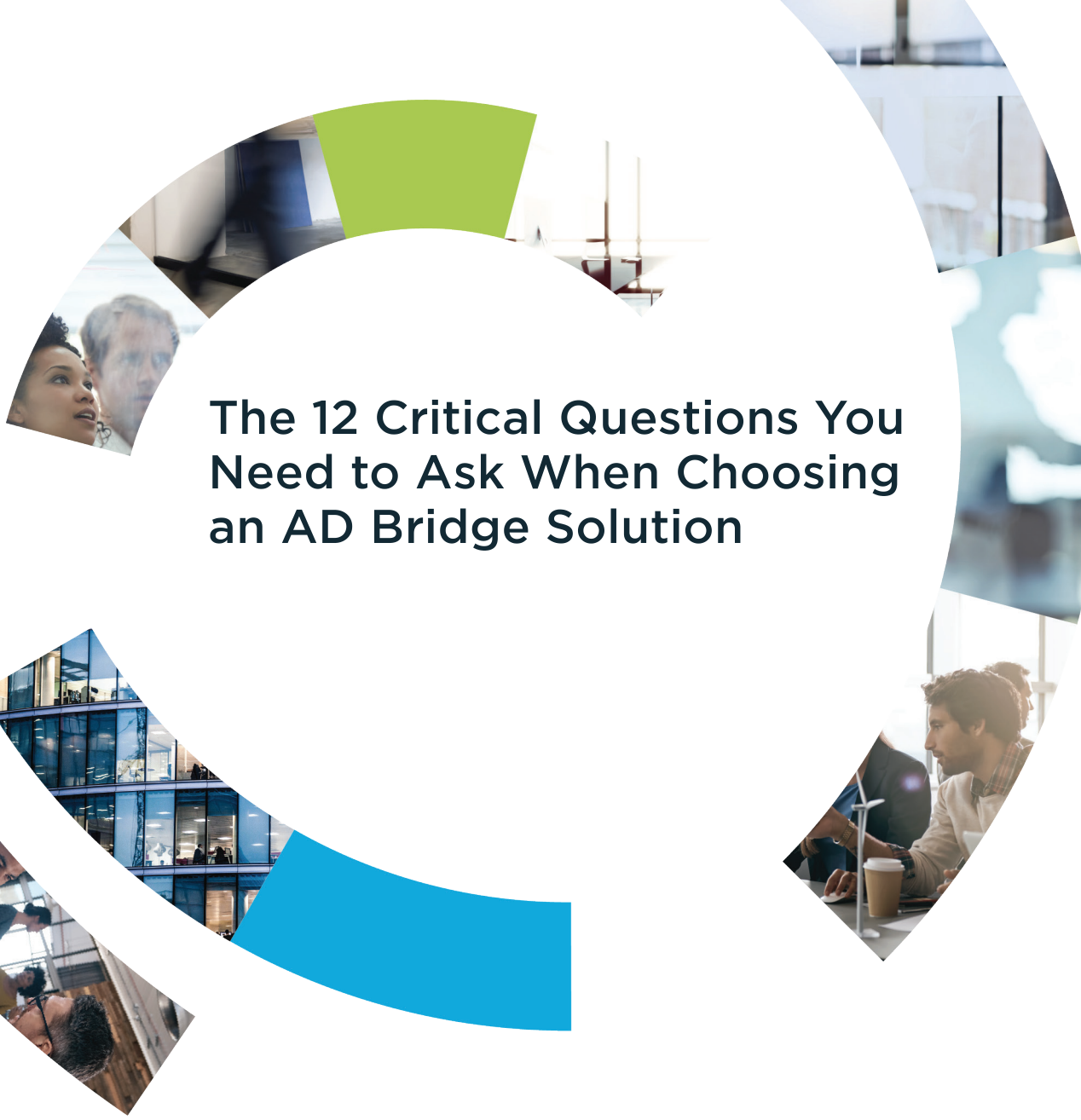
WHITE PAPER



The 12 Critical Questions You Need to Ask When Choosing an AD Bridge Solution

Abstract

Most enterprises today have heterogeneous IT environments, with Microsoft Active Directory (AD) providing Windows access for most users, but with other platforms such as Unix, Linux, and Mac OS X providing critical services as well. But each of these systems has its own identity, authentication, and access requirements. This means users can have dozens or hundreds of passwords to remember and enter, and administrators may have dozens or hundreds of identities per user to provision, re-provision, deprovision, and administer.

