One Identity Safeguard Authentication Services 6.0.1

Basic Authentication Walkthough Guide

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

Safeguard Authentication Services Basic Authentication Walkthough Guide
Updated - 12 September 2024, 17:23

For the most recent documents and product information, see Online product documentation.

Contents

Introduction **1**

Authenticating a password **2**

About us **8**

Contacting us 8

Technical support resources 8

Glossary **9**

1

Introduction

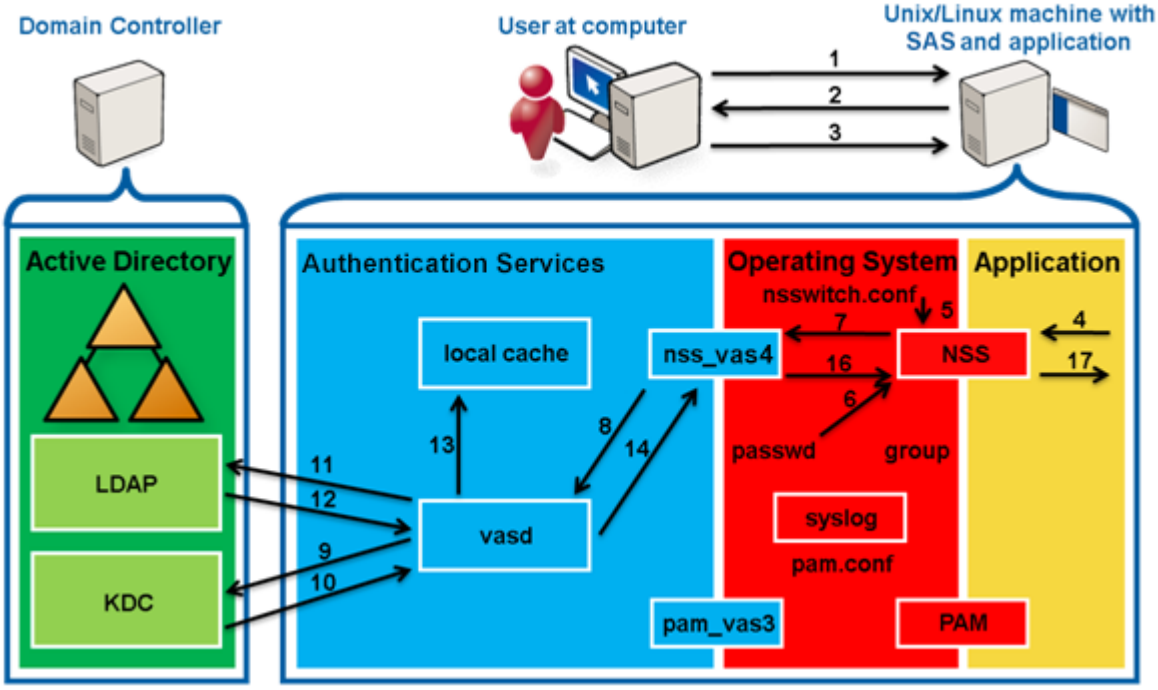
This document provides step-by-step instructions for authenticating a password for a normal Safeguard Authentication Services-enabled user through an ssh-like program onto a generic PAM/NSS using *nix system.

NOTE: This guide was last updated for Safeguard Authentication Services 6.0.1. Previous versions, as of version 3.5.2, work similarly with minor differences. For example, in very old versions, the Kerberos ticket request was done by the PAM module directly without involving the `vasd` process.

Authenticating a password

You can authenticate a password by performing the following steps.

NOTE: This example assumes the system is configured using default settings, Safeguard Authentication Services is configured from a default install/join; and, the user is Safeguard Authentication Services-enabled with a password.

