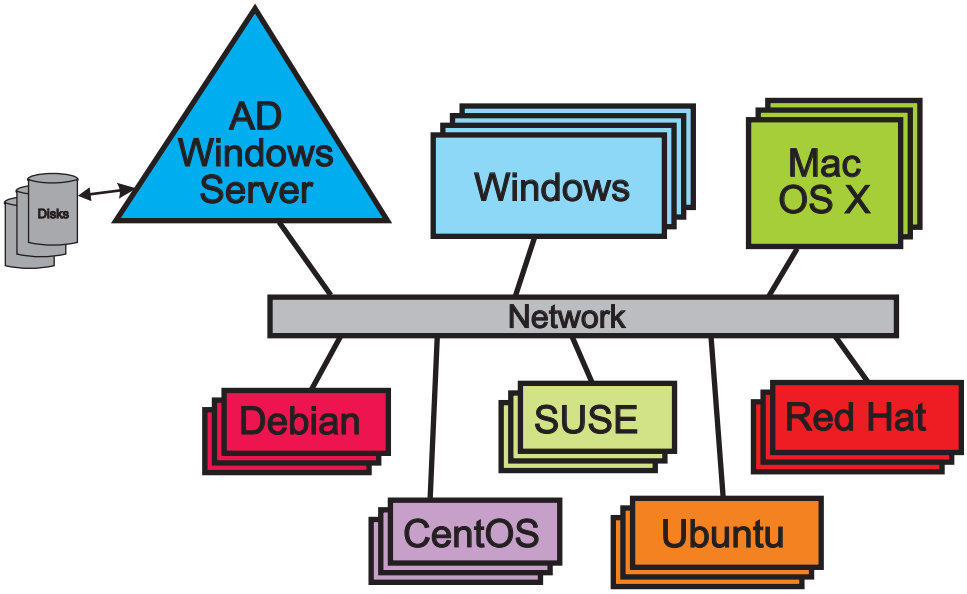
Comparing Free Active Directory Integration Offerings for Linux Systems

by Rodney Ruddock, Interop Systems



EXECUTIVE SUMMARY

Comparing the three different free products and evaluating them for effort to install, effort to maintain/manage and features offered can consume a lot of administrator's time. The interesting part of the evaluation comes from the differences among these three free offerings. This is also what helps you justify your final choice to yourself, fellow committee members and your management.

The free winbind offering is not a good choice given the high overhead for installing, maintaining and managing it. With the ease and additional capabilities of the other two products the winbind offering is not a top level player in this game.

Between the Centrify Express and Likewise Open products a quick glance at the basic capabilities shows similarities. But Centrify Express shows a marked difference in several areas that result in it pulling significantly ahead in the race because Likewise Open lacks these additional features: Samba integration, more login styles, pre-install verifications, extended management, centralized installation for multiple platforms, secure OS integration and more Kerberos enabled tools.

After exhaustive testing, and reviewing the results with the free products this makes the Executive Decision very clear: The freely available Centrify Express has more of the features you need with the comforting maturity from its commercial lineage.

July, 2010

Comparing Active Directory Integration for Unix & Linux Systems

by Rodney Ruddock, Interop Systems

Introduction

Many, if not most, IT environments are a mixture of heterogeneous computer operating systems. This means a mixture of Windows, Linux, Unix and Mac systems. Users naturally want and expect the ability to move as seamlessly as possible amongst all of these machines. With different login controls and security measures amongst the different operating systems this expectation is not automatically delivered. One approach is to unify login controls and security measures under Active Directory.

Today there are several software suites available, both free and commercial, to bring heterogeneous computing environments under Active Directory. In this paper we are going to examine, test and compare a few of the freely available suites to do this. The three software suites under examination are Centrify Express, Likewise Open and Samba's winbind.

Technical Background

When approaching a technical task such as unifying many heterogeneous operating systems (OS's) it is worth a brief review of the technical factors involved. Knowing some of these basic facts can help in the decision process for choosing a solution as well as preparing for, implementing and managing the solution. The time spent reviewing these technical factors should help make your decision better, faster and more reasoned. It should also help avoid problems.

