

# Connection

Novell Connection Magazine // SEPT\_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](mailto:editor@novell.com)

---

### Features

#### // **No More AD Chaos**

Novell File Management Suite Brings Even Greater Control to File Storage in Active Directory Environments

#### // **Visibly Simple**

Bringing Simplicity & Visibility to Access Certification

#### // **Effective Linux Resource Management**

Use Control Groups to Manage Complexity and Performance in SUSE Linux Enterprise Systems

---

### Departments

Proof Point

#### // **Hotel Camino Real**

Trend Talk

#### // **Protecting Your Data with Novell Compliance Management Platform**

Training Talk

#### // **ATT Live in Vegas**

**Novell.**

# No More AD Chaos

Novell File Management Suite Brings Even Greater Control to File Storage in Active Directory Environments

by Ken Baker

---

**Novell recently released an update to Novell File Management Suite, an offering that combines Novell expertise in file storage and identity technologies to deliver intelligent file management. With integration between Active Directory and the following three Novell products, the suite works together to provision, relocate, optimize and report on file storage based on user roles and customized business policies:**

- Novell Storage Manager
- Novell File Reporter
- Novell Dynamic File Services

## > Policy Power

The major update to Novell File Management Suite is that its Novell Storage Manager component now delivers feature parity between Active Directory and Novell eDirectory environments. The significant enhancements in this new version of Novell Storage Manager bring to Active Directory environments the same powerful file-level management capabilities that used to be available only in eDirectory environments. In short, there is no longer a requirement for any Novell infrastructure to enjoy the full benefits of Novell File Management Suite.

Novell Storage Manager ties together the directory, identity and file systems, enabling organizations to align user storage resources with corporate policy. The product accomplishes this by dynamically managing and provisioning storage based on user and group events that occur in either Novell eDirectory or Microsoft Active Directory.

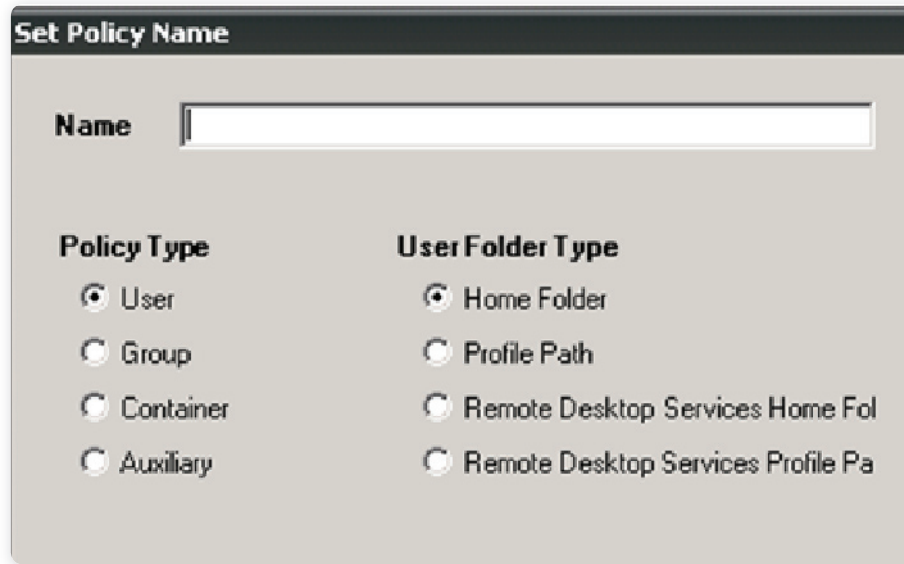
Prior to this update, Novell Storage Manager could only manage file storage in a user's home folder in Active Directory environments. Now it has the ability to manage almost every aspect of storage as it relates to Active Directory users and groups, including auxiliary or collaborative storage (discrete pieces of storage associated with a user or group).

Much of the power in Novell Storage Manager comes from its ability to apply a variety of changes to file-level storage based on policies that you define. For example, when users are created in Active Directory, a policy can dictate that home folders—as well as personal storage in collaborative or group folders—be created for those users with specific rights and permissions based on their roles in the organization. This can be especially helpful for Active Directory administrators who—by corporate policy—don't want users to have “full rights” in their folders that Active Directory assigns by default.

In the past, to correct Active Directory's over-assigning of rights, administrators would either have to manually scale the rights back or create scripts to change those rights assignments. Novell Storage Manager does away with this need for scripts or manual rights adjustment. You simply

create a policy that dictates what rights you want users to have, and Novell Storage Manager will assign those rights upon user creation. (See [Figure 1.](#)) The policy can also be used to change the rights and permissions of existing users and their storage.

---



*Figure 1: Novell Storage Manager lets you define policies to manage file-level storage in your AD environment, such as assigning specific rights to users' home folders.*

Additionally, if you have corporate user storage policies that your administrators are supposed to adhere to when they set up user accounts, Novell Storage Manager can automatically implement those policies to save your administrators time and ensure compliance.

But policy enforcement isn't limited to the assignment of rights and the creation of storage folders. In your Active Directory environment you can use Novell Storage Manager policies to govern what types of files users can store and how much storage they can have. For example, Novell Storage Manager provides what it refers to as file grooming and scrubbing capabilities. These new features—available to the Active Directory version for the first time—allow administrators to set policies that remove file types that the organization deems inappropriate for network storage. These file types might be MP3 or .AVI files, or files associated with specific MIME types like video or audio. When Novell Storage Manager finds any of these file types- based on policy - it can remove the files and either delete them or vault them to another storage device.

In terms of how much storage users can have, Novell Storage Manager now enables Active Directory environments to set quotas for users and groups. As part of this effort, you can use reports provided by Novell File Reporter (see File Storage Reporting on page 5) to get an overview of how storage space is being used by your users. Using the sizing information provided by these reports, you can create storage quota policies in Novell Storage Manager that provide appropriate storage capacity for different user types, as well as prevent unnecessary storage consumption by individual users.

As mentioned before, Novell Storage Manager allows you to use policies to set up collaborative storage for your users. With collaborative storage, you can set up folders to be used by groups of users, such as cross-functional teams. These folders might contain a general folder for common group documents, as well as personal folders where individual users can store their documents associated with the group's work.

To make it easy for you to set up this collaborative storage, Novell Storage Manager provides dynamic templates that represent optimal folder structures. (See Figure 2.) Based on how you structure your template, the policy will automatically set up the collaborative storage when a group is created or users are added to a group. You can also set up policies such that if a user becomes disassociated with a group, the user will no longer have access to the collaborative storage folders, including the user's personal folder. However, the remaining group members can still have access to that former member's personal folder to allow them to retain the knowledge and leverage the work.