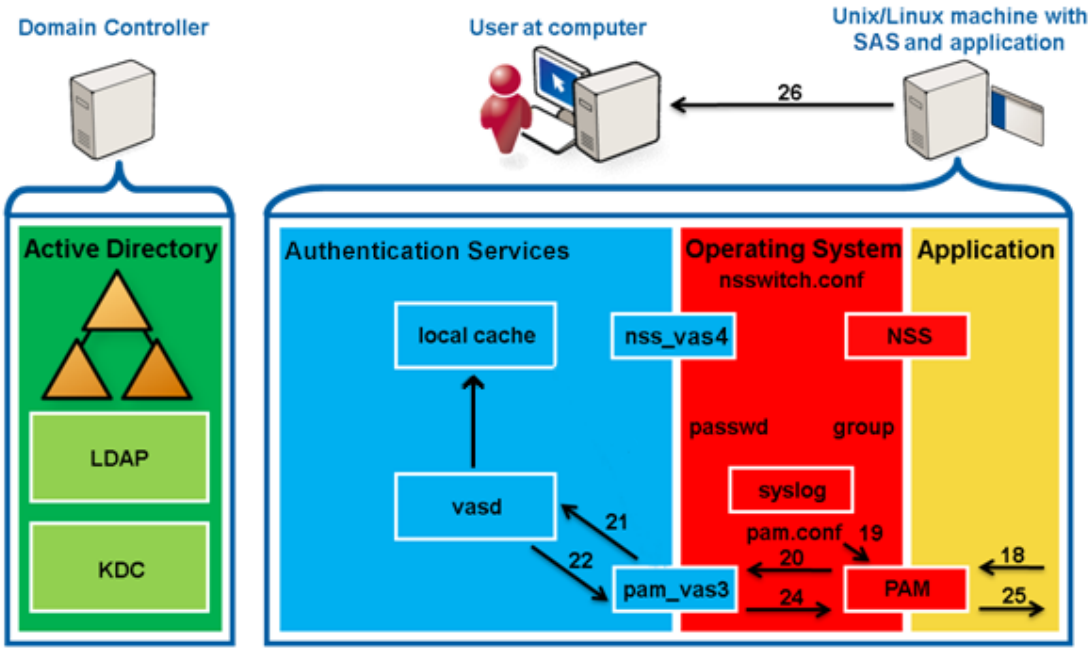


To authenticate a password

1. The user opens a secure connection with the application.
2. The application sends a prompt for the user name.
3. The user sends their user name to the application.
4. The application queries NSS (using `getpwnam`) about the user.
5. NSS reads `/etc/nsswitch.conf` and processes the `passwd: files vas4` entry.

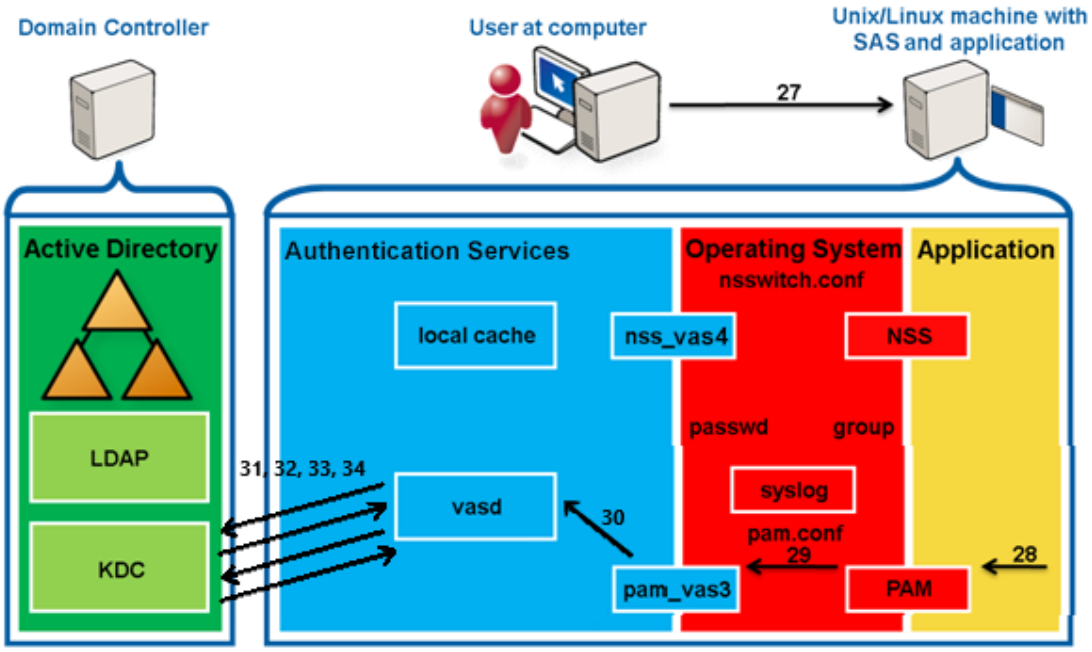
6. NSS queries `nss_files`, which reads `/etc/passwd`, and returns ENOENT because no matching user entry is found.
7. NSS queries `nss_vas4`.
8. `nss_vas4` sends an IPC to `vasd` to update the user.
9. `vasd` uses credentials from the keytab to request a ticket to talk to the LDAP/<DC> service in Active Directory.
10. AD KDC returns the requested service ticket.
11. `vasd` queries AD LDAP for the user information.
12. The user's information is returned.
13. `vasd` writes the user information into the local cache.
14. `vasd` returns the information about the user to `vas_nss`.
15. `nss_vas4` forms the data into a passwd-stlye response.
16. `nss_vas4` returns the passwd info to NSS.