Under Review

There are three products under review:

- Centrify Express 4.4.1
- Likewise Open 6.0
- winbind 3.5.4

For integrating Unix systems into an Active Directory domain.

Executive Summary: Cover
Complete Summary: Page 11

Active Directory (AD)

When Windows NT was released back in the early 1990's one of the design goals was a large network of machines being used by a large number of users. This included both the machines and the users being grouped into different tasks and needing an overall security control. Active Directory, or AD as it is regularly referred to, is Microsoft's solution. This solution was not created from scratch. AD is based on academic research that has been proven and tested and that have become standards. Microsoft's approach with AD was to unify several of these standards together to make it easier and more to secure to manage a network of computers. The major key components of Active Directory are Kerberos, LDAP and DNS.

Kerberos is used for authentication of computers (or nodes or clients) and users. This is done by securely communicating computer and user credentials over the network using

encryption to the server. The credentials are secret keys that are only known between the server and the clients. Users authenticate to a server from an already authenticated client. Once authentication is successful the Kerberos server issues a ticket. Each ticket contains specific information that identifies the computer or user, how long the ticket is valid for, the trust relationship of the ticket, etc. When the Kerberos server cannot be contacted then authentication is not possible, but Microsoft has extended the authentication to allow for caching locally on the client in this situation.

LDAP, or Lightweight Directory Access Protocol, provides directory services over the network. While Kerberos authenticates users and client machines, it is LDAP that stores and provides the information about users, machines and other topics. While on Unix systems LDAP is usually treated as a separate component, with Windows it is integrated into Active Directory to such an extent that Windows administrators rarely distinguish that this is the methodology for working with this information.

While Active Directory can stand alone in an isolated sense, connecting to the wider world necessitates DNS reaching outside of the Windows domain to other DNS sites to get or give resource information. While it is a major component to the structure of Active Directory it is usually regarded as a separate entity from Active Directory (unlike LDAP). The AD DNS information being correct is critical for the Windows domain served by AD to behave as expected. Often incorrect DNS information, or DNS information being obtained from another DNS resource than AD, will result in peculiar and/or confusing behavior for computers and users associated with the AD domain.

Unix User Information

Originally Unix user and group information was controlled individually on each machine without any structured sharing of information with others. It was the responsibility of the administrator to duplicate information across the different machines. This was not a difficult burden in the beginning because sites did not have many machines. However, as the norm changed to have one (or more) machines at every desk this became too much of a burden for administrators. Since very early on the use of DNS has been integral with Unix systems.

Network Information Service, or NIS, was the first Unix method for unifying user and computer information for a network of computers. In fact this orientation towards the network underlay the motto for the creator of NIS (“The network is the computer”). NIS created a central repository of user and group information for computers to reference. While useful, concerns about security and the need for other centrally controlled information has seen NIS eclipsed by NIS+, Kerberos and LDAP. While NIS+ is more secure and does provide more centrally available information, Sun Microsystems recommended installations migrate to Kerberos and LDAP methods several years ago.

Current methods for managing networks of Unix systems centers around the use of Kerberos, LDAP and DNS. Traditional local user and group information controls are still available to each machine. Both Kerberos and LDAP tend to be treated in a somewhat separate manner with Unix networks. DNS has always been treated with a network orientation with Unix networks and little has had to change in this regard for Unix administrators.

Kerberos on Unix networks is the same standard used with Windows networks. Kerberos was developed at MIT as a secure method of authenticating users and computers over non-secure networks. While this research was conducted on Unix systems many people are surprised to learn that Microsoft was one of the funding partners for this research. While there are a few different implementations of Kerberos all adhere to a standard allowing interoperability.

Heterogeneous Networks

Early networks of heterogeneous computer systems had interoperability fractured to like systems or had specialty software and/or special administration to improve shared information. As evident from the descriptions above, both Windows and Unix systems have moved towards nearly identical methods of managing many machines on a network. However, the final hurtles for complete interoperability of user, computer and other information is not automatic. Some of the suites of software that close these final hurtles are what this paper examines.

