



# Why is LDAP Failing Audits?

A FoxT White Paper

---

For Unix/Linux shops, the security and compliance shortcomings of NIS and NIS+ have become evident in recent years. Lightweight Directory Access Protocol (LDAP) initially seemed a viable alternative that would also allow organizations to manage their Microsoft and Unix user populations in a standard way. So why are LDAP-based management systems now increasingly falling foul of auditors? And what can enterprises do to avoid this?

When it was first introduced, NIS provided a handy mechanism for centrally managing user and host information in large networks. However, the protocol lacks any inherent support for authentication and authorization, and it is difficult to produce audit trails keeping track of changes to user and host definitions across the system.

With the advent of LDAP, many organizations saw the opportunity of consolidating user data for both Microsoft and Unix/Linux systems in one centralized directory. The problem is that organizations running LDAP are still failing security and compliance audits. LDAP simply does not per se include enough security features to satisfy auditors.

Unmanaged LDAP – that is, LDAP implemented as a core provisioning service within the enterprise, but without add-on functionality to secure and control its use - includes support for central controls on passwords, but without integrating security add-ons, LDAP password is the only authentication choice, unless users are allowed to set up their own authentication. In the latter case, a lack of centralized controls over authentication, for example being unable to prevent users from setting up SSH Public Key authentication with no password, can prove costly in audits.

Unmanaged LDAP does not provide enough fine-grained access controls to satisfy IT and compliance auditors. They want to know exactly who can access what resources, when. Unmanaged LDAP cannot control access for individual users or hosts, let alone at the service level.

Audit trails are another problem. Unmanaged LDAP provides no greater central auditing capabilities than NIS, and does not deliver the kind of documented output showing that provisioning and access policies are actually being enforced in the network that auditors require.

Finally, one of the biggest problems with relying on LDAP for network management is the issue of local functional accounts. When business critical applications require these local functional accounts to operate, application managers are rightly reluctant to hand over control of these accounts to external LDAP systems. However, not doing this leaves the enterprise with perhaps dozens of local accounts that are not under centralized control and not subject to policies. This leads to audit failures.

Given recent audit failures, more and more organizations are looking at strategies to manage LDAP across the different operating systems they use, releasing its potential as a provisioning and management tool while ensuring that it does not become a compliance liability.

One strategy on the table is to use Active Directory, Microsoft's implementation of LDAP, to manage all the resources in the network, both Microsoft and non-Microsoft. This category of solutions attempts to extend Active Directory authentication and Group policies to non-Microsoft resources including Unix and Linux systems.

While this approach leverages the investments many organizations have already made in Active Directory, solutions designed to graft Active Directory security models onto Unix and Linux environments typically control access on a host-by-host basis, and do not offer the granularity of managing access to individual Unix/Linux services. When it comes to the pressing problem of controlling the use of privileged accounts on Unix and Linux, a hot potato when it comes to audits, such solutions typically rely on variants of the free-ware sudo utility, but do not include features like specific controls on su operations or keystroke logging.

Another approach to centralizing identity and access management in the enterprise is to find tools that will manage Unix and Linux systems with sufficient granularity to satisfy auditors and will at the same time integrate with managed LDAP systems, even allowing an LDAP system such as Active Directory to be used as the principal repository of identity data.

This strategy recognizes that specialized management systems are needed to control the specifics of the Unix and Linux environment. With a security model that differs from the Microsoft Active Directory Model, controlling

Unix and Linux presents a different set of problems, including properly monitoring privileged accounts and the smooth deployment of secure protocols like SSH, to name but two. Such an approach will typically involve deploying a solution that can manage Unix/Linux authorization at the service level, not the host level, but can also securely integrate with LDAP directories to bring Unix and Linux into the enterprise's central provisioning and identity management system.

When it comes to auditing too, your audit output is only as detailed as the controls you have in place, so if you are controlling access at service level rather than host level, you have more detailed information to present to auditors. Similarly, robust controls on privileged account operations such as keystroke logging provide more evidence of accountability than using sudoers files to guarantee this vital element of Unix/Linux security.

This approach enables functional accounts to be safely run in a local context meaning application managers can rest easy, but at the same time includes these local accounts in a centralized system of controls, subject to enterprise-wide policies, and centrally audited.

As industry searches for a new paradigm to manage mixed Microsoft and Unix/Linux environments, one thing is for sure: Unmanaged LDAP systems are failing audits, and it is imperative for companies to assess and determine what their strategy will be moving forward.

FoxT provides an integrated LDAP solution that enables organizations to extend LDAP management benefits to Unix and Linux environments in a controlled way. BoKS Access Control for Servers provides centralized directory services for Unix and Linux domains and includes full integration with other managed LDAP systems such as Active Directory, but features granular controls developed specifically for Unix and Linux. FoxT works with enterprises to manage and secure LDAP systems and make sure they do not fail audits.

## About FoxT

At FoxT, we deliver best-in-class software solutions and services that secure access to information and related technologies. By enabling improvements in the integrity of IT systems and data, we seek to exceed the expectations of world class IT organizations in their need to meet governance and regulatory compliance requirements. Headquartered in Mountain View, California, FoxT serves Global 1000 customers in 32 countries. For more information – [www.foxt.com](http://www.foxt.com)



FoxT  
883 North Shoreline Blvd.  
Building D, Suite 210  
Mountain View, California 94303  
[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.