    NOTE: There is no password hash since `vasd` does not have access to that unless you are using a legacy auth setup.
17. NSS returns the information to the application.



18. The application calls PAM through `pam_start` then `pam_authenticate`.
19. PAM reads `/etc/pam.conf` or the config file relevant to the service from `/etc/pam.d` and processes the `pam_vas3` entry.
20. PAM queries `pam_vas3`.
21. `pam_vas3` asks `vasd` for the user info.

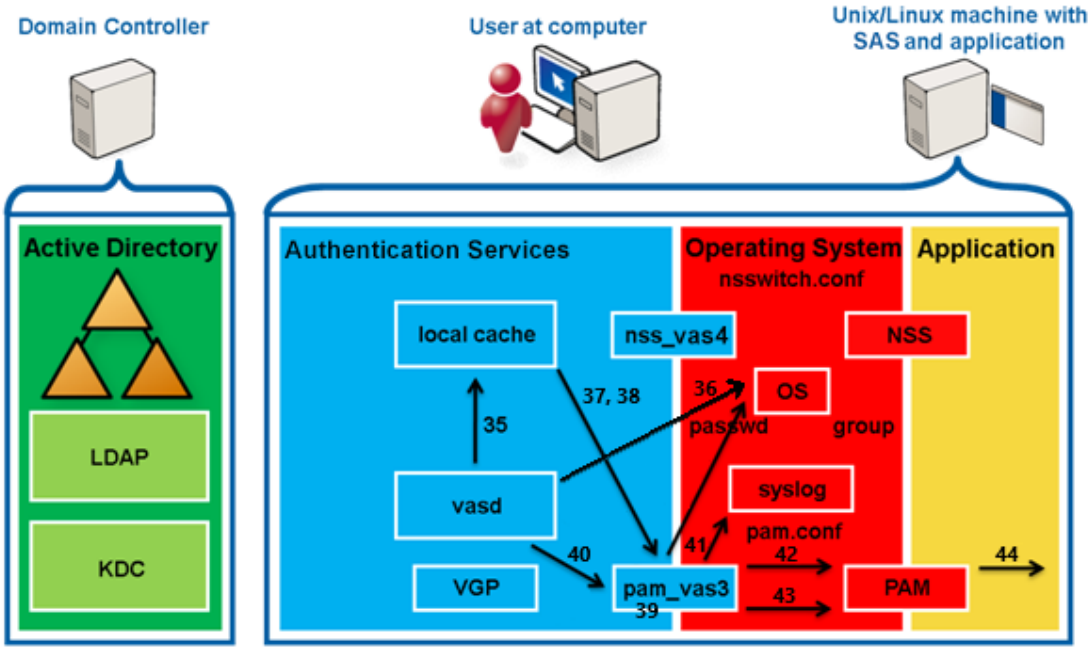
22. vasd returns the user info from the local cache.
23. The user is a Safeguard Authentication Services user, therefore pam_vas3 will continue to attempt to authenticate the user instead of ignoring and letting the PAM stack fall past pam_vas3.
24. pam_vas3 returns a request for credentials (password) using PAM conversations (including the prompt to use).
25. PAM returns the request to the requesting application.
26. The application presents the user with the prompt for their password. (If the application is PAM conversation-aware, it uses the prompt pam_vas3 set).