Preparations

Under examination are three products: Centrify Express, Likewise Open and winbind. These three have been chosen because they offer the ability to unify the administration of machines with a heterogeneous mix and are, costwise, freely available. While Centrify Express and Likewise Open both are derived from commercial companies, winbind comes from the F/OSS group

Which OS's can be used?

Which Operating Systems can be used is divided into two groups: Windows machines and Unix machines.

Windows machines for these interactions need to be Server systems. Support starts at Windows Server 2000 through Windows Server 2008/R2. If you are about to begin placing Unix machines under the AD umbrella then the most recent release is the best initial idea as you work out planning the job. Going with a Server older then Server 2003/R2 will not be helpful to your long term administrative planning. However, you must of course remember your Windows workstations. If you are accessing NFS filesystems on Unix systems from Windows systems with the Windows Server providing UID/GID information for the NFS communications you must be aware that older XP systems will need to work with Server 2003/R2 not using RFC 2307 while Windows 7 must use a server using RFC 2307.

The number of different Unix systems is large. This includes Solaris, HP/UX, AIX, Linux by many different names, Apple, BSD, etc. each of which has several different releases. While a particular release may not be supported, updating to a newer release will likely solve the problem of your particular system being supported. That stated, it is easier to conclude that for winbind there are very few system that it cannot be built for. Both Centrify and Likewise provide binary ready packages that will reduce your effort and lower your frustration levels. Both provide current OS listings on their web sites and cover the major OS's used in business environments such as Solaris, AIX, HP/UX, SUSE, Red Hat, Ubuntu and virtualization environments like Xen and VMware. If your Unix OS is not listed then send some e-mail to check since demand often dictates which OS gets supported.

Samba. While similar with their intended results there are difference amongst the products. All attempts will be made to make “level playing field” comparisons to help keep the discussions clear.

Most administrators want to try and test software before deploying for their entire network. Naturally this involves creating test machines and test information. This same approach was taken for the testing of these products. A Windows 2008 server was prepared and duplicated cleanly for each product test. In this manner no installation or configuration will interfere with another product, and every product gets an equal start. After some planning and some testing the Windows 2008 server was given it's own domain (without any trusts), a sub-block of network addresses provided for this domain (no other systems had information about these addresses or machine names) and a set of test users. Computers would be added to the domain during the installation and/or use of the products being tested. Correctly preparing the Windows Server domain is important for the successful installation and functioning of the products. In particular the preparation of the DNS information is important. If a Unix or Linux system is installed using a machine name that is duplicated in the real DNS and the test DNS then name resolution problems can happen that may be difficult to rectify. Preparing the firewall on the test server is also important so that the correct ports are open.

Centrify Express comes with a pre-check program named "adcheck" that can be run stand-alone or as part of the Centrify Express installation. For Centrify, passing all of the checks with the adcheck program is important because it tests and verifies (from the Unix machine) that joining the domain will work successfully. It gives a report of the diagnostics check while it's running. It checks a number of things including ports being open, DNS contact, etc. and reports problems when encountered so you can address them. Likewise Open and winbind do not come with a similar pre-check program. Getting your network environment is important when you are planning installations on many Unix systems.

Installing the Products

We'll address each product installation without cross-reference to the other products. The assumption is that a Unix or Unix like system (the client) has already been installed. The chief component of the products is installed on the client. An Ubuntu system and a Red Hat system were the initial client choices. All documentation provided with the software products was read before to ensure installations proceeded as smoothly as possible. The 'sudo' command was used extensively for the installations so you should, if not already, be familiar with it.

Centrify Express

The software came as a 'tgz' file that was extracted into a directory. The expanded files included the important “install-express.sh” file along with PDF documentation. The documentation provided gave detailed step-by-step actions and expected results. The documentation also has troubleshooting information too.

The installation proceeded as per the documentation without any surprises. The installation could have been done without reading the documentation by most

administrators experienced with Windows and Unix-like systems. The default answers offered with each question provided the best course of action. Part of the installation process is to run Centrify's adcheck to ensure your environment is correct configured. This will save time over verifying this manually.

