An Oracle White Paper
Dec 2011

Identity and Access Management: Comparing Oracle and NetIQ/Novell

ORACLE

Executive Overview

While compliance regulation drove much of the interest in Identity and Access Management in the past decade, reducing risk and improving security have moved into the foreground. To address the concerns of rising security threats and more complex audits, many organizations are faced with the challenge of modernizing their Identity and Access Management infrastructure to address the gaps and align with their changing business requirements. This paper compares how Oracle's Identity and Access Management platform compares to the NetIQ suite of Identity and Access products. NetIQ is the new brand for Novell's Identity and Access Management portfolio after the acquisition of Novell by Attachmate.

The business requirements have changed: organizations need to be more adaptive, flexible and responsive. The business environment, threat landscape and compliance demands have also changed. In this changed environment organizations require more from their Identity and Access Management (IAM) investments. New IAM functionality is required to adapt to risk and new business needs. In addition, new levels of platform consolidation are required to support on-demand Identity Intelligence, visibility and control. Critical new IAM capabilities include real-time adaptive analysis for business transactions, business centric fine-grained authorization, and identity analytics for near real-time business intelligence.

As organizations look at the evolution of their Identity and Access Management roadmaps, many are realizing that a platform approach that consolidates security policies, identity intelligence and workflows can allow an organization to reduce cost, improve security and better address changing compliance requirements. A recent study by the Aberdeen Group, titled *IAM Integrated: Analyzing the "Platform" versus "Point Solution" Approach*, found that companies who use an integrated IAM platform reported a 48% cost of ownership savings over companies that purchased IAM point solutions and did the integration in house.

Oracle's strategy has focused on consolidating Identity content, including access policy, entitlements and analytics, into a single platform that can be utilized as point products but allow a customer to add additional components without the integration costs. The approach is similar to the way spreadsheets can share content across word processing software and presentation software in an office suite. Instead of integrated components, they share a common data model and common policy model that reduces complexity. In contrast, NetIQ's offerings show different levels of integration depending on the product offering. While the Oracle platform has matured as the company consolidates innovative products into the platform, NetIQ's innovation has slowed. The Oracle stack is differentiated by a strong focus on risk and compliance with adaptive access, role management, certification review, fraud detection and external authorization. In addition, Oracle's virtual directory capability provides a distinct advantage to the Oracle platform.

Comparing Oracle and NetIQ/Novell Identity Management Suites

Here is a comparison of the Identity and Access Management offerings from Oracle and NetIQ/Novell:

	Oracle Offerings	NetIQ/Novell offerings
User Provisioning	Oracle Identity Manager	NetIQ/Novell Identity Manager
Identity Intelligence	Oracle Identity Analytics	NetIQ/Novel compliance management
Federation	Oracle Identity Federation w/ Fedlet	NetIQ/Novell Access Manager
Directory Service	Oracle Internet Directory Oracle DSEE Oracle Virtual Directory	NetIQ/Novell eDirectory (No Virtual Directory Capability)
Enterprise SSO	Oracle Enterprise Single Sign-On	NetIQ/Novell Secure Login (Licensed Actividentity source code)
Fine Grained Entitlements	Oracle Entitlements Server	
Web Access Management	Oracle Access Manager	NetIQ/Novell Access Manager
Identity Governance	Oracle Security Governor	
Strong Authentication / Risk Based Authorization	Oracle Adaptive Access Manager	
(Gray blocks indicate areas compared in this paper)		

Comparing Oracle and NetiQ/Novell IAM Suites

Business Relevance of IAM

The role of IAM is changing: IAM is expanding beyond IT and operations. Increasingly, IAM is a business enabler helping companies manage the identities of their customers and subscribers. Many companies estimate the value of the business as a multiple of the number of clients and subscribers. The cost of acquiring, securing and providing access to customers directly impacts profits. Identity management is now a critical enabler that allows businesses to expand while reducing their compliance and operating costs. Reports show that compliance spending can consume up to 40% of the IT budget in regulated industries. Money spent on compliance goes to auditing, reporting and compliance specific activities, and may have little beneficial impact on overall security and risk management. The emerging discipline of Identity Analytics (IA) enables organizations restore the focus on risk while providing proof to address regulatory compliance. Primary benefits of integrating compliance reporting and compliance processes into IAM include smoother compliance operations and greater IAM insight/visibility.

