

## TEST CENTER REVIEW

# THE IDENTITY CHALLENGE

Courion, IBM, Microsoft, Novell, Sun, and Thor Technologies steer their identity management solutions through our test course

(Excerpted)

**T**HE BENEFITS OF IDENTITY MANAGEMENT ARE AN EASY SELL. OF course IT organizations want to automate user provisioning, put an end to “I forgot my password” help desk calls, and bring sanity to access management across the enterprise. Connect these dots to Sarbanes-Oxley, and even CEOs and CFOs are on board.

The question now is, What are the true costs — in terms of blood, sweat, tears, consultants, and unmet expectations — of implementing a solution that, one way or another, touches every system in the enterprise? And which solutions are ready for prime time?

These were the questions we set out to answer in *InfoWorld's* first identity management shootout at the Advanced Network Computing Lab at the University of Hawaii, Manoa. We invited nine vendors: Computer Associates, Courion, Hewlett-Packard, IBM,

BY OLIVER RIST and PAUL VENEZIA

# Novell has probably the most intuitive and polished user interface of the bunch.

Microsoft, Novell, Oracle, Sun Microsystems, and Thor Technologies. Six accepted, with CA, HP, and Oracle being the three holdouts who resisted our charms.

The lucky participants sent their solutions and engineers to paradise to do battle, which required each solution we tested — Courion Enterprise Provisioning Suite 7.20, IBM Tivoli Identity Manager 4.6, Microsoft Identity Integration Server 2003 Enterprise Edition, Novell Identity Manager 2, Sun Java System Identity Manager 5.5, and Thor XellerateIM 8.0 — to step through a series of identity management tasks based on a common business plot and simulated employee lifecycle.

We built a test network for TCPIP Corp., a fictitious company. The network was based on AD (Active Directory) and was stocked with a Microsoft Exchange 2000 server, a Linux-based HR application called e-HRMS, a Linux-based accounting application called webERP, and a few other systems for good measure. Our vendors needed to integrate

their solutions with all of these systems and then tackle certain identity management challenges, including the hiring, firing, and criminal breach of a junior accountant named Harry, as well as TCPIP's acquisition of rival Fergenshmer Inc. and the resulting directory migration (additional details of the test bed and test scenarios are available at [infoworld.com/3335](http://infoworld.com/3335)).

To accomplish our required tasks, each identity management solution had to integrate with the e-HRMS system, AD, the webERP system, the Exchange server, and, in some cases, a Windows file server. Each of our six solutions took a slightly different path to achieve this, but the basic procedure was for each vendor to create custom connectors to the MySQL back end of e-HRMS and map various data fields present in the database to the same fields in AD. Various policies had to be created for user-name format, password strength, and so on.

When all this was functional, an initial reconciliation task had to be run to

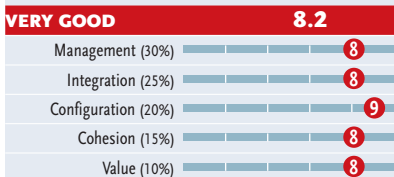
synchronize the data between the identity management server, the e-HRMS database, and AD. Following this, a subsequent reconciliation task would detect changes in the e-HRMS system that then triggered actions within the identity management solution.

We watched each vendor struggle in the lab to some degree, and we played devil's advocate with them all. In the end, only one vendor couldn't complete all of our tests, and this was due more to a lack of additional test time and product complexity than not having the required features.

All of the solutions we tested met our essential requirements, but important differences emerged. Some products worked well on the back end but lacked a unified management and reporting interface. Others presented the slick front end but a problematic foundation. Moreover, some vendors did a better job than others of tying together the multiple tools for identity management into a single, unified solution.

## Novell Identity Manager 2

Novell [novell.com](http://novell.com)



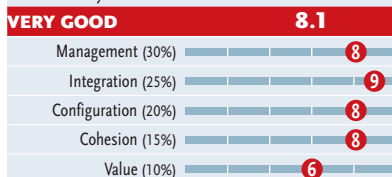
**COST:** \$105,000 as tested for 2,700 users

**PLATFORM:** Server: AIX, Linux, NetWare, Solaris, Windows; database: SQL Server, MySQL, IBM DB2, Informix, Oracle, Sybase

**BOTTOM LINE:** Novell does well on integration via eDirectory's capabilities as an Identity Vault. This suite had powerful graphical workflow and front-end design tools and perhaps the most intuitive user interface in our roundup, but there's still some XML validation work even here.

