



# Centralizing Identity and Access Management in Unix/Linux Environments

Using BoKS<sup>®</sup> to overcome the inherent  
security gaps of NIS

A FoxT White Paper

“User provisioning has six components: a framework for managing access control policies, usually by role; interconnections with IT systems; workflows to guide sign-offs; delegated administration; password management; and auditing. By automating these processes, organizations ensure employees only get access to the information they need to do their jobs. If their job role changes, so will their access levels.”

Jonathan Penn  
Forrester Research analyst

## ● The Problem

User administration in a large Unix/Linux domain is a complex task since each host potentially serves as an autonomous authority. It authenticates and authorizes its users based on local settings. Furthermore, services such as SSH represent trust domains of their own. Tools like ‘sudo’ introduce yet another layer of user management and authorization on top of the operating system.

As a result, centralized administration of user identities and configuration settings can radically simplify management of large Unix/Linux domains. Yet, administration alone is not sufficient. Auditors require access controls and auditing capabilities to verify that only authorized users access data and that they do so in compliance with existing security policies.

## ● Centralizing Identity Management Foundations

Network Information Service (NIS) originally Yellow Pages, was introduced by Sun Microsystems in the 1980s to provide centralized administration of users and configurations. Today NIS has evolved to an industry standard and most of the code has been released to the public domain.

NIS is essentially a protocol for distribution of configuration files from a central point within a local area network. It was designed to simplify user and network administration which was achieved, however, at the cost of considerable security drawbacks. NIS is an RPC service used to share maps of usernames, passwords, and sensitive configuration data with any computer claiming to be within its domain. It provides no host authentication and passes unencrypted information over the network, including password hashes.

With Sun OS 5.0, NIS was replaced by NIS+, a completely rewritten service. NIS+ adds authentication and encryption services to improve security. It also extends services and allows a hierarchical name space as opposed to the flat name space of NIS. Yet, the overall goal remains the same – to provide centralized administration of user accounts.

Today large organizations already use Lightweight directory Access Protocol (LDAP) to establish platform independent corporate directory services. And modern Unix/Linux operating systems can be configured to use LDAP authentication. Thus, many organizations looking to replace NIS have seen LDAP as an alternative. As a result, NIS+ never became the natural migration path away from NIS as intended. Some vendors have even replaced NIS+ support with LDAP services in their software distributions which further accelerated a trend towards LDAP.

## ● Identity Management, Access Management, Enforced Security Policies and Audit Logging

While centralized administration of user accounts is one important achievement in itself, it only addresses one aspect of the problem. Without the ability to control related permissions and security policies and to audit their enforcement, user management on its own remains inadequate.

Today, with regimes such as Sarbanes Oxley challenging IT management teams with ever increasing compliance and auditing requirements, identity management without the ability to enforce centrally managed access rules and security policies leaves an organization vulnerable to audit failures and security threats.

Thus, these aspects need to be combined while at the same time ensuring that efforts to achieve efficient corporate directory services are fully supported.

### FoxT Solution - BoKS Access Control for Servers

BoKS<sup>®</sup> Manager, the security server used by BoKS Access Control for Servers from FoxT, combines centralized identity management, access management, security policies and audit logging. Through tight integration with directory services and account management tools it serves as an extension of corporate identity management to handle user provisioning in Unix/Linux domains. BoKS Manager then offers centralized administration of access rules and security policies. On BoKS protected nodes, BoKS clients enforce these centrally managed access rules and report all events back to the security server to achieve centralized audit logging of all user activities and related security events.

Thus, for an organization striving to go beyond centralized identity management, to add the ability to centrally configure fine-grained access rules and to audit their enforcement, BoKS becomes an interesting alternative. FoxT customers conclude that BoKS-managed Unix/Linux domains pass their Sarbanes Oxley audits where LDAP- or NIS-managed domains fail. And this is very much due to the fact that BoKS adds access management, enforcement of security policies and centralized audit logging to the identity management process. Through its tight integration with LDAP, the benefits of centralized directory services remain.

“Lost business because customers don’t have access when they need it. Months spent producing regulatory compliance reports for auditors. Breaches of identity and access management (IAM) lead to billions of dollars of losses each year, both reported and unreported.”