AD bridge solutions address this problem by enabling Unix, Linux, and Mac OS X systems to participate as "full citizens" in Active Directory. Consolidating identities into AD reduces complexity and costs while improving security, compliance, and productivity. This white paper identifies a number of key questions to ask when evaluating AD bridge solutions, and explains how One Identity delivers the ideal solutions to meet the needs of every organization.

Introduction

The problem with Unix

The vast majority of modern enterprises consist of heterogeneous systems. Typically, an enterprise will have a large Microsoft Active Directory (AD) environment that houses identities and provides Windows access for the largest portion of its user population. In addition to AD, most organizations also have a large mix of other

ONE IDENTITY

platforms, including Unix/ Linux, Mac OS X, mainframes, and midrange systems, along with myriad applications—each with its own identity store, authentication, and access capabilities and requirements. This overabundance of identity and authentications is the source of many efficiency, security, and compliance problems, especially for organizations with dozens, hundreds, or even thousands of Unix/Linux servers.

For instance, users in an organization with AD and 100 Unix servers could have 101 separate identities, 101 separate passwords, and 101 separate logins to get access to the resources necessary to do their job. In addition, the IT department would have 101 identities to provision, 101 passwords to reset, and 101 directories to audit for compliance purposes. And that complexity would be repeated for each user throughout the organization.

This problem has been plaguing heterogeneous organizations since the early days of Unix. It was thrust into the spotlight with the introduction of AD with its obvious advantages: a unified identity namespace, Kerberos single sign-on (SSO), and centralized identity and access management. If Windows could do it, why couldn't Unix?

Thus we saw the birth of Active Directory bridge technology and the now mainstream AD bridge market.