## Sun Java System Identity Manager 5.5

Sun Microsystems [sun.com](http://sun.com)



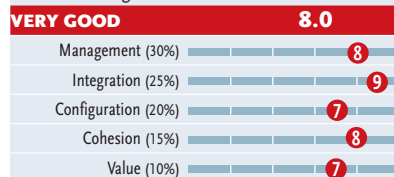
**COST:** \$322,000 as tested; \$150,000 base plus \$25,000 per resource adapter

**PLATFORM:** Server: AIX, HP-UX, OpenVMS, OS/400, Red Hat, Solaris, Windows; database: DB2, MySQL, Oracle, SQL Server, Sybase

**BOTTOM LINE:** Sun's Identity Manager stood out mostly on maturity. This isn't a gee-whiz package, but everything you expect is there, and it simply works. Implementation and pricing are definitely enterprise-oriented, and certainly this solution deserves a close look for large deployments.

## Thor XellerateIM 8.0

Thor Technologies [thortech.com](http://thortech.com)



**COST:** \$250,000 as tested for 2,700 users

**PLATFORM:** Server: AIX, HP-UX, NetWare, Red Hat, Solaris, Windows; database: DB2, Informix, Oracle, SQL Server, Sybase

**BOTTOM LINE:** Powerful, capable, and complex, Thor's XellerateIM breezed through the test scenarios with ease. The focus on agentless operation is a bonus, and the reporting and alerting is handled very well. The cost is quite significant, but you get what you pay for.

# Novell Identity Manager proved to be one of the easiest-to-use solutions in the roundup. The addition of Designer adds even more intuitive functionality on top of this suite.

## Novell Identity Manager 2

Novell's identity management solution relies heavily on the company's directory server, eDirectory, which does a fine job as an Identity Vault. Building on eDirectory's aggregated view of directory information across the enterprise, Identity Manager takes care of the rest.

You'll find all the bells and whistles in Identity Manager 2, including password management, role-based provisioning, cross-application user management, user deprovisioning, and corporate white pages functionality. Furthermore, Novell has probably the most intuitive and polished user interface of the bunch.

Running through Harry's ups and downs revealed some clear benefits of the Identity Manager suite. The eDirectory and Identity Manager combo tied all of our disparate data sources together, allowing for as much flexibility and granularity as most enterprises require.

Identity Manager handles these tasks

largely with administrator-defined identity policies, which allow admins to manage complex application relationships and workflow. All this information is pumped through a two-lane highway between the Identity Vault and the subordinate applications on the network. All this, of course, depends on Identity Manager Drivers, which are the agents needed to manage all applications. Communication among Vault, Drivers, and Identity Manager is based entirely on XML.

With the exception of Novell's fairly granular workflow capabilities, this is all standard stuff. And though the Identity Manager implementation went smoothly, there wasn't much to differentiate it from the others save Novell's carefully designed, glitzy user interfaces. Defining things such as the corporate white pages or the HR-to-IT workflow that our tests required was done in a slick Web-based administration tool that offered speed and customizability.

We'd seen this before, but Novell had

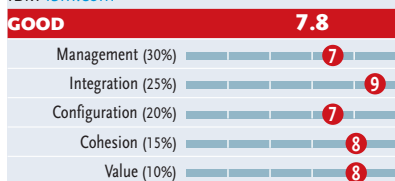
a definite edge in the UI department. In fact, we were already sufficiently impressed, and then they pulled out Designer.

Designer gives the Novell solution a definite ooh-aah factor not found in any of the other products here, but it's important to note that this is an optional add-on. Fortunately, right now it's a free, optional add-on, and if you're using either eDirectory or Identity Manager, we highly recommend you download it ASAP.

Based on the Eclipse framework, Designer allows administrators to lay out almost the entire identity implementation visually and then drill down for configuration. Designer configures the entire Identity Manager front end using portlets, allowing administrators not only to modify the look and feel of each portlet (for easy integration into an existing intranet design) but also to modify each portlet at the field level — in effect deciding exactly what users do and don't see one field at a time. Even better, Designer allows much of the

## IBM Tivoli Identity Manager 4.6

IBM [ibm.com](http://ibm.com)



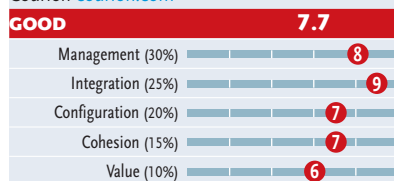
**COST:** \$120,000 as tested for 2,700 users

**PLATFORM:** Server: AIX, Linux, Solaris, Windows; database: DB2, Oracle, SQL Server

**BOTTOM LINE:** IBM Tivoli Identity Manager showcased back-end prowess, but the front end was more complex than it should be. The directory integration tool is powerful and capable, and the solution as a whole is solid. ITIM just needs more work on the UI and reporting functions.

