortcut when you hear gunshots down that particular alleyway. You decide it might be more prudent to take the slightly longer way around.

I submit that future workloads will be capable of something similar to this behavior. Based on their initial programming and what they learn from their experiences, they will be able to better predict outcomes to scenarios encountered in any given environment and make wise choices. Hence, they will be more capable of completing their functions, protecting their data and staying within compliance.

Novell Operations Center: Turning Knowledge into Wisdom
The ultimate solution for making workloads wise is Novell Operations Center. This customizable console plays a critical role in reducing costs and gaining control over complex physical, virtual and cloud infrastructures. Novell Operations Center simplifies and automates this process of monitoring and measuring business service levels (including the customer experience) of virtually all business service you define.
Putting Intelligent Workloads on the Path to Wisdom // Novell Connection Magazine

> Sentinel 7
While Novell Operations Center may be the majordomo of wise workloads, Novell Sentinel 7, its able-bodied counterpart, has its back. This newest version of Novell Sentinel offers improved data baseline and trending, enhanced corporate interaction, advanced reporting tools and numerous productivity-enhancing features.

> Improved Data Baseline and Trending
Essentially, there are two primary methods used to detect threats: The first involves knowing exactly what the threat is and what it looks like. The second requires a good understanding of your operating environment and the ability to identify when something out of the norm is occurring. To protect your organization against both known and emerging threats, you need to be able to establish rule sets that can detect threats in both ways.

However, this second detection method has been historically difficult to enable. Other vendors have tried and failed, as they haven’t been able to solve the problem of false positives. That’s because their systems haven’t included enough intelligence to be able to tune them such that you know the anomalies you are seeing are actual anomalies.

With Novell Sentinel 7, Novell has raised the bar on detecting emerging threats. Through real-time analytics, IT environments can proactively trend the data it sees against set baselines and alert IT staff when they detect an anomaly. Now organizations are able to protect against unknown threats before they occur.

For example, say IT staff have established a baseline for the typical number of unsuccessful login attempts encountered after hours. Novell Sentinel 7 notices an unusually high number of unsuccessful logins late one night—a pretty good indication of a hack attempt—and alerts a security analyst by text message, so they can look into it.

> Enhanced Corporate Interaction
Another area where Novell has made improvements to Novell Sentinel is in bridging communications between corporate security analysts and the administrators who actually configure the security policies. Through shared interfaces, security analysts and system administrators can work together to create correlation rules that target current and future anomalies that may threaten the organization.

> Advanced Reporting Tools
It’s no secret that a reporting war is raging among security vendors. Vendor A says they offer 500 out-of-the-box reports. So guess what. Vendor B’s next product release features 520 reports. How many of those generic reports do you think are actually usable by the average organization? Likely only a small fraction. Organizations want to be able to search through data and turn it into reports that are meaningful to them.

With Novell Sentinel 7, Novell has changed the game in the reporting wars. Our base reports focus on specific security analytics, based on a unified compliance framework. This puts the right information in the hands of the right people.
Putting Intelligent Workloads on the Path to Wisdom // Novell Connection Magazine

> **Productivity-Enhancing Features**
Perhaps the best aspect of Novell Sentinel 7 is that it’s designed to enhance productivity. After all, who has the resources to have humans monitoring their systems 24x7? Systems need to learn how to monitor themselves and make the appropriate decisions based on what they learn. Or, as Norman Cousins put it, “Wisdom consists of the anticipation of consequences.” In my book, therein lies wisdom.

> **Novell Sentinel 7’s Place in the Cloud**
When designing the newest release of Novell Sentinel, Novell surveyed its customer base as well as the market to understand the perceived security vulnerabilities and associated threats. The resulting Novell Sentinel 7 fits perfectly into the company’s WorkloadIQ paradigm, as it is at once intelligent, secure and cloud-ready.

While other security vendors continue to focus on the network, Novell has moved beyond the firewall to the cloud, where an increasing amount of application activity is taking place. Novell Sentinel 7 is fully capable of monitoring applications running in the cloud and correlating that activity with what’s happening inside the firewall—to give companies a truly complete picture of their security.

> **Putting Wisdom to Work**
One company that’s seen the wisdom of putting Novell Sentinel to work for it is Sony Italia. To meet new Italian government regulations for protecting personal data privacy, Sony Italia worked with Novell and H4T to implement Novell Sentinel Log Manager. In little more than a week, Novell Sentinel Log Manager was up and running, monitoring multiple servers and pulling all relevant data into a single database for easy reporting. Today, Sony Italia is able to comply with the new privacy legislation with minimal effort.

You can learn more about Sony Italia’s story at [www.novell.com/recording/videos/review/sony_italia.html](http://www.novell.com/recording/videos/review/sony_italia.html)

> **“When You Can Take the Pebble from My Hand…”**
While we talk about intelligent identity, smarter security and craftier compliance, the ultimate goal is wise workloads. Workloads that are able to care for themselves and stay out of harm’s way. It’s an achievable goal. And we’re already on the path. Who knows, someday soon, we may be able to say that the student has become the master.

—Richard

---

**Online Resources // Novell Connection Magazine**

**Learn More**

- [Novell Operations Center](#)
- [Novell Sentinel 7](#)