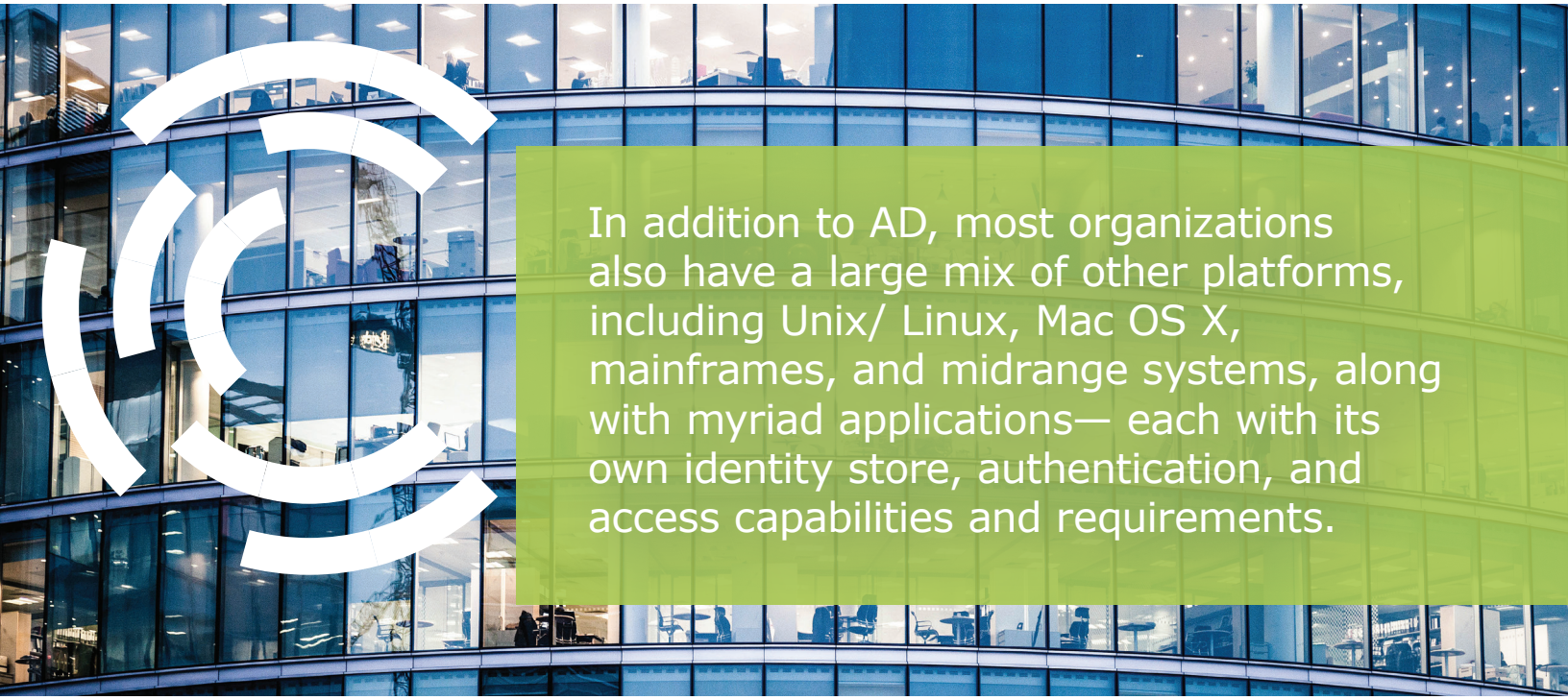
A brief history of AD bridge

In 2003, several Linux developers at Caldera Labs undertook a project to build a Kerberos authentication solution and unifying directory for Unix and Linux systems. They soon realized that they were attempting to build something that Microsoft had already mastered—Active Directory—and they switched their focus to creating a solution that would "bridge" the gap between Unix/Linux and AD. The team then formed a company called Vintela, which was dedicated to building the first "AD bridge" solution. That solution debuted in 2004 as Vintela Authentication Services (VAS).

Other companies followed suit, and by late 2009, five vendors were vying for the quickly growing Unix-to-AD integration customer. In July 2005, Vintela was acquired by Dell, and VAS continued its market leadership under the name Authentication Services. Through it all, the first solution continued to experience the most rapid growth, largest deployments, and most technical depth. Today, Authentication Services and its patented technology boasts nearly 1,000 customers and more than 5 million installed "seats."

What is an AD bridge?

An AD bridge solution enables Unix, Linux, and Mac OS X systems to participate as "full citizens" in Active Directory. According to Burton Group:



In addition to AD, most organizations also have a large mix of other platforms, including Unix/ Linux, Mac OS X, mainframes, and midrange systems, along with myriad applications— each with its own identity store, authentication, and access capabilities and requirements.

These "commodity" [AD-bridge] solutions lack enterprise-level functionality—such as extending AD Group Policy, audit, and management capabilities—nor can they consistently deploy the solution across multiple operating systems.

"….most of the large enterprises Burton Group surveyed in its authentication contextual research project had implemented (or were planning to implement) an Active Directory (AD) bridge product to improve compliance and reduce costs and user sign-ons. AD bridge products enable organizations to manage UNIX users (i.e., "traditional" UNIX flavors such as Sun Solaris, but also Linux and Mac OS) from AD, extend Windows Kerberos authentication and single sign-on (SSO) to UNIX users, and enable centralized policy management of UNIX systems via standard AD tools."

More specifically, the Burton Group's report stated:

"AD bridge products unify the Microsoft and UNIX environments by leveraging an organization's Active Directory infrastructure and existing Microsoft toolsets. The result is lower total cost of ownership for UNIX platforms. Some AD bridge products extend Windows Kerberos SSO to applications (e.g., SAP enterprise resource planning [ERP], Tomcat, and WebSphere) hosted on UNIX servers. AD bridge products also provide a single identity (including password) for UNIX and Windows platforms, and provide Kerberos SSO to Microsoft applications (e.g., network fileshares, Internet Information Services [IIS], SharePoint)."

A number of non-AD bridge options provide the basic functionality of integrating a Unix, Linux, or Mac OS X operating system with AD, including offerings from Sun, Apple, IBM and several Linux distributions. These vendors include basic Kerberos/LDAP agents that execute the "join" of non-Windows systems to AD. However these "commodity" solutions lack enterprise-level functionality—such as extending AD Group Policy, audit, and management capabilities—nor can they consistently deploy the solution across multiple operating systems. These capabilities separate the true AD bridge solutions from the rest.

The range of management features offered by the various AD bridge vendors varies widely. The major business benefits AD bridge users should expect from their solution include:

- **Efficiency** – When the net number of identities in an enterprise shrinks, a single AD-based identity administration task can be extended to the entire population of Unix, Linux, and Mac OS X systems and users.
- **Security** – Extending the Kerberos authentication, strong password policy, and access control principles of AD to Unix, Linux, and Mac OS X strengthens security.
- **Compliance** – Because NIS can be eliminated in favor of a more secure directory and authentication mechanism, security can be improved and managed centrally for Windows, Unix, Linux, and Mac OS X, making compliance with internal policies and external regulations easier.