After re-booting we were able to login to the test systems still as a local user and as a user in our Windows test domain without a difficulty. No additional editing of configuration files was needed.

Likewise Open

The software came as a single executable file. Documentation is separate at the Likewise website. Using 'sudo' to execute the file directly started the installation.

The installation proceeded as per the documentation without any surprises. The installation could have been done without reading the documentation by most administrators experienced with Windows and Unix-like systems. There is not an automated pre-check program with Likewise but it does provide a 20-point checklist for you to manually check. When installing on multiple systems this could get very time consuming.

After re-booting we were able to login to the test systems still as a local user and as a user in our Windows test domain without a difficulty. No additional editing of configuration files was needed.

Winbind

The installation of Winbind requires several major steps and does not install with a short set of questions with default answers to select. For a Unix or Linux system you will need to have the packages for Kerberos, Winbind and Samba plus several others. Many of the default OS installations come with these packages already installed or just needing some configuration for working with Active Directory. For example, with Ubuntu the ntp (Network Time Protocol) and winbind packages are already installed. Were these packages not already installed then they can easily be added using the packaging system appropriate to the system (e.g. apt with Ubuntu). Once each of the required packages are installed then configuration can begin.

Configuration consists of a long list of relatively non-complex tasks that most experienced administrators can handle. Very detailed information is available through OS websites, the Samba website and other web pages. Overall the tasks required include setting NTP, running the Kerberos configuration, testing the configuration, setting DNS to the AD server, configuring the SMB file, restarting the winbind and samba daemons, joining the machine to AD, configuring user authentication order and creating home directories locally for users. It is usually a good idea to perform additional tests after each task so any problem can be closely associated with a particular task since a mis-configuration of any one will result in the machine not being allowed to join the domain or a user not getting authenticated. A user not being authenticated will take a fair amount of time to determine the cause because, for security purposes, telling too much information is not security-wise. As mentioned earlier there is no tool for checking

your environment configuration so it will need to be done manually.

The on-line documentation, depending on your client system, often includes some help for troubleshooting when the configuration doesn't work correctly.

Installation Summary

Overall the installations seemed very clear and straightforward for the two products provided by the commercial vendors. If you do encounter problems then it is most likely due to your test (or real) domain not being correctly prepared (usually related to DNS). The differences between these two products for questions and selection choices during installation are not significant enough to cause a great discussion. The installation of winbind (and related packages) is much more involved and time consuming with more locations to mis-configure something. However, after doing one installation successfully for your network additional installations should be repeatable in an almost identical fashion although time consuming.

Installation	**Centrify Express**	**Likewise Open**	**Winbind**
Number of steps	Few	Few	Many
Complexity	Low	Low	High
Troubleshooting	Good	Good	Poor

For these freely available products, the installations described above are for one machine at a time. With Centrify there is an additional free product, DirectManage Express, that can be installed on the Windows server. With this product you can automate the installation from the server to one or more client machines. This can save you the footwork of physically visiting each machine for an installation. DirectManage Express also runs the Centrify adcheck to verify before an installation just as you can do with each individual Centrify Express installation.

Simple Task Evaluations

With all of the products the normal controls available with Active Directory are still available. Because AD controls the authentication of a user separate from information about the user, the time of day restrictions, password expiration time, etc. will work the same for a Windows client as well as a non-Windows client. For many sites this amount of control is sufficient enough to meet their requirements because it matches the control available with Windows.