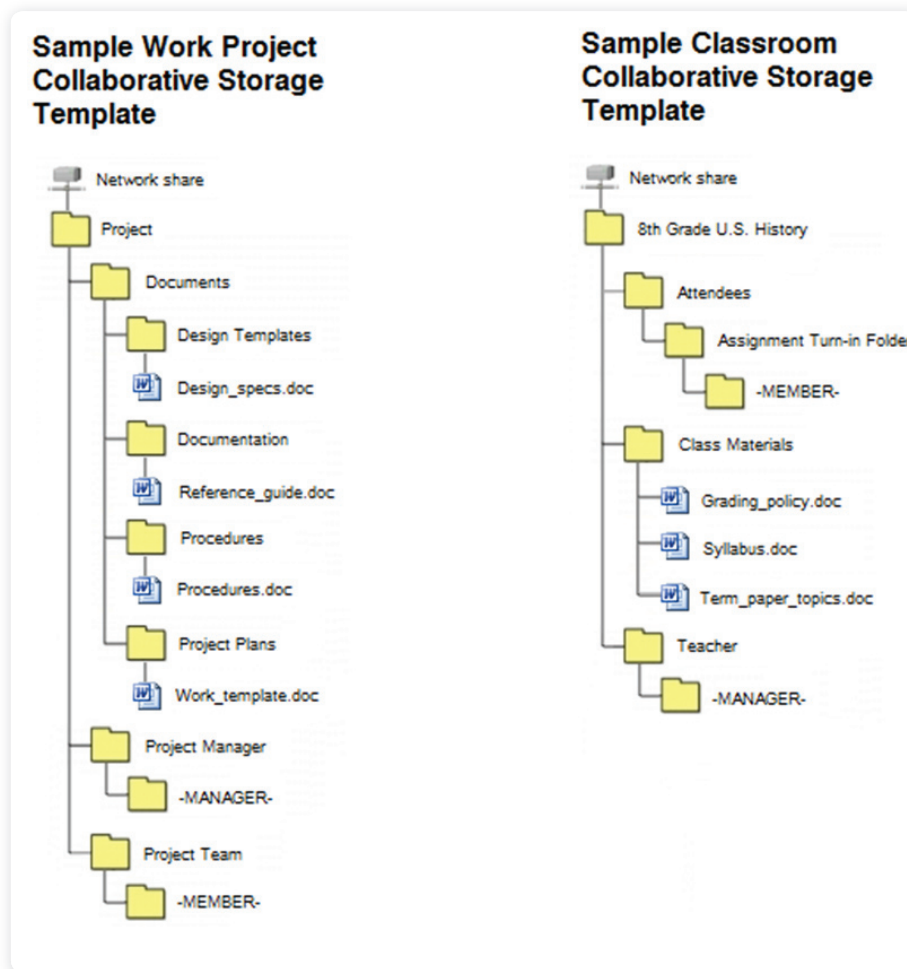


Figure 2: Novell Storage Manager provides dynamic templates to help you easily set up optimal folder structures for your collaborative storage.

Novell Storage Manager also allows you to set up policies to redistribute user and group storage among multiple servers. This can be helpful when you need to offload storage because a server is approaching its capacity limits. Novell Storage Manager delivers a wide variety of policy options that give you extensive power and flexibility in managing user and group storage in

---

**Info** // Novell Connection Magazine

## MORE GOOD NEWS

Another piece of good news in the newest version of Novell Storage Manager is that it no longer has any NetWare dependencies. Instead of having to run the Storage Manager engine on a NetWare server, you can now run the engine on Novell Open Enterprise Server running Linux.

Active Directory environments. In some areas, it delivers even more capabilities than it provides for eDirectory environments. For example, it provides support for policies for managing storage access through Remote Desktop Services and profile paths.

In addition to its policy enforcement, Novell Storage Manager provides a variety of anomaly reports to assist you in managing storage for your Active Directory users. Anomaly reports can help you spot orphaned folders, users without a home folder, folder assignments that don't match user object names, duplicate storage points and more.

Also new to this latest release of Novell Storage Manager is expanded support for Network Attached Storage (NAS) devices. In addition to supporting EMC Celerra devices, Novell Storage Manager can now manage NetApp NAS devices. This support enables an extensive array of new file-level storage management capabilities to be applied to these NAS devices, including support for clustered NAS devices.

### > **Expanded Options**

A major enhancement has also been added to the Novell Dynamic File Services component in the latest release of Novell File Management Suite. Novell Dynamic File Services dynamically allocates and optimizes storage resources on your Windows servers based on actual data usage. It transparently directs less valuable and infrequently accessed files to less expensive, secondary storage devices so you can reduce hardware, power and cooling costs while streamlining back-up processes. And it does all this in an automated, seamless manner with no impact on your end users.

Prior to this release, the secondary storage used by Novell Dynamic File Services needed to be on the same Windows server that hosted the primary storage, such as direct attached storage, iSCSI or a SAN. Now Novell Dynamic File Services supports remote network shares, allowing the secondary storage to be hosted on a different Windows server, as well as NAS devices and even cloud storage. This added support is possible because the product no longer requires any Novell Dynamic File Services software to be installed on the target secondary storage.

In terms of using cloud storage for your secondary target, Novell Dynamic File Services currently only supports Amazon's Elastic Compute Cloud (EC2) Web storage service. This limited support is more of a testing constraint than a technical constraint. Using the product's ability to target iSCSI devices for secondary targets, support for additional Web storage providers will be added over time.

A major benefit of this cloud storage support in Novell Dynamic File Services is that it addresses the fear that some organizations have about cloud storage: that once their data is in the cloud, it becomes trapped in the cloud. This new enhancement in Novell Dynamic File Services allows you to liberate your cloud data. If you want to pull some or all of your data off of cloud storage, you simply reverse your policy for secondary storage, and the product will automatically migrate that data back to your primary local storage. Also, as support for other Web storage providers is expanded, if you become unhappy with one cloud provider, you can set the policy to move the data from your original provider to a different provider. So, simply by having Novell Dynamic File Services enforce the policy you set, you can control how and where your static data is stored—whether it's in the cloud or on a NAS, a remote network share or a local network share.

---

**Info** // Novell Connection Magazine

## FILE STORAGE REPORTING

Novell File Reporter, one of the three components that make up Novell File Management Suite, also offers significant Active Directory integration. It lets you dig deep into your Microsoft Active Directory file systems, giving you file-level visibility of your storage usage resources. It exposes the "junk in the drawer" and gives you an accurate assessment of your unstructured data so you can make more informed decisions on where to store files, what files can be deleted, how to tier your storage, how to plan for storage growth and more. It answers vital questions to help you determine the best means of addressing your storage content.

In addition to the expanded support for locating secondary storage, Novell Dynamic File Services has new capabilities for managing your secondary storage. It has a new yearly policy option that makes it easier for you to reevaluate your policies on an annual basis. The new version also supports using wildcards, file patterns and file mime types to determine what files should be moved to secondary storage or retained on primary storage.

### > **Intelligent File Management for the AD World**

As you look at all the new policy and storage target enhancements in Novell File Management Suite, you'll realize that the new version is not just about bringing feature parity to Active Directory environments. Novell File Management Suite focuses on the unique needs of Active Directory environments to allow administrators to optimize existing storage investments and derive greater business value from their digital assets. To learn more about Novell File Management Suite, visit [www.novell.com/products/file-management-suite/](http://www.novell.com/products/file-management-suite/).

# Visibly Simple

## Bringing Simplicity & Visibility to Access Certification

by Ken Baker

Simply put, meeting business security and compliance mandates can be extremely difficult. This is especially true when it comes to certifying that the proper identity and access management controls are in place and followed. Much of this difficulty comes from the fact that many organizations rely on manual processes for certifying compliance of user access to IT resources. These manual processes lead to complexity, coverage gaps, human errors, excessive time and money spent, and ultimately untrustworthy certification data.

To achieve trusted, enterprise level access governance and eliminate the problems associated with manual certification efforts, you need to implement an access governance maturity model comprised of the following key stages (See Figure 1.):

- **Access Visibility** of who has access to what and how they received access.
- **Automated Certification and Controls** that facilitate the determination of who should have access, who approved access, and whether policy and control objectives are being met.
- **Role Management** that simplifies the definition and maintenance of roles, measures role effectiveness and uses roles in a way to reduce the compliance burden on the organization
- **Access Request** processes that provide an effective business level interface for access requests, implement preventative controls to ensure compliant request approvals, simplify access change management and speed up access delivery.