Source: "Active Directory Bridge Products: Getting More Value from the Windows Infrastructure," Identity and Privacy Strategies In-Depth Research Report; Jan 07, 2009 #126536

Our Authentication Services solution provides immediate relief for password and NIS issues as well as improves your organization's long-term compliance posture. This solution uses open architecture, standards, and proven execution to achieve both immediate and long-term compliance goals.

The 12 critical questions you need to ask when chosing an AD bridge solution

Organizations evaluating AD bridge technologies have an extremely important decision ahead of them. To ensure maximum benefit from the solution, you must carefully evaluate your requirements, as well as your present and future IT environment. You also must identify your strategies, possible obstacles, and goals for the technology.

With that in mind, and using the experience of hundreds of real-world AD bridge deployments, here are some questions you should ask to help choose the right AD bridge solution for you and your organization.

Compliance

How will the AD bridge solution help me address my specific compliance concerns?

Compliance is the main driver behind many AD bridge evaluations. But the ability of solutions to adequately address compliance concerns out of the box varies widely. It is vital to consider the tool's ability to help you solve a short-term problem, such as passing an upcoming audit. You must also evaluate its ability to help you maintain and improve compliance by making your organization "audit-proof."

Key compliance considerations include:

Password policy

- Does the AD bridge solution address your short-term Unix, Linux, Mac OS X password challenges?
- Does the solution provide a path to long-term password compliance?

NIS

- Does the solution address your immediate need to authenticate from AD instead of NIS?
- Does it provide a safe and controlled path to eliminating NIS entirely?

Strong authentication

- Does the AD bridge solution integrate with the two-factor authentication solutions you need to satisfy regulations (such as PCI DSS)?
- Does the two-factor solution complement or undermine the simplicity provided by the AD bridge solution for administration and standard authentication?

Privileged account management

- Does the AD bridge solution integrate seamlessly with a solution for Unix root delegation and auditing?

Auditing, alerting, and change tracking

- Does the AD bridge solution provide the depth and breadth of information that auditors demand of Unix information housed in AD
- Is that information easy to access?

The right AD bridge solution will deliver each of these needs without cumbersome third-party integration or custom workarounds.

Authentication Services can help you implement AD password policy on Unix and Linux systems in a matter of hours, and then systematically transition to the fully reconciled and unified single identity in AD.

Deployment

How quickly will the AD bridge solution help me achieve my immediate goals — without sacrificing my long-term ones?

More often than not, the driving force behind an evaluation of AD bridge technology is a compliance or security concern that must be addressed immediately (or at least before the next audit). Examples of short-term goals of AD bridge solutions include:

- Implementing AD password policy on Unix systems
- Overcoming delays in de-provisioning Unix accounts when users leave the organization
- Providing a more secure and compliant alternative to NIS authentication
- Single sign-on
- Implementing stronger access control on non-Windows systems

An AD bridge solution can provide rapid resolution of all of these issues. But be aware that the immediate pain relief created by the AD bridge solution may sacrifice your ability to achieve your ideal end-state. Some solutions can address specific pains rapidly, but fail to resolve the underlying cause of the pain—for example, unstructured and disjointed identities across a high number or Unix systems—and therefore do not provide a path to long-term compliance and security. Other solutions, including those that have proprietary architectures, obscure Unix identity data by storing it in non-standard "containers," or take a one-size-fits-all approach, failing to quickly provide even short-term benefits.

For example, suppose an organization has 200 Unix systems and each has its own /etc/passwd file. The ideal AD bridge solution would provide centralized authentication quickly for these local accounts without requiring any data import or migration tasks. The solution would also provide a clear path to identity consolidation if and when it makes sense. In contrast, less capable solutions ask organizations to first migrate all accounts into AD and a proprietary management console before the organization can get the full benefits from the AD bridge tool. Later, if the organization decides to consolidate accounts, it would be required to migrate the identities back from AD prior to identity reconciliation.

Smart organizations will select a solution that not only relieves immediate pains, but does so in a way that ensures on-going success and a path to the ideal end-state.

Has the AD bridge solution been proven in an environment that matches the scale, complexity, and diversity of my enterprise?