The User Experience

While administrators are responsible for getting the Unix machines integrated into AD, the people using the machines are the ones who will (or won't) provide feedback to the administrator about how well the integration experience is or is not. Which software packages are installed is up to the individual site and user experience really happens once a user is logged in. For the purposes of the integration software it is the login experience: at the console and with a remote connection (such as ssh). Logging onto a

Logon Styles	Centrify Express	Likewise Open	Winbind
DOMAIN\USER	Yes	Yes	Yes
USER@DOMAIN	Yes	Yes	Maybe
Default Domain	Yes	Yes	Yes (if configured)
DOMAIN+USER	Yes	No (by Default)	Maybe (if configured)
Unix Name	Yes	No	No
Display Name	Yes	No	No
Cache Credentials	Yes	Yes	No
Single Sign-on	Yes	Yes	No

Windows machine a user can specify the domain and user in the format “DOMAIN\USER” or the newer format of “USER@DOMAIN”. A default domain may also be assumed requiring just the username. Among the choices available, Centrify Express allows for the most flexibility with the larger number of logon styles permitted. This helps reduce the amount of typing a user has to do (a strong Unix trait for many years) and a less complex logon reduces account lockouts when users make typos or are guessing at more complex styles.

One of the complexities of a user account under Active Directory is the cobbling together of all group information. AD groups can be members of other groups and those groups can be members of yet more groups and so on. The cascading complexity can add a lot of overhead when an account is properly being generated after the login has been authenticated. At "simple" sites this overhead, or the difference in overhead between these freely available products, may not worry you. But testing this is essential so that all users have a good experience. This will mean creating test accounts that have many groups (cascading) plus other overheads. This is a moving target as competitors vie to be the best with new product releases. At the time of our testing Centrify Express has the edge.

Users remotely connecting to one of the client machines from the command line of another Unix system will have to use two backslashes (“\\”) since a backslash is an escape in a shell. It's better to use one of the other formats since it requires less explanation to users and will reduce login errors. The “DOMAIN+USER” format is what Microsoft uses with SUA.

The single sign-on (SSO) capability allows the authentication of a user on one machine to be extended to other machines within the same domain using the Kerberos ticket from the login authentication. The ticket is provided between domain clients with the domain server verifying the ticket as valid. This differs from a public key exchange between two systems used by some software. This can be used with software that is Kerberos-aware.

Large Deployment

Testing and deploying on a single machine is not an onerous job. Any mistakes made or actions missed are useful knowledge when the larger deployment for all Unix machines in your network happens. It can also provide you with time and effort estimates for the big deployment.

Installing and configuring winbind is the most time and effort consuming of all three products under review. Installing winbind over numerous machines will get tedious and operator errors are more likely to creep into the process. Either of the other two products will be better, faster and more accurate.

At a single machine installation test Centrify Express and Likewise Open provide easy installation with a few questions. Operator error is unlikely to happen as you move from machine to machine installing. However, Centrify does include a free deployment tool aptly named DirectManage Express. This tool can be installed on any Windows machine to control the deployment in an automated method so you don't have to move from machine to machine installing; it doesn't need to be installed on Windows server. DirectManage Express does a pre-check (similar to the adcheck tool) and allows you to specify in several different ways which machines to deploy the software on. Machine selection can be done by subnet, IP range or a special list file. As part of the pre-check a report on the targeted systems generates a potential to-do list for each target machine. All this information is kept in a local database. The tool also downloads the binaries matching the target machines so you don't need to determine this yourself. And, of course, the installation is pushed out automatically by a method of your choice (ssh, telnet, etc.). This will be a big time and effort saver when deploying to more than just a few machines on your network. Likewise Open doesn't have a similar tool.

Limitations

From a domain and network design viewpoint you will want to determine the number of BDCs needed to support the PDC so that all clients can have a good quality of service.

With Unix systems users and groups are identified by UID's and GID's respectively. Windows systems identify users and groups with SID's. With these free products the software installed on the Unix systems determines the UID's and GID's to be used independent of other Unix systems and independent of any AD information. An extra, non-free product from Likewise called the “UID-GID module” is available to use UID and GID information stored in AD. Centrify's full version, DirectControl, co-ordinates UID and GID information with AD.