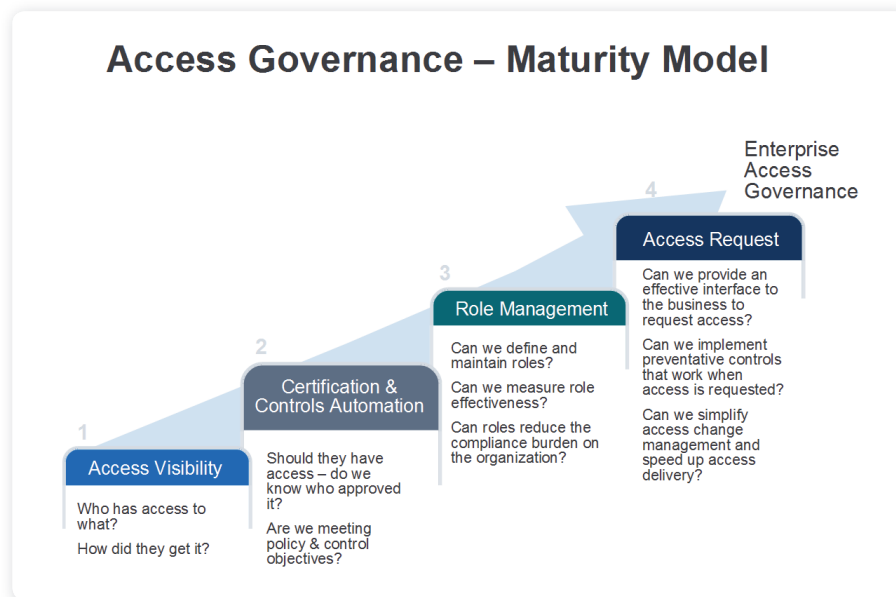


Figure 1: Novell Access Governance Suite can help you easily and cost effectively implement an enterprise level access governance maturity model that eliminates the problems associated with manual certification efforts.

> **Access Visibility**

Access certification is all about certifying that everybody who has access to certain IT resources should have access. But most organizations lack the visibility they need to easily, accurately and consistently document who has access to what. Often this is because the information regarding all their different users' access privileges is embedded within a multitude of different information resources, such as directories, application user data stores, and other enterprise systems. Extracting that information manually from all the different data stores and then trying to consolidate it into a meaningful, easy to understand report can be quite a challenge.

---

**Novell Compliance Certification Manager—  
one of the three products that make up the Novell  
Access Governance Suite —makes it easy to get  
a complete, enterprise-wide view of all your user  
access data, letting you know exactly who has  
access to what.**

---

For many organizations this manually collected information ends up in a spreadsheet containing long lists of user names with each user's entitlements identified by some cryptic codes or definitions that only make sense to IT administrators or the people responsible for collecting the information. Seldom can such reports be easily or accurately deciphered by the business line managers that have to verify that each user has the appropriate accesses. As a result, the managers will often simply say "Yes" to all the accesses, in essence rubberstamping the report before forwarding it on to whoever is in charge of the organization's compliance.

Novell Compliance Certification Manager—one of the three products that make up the Novell Access Governance Suite —makes it easy to get a complete, enterprise-wide view of all your user access data, letting you know exactly who has access to what. And then it provides that data in a business friendly context that enables business line managers to make intelligent evaluations and decisions regarding user access.

To simplify data collection, Novell Compliance Certification Manager provides out-of-the box collectors that on a regularly scheduled basis can automatically pull access entitlement, identity and role information from a variety of different target systems, such as Novell eDirectory, Active Directory, SAP, WebLogic and more. It can also pull access information from other data source types, including flat files, industry standard databases, LDAP directories, XML files and a variety of different applications. Once Compliance Certification Manager pulls the access information from your different data sources it aggregates, normalizes and correlates that information into a unified business context and view of your users' access entitlement information.

## Novell Compliance Certification Manager also makes it easier for you to determine who should have access to certain resources, as well as simplify approvals of access and make sure that compliance policies and access control goals are being satisfied.

---

### > Automated Certification and Controls

Novell Compliance Certification Manager also makes it easier for you to determine who should have access to certain resources, as well as simplify approvals of access and make sure that compliance policies and access control goals are being satisfied. It provides an automated process that ensures access is appropriate and compliant. It streamlines the review, certification and reporting process as well.

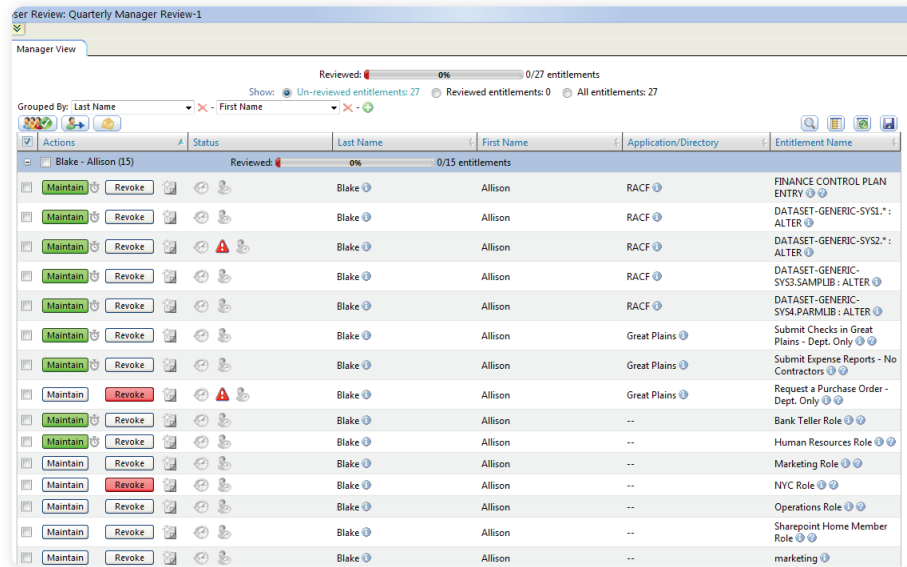
For example, the wizard based user-interface in Novell Compliance Certification Manager can guide you through the creation of review workflows, stepping you through the key information, criteria and actions that need to be part of different types of reviews that you might need to conduct. It helps you decide who should participate in a review, such as the entitlement owners or supervisors of any users included in a review.

Once you define a review, Novell Compliance Certification Manager can run the review on demand, on a scheduled date or based on a specific event. When a review runs, it sends all review participants an e-mail notification with a link to the review process interface. For example, supervisors might be presented with a list of their direct reports, showing a business friendly description of all their entitlements. It lets you use automated workflows that can immediately alert the proper people in your organization if potential violations have been committed.

One of the ways that Novell Compliance Certification Manager puts these access entitlements in a business friendly context is through the use of roles. For example, in an organization of a thousand users, you can group those users into different business friendly roles that you define. So, if you have one hundred roles, instead of having to look at and verify each of the individual one thousand user's different entitlements, your business managers only have to verify that those business roles have the appropriate access.

Additionally, as part of the review, Novell Compliance Certification Manager can let you see the last time certain users accessed a certain system. This can be helpful in ensuring you have least privileged accesses in place, giving your users only the access they need to do their jobs and no more. For example, if Joe hasn't accessed the vendor management system in the last six months, it will likely cause you to evaluate whether or not he needs access to that system.