AD bridge technology is running successfully in some of the largest, most complex and demanding environments. However, here's a word of caution: no matter how impressive an AD bridge solution demo is, how interesting features appear, or how convenient the

Our Authentication Services service has been successfully deployed in some of the most complex and demanding environments, including those in Fortune 500 companies and large government agencies. Many One Identity customers had actually sought out Authentication Services after other AD bridge solutions failed to live up to their requirements.

solution seems, if it doesn't work in your environment, it isn't worth pursuing. Some AD bridge solutions work very well in controlled demos or limited proof-of-concepts, but fail when use must be expanded to production environments that are many times larger and more complex.

The very nature of bridging the gap between AD and Unix demands high performance across the entire environment. Because every environment is different, an AD bridge strategy that hides the underlying Unix complexity behind proprietary technology and obscured architecture may not scale to the level required for true benefit. An AD bridge can be a complex undertaking; for example, when multiple NIS maps, varying user and group parameters, and high numbers of diverse systems are involved. A "one size fits all" approach more often than not actually equates to "one size fits none." Flexibility, scalability, and options are critical to the success of any AD bridge solution.

Ask your AD bridge vendor to provide examples of real customers who have deployed their solution, then ask the following questions to ensure success:

- Are the reference customers' size, scope, and complexity similar to my organization?
- How many other customers also match my complexity and size requirements?
- How many of those customers are fully deployed and running in production?

Then contact the referenced customers and ask them the following:

- Are your solutions fully deployed and running in production?
- What obstacles did you confront during deployment?
- Are the AD bridge solution and vendor delivering on their promises?

Auditing

After integrating Unix with AD, how will the solution enable me to "prove" I have control over the Unix data stored in AD?

Compliance is perhaps the biggest driver influencing the growth of the AD bridge market. Unfortunately, uniting Unix, Linux, and Mac OS X systems with AD is only half the compliance battle. Most organizations not only need to "become" complaint through the use of AD bridge technology, they must also be able to continually "prove" that compliance. Many key pieces of information are notoriously difficult to gather and interpret natively in Unix —and the same information is often obscured behind proprietary architecture and closed auditing tools in some AD bridge solutions.

For example, if an organization uses AD to control user access to specific Unix systems, how can the organization know when an AD administrator makes a change to this access? The ideal solution would send an alert when a change is made to the access control policy. It would also alert Unix administrators whenever someone changes the AD-housed

Authentication Services includes a full-featured, targeted version of ChangeAuditor that is optimized for the specific needs of AD bridge users.

value of a user's Unix shell or home directory. Organizations looking at AD bridge technology should ask whether the out-of-the-box solution can audit and track these types of events, and provide a full history of who made the change and when. They should also ask: does this solution provide this level of visibility and alerting across all of the Unix and AD information that is relevant to our compliance and security initiatives?

Management

How flexible and powerful is the AD bridge solution's management interface?

Most AD bridge solutions offer a broad range of capabilities, but all too often these capabilities are accessed through a mismatched set of processes and tools. Some solutions boast powerful Windows-based consoles that consolidate administration centrally. But what if an organization wants to administer the solution from Unix, or remotely? Some tools require the use of the Unix command line for some tasks, while others require some tasks to be performed from the Windows console—failing to accommodate administrators who prefer to work from the command line. Finally, and perhaps most importantly, the administrative interface for some tools is so solution-specific that tasks like managing local Unix users and groups must still be performed independently of the AD bridge technology.

Organizations looking at AD bridge technologies should consider the value of administrative interfaces designed with their needs in mind. Again, flexibility is the key; maximum interface and functionality flexibility delivers the quickest and longest lasting benefits. The ideal solution would include a wide variety of management options and interfaces, including the following:

- Unix command-line interface tools
- PowerShell cmdlets
- Win32 applications
- A multi-platform, multi-browser Web console

Reporting

How well does the AD bridge solution report on vital information in my environment?

Authenticating non-Windows systems through AD is only half of the AD bridge battle. Most organizations find that the accessibility of critical information on those newly-integrated systems is just as important as the actual integration itself. The right AD bridge solution should include: easy access to all of the data required to migrate to the AD bridge, the ability to manage non-Windows identities and activities within AD, as well as the ability to prove compliance of those identities and access. In addition, the right solution will provide visibility into both local Unix information and Unix information stored in AD. The following are some examples of the data that should be included in comprehensive reports:

- Local Unix accounts
- Unix-enabled AD users and groups

Authentication Services gives administrators their choice of OS and browser. It even provides centralized management of local Unix users and groups from the same browser- and OS-agnostic console that is used to administer the AD bridge functionality. AD bridge vendors provide base functionality, but only One Identity delivers the enterprise-level management interface that ensures maximum benefit from the investment.