Gartner, IAM Summit 2006

## Multi-Service Security Server - BoKS<sup>®</sup> Manager

BoKS<sup>®</sup> Manager is a multi-service security server. It provides flexible role-based access control by means of specifically configured “access routes” granting access to a certain service on a given target from a given source provided rules regarding time constraints and authentication strength are met. The BoKS Manager authentication server can be configured to demand authentication strength based on the type of request made. All access is recorded in the central audit log server.

### ● Administration, Authentication, Authorization and Audit Logging

The all-inclusive approach taken with BoKS<sup>®</sup> has paid off for FoxT customers. In recent years, while NIS/NIS+ managed or LDAP enabled environments often have failed, especially in Sarbanes Oxley-driven audits, BoKS-managed domains have proven to be well aligned with the new requirements.

A comprehensive solution needs to take all aspects of the four As into consideration and ideally centralize these services to a single point:

- **Administration** of users, host groups, access permissions and security policies such as password rules. Smooth delegation of administration privileges in the administration interface itself is typically also a requirement.
- **Authentication** of users and processes logging on to the system including support for different types of authentication methods and strengths. Depending on classification of an accessed service you may need to enforce security policies mandating strong authentication - for instance smart cards or tokens. To enable flexible batch processing, you may need the ability to allow trust-based auto-logon for instance via host-based SSH while denying the same authentication scheme for user interactive logins.
- **Authorization** of users and processes based on configured access rules and security policies to control access to services. A user should perhaps be allowed to use ftp but not telnet, or be

“Core infrastructures for managing your most important assets - It’s the irresistible force meeting the immovable object. To increase transparency and agility, today’s enterprises need to start opening up systems to staff, customers and partners. However, the need to secure applications, data, and networks has never been so pressing.”

Gartner, IAM Summit 2007

forced to use sftp over SSH while still being denied access to an interactive SSH shell. To comply with auditor guidelines, you will need the ability to prevent direct login using service accounts or ‘root’. Security policies typically stipulate that a personal account be used for login after which ‘su’ or ‘sudo’ - like methods can be used for delegation of privileges. This also requires rules-based control over commands such as ‘su’ and ‘sudo’. To achieve all of this your authorization scheme should provide the ability to allow or deny connections based on parameters such as “from which machine”, “to which machine”, “to which service”, “when”, with which “authentication method/strength”, based on which “user role” assignment, etc.

- **Audit logging** with detailed information about logins, failed logins, configuration changes, services used etc. Moreover, audit log data must be consolidated to a safe and central place, made available for compliance reporting without elaborate data mining efforts. Auditors will want to verify that users, including administrators, are unable to tamper with audit log data. For sensitive sessions they may even recommend keystroke logging capabilities.

## ● BoKS® versus NIS/NIS+ and LDAP

While NIS/NIS+ and LDAP approach these management problems from the administrative perspective of identity management, to a certain extent also recognizing the need to achieve centralized authentication services, BoKS® provides a platform addressing the complete scope of tasks: administration, authentication, authorization and audit logging.

In the light of the four As outlined in the previous section, the table below provides a summary of the capabilities provided by these different technology solutions.

	NIS	NIS+	LDAP	BoKS®
Administration	—	✓	✓	✓
Authentication	✗	—	✓	✓
Authorization	✗	✗	—	✓
Audit Logging	✗	✗	✗	✓

“As identity management initiatives become increasingly mission-critical, organizations need a way to centralize the management and monitoring of their identity systems from the operating system through the application layer to the end-user.”