If you determine he doesn't need access, from the review interface you can initiate an access change request to revoke that access. Based on the policy you've defined, that change request might be sent to the owners of the IT asset (i.e., vendor management system), a help desk system, or your automated provisioning system. (See [Figure 2.](#))



*Figure 2: Novell Compliance Certification Manager automates and streamlines your access review, certification, and reporting process to help you ensure your access entitlements are appropriate and compliant.*

Using standard and customizable business rules that enforce security and policy compliance, you can use Novell Compliance Certification Manager to conduct re-certifications based on events that could introduce compliance violations, such as when an employee changes roles or gains new entitlements.

Novell Compliance Certification Manager also includes an extensive set of built-in detailed, summary and customizable reports to further facilitate your compliance efforts. It also provides a set of dashboards with key risk indicators and metrics that can help your business and security managers easily evaluate certification and compliance status, as well provide insights on potential high-risk users and applications and access violations.

### > Role Management and Access Request

While Novell Compliance Certification Manager takes care of the first two stages of the access governance maturity model, the other two products that make up Novell Access Governance Suite address the model's remaining two stages. For addressing Role Management, there's Novell Roles Lifecycle Manager and for Access Request there's Novell Access Request and Change Manager.

As mentioned before, the use of roles can greatly simplify your certification and compliance efforts. But defining and making sure you have the appropriate roles can be a challenge. Novell Roles Lifecycle Manager simplifies this effort through role discovery, modeling, analytics and full role lifecycle maintenance. It gives you visibility to patterns and logical groupings in your organization to assist in role creation and management. It helps you make sure you've assigned the appropriate access rights to your roles. (See Figure 3.)

Role Name	Users	Entitlements	Role Quality	State	Role Set	Description
Accounting Role	3	0	0%	Committed	Novell Role Set	Dept-Accounting
Accounts Payable	1	0	0%	Committed	Novell Role Set	Dept-Accounts Payable
Accounts Payable Employee	0	0	0%	Committed	Novell Role Set	All users in the Accounts Payable dept
Accounts Receivable	0	0	0%	Committed	Novell Role Set	Dept-Accounts Receivable
Accounts Receivable Employee	0	0	0%	Committed	Novell Role Set	All users in the Accounts Receivable dept
Bank Teller Role	1	3	4%	Committed	Novell Role Set	Bank Teller Role
Banker Role	1	0	0%	Committed	Novell Role Set	Banker Role
Employee	0	0	0%	Committed	Novell Role Set	All Employees
Human Resources Role	3	0	0%	Committed	Novell Role Set	Dept-Human Resources
Information Services	4	0	0%	Committed	Novell Role Set	Dept-Information Services
London Role	11	1	8%	Committed	Novell Role Set	London
Management Role	5	0	0%	Committed	Novell Role Set	Dept-Management
Marketing Role	4	0	0%	Committed	Novell Role Set	Dept-Marketing
NYC Role	11	1	8%	Committed	Novell Role Set	NYC
Operations Role	33	0	0%	Committed	Novell Role Set	Dept-Operations
Sales Employee Role	1	0	0%	Committed	Novell Role Set	Sales Employees
Sales Manager Role	5	0	0%	Committed	Novell Role Set	Sales Managers
Sales Role	18	0	0%	Committed	Novell Role Set	Dept-Sales
Sharepoint Home Member Role	1	0	0%	Committed	Novell Role Set	SharePoint Home Member
Sharepoint Home Owner Role	0	0	0%	Committed	Novell Role Set	SharePoint Home Owner

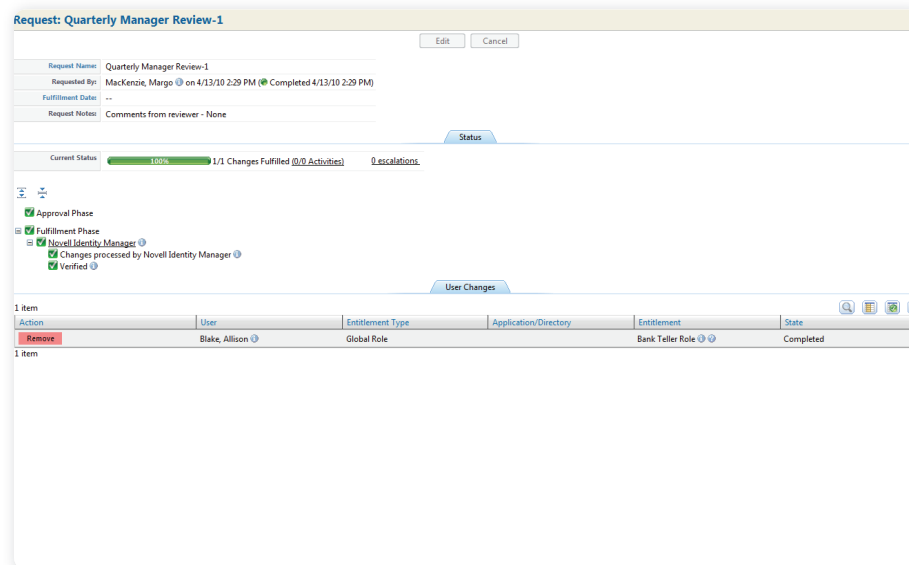
Figure 3: Novell Roles Lifecycle Manager provides role discovery, modeling, analytics and full role lifecycle maintenance to assist you in role creation and management.

Novell Roles Lifecycle Manager can also optimize your overall role structure so you have fewer roles to actually certify, simplifying your overall certification process. One of the main ways it can do this is by eliminating or consolidating redundant roles. Any redundant roles you have add unnecessary complexity to your certification process. If you have a hundred defined roles and twenty of them are redundant, you're not only having to deal with twenty extra roles, but you're dealing with all the systems and applications entitlements associated with those redundant roles. Using Novell Roles Lifecycle Manager to eliminate those redundancies can result in significant reduction in your overall certification efforts.

The discovery and reporting tools in Novell Roles Lifecycle Manager also enable you to find any orphaned entitlements you might have. An orphaned entitlement is basically an access or authorized action that's not tied to a specific role. Discovering these orphaned entitlements and then assigning them to a role further simplifies the execution and management of your compliance activities.

## Each component of the Novell Access Governance Suite provides the operational simplicity and business visibility you need to improve your overall compliance efforts.

Novell Access Request and Change Manager, a recent addition to Novell Access Governance Suite, provides a business friendly interface that allows users to request access to a particular resource or system. It also provides a business friendly interface for the business manager that receives the request and has to decide whether or not to approve it. (See [Figure 4.](#)) It also has built-in compliance controls and policy checks that can warn the business manager of any potential compliance concerns associated with the request. For example, if a user makes an access request that violates SOD rules, that access request will automatically be flagged with that warning.



*Figure 4: Novell Access Request and Change Manager provides business friendly interface that simplifies user access requests and access change management, while providing compliance controls and speeding up access delivery.*

When a manager does accept a request, the workflow in Novell Access Request and Change Manager can forward that approval to your IT group, a help desk or your automated provisioning system. The workflow and self-service nature of the product help you eliminate IT bottlenecks, and ultimately lower your IT administration costs and streamline access delivery in a way that lets you maintain compliance.

### > **Certification Simplified**

With the goal of simplifying how information resources are governed and certified, the Novell Access Governance Suite addresses all four stages of the access governance maturity model – Access Visibility, Automated Certification and Controls, Role Management, and Access Request. Each component of the Novell Access Governance Suite provides the operational simplicity and business visibility you need to improve your overall compliance efforts. The suite simplifies access requests. It enables you to better manage your entire user entitlement lifecycle. It makes it easier to certify the compliance of all your roles and entitlements. And it helps you ensure that all the users in your organization always have the right set of entitlements.