- System readiness for the move to the AD bridge solution
- Which local accounts have been secured with AD authentication and which have not
- Which AD user can log into which Unix host
- The specific Unix host that specific users have been granted rights to

Important Authentication Services reports include:

Report name	Report description
Unix Host Migration Planning	Provides a snapshot of the readiness of each host to integrate with Active Directory. This report is best used for planning and monitoring the readiness of each host to track progress of projects.
Unix Host Profiles	Provides a summary of the information about each host gathered while profiling the hosts.
Unix Computers in Active Directory	Displays all Unix computers in Active Directory in the requested scope.
Local Unix Users	Reports on all users on all Unix systems, or the Unix systems where a specified user account exists in /etc/passwd.
Local Unix User Conflicts	Identifies local user accounts that would conflict with a specified user name and UID on other hosts. This report is useful for planning user consolidation projects across Unix systems.
Local Unix Users with AD Login	Identifies which local Unix accounts are required to use Active Directory credentials for login to the host.
Unix-enabled AD Users	Displays all Active Directory users that have Unix user attributes.
AD User Conflicts	Displays all users with Unix UID numbers that are assigned to other Unix-enabled user accounts.
Local Unix Groups	Identifies the hosts where a specified group exists in /etc/group.
Unix-enabled AD Groups	Displays all Active Directory groups that have Unix group attributes.
AD Group Conflicts	Displays all groups with Unix GID numbers that are assigned to other Unix enabled groups.
Login Policy for AD User	Identifies the Unix systems where one or more AD users have been granted login permissions.
Login Policy for Unix Host	Identifies the AD users that have been granted login permissions for one or more Unix systems.

AD bridge vendors provide base functionality, but only One Identity delivers the enterprise-level management interface that ensures maximum benefit from the investment.

Group policy

How powerfully will the AD bridge solution leverage Group Policy for Unix, Linux, and Mac OS X?

Many organizations have discovered that significant benefits can be achieved when an AD bridge solution has the power to extend Group Policy to Unix, Linux, and Mac OS X. The ideal AD bridge solution will not only extend Windows Group Policy to the entire range of supported platforms, but will do it in a manner that both mimics the elegance of Group Policy in AD and doesn't discount the unique requirements of Unix, Linux, and Mac OS X platforms.

To achieve these capabilities, AD bridge vendors have used two prevailing strategies:

- **ADM templates** – This is the easier option. ADM templates enable the AD bridge vendor to easily deliver high numbers of pre-built policies with the solution. However, because all Group Policies must fit into pre-defined formats and a limited UI, solutions that take this approach lack the flexibility to take full advantage of Group Policy on non-Windows systems.
- **Client-side extensions (CSE)** – This is the preferred option. CSE provides maximum flexibility through a much more robust user interface, which translates to more scalability and powerfully customizable policies (for example, scripting and file copying). With the CSE strategy, organizations find they can easily complete tasks that were once considered difficult or impossible by using Group Policy.

Organizations evaluating AD bridge technologies should ask themselves whether the ADM template approach is good enough (and whether the delivered pre-built policies will achieve desired results), or whether the CSE approach will more closely match their objectives and performance expectations.

Application integration

Do I need single sign-on for systems beyond Unix, Linux, and Mac OS X?

As we have seen, AD bridge solutions extend Active Directory's Kerberos authentication and single sign-on to Unix, Linux, and Mac OS X. But Kerberos is the ideal single sign-on technology, and Active Directory is a widely deployed and practical Kerberos implementation, so it is only natural for AD bridge users to want to extend Kerberos single sign-on beyond the Unix, Linux, and Mac OS X operating systems.

Any organization evaluating an AD bridge solution would be well served to ask, "What else in my environment would benefit from Kerberos single sign-on?" Some systems and applications support standards that make it possible to extend AD/Kerberos (or "true") single sign-on, while others simply are not equipped for the true SSO scenario. While achieving enterprise-wide true SSO is impossible for most organizations, the benefits of implementing Kerberos for as much of the enterprise as possible are very compelling.