Samba is regularly used on non-Windows machines to access Windows shared filesystems. The normal installation of Samba does not co-ordinate UID and GID generation with other programs such as Centrify and Likewise. Centrify has, freely available, a modified version of Samba so that UID and GID usage is co-ordinated. Further the Centrify-enhanced Samba permits the use of the existing Kerberos ticket (Single Sign-on done at logon) for authenticating the use of Windows filesystems. Likewise Open uses Likewise-CIFS instead of current versions of Samba meaning there can be operational difficulties if you do not use CIFS. While older versions of

Samba (3.0 to 3.2) interoperate with Likewise Open, Likewise seems to discourage this in favor of CIFS.

While these products successfully allow users already in Active Directory to login to the Unix systems, larger sites will already have a large database of users (i.e. file or LDAP) that will need to be integrated into AD. To integrate users and groups into AD you will have to create scripts or upgrade to a commercial product that will help you automate this task.

Upgrade Potentials

Integrating Unix-like systems under the control of Active Directory sometimes does not provide enough fine control. While for some small networks it is sufficient to group all of the machines under the same domain for user control, for others it is not. In these more complex environments Windows administrators will often create multiple domains and then allow (or not allow) trust relationships among these domains. It is possible to have the Unix-like systems integrate into this style of logical organization with commercial upgrades from Centrify and Likewise. There is no equivalent upgrade path with winbind.

Additional reasons for upgrading include, but are not limited to, improved auditing/compliance, UID/GID control, zone controls (by users and by machine system types).

While both Centrify's and Likewise's upgrade paths include Server resident software, particularly for UID and GID values plus other GEOS information, there are some differences. Centrify allows using AD's RFC 2307 (this is preferred), using Services for Unix (SFU) schema extension (good if you are using SFU on Server 2000 or 2003) or within an AD container (no schema extended). All the Centrify methods can have the data accessed from any tools using LDAP or ADSI queries. Likewise allows for schema mode (using AD's RFC2307) and non-schema mode (not using AD's RFC2307 but using RFC2307 keywords/attributes, usually with Server 2000). If you are migrating user data from a Unix LDAP then an RFC2307 path will be the clearest choice.

Likewise's upgrade path includes their UID-GID Module and Enterprise. The UID-GID module allows for consistent ID's to be issued through Active Directory for all of the client Unix machines. The Enterprise edition is extended to add a number of features including central management, a configuration wizard, UID/GID mapping and more group policy actions/controls. The Likewise website has a complete listing (URL in the reference section).

Centrify's upgrade path includes four possible upgrades. The reference section at the end lists the web page comparing all five products (Express, Standard, Enterprise, Platinum and Application). All of the upgrades include a core of upgrades such as more user auditing, more authorization/privilege management, UID/GID mapping control, zone control and rapid migration tools. Each upgrade has additional features (such as PKI certificate renewal with Platinum) so the web page is the best way to get a full comparison of everything available.

Product Support

Support for products during installation and during use grows in importance as the size of the supported set of machines under your administration. While grace is often given to administrators by users at smaller sites, this grace gets very slim at larger sites as more users become affected. So having technical support can provide a lot of confidence in the chosen product by yourself and your management.

Winbind has support through on-line technical manuals at the Samba website, through forums on the Internet and some Linux community web sites.

Likewise Open has support that can be purchased on a per incident basis (regular business hours), self-service support through a community forum and on-line documentation. The per incident support can be increased to 24x7 when Likewise Enterprise (the commercial version) is purchased.

Comparison Chart

You can find a product comparison chart on page 13 that summarizes important points. This chart can help you see how each product compares directly with the others.

Centrify Express support can be accessed through a community support forum and the extensive documentation that comes with it. For telephone or e-mail support you will need to upgrade to one of the commercial products which include the possibility 24x7 access as well as access to a knowledge base and more on-line documentation. Centrify has several support offices around the globe offering support in English, German and French.

If you do plan to upgrade to one of the commercial products you will want to investigate how well it can meet your requirements and what level of service is available such as hours available (does it match your time zone?), staff available, languages, response times, etc. You may want to ask if you can evaluate the support during your testing and evaluation.

Product Comparisons

The products discussed all naturally aim at the obvious target of allowing a user to login to a Unix system using Active Directory. And several other of their functions cover the same ground. Where products differ is often what helps make a decision about the choice for your site. A few of these differences have been discussed earlier. Here are some additional comparison points worth noting with more key points being highlighted in the table that follows.