Visit [www.novell.com/products/accessgovernancesuite/](http://www.novell.com/products/accessgovernancesuite/) to learn more about how Novell Access Governance Suite can bring simplicity and better business visibility to your compliance efforts.

# Effective Linux Resource Management

Use control groups to manage complexity and performance in SUSE Linux Enterprise systems

By Matthias G. Eckermann and Bill Tobey

---

**When Linux servers under perform—particularly multi-purpose systems running multiple applications for multiple user groups—the root cause is frequently resource monopolization by one or more processes or users. Wouldn't it be wonderful if you could set and enforce some ground rules to govern how much CPU, memory, disk I/O or network I/O each process or user could command?**

Well you can! Control groups (cgroups) are a feature of the Linux kernel that provide mechanisms for partitioning sets of tasks into one or many hierarchical groups, and associating each group with a set of subsystem resource parameters that affect their execution performance. You might use control groups:

- To keep a Web server from using all the memory on a system that's also running a data base
- To keep a backup system from using too much network I/O bandwidth and crashing the business apps running on the same system
- To allocate system resources among user groups of different priority (the faculty, staff and students of a university, for instance)

There are two types of control group subsystems. Isolation and special controls subsystems include five different controls: CPUset, Namespace, Freezer, Device and Checkpoint and Restart. Resource subsystems are a group of four controls: CPU, Memory, Disk and Network. Before we investigate the functions of each subsystem, it's important to note that all are implemented in exactly the same manner, by mounting one or more subsystems as virtual file systems.

Subsystems can be mounted individually—in this case, the CPUset subsystem—as follows:

```
- mount -t cgroup -o cpuset none /cpuset
```

Or, all cgroup subsystems can be mounted at once:

```
- mount -t cgroup none /cgroup
```

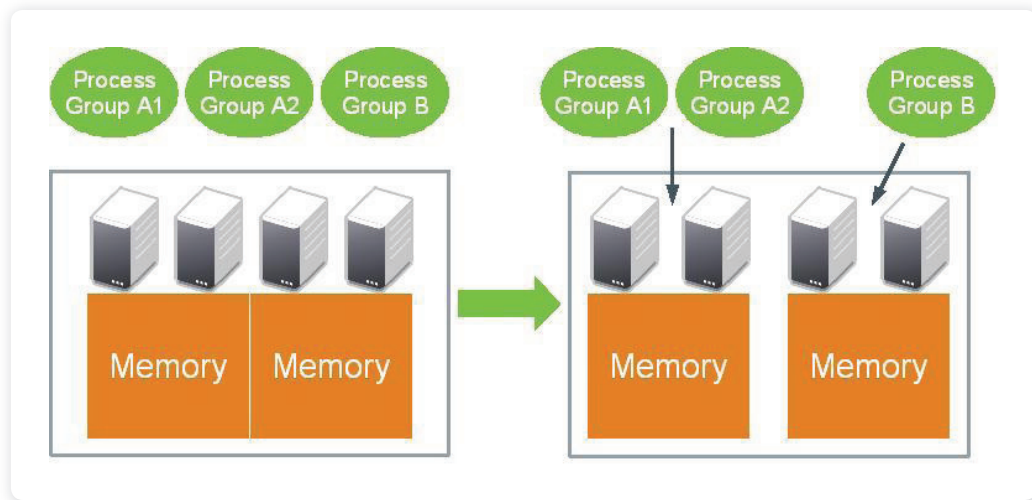
---

**When Linux servers under perform, the root cause is frequently resource monopolization by one or more processes or users.**

---

## > The Isolation and Special Control Subsystems

1. **The CPUset subsystem** ties processes to specific CPU and memory nodes (See [Figure 1](#)). In an SMP system, CPUset may restrict a process to a specific set of CPUs, or, in a system with multi-core processors, to a specific set of CPU cores.



*Figure 1: The CPUset subsystem ties groups of processes to assigned CPU and memory nodes.*

2. **The Namespace subsystem** provides a private view of the system to the processes in a cgroup, and is used primarily for OS-level virtualization. It has no special functions other than to track changes in namespace.
3. **The Freezer subsystem** stops all the processes in a cgroup from executing by removing them from the kernel task scheduler. Once you've mounted the Freezer subsystem you can stop any process completely by placing it in the cgroup, using the FROZEN command:  
`echo FROZEN > /freezer/freezer.state`

When you're ready, the frozen group of processes can be restarted using the THAW command:

```
echo THAWED > /freezer/freezer.state
```

The primary application for the Freezer subsystem is backing up write-intensive applications. First you freeze the application, then you freeze the file system. Create your snapshot or backup, then unfreeze the file system. Finally, unfreeze the process and resume normal operation.

4. **The Device subsystem** provides device white lists for groups of processes, allowing or denying read/write access to listed devices or file systems.
5. **The Checkpoint / Restart subsystem** supports process migration between machines by stopping all the processes in control group and saving their state information to a dump file for convenient relocation and restart.

### > The Resource Control Subsystems

1. **The CPU control subsystem** uses the kernel's CFS task scheduler to share CPU bandwidth among groups of processes. It's an effective but somewhat mechanically complicated way to allocate CPU capacity.
2. **The Memory control subsystem** limits memory usage in user-space processes, primarily by discarding least recently used pages (LRU) to reclaim memory when a group of processes exceeds a preset limit. This subsystem imposes no restrictions on memory use by the Linux kernel.
3. **The Disk I/O control subsystem** allows or denies disk access to groups of tasks. Several approaches to this function have been proposed and are under active consideration by the Linux kernel community. A provisional controller subsystem is included in SUSE Linux Enterprise Server 11 Service Pack 1 that allows specific parameters of the CFQ I/O scheduler to be managed on a per cgroup basis.
4. **The Network I/O control subsystem** allows or denies network access to groups of tasks. This control is also under continuing development and discussion by the kernel community. A provisional subsystem is included in SUSE Linux Enterprise Server 11 Service Pack 1.

---

**Info** // Novell Connection Magazine

#### CPUSET VS. CPU: WHAT'S THE DIFFERENCE?

A number of things make control groups unnecessarily confusing: naming conventions for one.

Both the CPUset and CPU subsystems constrain process access to CPU bandwidth, for instance, but they do so by entirely different mechanisms. CPUset binds a group of processes to a designated set of CPU and (in a NUMA machine) adjacent memory nodes. This not only limits resource consumption, but can also enhance efficiency. Consider the case of an I/O-intensive process, where binding a network card interrupt to one CPU might benefit both the target process and the system at large.

In contrast, the CPU subsystem sets an overall limit on the execution bandwidth a control group can use, through configuration settings on the kernel task scheduler. It offers no memory allocation functionality; that capability being separately provided by the Memory subsystem.

---

## > Cset: An Easy Approach to Control Groups

Managing control groups manually—mounting the virtual file systems, creating the cgroup hierarchy, starting new processes in the appropriate groups, moving existing processes into or between groups, tracking group membership, then closing down unneeded groups—can become confusing and complex. Fortunately for Novell customers who want a simpler point of entry, there is a Novell-developed tool, first introduced in SUSE Linux Enterprise, that greatly simplifies cgroup implementation and management.