IAM will play an increasingly critical role in helping organizations unlock the potential of cloud computing without compromising security or compliance. Bridging enterprise security policy and service level with public and private clouds will require IAM capabilities such as federation,

identity cloud provisioning and adaptive authentication to provide secure flexible frameworks for business expansion and external collaboration. In addition, IAM bridges the gap by providing the end-to-end business linkage in terms of functional roles complete with compliance support and access governance.

The new business focus of IAM is also evident in the high level IAM policy extensibility that is now part of leading IAM solutions. These high-level interfaces enable non-technical business managers to tune business processes to changing business conditions without requiring technical intervention. Examples include modification of functional roles and setting security policy without re-engineering applications. In addition to control interfaces, IAM can provide business decision support. Examples of this include using Identity and Access Governance to monitor SLA conformance, to provide service usage trends for service optimizations, for forensics, and for HR on-boarding/off-boarding reports.

The increasing business relevance of IAM drives requirements for new IAM functionality. Equally significant is that the expanded role of IAM also demands tighter integration across IAM functional blocks.

Directory Services

Directory services are foundational to any Identity and Access platform. Most Identity suites today include directories for high scale authorization and authentication. Recently, as organizations have tried to consolidate identity information, virtual directories have become a critical component. The lack of a virtual directory is a significant gap in the NetIQ portfolio. Any company considering a strategy around directories should examine a solution set that consolidates capabilities and provides a complete solution.

Identity Intelligence

The business value of Identity intelligence is that it enables business managers to harvest actionable intelligence from repositories of identity data. IAM systems contain information about how systems are used and how systems respond. Mining this information can produce actionable intelligence for a variety of purposes, such as: role optimization, SLA conformance and forensics. Identity analytics can also automate compliance reporting and compliance processes.

Identity Intelligence with Oracle Identity Analytics

Oracle Identity Analytics (OIA) is built on the Oracle identity warehouse, which contains integrated analytical, reporting and remediation engines. OIA also contains a wide variety of methods to import identity data, entitlement data, reconciliation data and audit data from diverse systems. OIA is designed to support:

- Rapid compliance
- Strengthened role governance
- Streamlined access processes

The strength of OIA is its powerful data architecture, which is optimized for complex analyses and simulations. OIA offers an out-of-the-box integration with Oracle Identity Manager and also supports flat-file imports of identity and organizational data from a variety of sources. OIA has an integrated compliance dashboard with over fifty canned reports.

OIA automates certification and attestation and enables managers to approve roles and entitlements based on business-centric descriptions of access privileges. It enables the overlay of audit data on certification and attestation forms to enable richer decisions based on actual usage data. This 360-degree view coupled with change events provides early identification of potential policy violations. In conjunction with Oracle Identity Manager, OIA enables closed-loop remediation to remove conflicting privileges. OIA automates and aligns compliance activity with the business goal of reducing operational risk.

OIA enables comprehensive role governance. The traditional inhibitor to deployment of role management is a fear of business disruption during the introduction of role based management. OIA is architected for complex analytics and is ideal for clean-up of existing entitlements and role mining and rule discovery. OIA also enables powerful simulation for role impact analysis based on policy, entitlements, reconciliation data and audit data. This reduces the risk of business disruption when migrating existing users and applications to role-based management.

With OIM, role governance is simplified via integrated change management and highly-automated role certification. Role versioning, impact simulation, and a rollback capability ensure smooth deployment of role changes. OIA automatically initiates role approvals based on detection of entitlement changes associated with a role. OIA enables identification of excessive role privileges and tags them for removal or automated remediation; this achieves the control of least privilege.

Identity Intelligence with NetIQ/Novell NAGS

NetIQ provides some identity governance via the NetIQ/Novell Access Governance Suite (NAGS). The NetIQ/Novell suite does not have a role manager and is most commonly deployed with a third-party role management product from Aveksa. NAGS is primarily the Aveksa product redistributed by NetIQ. NAGS is disjoint from NCMP (Novell Compliance Management Suite) which is an integration of NetIQ/Novell Identity manager and the NetIQ/Novell Security Event and Information Management (SEIM) product. NCMP also has an embedded instance of NetIQ/Novell eDirectory. NCMP does provide a limited ability to modify pre-defined roles if they are stored in the correct data structures. This is very limited and is primarily a role-mapping tool.