One of the largest difference today between Centrify and Likewise is the SMB support. Centrify integrates with Samba while Likewise has built its own CIFS (SMB) software. Samba has been the de facto standard for Unix systems for a very long time so much that adding another filesystem product into your network of computers will need to be tested separately because there are many reports of Likewise Open not interoperating with current Samba (3.3 or later), older Samba (3.0 - 3.2) may work. Since Likewise

Open does not ship with Likewise-CIFS this can cause a operational gap for your network because, though freely available, Likewise's CIFS 5.4 (current) download page states "This preview version is intended for evaluation only..." and "...should not be used on systems where the data stored on the file server is critical". It seems very odd and confusing for CIFS to have this disclaimer considering current versions of Samba cannot be used and Likewise seems to promote using CIFS. Centrify Express, like Centrify Direct Control, works with Samba. Centrify has a free enhanced version of Samba that allows for Centrify and Samba to cooperate about UID/GID use and is extended so that Single Sign-on (SSO) can be used by Samba. That means the Kerberos ticket created for logon is seamlessly used for access to the Windows filesystems.

Centrify has more customers (2500+) listed on easy-to-find web pages. It was difficult to find identifiable customers on the Likewise site though there are several anonymous case studies. A recent Likewise webinar claims 380 customers. Likewise claims a very large number of "organizations" are using their products, but it is unclear how this was determined so you may need to be wary during number comparisons. It would be helpful for administrators to have all of the information as easily available as it is on the Centrify website instead of having to hunt around for hours to find similar Likewise information. Matching an existing customer with a vendor that closely resembles your situation, particularly if a white paper discussion is available, may alert you to a situation that needs to be addressed or help you scope your requirements..

Support is important in many different facets: availability, cost, response, language. Your requirements may lead you to decide that a commercial product with extensive support is the functionality and insurance you need. Even with the selection of a free product evaluating available commercial support and free support is good planning and preparation. Administrators often overlook the troubleshooting sections with installation documents. These sections are easy to find and, not surprisingly, cover the problems most often encountered even after installation. On-line documentation is also freely browsed for evaluation and community-based forums are also good to see which questions (and answers) have appeared. You may also want to ask a question or two in those forums with users who have product experience. If you are located in Europe or Asia (rather than the US) the different languages for support communications may play a role in your decision.

Summary

Having these three freely available products certainly helps administrators of small and large systems get started integrating user and computer resources under a single control (Active Directory). While winbind can get you started, the amount of time and effort restricts using it to one or two machines at most. Even with only one Unix system the greater ease of installation with Centrify Express and Likewise Open are better choices.

While both Centrify Express and Likewise Open allow Unix systems to be placed into an Active Directory domain they both are not as extensive as their commercial counterparts. Several of these points were discussed earlier in the Upgrade Potentials section. Those points may not be critical for a very small to small operation, but for

operations at medium size and larger those points are going to become more important particularly if you have audit compliance requirements or need more privilege control.

With the scope of freely available products it is worth heeding the advice of the Roman General Julius Caesar: “Experience is the teacher of all things.” Product testing in your environment before going to complete, network-wide usage will provide valuable experience. Further consider that you must test how products work in conjunction with other important software in your environment and not just in isolation.

Several points begin to separate the products beyond the core functionality of being able to login.

The important condition of Samba, for example, may provide much more weight to your final decision than initially thought (even if you upgrade to the commercial versions). With Likewise Open you will need to use Likewise CIFS so it can interact with the Windows filesystems shared to the network or downgrade your Samba to an older version (3.0 to 3.2). Centrify Express, like its commercial counterpart, includes an enhanced Samba without an additional cost. This means the same Samba configurations continue to work while getting a tighter integration with Active Directory (with the SSO capability added to Samba).

More secure, or hardened, computing environments must, by their nature, be less forgiving. Centrify Express works with SELinux and AppArmor. Likewise Open currently does not work with SELinux fully -- SELinux must be turned off or set to permissive which can defeat the purpose of having a more secure installation.