## Courion Enterprise Provisioning Suite 7.20

Courion [courion.com](http://courion.com)



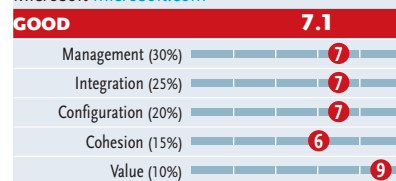
**COST:** \$355,000 as tested: Courion Enterprise, \$180,000; Citrix Password Manager, \$175,000

**PLATFORM:** Server: Windows; database: any SQL

**BOTTOM LINE:** Courion's suite represents not only one of the fastest and most flexible solutions we saw but also one of the most complicated and expensive. If you can get past these hurdles and need the depth it offers, this solution will certainly serve you well in the long term.

## Microsoft Identity Integration Server 2003 Enterprise Edition

Microsoft [microsoft.com](http://microsoft.com)



**COST:** \$68,100 as tested

**PLATFORM:** Server: Windows Server 2003; database: SQL Server 2000

**BOTTOM LINE:** MIIS benefits from deep integration with Windows Server 2003, but you'll need expertise in multiple aspects of that Windows environment to accomplish tasks that should be handled by MIIS alone. On the upside, MIIS sports the lowest price tag in the roundup.

# Designer gives the Novell solution a definite ooh-aah factor that is not found in any of the other products here.

configuration to be done in a simulated sandbox mode. That means you could design an identity implementation blueprint and play what-if games by altering underlying systems or configuration settings. Novell even added version control to make those games easier.

In the end, Novell conquered our lab scenario with few hiccups and went on to finish all the extra-credit tests, including Lotus Notes and z/OS integration, Web GUI- and e-mail-based workflow provisioning, and populating our e-HRMS database from AD, all handled centrally from the smooth iManager console.

When Harry turned naughty, Identity Manager found his illegal administration account so fast we didn't even have time to fully provision the account. Harry was immediately dumped into the Illegals group, which not only disabled his admin access but also kept a handy record of the attempt. It did not send us an alert, however.

The only area of the test where Novell would have relied on outside tools was our Fergenschmeir-to-TCPIP AD joining. As did a number of the other competitors, Novell would have used Microsoft AD tools for the initial migration and then used Identity Manager to manage the Fergenschmeir data through Identity Vault after it was part of the TCPIP AD forest. (Because third-party tools were necessary, we didn't bother to make this part of Novell's test.)

From administration to reporting, Novell Identity Manager proved to be one of the easiest-to-use solutions in the roundup. The addition of Designer adds

even more intuitive functionality on top of this suite. Nevertheless, Novell has work to do: Although the glitzy front end was used for initial configuration, all subsequent validation was done largely looking at raw XML data.

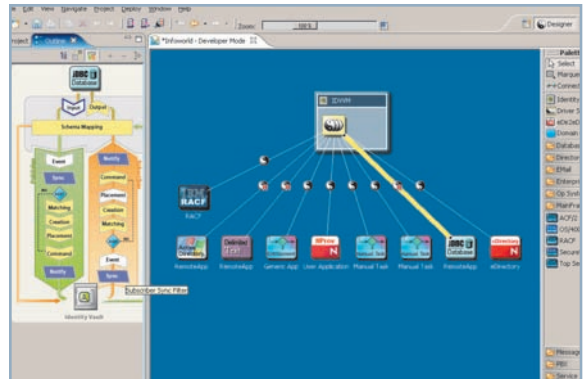
## Meet the Challenge

Every so often, when we're lucky, widespread necessity and solution maturity collide head-on. This is exactly what's

happening today in the sphere of identity management. Although the underlying concepts of identity management aren't new, it's becoming clear that the execution of these concepts by solutions vendors is ready for the mainstream.

Between mandates from on high, such as Sarbanes-Oxley, and needs from below, such as the need to address management headaches associated with the constant march of new applications into the core infrastructure, the time of managing disparate systems and applications in silos is necessarily drawing to a close.

Bringing disparate systems together for centralized user provisioning and access management is a significant challenge, as our testing showed, but it's more than possible — it's inevitable. Automating your infrastructure by implementing an identity management solution is likely to be the largest IT project you'll undertake for years to come, but it also has the potential to be the most rewarding. The potential calm after the storm is not to be overstated.



Novell Designer is an impressive add-on tool that allows admins to map out identity relationships and agent processes before implementation, and it even bundles what-if and sandbox tools.

Even within our limited testing scenario, it was clear that these products are still evolving.

Sun Identity Manager seemed the most mature overall, with strong integration and management capabilities, but still lacks the reporting and front-end polish we were expecting. IBM and Courion have similar work to do on the manageability front. Indeed, Courion needs to keep working on making the flexibility of its solution more accessible. Novell has paid much attention to its front-end tools, producing the easiest solution to configure and manage by far, but it still needs work on the back end to match the depth of Courion or Thor. Finally, Thor was strong from stem to stern, although their implementation process required a good share of custom coding as well. ☞

*Brian Chee, InfoWorld senior contributing editor and manager of the Advanced Network Computing Laboratory at the University of Hawaii, contributed to the design and management of this test.*