Business has changed. Today' business environment demands open networks and interconnected businesses processes. Business managers need to understand and manage how services are being accessed and used. IAM must be able to enforce complex real-time policies and also provide insight required to achieve the correct balance between control and efficiency, while at the same time meeting ever changing compliance requirements. Oracle Identity Analytics provides 360 degree control with all enterprise identity, entitlements and policy information coupled with powerful analytics and simulation capability. This enables business managers to understand how business privileges are used and see the impact of changes prior to release. OIA has full lifecycle management, versioning and rollback for policies and roles coupled with an integrated compliance dashboard. OIA provides the identity intelligence business managers require to monitor and control their business. NetIQ/Novell Identity Manager does not provide a 360 degree view, but is limited to comparing historical SIEM data with policy.

TABLE: IDENTITY INTELLIGENCE

Comparing OIA with NCMP and NAGS

While NAGS aligns with the Oracle Identity Analytics product, NCMP aligns with several Oracle Identity offerings. Because of the integrated business requirements, these offerings need to be compared in conjunction. There are functional similarities between OIA and NAGS, but the identity warehouse of OIA is a clear differentiator. The identity warehouse unifies all policy, roles, business structure, identity information and application information along with audit and reconciliation data, and supports data classification to enable organizations to prioritize compliance and analytical tasks. OIA supports full role management and full role lifecycle management with versioning, change impact simulation, and a roll-back capability. It also enables highly automated role approval, certification and attestation. While NetIQ has a distinct separation between NAGS and NCMP, the Oracle approach provides a unified platform that allows compliance audits to be remediated automatically for a closed loop approach. Because NAGS is primarily an external product for NetIQ as opposed to OIA, which is an in-house Oracle owned product, the integration between NAGS and NCMP has been less robust.

NCMP and NAGS exhibit some fundamental limitations:

- NCMP only analyzes two data points: the user provisioning data from the identity manager and the historical data from the SIEM function.
- NCMP does not support bulk reconciliation.
- NCMP only learns about entitlements that are exercised. NCMP is blind to invalid entitlements which have not been exercised; this includes illegal entitlements assigned locally at the application.
- Role management in NCMP is limited to role mapping: it can only add resource access to a predefined role or remove a resource from a role. Neither role hierarchy nor role change impact simulation is supported.
- NAGS lacks closed loop remediation with provisioning.
- NAGS does not include preventative risk aggregation during the user lifecycle.

Externalized Authorization

The migration away from application-centric flows to business-centric processes requires externalized fine-grained authorization. Business processes increasingly span multiple applications as well as the cloud. The traditional IAM approaches depend on roles defined locally within the application for fine-grained authorization. This is cumbersome in a mixed platform environment and impossible when the application-embedded role is owned by a third-party, such as in a SAAS environment. To respond to changing business needs, managers need a way to control fine-grained entitlements without having to launch an IT project or an engineering project to modify specific roles baked into each application. The best way to accomplish this is to externalize fine-grained authorizations and provide high-level declarative or graphical management interfaces. This enables non-technical business managers to implement consistent authorization controls across multiple applications or across multiple platforms.

Externalized authorization provides rich information for business optimizations. With externalized authorization not only can managers see who is accessing the service but also they how users use the service. In an integrated IAM platform containing identity analytics this level of usage detail can be very valuable in planning service optimizations.

Oracle Entitlements Server (OES)

Oracle Entitlements Server provides a practical, intelligent framework for fine-grained access control using an authorization engine that manages authorization and entitlements for a wide range of entities: service resources, software components (such as URLs, Enterprise JavaBeans, and Java Server Pages), and arbitrary business objects (such as customer accounts or patient records in a database). OES evaluates fine-grained access requests in real time at the policy decision point (PDP), which supports multiple connectors to attribute/identity sources such as LDAP, and enforces them at the policy enforcement point (PEP).

The PDP and the PEP are available in a single package to enable either distributed application-embedded deployment or deployment as a shared PDP server. Along with the security module containing the PDP and PEP, OES has a Policy Administration Point (PAP), which manages configurations, organizations, applications, policies, and roles. OES can enforce both role-based and attribute-based authorization policies. Separating fine-grained privileges from role-based access reduces the number of unique roles and simplifies role mining and role management.

OES has broad platform support with out-of-the-box solutions for a range of scenarios, including:

- Content portals and content management servers such as SharePoint and Oracle Universal Content Management.