The cpuset management utility is a Python application that provides an easy-to-use command line interface for the cpuset functionality in the Linux kernel. Called cset after installation (yes, it's admittedly a little confusing) the tool addresses only the CPU and memory partitioning functionality of the cpuset subsystem. But since these are the obvious starting points for resource management and performance optimization, the cset tool offers an ideal way to sample the power and potential of control groups.

## > Preparing to Use Cgroups

To prepare a system for performance optimization with control groups, begin with a patched SUSE Linux Enterprise 11 SP 1 install, then add the following packages:

- **Libcgroup1** – The library for controlling and monitoring cgroups
- **Libcpuset1** – A library that provides a convenient 'C' API to the CPUset subsystem
- **Kernel-source** – The source code for the Linux kernel
- **Cpuset** – The cpuset management utility
- **Stress** – A simple workload generator for testing the impact of our process grouping and resource allocation measures on application and system performance. Available through the opensuse build service at: <http://software.opensuse.org/search?q=stress&baseproject=SUSE%3ASLE-11%3ASP1&lang=eng>.
- **Lxc** – Linux containers (optional). We'll talk a little more about this important new development at the end of this article.

## > Simple Cgroups with Cpuset

The cpuset (cset) utility makes it quite easy to execute the basic tasks of control group setup and management.

**Step One:** Discover the available CPU and memory resources on your system. Use the set command as follows:

```
- cset set --list
```

to create a list of the available resources.

**Step Two:** Create the CPUSET hierarchy. In the simplest configuration there are at least three cpusets. The root cpuset which contains all CPU and memory nodes, the system cpuset which is assigned cpu and memory resources for lower-priority system tasks, and at least one user cpuset which receives sufficient resources to ensure adequate performance of higher-priority user tasks. Assuming we have a four-way NUMA machine, the command:

```
- cset set --cpu=2-4--mem=1 --set=Charlie
```

will create a user cpuset named Charlie, to which are assigned the complete capacity of CPUs 2, 3 and 4, and their respective memory nodes.

**Step Three:** Start a process in a user CPUSET. The command:

```
- cset proc --set Charlie --exec -- stress -c 1 &
```

will start a process in the user CPUSET we just created. In this case, the new process is our workload generator.

**Step Four:** Move an existing process to a CPUSET. The command:

```
- cset proc --move --pid PID --toset=Charlie
```

will move an existing process (PID) into the CPUSET Charlie.

**Step Five:** List the tasks in a CPUSET, by using the command:

```
- cset proc --list --set Charlie
```

**Step Six:** Removing a CPUSET. Use the command:

```
- cset set --destroy Charlie
```

to remove the user CPUSET Charlie.

There, in six simple steps, is the complete lifecycle of a cpuset control group.

## > Linux Containers: The Future of Kernel Resource Management

Even as work continues on the subsystems for disk and network resource management, the next generation of kernel resource management technology is fast approaching production readiness. Linux containers (lxc) builds on all the control group infrastructure that we've talked about in this article—CPU, Memory, Namespace, Freezer, Checkpoint/Restart and Network—to provide fast, lightweight, OS-level virtualization without the need for the instruction interpretation or emulation normally provided by a hypervisor. It's similar to Linux-VServer or OpenVZ.

Linux containers can be used to run an application, a service or a full (Linux) operating system, partially separated from the rest of the system, but with essentially native performance. In particular, disk I/O is undiminished and cpu and I/O scheduling are much more fair and tunable than with full virtualization. This makes it possible to contain disk I/O intensive applications such as databases, to manage their impact on other applications and processes.

Linux containers is provided as a technology preview in SUSE Linux Enterprise Server 11 Service Pack 1, and it is our intent to provide full production support in Service Pack 2. The lxc technology preview comes with rich online documentation (man lxc), including some implementation examples. Information on building and using Linux containers can be found on SourceForge (<http://lxc.sourceforge.net/>), and on opensuse.org (<http://en.opensuse.org/LXC>).

# Hotel Camino Real

---

**Seeking to improve the security and scalability of its e-mail system, the Hotel Camino Real migrated from Microsoft Exchange to Novell GroupWise. The solution has boosted productivity by easing the associated administrative workload and increasing opportunities for employee collaboration.**

## > Overview

The Hotel Camino Real is part of the Ángeles Group, which owns hospitals, a TV and radio station and 29 hotels. The hotel has 700 rooms and offers a range of amenities, including conference rooms, a travel agency and gym in an eight acre complex in Mexico City.

## > Challenge

Over the last two years, the Hotel Camino Real has experienced considerable growth. The hotel's IT staff encountered significant issues when it came to scaling up the existing e-mail solution – Microsoft Exchange Server – to meet these new demands.

**“As our business grew, we wanted to add new users and make changes to the e-mail system at short notice,” said Alsacia Sanchez, IT Director at the Hotel Camino Real. “We found that Microsoft Exchange made this process unnecessarily complex, and we hoped to find an alternative that would give us greater flexibility.”**

The Hotel's IT staff was spending a substantial proportion of time and resources dealing with a large administrative burden and numerous virus attacks.

**“Our system was very vulnerable to viruses,” said Sanchez. “This placed a strain on resources, and our staff was forced to neglect other duties to focus on tackling security breaches. We saw the opportunity to improve this situation by implementing a more robust solution which required less upkeep.”**

## > Solution

The Hotel Camino Real conducted a cost-benefit analysis to compare offerings from a number of software vendors. Novell GroupWise emerged as the clear winner in terms of cost and stability.

**“This was a highly significant upgrade for us, as the e-mail system is vital to our day-to-day operations,” said Sanchez. “As long-time users of Microsoft Exchange, we needed to be confident that the improvements in performance would be worth the disruption of moving to a new solution. It was the balance of stability and scalability that convinced us Novell GroupWise was exactly right for us.”**

The hotel had been steadily migrating to SUSE Linux Enterprise Server as its strategic operating system, and took the opportunity to run Novell GroupWise on this platform as well.

**“SUSE Linux Enterprise Server is our operating system of choice,” said Sanchez. “We wanted our e-mail system to be similarly virus-resistant, and so it made sense to select Novell GroupWise.”**

The hotel worked with Novell Consulting in Mexico to migrate its e-mail solution to Novell GroupWise. The joint team completed the migration of 1,500 users rapidly, with minimal downtime.

**“The transparency and speed of the migration process really impressed us,” said Sanchez. “The seamless transition to Novell GroupWise 7 has encouraged us to plan an upgrade to version 8 in the near future.”**

The Hotel Camino Real also takes advantage of the collaboration features in Novell GroupWise, using the calendar sharing functionality to increase employee productivity. This allows users to publish their calendars so that colleagues both within and outside the organization can search their schedules.

**“Novell GroupWise has introduced new tools for collaboration and teamwork,” said Sanchez. “Our employees find it much easier to arrange meetings using the shared calendar functionality.”**

### **> Results**

**“Novell GroupWise has proven its performance and reliability, more than satisfying our expectations,” said Sanchez. “It has provided a definite improvement over Microsoft Exchange, especially in terms of administration. Since the implementation, it has needed barely any upkeep, a massive advantage for our staff who are free to focus on more profitable work.”**

Moving from Microsoft Exchange to Novell GroupWise has enabled the Hotel Camino Real to realize its aim to expand capacity as the business grows, without purchasing additional servers or hiring more staff.

**“Adding new users is a straightforward process with Novell GroupWise – we no longer have the headaches we experienced when trying to expand with Microsoft Exchange,” said Sanchez. “We can make changes and customizations to support our users, without worrying about disrupting e-mail communications which are critical to our business.”**

Novell GroupWise Messenger means employees can move beyond interacting exclusively through e-mail chains.