The ideal solution would provide the immediate relief of AD authentication for Unix access while also providing a clear and safe path to full migration from NIS.

Wise AD bridge evaluators will thoroughly assess the ability of each solution to support SSO on the desired platforms. Moreover, understanding the way in which the solution achieves single sign-on is equally important. For example, the best solutions provide single sign-on for Java applications through a portable Java Kerberos implementation, while others require an underlying implementation of Kerberos for Java support.

Finally, organizations should also consider the systems that cannot "join" AD for single sign-on. Does the AD bridge vendor provide a means to include them in an AD-based enterprise single sign-on scenario, or must the evaluator turn to third-parties for SSO for the rest of the enterprise?

Active Directory

What effect does the AD bridge solution have on Active Directory?

AD plays an important role in organizations that are considering AD bridge solutions, and, for this reason, a clear understanding of how the solution impacts AD is prudent. Prior to Windows Server 2008 R2, Unix attributes (the five characteristics defined by the RFC 2307 standard) had to live somewhere in AD. This meant either using a schema extension, which has low impact on AD, or placing the attributes in an obscured "container" stored elsewhere in AD (usually in a Service Connection Point). This container would add hundreds, or even thousands, of new objects to AD. However, more modern versions of AD include the RFC 2307 schema definition, which eliminates the need for the schema extension. Microsoft added RFC 2307 to AD in response to the quickly growing population of its customers that were adopting AD bridge technologies.

Organizations evaluating AD bridge technologies should carefully consider the impact the solutions have on AD. Leveraging the standard AD schema produces higher performance, simpler management, and, most importantly, a path to the ideal end-state. But many organizations prefer to implement the solution in a "schema-less" mode. Therefore, the best solution will provide the flexibility to do both. Organizations should also carefully consider the impact of storing transitory data in AD, requiring that all Unix data first be migrated into AD. This data would then need to be migrated back out if an identity reconciliation project arises in the future. The right solution will enable AD bridge users to manage and secure Unix data in its current location, enabling them to rationalize and import data just once.

In addition, the AD bridge solution should support Windows Server 2008 features such as AES encryption, read-only domain controllers, and fine-grained password policies. The solution should also support the most demanding AD topologies, such as two-way trusts, one-way trusts, non-way trust, multiple forests, and more.

Authentication Services provides organizations running Mac OS X with a powerful Group Policy management console. Users can also control every setting and preference on the Mac OS X desktop centrally with the elegant CSE approach.

NIS

How will the AD bridge solution help me resolve my NIS issues?

Overcoming the compliance and security deficiencies of NIS is often the primary driver for companies looking at AD bridge technologies. But often these companies face the dilemma of addressing the immediate, short-term NIS pain or making a fundamental shift that eliminates the problem altogether. The correct choice would probably be to go for both. Immediate relief can be found by implementing AD-based authentication for Unix and Linux systems, but long-term viability demands a complete migration from NIS and reconciliation of NIS data and structure with the AD identity namespace.

The ideal solution would provide the immediate relief of AD authentication for Unix access while also providing a clear and safe path to full migration from NIS. The solution should include tools that help reconcile NIS data with AD, migrate the data, and ultimately move the organization away from NIS entirely. Migrating from NIS to AD is not a simple "flip-of-the-switch"; it requires planning, time, and maintaining synchronization between NIS data and AD data during the transition.

Organizations looking to AD bridge technology as a means to migrate away from NIS should ask the following questions:

- What do I need to address with NIS in the short term?
- Does the AD bridge solution allow me to do it in the timeframe I require?
- What impact does that strategy have on my long-term plans?
- Has that strategy been successful with other organizations of similar size and complexity?
- What is my ultimate goal? Would I like to migrate from NIS entirely?
- Does the AD bridge solution provide the tools necessary to achieve that goal?
- Can the vendor provide examples of customers who've done that?

Strong authentication

Does the AD bridge solution support my strong authentication needs?

Many organizations are being pushed to implement strong authentication, such as one-time password tokens or smart cards, in response to regulatory demands (for example, PCI DSS). While Kerberos authentication is a dramatic improvement over traditional Unix authentication, the advantages of a second factor are compelling. For this reason, AD bridge vendors offer varying levels of support for strong authentication.