- Service Oriented Architectures including support for XML gateways such as Oracle Enterprise Gateway, Vordel, DataPower and Layer 7. For low latency scenarios, OES can be directly embedded into XML Gateways such as Oracle Enterprise Gateway and Vordel.
- OES supports standard Java EE containers including but not limited to WebLogic, WebSphere and JBoss. The OES naming mechanism supports clustered architectures
- Java SE is supported by OES with pre-integrated SM for Java SE, which has ABAC & RBAC policy support.
- OES supports all major business application platforms, including WebLogic, IBM WebSphere, Microsoft .NET, Tomcat, Java Applications, and Documentum. OES is integrated with the Oracle IDM suite.

OES supports Oracle Virtual Private Database (VPD) technology and enables fine-grained access control from within the database itself. OES can be used in conjunction with VPD filters to apply fine grained access control to rows and columns in the database. Implementing fine-grained policy based entitlements in the database is highly effective for applications where authorization externalization cannot be accomplished in the business logic layer.

Externalized Authorization with NetIQ/Novell

NetIQ/Novell does not have externalized fine-grained authorization. Implementing externalized authorization in the NetIQ/ Novell suite requires custom coding. J2EE agents can be configured to use the Java Authentication and Authorization Service (JAAS) and Java Authorization Contract for Containers (JACC) standards. The administrator of the Identity Server can use policies to define how properties of a user's authenticated identity map to the set of active roles for the user. This role definition serves as the starting point for the role-based authorization policies of the Access Gateway and J2EE components. Additionally, authorization policies can be defined that control access to protected resources based on user and system attributes other than assigned roles.

Using JAAS to extend NetIQ/Novell Identity Manager to implement fine-grained authorization for Java applications requires custom technical work to implement and refine, this approach means that:

- Implementation and modification of fine-grained authorization is complex and requires an engineering project.
- Business managers are dependent on support from technical groups, which limits their agility when responding to market or regulatory changes.
- Custom technical solutions are complex, error-prone, and require sophisticated production integration strategies.

In addition, neither NetIQ/Novell nor JAAS have systematic versioning, impact simulation, or rollback capability to assist with production rollout.

Business has changed. Organizations are moving to business-centric process flows, which may incorporate multiple heterogeneous applications as well cloud / SAAS based applications. Traditional application-centric IAM strategies that rely on roles baked into the application are no longer effective. Oracle provides fine-grained authorization as a service, which enables business managers to tailor business entitlements to business needs regardless of the underlying complexity of the business process

TABLE : EXTERNALIZED AUTHORIZATION

Adaptive Access Control

The business value of adaptive access is that it enables organization to adapt to increased transaction risk without impacting usability. To be competitive businesses must offer a consistent service experience to users across all of their endpoint devices regardless of location. This increases transaction level business risk and to remain competitive businesses cannot overburden users/customers with excessive security steps.

Adaptive access solves this problem by auto-learning behavioral characteristics of users in terms of device identity, IP location, transaction types etc. Then adaptive access then identifies changes in a user behavior and can issue a conditional demand for stronger identity assurance. Even in cases where the user already has a token, adaptive access protects that token by incorporating contextual factors into the access decision.

Oracle Adaptive Access Manager (OAAM)

Oracle Adaptive Access Manager is an adaptive threat management solution that is part of the Oracle Identity and Access Management suite and comes 'business-ready' and pre-integrated with Oracle Access Manager. OAAM's adaptive capability comes from a self-learning risk engine coupled with a variety of virtual authentication options that can be conditionally triggered. Its modular architecture enables control of web flows without requiring reengineering of the application. OAAM risk decisions are configurable via a graphical user interface that does not require technical knowledge and allows non-technical business managers to tune OAAM to changing business, regulatory, and threat conditions.

The major components of OAAM include:

- OTP Anywhere: risk-based one-time-password authentication
- Risk Analytics: real-time analytics to evaluate risk based on behavioral and contextual factors
- Automated behavioral profiler: auto-learning of user behavior to build a behavioral history that is used for real-time profiling of user requests.