**“Novell GroupWise Messenger helps users solve problems in real-time rather than relying on exchanging e-mails, which can be time-consuming and unhelpful,” said Sanchez. “Our users work more closely with one another – they have new, simpler ways to interact and have an e-mail solution they know they can rely on.”**

Following the successful migration to Novell GroupWise, the Hotel Camino Real is already looking to the future.

**“Introducing Novell GroupWise was an excellent decision for the Hotel Camino Real, as its contribution to the business cannot be underestimated in terms of performance, resilience, value and stability,” said Sanchez. “We look forward to upgrading to version 8 soon, confident that it will add further benefits to our business.”**

# Protecting Your Data with Novell Compliance Management Platform

Integration of IAM and SIEM Crucial to Regulation Compliance

by Eric Harper

---

Most organizations today are governed by one or more of the regulations directing the protection of personal information. These regulations, such as HIPAA or PCI DSS for example, were written to control the collection, storage, maintenance, distribution and disposal of private data. Most of these guidelines include somewhat vague mandates to “protect” or “restrict access to” customer, patient or member data. Consequently, many vendors have come forward to help organizations comply. And most modern identity and access management (IAM) products do a fine job of validating identity, provisioning resources and enforcing access roles.

However, IAM covers only part of the rules. Another important aspect of these regulations involves data access auditing. Auditors want you to track what happened, when it happened and who did it. Again, a large number of security information and event management (SIEM) vendors are able to satisfy the audit-log requirements of these various rules, laws and regulations. And again, most SIEM products do a good job aggregating security data from throughout the organization.

## > Without Novell: Two Silos, No Communication

The result is two distinct sets of data: one set controls who has access to the organization’s resources (through the IAM access policies) and another set shows who is accessing the organization’s data (via the SIEM system). Unfortunately, they’re usually not very good at talking to each other, causing all sorts of problems. Here’s one example:

---

**Lincoln National lacked a system that would have noticed whenever two different people logged in with the same username at the same time. If they had such a system, security personnel could have been notified, those users sharing credentials could have been identified and the policy violation could have been rectified. Because there was no integration between the IAM and SIEM systems, the policy violation went on for eight years.**

---

In January 2010, Lincoln National Corp., a financial services company based in Radnor, PA disclosed a security vulnerability that may have leaked the personal data of 1.2 million customers. An investigation revealed that some employees of Lincoln National and another one of its subsidiaries, Lincoln Financial Advisors, were using shared user names and passwords to access the portfolio information management system. Six shared user names and passwords, which were created as early as 2002, were found.

Obviously, sharing user names and passwords was a violation of Lincoln National's security policy. But they lacked a system that would have noticed whenever two different people logged in with the same username at the same time. If they had such a system, security personnel could have been notified, those users sharing credentials could have been identified, and the policy violation could have been rectified. Because there was no integration between the IAM and SIEM systems, the policy violation went on for eight years.

And here's the real scary part. The vulnerability was discovered in August of 2009 (five months before Lincoln National disclosed it), but not by Lincoln National! Someone sent an anonymous tip to the Financial Industry Regulatory Authority (FINRA) who notified Lincoln National. A forensic security company was hired to investigate, and they're the ones who found the violation. Unfortunately, it's fairly common for an outside party to discover security problems like this.

According to the "2010 Data Breach Investigations Report" from Verizon Business, while 86 percent of data breach victims had evidence of the breach in their audit logs, 61 percent of victims didn't uncover the breach themselves—they were notified by a third party! As the report states, "Verizon's past research consistently finds that breaches are not found by the victim organization but by an outside party." How'd you like to be the one who got that call?

Not only do organizations regularly fail to discover evidence of breaches in their own audit logs, but the length of time needed for a third party to discover the breach is inordinately long. The Verizon Data Breach report notes that fully 70 percent of breaches go undetected for months or more. In fact, "Over the last two years, the amount of time between the compromise of data and discovery of the breach has been one of the more talked about aspects of this report. It is not without reason; this is where the real damage is done in most breaches. That a breach occurred is bad enough but when attackers are allowed to capture and exfiltrate data for months without the victim's knowledge, bad gets much worse."

If only Lincoln National had a solution that integrated their IAM and SIEM systems in real time—a system that constantly correlated identity access and policy information, as the events happened, across the entire enterprise. With such a system in place, if anomalous activity occurs, the proper people could be immediately notified—not months after the damage has been done, and not by a third party. If Lincoln National had a system like the Novell Compliance Management Platform, they could have avoided the embarrassing public disclosure and regulatory admonishments. If Lincoln National had the Novell Compliance Management Platform, it could have uncovered the sharing of user names and passwords when that activity first occurred—eight years before the bank became aware of it.

**The Novell Compliance Management Platform can tell you which users have been provisioned for a particular application, which employees are actually using the application, when they use it and what they do within the application. Only the Novell Compliance Management Platform can monitor those activities, not just for audit purposes, but to intervene—with remedies—at the time the activity is occurring.**

---

The Novell Compliance Management Platform can tell you which users have been provisioned for a particular application, which employees are actually using the application, when they use it and what they do within the application. Only the Novell Compliance Management Platform can monitor those activities, not just for audit purposes, but to intervene—with remedies—at the time the activity is occurring.

You may have also heard about the case of France's second largest bank, Société Générale. In 2008, they reported that “rogue” trader Jerome Kerviel had misappropriated over US\$7 billion—the single largest fraudulent act ever in the securities industry. Apparently, Kerviel built-up entitlements as he moved from one position to another, and from one department to another. Société Générale had policies in place prohibiting this accretion of entitlements. These policies specifically forbid someone with one authorization (such as invoice approval) from having other authorizations deemed to conflict (such as check signing). But Kerviel didn't simply acquire authorizations for his own account, he also tapped into accounts shared among traders (and others) in violation of the bank's policies.

### **> Industry-leading Technologies**

Novell has been in the identity and security business for over a decade. In that time, they've built a host of technologies—such as Novell Identity Manager, Novell Access Manager and Novell Sentinel—that are considered industry-leading technologies. Novell is positioned in the Leader's Quadrant of Gartner Inc.'s Magic Quadrant for User Provisioning, Magic Quadrant for Web Access Management and, most recently, its Magic Quadrant for Security Information and Event Management.<sup>1</sup>

> **Conclusion**

Examples such as the data breach at Lincoln National and the fraud at Société Générale show how companies continue to struggle with issues of policy compliance. Novell delivers a platform that provides a real-time, enterprise-wide view of the enterprise to mitigate the risk posed by internal and external threats and, ultimately, to ensure an organization's image, brand and reputation are safe.

The Novell Compliance Management Platform combines powerful technology with documented best practices to provide the only real comprehensive approach to policy compliance. To learn more about the Novell Compliance Management Platform and how it can help organizations bolster security, go to: [http://www.novell.com/promo/home/integrated\\_identity.html?nov\\_gaevent=Homepage|Banner|Integrated\\_identity](http://www.novell.com/promo/home/integrated_identity.html?nov_gaevent=Homepage|Banner|Integrated_identity).