The amount of time to create a proper login depends largely on the number of groups a user has membership. This cascades when those groups have membership in other groups. This creates a lot of communications overhead. With the newest Likewise Open, version 6.0, the length of time waiting for a login to complete has been significantly reduced from earlier versions. This brings Likewise a lot closer to the login speed that Centrify has had for quite a while. But even in environments with small group cascades Centrify maintains an edge.

The CentrifyManage Express provides additional capabilities that are just not offered with any part of Likewise Open. The ability to remotely install, update and manage all of the Unix systems joined to Active Directory is a boon to resource efficiency for every administrator.

Conclusion

The Open Source winbind from the Samba project is a nice tool to have when there are only one or two Unix systems to integrate into an Active Directory domain. However, even at this small number of systems installing and maintaining it is much higher than with the other two free offerings.

Centrify has been working in the Active Directory integration space the longest and has the most product maturity with Express deriving from DirectControl. Likewise Open is

Comparisons	Centrify Express	Likewise Open	Winbind
NTP sync	Auto	Auto	Manual
Hardened Linux	SELinux, AppArmor	No, must be off	Self build
Bit Support	32, 64	32, 64	32, 64
OS Platforms	13 OS, 225 versions	13 OS, 180 versions	N/A
Windows AD extended controls	Yes (with Express)	No (only with upgrade)	No
SMB Interop	Samba + with SSO (current & older vers)	Likewise-CIFS (+Samba 3.0-3.2 only)	Samba
PAM/NSS	Auto	Auto	Manual
Kerberos Putty	Yes, with SSO	Yes	No
Kerberos SSH	Yes (included)	No	No
Other Kerb. tools	Yes (ftp, telnet)	No	No
Windows Certification	Yes	No	No
Microsoft Partner	Yes	Yes	No
Product Maturity	Since 2005	Since 2008	Since Samba 2.2.2
Customer Base	2500+ customers with 250K+ systems, e.g. Microsoft, RIM, Adobe, Disney	380 customers with 20K+ systems, e.g. Gap, Omneon, Tecplot, NIH	no list
Support Offices	US, Europe, Asia	US	none
Upgrade Path	Yes (5 possibilities)	Yes (2 possibilities)	No
Regulatory reqs	Yes	Yes	none
Offline Authentication	Yes	Yes	No
Single Sign-On	Yes	Yes	No
Login Speed	Good	Good	Fair
Multiple/Cross Domains	Yes	Yes	No
Large Deployment tool	Yes	No	No
Precheck tool	Yes	No	No

Notes significant advantage

derived from Likewise Enterprise which has been around for a couple of years but definitely has less maturity though with the 6.0 release more is attained.

There are a collection of small and large differences between Centrify Express and Likewise Open that separate them in their race to gain more users. Many of the smaller differences are described in the tables earlier in the paper (login styles and comparisons). Alone each of these smaller difference may not burden your decision process too much, but accumulated together they make a significant weight that do tip the balance scales. The large differences, the Deployment Manager and Samba to name two, fully close the discussion. The additional ease for installation and management of Unix machines saves so much time, resources and administrative stress that these tools make the decision: Centrify Express.

Resources

Here are web site resources so you can access the free downloads, documentation and other things.

www.centrify.com/express
This is the start location for accessing the Centrify Express downloads, PDF documentation and on-line videos. There is also a details link to currently available binaries. A Centrify Community site is also has a link from here.

www.centrify.com/products/centrify-suite-editions.asp
Page showing all of the upgrade possibilities from Centrify Express.

www.likewise.com/products/likewise_open
This is the start location for accessing the Likewise Open downloads as well as links to information about available binaries and the Likewise Open OSS site.

www.likewise.com/products/likewise_open/comparing_enterprise_and_open.php
Page comparing Likewise Open versus Enterprise (the upgrade path).

www.samba.org/samba/docs/man/Samba-HOWTO-Collection/winbind.html
This is the HOW-TO documentation from Samba for how winbind works plus information about installing and configuring it.