- Configurable decision engine: a graphical, declarative interface to enable non-IT personnel to manage and optimize OAAM for new business, regulatory, and threat risks
- Answer logic: balance security and ease of use for knowledge-based authentication (KBA)
- Self-service: users can create and reset challenge/response pairs.
- Device fingerprinting: a clientless mechanism for device identification

OAAM combines these features to mitigate insider fraud, prevent session hijacking, and identify stolen credentials. OAAM automatically learns user behavior is for users in contextual terms such as; devices, locations (IP addresses, city/state/country, etc.) and entities (credit card, address, etc). OAAM establishes behavioral baselines for users, deviations from the baseline are calculated as a transaction risk score in real-time. Automatic learning is "always-on" and the system automatically adjusts to changes in user populations and user habits without the need to re-architect policies and settings. When anomalies are detected, OAAM can trigger a demand for alternate authentication, using devices such as a virtual keyboard streamed from the server, knowledge-based questions or out-of-band server-generated one-time passwords.

Adaptive Access capabilities of NetIQ/Novell NCMP

The NetIQ/Novell IAM suite does not include adaptive access capability. With the NetIQ/Novell suite there is no way to incorporate contextual factors into a real-time risk based access decisions. NCMP supports standard authentication based on a set of credentials. Evaluation of the credentials results in a binary access decision: either transaction granted or transaction denied. NCMP cannot build a risk score to trigger a demand for alternate authentication based on contextual anomalies.

Comparing OAAM to NCMP

As the volume and value of electronic business transactions increase, companies require the ability to incorporate advanced authentication methods into their IAM platform. With OAAM Oracle customers can add adaptive access capability to their platform as required. OAAM is pre-integrated by Oracle and is business-ready on purchase. NetIQ/Novell customers who required adaptive access have to select and integrate a third-party adaptive authentication vendor. The benefits of adaptive access are summarized in the following table:

ITEMIZED ADAPTIVE ACCESS BENEFITS	Oracle	NetIQ/Novell
Increase transaction security by including access decisions based on contextual factors i.e. transaction amount, device identity or geographic location.	Yes	No
Auto compilation of behavioral profiles based on contextual transaction history	Yes	No

Graphical control for decision engine to enable non-technical business managers to structure rich metrics and conditional trigger points	Yes	No
Platform integrated adaptive access for integrated provisioning and integrated analytics	Yes	No

TABLE: ITEMIZED ADAPTIVE ACCESS BENEFITS

Business has changed. The growth in volume and sophistication of online transactions has exploded. Oracle has developed IAM- integrated contextual analysis for transactions to enable business to implement risk-based access control based on behavioral attributes. NetIQ/Novell IAM platform has no adaptive access capability.

TABLE: ADAPTIVE THREAT PROTECTION

Conclusion

IAM is at a turning point. Growth in network porosity, cloud adoption, user mobility, endpoint diversity, and the shift to business-centric processes are placing new demands on identity and access management. At the same time the cost of failure is becoming higher due to increased threat sophistication and increased regulatory consequences. Today the business value of IAM transcends the traditional functions of user provisioning and access management to encompass every aspect of identity governance and control, thus greatly increasing security, easing the burden of compliance, and increasing business efficiency.

In today's business environment, organizations must evaluate IAM platform on the following axes:

- Functional completeness
- Platform consolidation
- Innovation in IAM

Business has changed and organizations must change how they evaluate IAM solutions. Oracle is investing heavily in the Oracle IAM suite to deliver integrated business ready solutions. This allows Oracle IAM customers to focus on core business issues instead of focusing IAM customizations and 3rd party IAM integrations.

TABLE : ORACLE IDENTITY MANAGEMENT

Oracle has a complete suite of best-in-class IAM capabilities: High performance directory services, Identity management and provisioning, access management, SSO, Federation, Adaptive access, Fine Grained Authorization, Identity Analytics, Enterprise Gateway, Service Platforms, Governance. The Oracle suite is tightly integrated not just in the data/provisioning plane but also in reconciliation, analytics and governance.

- OES enables business to implement consistent authorization policies across heterogeneous applications and cloud based applications.
- OAAM enables businesses to automatically compile behavioral baselines and leverage contextual intelligence for risk based access control
- OIA enables businesses to mine identity and access information and distil organic intelligence for support of business decisions and compliance/threat analysis

Business is changing and the role of IAM is expanding beyond IT and operations. Externally, the threat landscape is changing and the regulatory compliance landscape is changing. Now more than ever choosing the right IAM Vendor is critical.

Comparing Oracle and NetIQ/Novell
Dec 2011

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Oracle is committed to developing practices and products that help protect the environment

0109