---

**Info** // Novell Connection Magazine  
SO LOGICAL, YET SO RARE

But don't all vendors' solutions integrate IAM and SIEM technology? Unfortunately, no. Most contemporary applications, which are called Compliance Management Systems, simply write potentially interesting events to a log file. When compliance to a regulation must be documented, someone must read, digest and extract the data in these files. Most vendors will tell you they have a tightly-integrated system, but most are IAM solutions with a SIEM system tacked on, leaving customers to build the integration themselves or pay consultants to do it for them. And those "integrations" are definitely not real-time. The Novell Compliance Management Platform is more than just a bundle of products. It's the marriage of technologies. It helps you close the gap between what's supposed to happen and what's actually happening.

---

1The Magic Quadrants are copyrighted 2009 and 2010 by Gartner, Inc. and are reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

# ATT Live in Vegas

Betting on a Sure Thing

by Sheila Mangione

Playing the slots is a gamble. Chances are you'll lose. But there's one sure bet in Vegas this year: [Novell ATT Live 2010](#)

ATT Live is four days of intense, hands-on training delivered by engineers for engineers. This year's conference will be held December 7-10 at the new [M Resort, Spa & Casino Las Vegas](#).

This four-day, real-time, in-class experience is the best bet around for expanding your knowledge and sharpening your skills. It's a bargain at \$1,695.00, but you can get an even better deal with our early-bird discounts. [Register](#) by September 30 and we'll take 20 percent off. [Register](#) between October 1 and October 31 and we'll take 10 percent off.

## > Unique Training Opportunity

Novell offers a broad range of training options to meet the broadest possible range of learning needs. Independent research reveals, however, that classroom-based training yields the best overall results in critical areas. (See [Figure 1](#).) [Novell Advanced Technical Training \(ATT\)](#) provides that in-class experience, with engineer-to-engineer instruction and a troubleshooting emphasis. Delivered at a highly technical level, ATT classes give you real-world expertise you can put to immediate use.

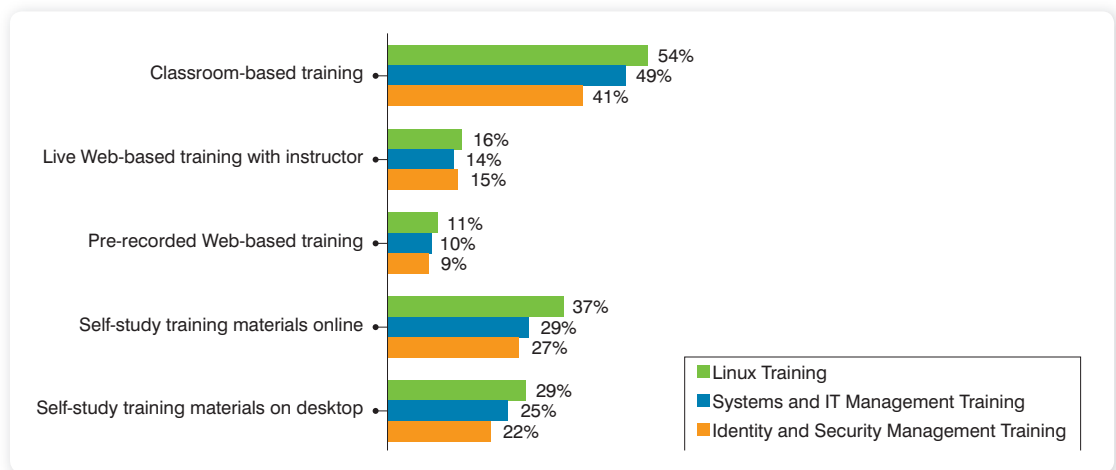


Figure 1: Classroom-based training still yields the best overall results in critical fields such as Linux, Systems & IT Management and Identity & Security Management Training.

**ATT Live** packs the best of our ATT offerings into a single four-day event. In the past, Novell has offered ATT Live only at the Novell Provo campus. In 2009, Novell took the conference to Vegas, making it more accessible than ever. The response was extraordinary. Nearly 200 Novell specialists from around the world learned from veteran Novell instructors, mingled with leading industry consultants, and exchanged knowledge and ideas with their peers.

As good as last year's conference was, **ATT Live 2010** promises to be even better. Novell sought out feedback from last year's attendees and is using their input to improve the venue, ensuring better access to the airport and the Strip, better food, more space, and a better room rate for our guests.

---

## ATT Live packs the best of Novell ATT offerings into a single four-day event.

---

During our four days of solid technical training, we'll offer more than 80 sessions, including many new sessions. The line-up includes first looks at new products as well as updates to current ones. For example, we're introducing sessions on exciting new releases around Novell ZENworks Configuration Management 11, Novell Identity Manager 4 and other products on the FY11 roadmaps.

We limit conference attendance to 200, which means smaller classes and more personalized instruction. We provide all the hardware needed for hands-on training. What's more, the registration fee includes a CD containing all conference presentations, not just the ones you attend. As a result, you can continue your learning experience when you return home.

### > **A Worthwhile Investment**

As you consider your training needs and budgets, this is an experience you really should consider for yourself and your IT staff. The investment you make in **ATT Live** will keep you on top of your game and help your business be as competitive as possible.

ATT Live is surprisingly cost effective. If you register by September 30, you get four full days of classroom instruction for only \$1,350 (a 20 percent discount). That's less than half of the \$2,900.00 cost of a typical four-day, on-site, hands-on class. Four days of online modules would cost you \$2,800.00.

So, if you're a server or network administrator, network engineer, consultant or s who just needs more in-depth technical training directly from the source, don't miss this event. [Register now](#) to take advantage of our great discounts!

**> Award-winning Resort Location**

As noted above, the site of this year's conference is The [M Resort Spa & Casino](#). This 2010 Forbes Mobil 4 STAR award winner offers full amenities and a convenient location. The hotel is 10 minutes from the Las Vegas Strip, so the city's unique entertainment and shopping opportunities are close by. If you prefer to avoid the night life, the hotel is far enough removed that it won't be a distraction. The hotel offers spacious accommodations, fine dining and a variety of entertainment and leisure activities.

The M Resort is offering ATT Live attendees the incredible extended rate of \$95.00 per night, which includes a variety of complimentary services such as free in-room wireless Internet access (usually \$12.99 per day) and daily access to the fitness center (usually \$14.99 per day). A complimentary shuttle service to and from the airport is also included. For more details on the extras available to ATT Live attendees visit the ATT Live site and click the Hotel Information tab.

These rates are good from December 4 - 13 so you can come early and stay late to enjoy the town. Taking advantage of this special rate could save you up to \$930.00. To get the special ATT Live pricing you must [book your stay](#) before November 17.

**> Bonus for Returning Alums**

If you attended ATT Live in previous years, Novell has a special gift for you. Simply [register](#) before September 30 and we'll give you an ATT Live alumni jacket that's built to Nike Golf's exacting standards. (See [Figure 2](#).) This Cyprus blue, 70/30 polyester/cotton jacket is embroidered with "ATT Live Alumni" on the left breast side to put the spotlight on our alums.



*Figure 2: The ATT Live alumni jacket is free to previous ATT Live participants who register before September 30.*

**> Savings for Early Registrations**

Visit the [ATT Live homepage](#) today to get the latest news on this unique training opportunity. While you're there, go ahead and [register](#) to secure your place before the conference fills. Register by September 30, and pay only \$1,350, a 20 percent savings. Register between October 1 and October 31, and pay only \$1,525, a 10 percent savings. If you miss the early-bird pricing, you can still save by using the Novell Connection \$100.00 discount through November 30 (code: ATTL90-NCMAG).

Remember, Las Vegas may be the gambling capital of the world, but ATT Live in Vegas is a sure bet for advancing your technical skills and increasing your knowledge. See you in Vegas at the industry's training event of the year!