Director, IT Security,  
Fortune 500 Company

In real life, things are naturally much more complex and there are numerous variables that are worth noting:

1. Authentication: LDAP by default uses an unencrypted protocol which means both user names and passwords are sent in clear text over the network. This will naturally not make auditors happy. Yet, most LDAP repositories come with the ability to use SSL or TLS. NIS+ stores passwords encrypted, as opposed to NIS, but still sends them in clear over the network, although remedies are available here as well. BoKS uses a multi-session/multi-service protocol between the security server and managed hosts through which data is sent safely encrypted. Furthermore, BoKS can be used to configure rules mandating strong authentication for sensitive sessions/services, something the other solutions do not offer. In fact, BoKS supports a wide variety of authentication methods. Combined they not only provide improved security but also enable various secure single sign-on alternatives. So while overall security is improved, the user experience and efficiency gains are considerable as well.
2. Authorization: BoKS Manager by default locks down the entire domain. For authorized users, access is provided along explicitly approved so called Access Routes, a path defined with the parameters “from host”, “to host”, “service”, “time of day”, “day of week”, combined with the definition of the required authentication strength - RSA SecurID, SafeWord tokens, X.509 certificate-based SSH connection, user name and password etc. etc. Rules can be assigned to User Classes (roles) and apply to Host Groups (a logical segment of the domain). NIS/NIS+ and LDAP allow grouping of computers but completely lack the kind of “rules engine” that BoKS Manager provides.
3. Audit Logging: Naturally, both NIS and LDAP services are able to provide audit trails. However, to get a complete picture of the chain of events for instance in a network where clients use an LDAP bind request to login, you have to combine data from 1) the LDAP log file and 2) the native Unix/Linux wtmp log file on the machine where the login request was made - unless the login failed, in which case you need to check with the 3) failedlogin file - for ‘su’ commands include the 4) sulog file and 5) syslog is always relevant as well etc. etc.

The central LDAP audit file itself reveals that the user attempted to login, but says nothing about the service used (telnet, ftp, ssh, rsh etc.), the authentication strength and from where the login request was made.

As a result, audit data is scattered across the network. It takes considerable data mining efforts to combine and cross-reference all these data sources to achieve even the most basic types of compliance reports. And when done, you still cannot trust the data you are viewing, because such distributed storage is far from tamper-proof.

By contrast, BoKS-managed machines send audit log data in real time to the security server where a centralized audit log is maintained. For sensitive sessions, BoKS protected hosts can be configured to record every keystroke even and these log files are also sent to the security server.

The centralized log files then contain data that match the abilities of the access rules: from where connection was made, to where, which service, when, etc.

To enable smooth compliance auditing, BoKS Manager comes with reporting tools. Using these tools, auditors can review access rules and audit trails at one central point. This means queries regarding permissions granted as well as permissions used can be combined: “Who is allowed to ‘su to root’ on machine X according to current security policies?” and “Who did actually ‘su to root’ on machine X last Monday?” The answers are delivered from centralized audit files kept out of reach from the users whose activities are being monitored.

## ● Conclusions

BoKS Access Control for Servers from Fox Technologies offers what is probably the most comprehensive identity and access management tool available on the market for mixed Unix and Linux environments. For organizations in need to review their NIS/NIS+ or LDAP-managed environments, BoKS Access Control for Servers represents a cost-efficient alternative. Rather than applying numerous point-solutions to mend the countless holes revealed by tough compliance audits, organizations implementing BoKS can streamline their administration and achieve fast return on investments while satisfying current and future auditor demands.

Integration with enterprise identity management processes and technologies is essential as well, and BoKS Access Control for Servers offers flexible options to achieve a robust and automated connection to corporate directories.

## ● About FoxT

FoxT offers a comprehensive and effective controls solution for corporate governance, risk, compliance and information security management. FoxT combines corporate controls, application controls and secure IT controls software into a single, integrated platform that provides continuous visibility into business processes and performance. Through smart integration and automation, FoxT solutions reduce total cost of ownership, deployment risk, and time to market, making compliance sustainable and transforming it into a source of competitive advantage. Headquartered in Mountain View, California, FoxT serves Global 1000 customers in 32 countries. For more information, contact Elliott Zember at +1 650 687 6248 or visit [www.foxt.com](http://www.foxt.com).



FoxT  
883 North Shoreline Blvd.  
Building D, Suite 210  
Mountain View, California 94043  
[www.foxt.com](http://www.foxt.com)  
650.687.6300

Copyright © FoxT. All rights reserved.  
The document is provided for informational purposes only and the contents herein are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior permission.

FoxT logo is a trademark of FoxT, Inc. Other product and company names herein may be registered trademarks and trademarks of their respective owners.