The right AD bridge solution will support strong authentication for every platform that can be integrated with AD. In addition, the solution will enable users to select the most affordable and flexible strong authentication option without cumbersome third-party offerings. It should

also enable the administration of strong authentication through the AD bridge solution's existing management interfaces and principles.

Vendor strength

What is the long-term viability of my AD bridgevendor?

With AD bridge technologies playing such a vital role in many organizations' ongoing identify and access management (IAM) strategies, it is imperative that the provider of the technology can assure the evaluator of its long-term viability and commitment to the AD bridge space.

Identity and access management

Does the AD bridge solution support my other identity and access management initiatives?

AD bridge technologies have quickly grown to be critical components of many organization's enterprise identity and access management strategies. But AD bridge cannot do it all, and smart organizations will look to leverage the AD bridge, as well as their AD bridge vendor, beyond joining non-Windows systems to AD. Common identity and access management projects that can benefit from AD bridge technology, as well as the questions to ask, include:

- **Single sign-on** – Does the AD bridge vendor address single sign-on beyond those systems that can be "joined" to AD?
- **Account Set-up** – Does the AD bridge solution integrate with an AD account management solution to automate tedious and non-secure practices on Unix, Linux, and Mac OS X? Is the AD account management solution available from the same vendor?
- **Strong authentication** – Does the AD bridge vendor offer strong authentication? And how tightly is strong authentication integrated with the AD bridge solution?
- **Privileged account management** – Does the AD bridge solution integrate with a Unix root delegation and auditing solution, and how tightly are they integrated? Are users required to run the AD bridge solution to use Unix root delegation, or can it run independently of the AD bridge solution? Finally, does the AD bridge solution also integrate with other key components of a full privileged account management strategy such as password vault, sudo, and session audit solutions? Are those solutions also available from the same vendor?
- **Password management** – Does the AD bridge solution integrate with a password policy definition and enforcement tool? Does it integrate with a self-service password reset solution? Are those tools available from the same vendor as the AD bridge solution?
- **Auditing** – Does the AD bridge solution include auditing, alerting, and change tracking capabilities that enable you to get all the information you need in a convenient, centralized location? Does the AD bridge vendor offer audit tools that provide similar information for other system in your enterprise?
- **IAM frameworks** – How does the AD bridge solution integrate with an IAM framework? Has the vendor had success simplifying a framework deployment with its AD bridge solution?

Smart evaluators of AD bridge solutions will carefully consider the solution's place in their larger IAM initiatives and look for opportunities to consolidate tools, vendors, and functionality through the inherent advantages of AD bridge technologies.

Conclusion

Active Directory bridge technology is no longer the realm of risk-taking innovators. It has grown into a vital, irreplaceable component of many organizations' identity and access management strategy. With this growth, several solutions have emerged on the market, prompting those evaluating AD bridge technologies to carefully consider a number of questions before choosing the right solution for them. These questions include evaluating the vendor's strength and proven real-world success, along with the solution's technical excellence and architectural purity. In short, the question is: "Does the AD bridge solution I'm selecting solve my immediate problems, give me a clear path to long-term success, and offer the flexibility, scope, and power to help me reach my objectives?"

Authentication Services, a major component of One Identity Solutions, is the only solution

that can answer "yes" to all of these questions.

Use the worksheet below to determine which AD bridge vendor best suits your needs:

Report name	One Identity	Vendor 2	Vendor 3	Vendor 4	NA
Deployment					
Auditing					
Management					
Reporting					
Group Policy					
Application integration					
Active Directory					
NIS					
Strong authentication					
Vendor strength					
Identity and access management					

Authentication Services from One Identity offers SAP-certified single sign-on for SAP GUI applications hosted on Unix or Linux. It also offers Kerberos single sign-on for Siebel, DB2, PuTTY, SSHD, and Apache, as well as for any application that is Kerberos-enabled, LDAP-aware, or supports pluggable authentication modules (PAM). Single Sign-on for Java from One Identity delivers similar Kerberos single sign-on for Java applications. This technology has also been adopted to extend Kerberos SSO to BlackBerry Enterprise Server and commercial solutions from Adobe, SAP, and Jive Software.

For More Information

About One Identity

The One Identity family of identity and access management (IAM) solutions, offers IAM for the real world including business-centric, modular and integrated, and future-ready solutions for identity governance, access management, and privileged management.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (**www.oneidentity.com**) for regional and international office information.

ONE IDENTITY