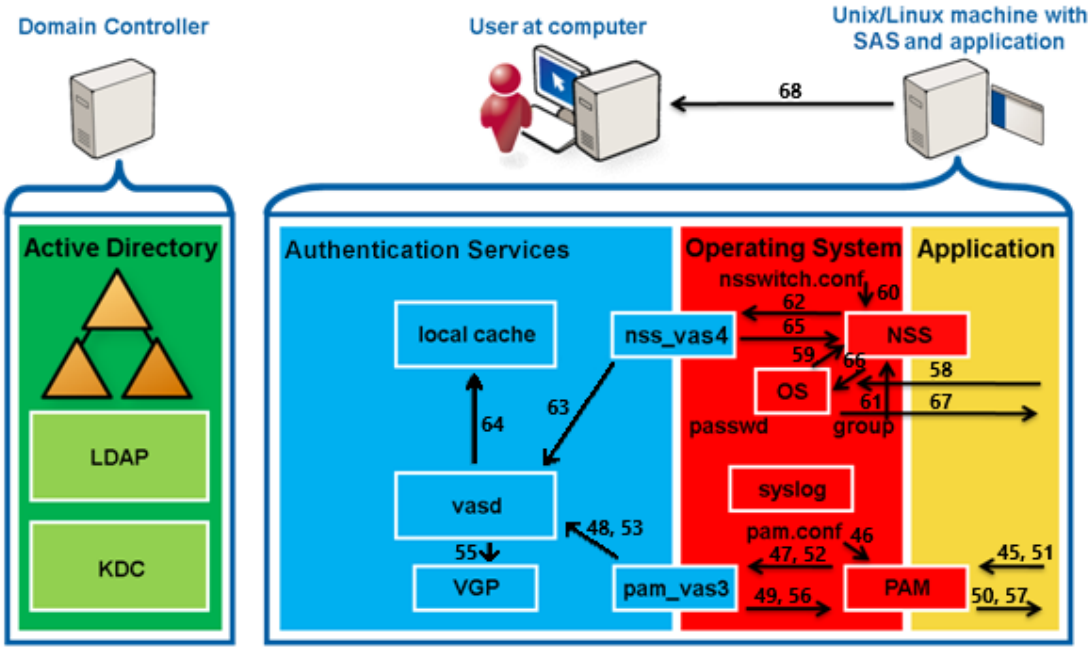
27. The user enters their password.
28. The application passes the password to PAM.
29. The password is passed back to pam_vas3 through the conversation mechanism.
30. pam_vas3 sends the password to vasd through a secure IPC asking for authorization.
31. vasd requests a Kerberos TGT (Ticket Granting Ticket) for the user using a user key derived from the user's samaccountname@realm and the supplied password.

    NOTE: Kerberos does not actually use passwords; it uses keys derived from them for security.
32. AD KDC returns the TGT (AS-REP).
33. vasd decrypts the response using the user key, obtaining a TGT and Session key. TGT and Session key are used to request a service ticket (TGS-REQ) from the AD KDC for the user to authenticate against the host/ (local machine) service.

34. The AD KDC returns the service ticket (TGS-REP), which is decrypted using both the Session key (user portion) and the `host/` key (service portion) that is stored in the host.keytab file.



35. `vasd` processes the payload of the service portion of the service ticket, which is the PAC (Privileged Access Certificate), a list of SIDs of groups of which the user is a member and modifies the local cache to set the current group memberships.
36. `vasd` creates the user's home directory if needed.
37. `vasd` reads the user account information from the local cache. It verifies the user is within any configured logon hours and has a valid shell (not `/bin/false` in AD).
38. `vasd` verifies the user's group membership information and confirms that the user has access based on any configured access control.
39. `vasd` performs UID and GID conflict checking.
40. `vasd` returns success to `pam_vas3`.
41. `pam_vas3` writes a syslog entry that the authentication succeeded.
42. `pam_vas3` sets a PAM stack variable to note that it has already processed the above.
43. `pam_vas3` `pam_authenticate` returns `PAM_SUCCESS`.
44. Because the `pam_vas3` entry is configured with `sufficient`, `PAM_SUCCESS` is returned to the querying application, ignoring the rest of the PAM stack.



45. The application calls PAM through `pam_setcred` and `PAM_ESTABLISHED_CRED`.
46. PAM reads `/etc/pam.conf` and processes the `pam_vas3 entry`.
47. PAM queries `pam_vas3` for `pam_sm_setcred`.
48. `pam_vas3` asks `vasd` to store the user's TGT and host/service ticket a local file-based cache for the user to use again if desired.
49. `pam_vas3` returns `PAM_SUCCESS`.
50. PAM returns `PAM_SUCCESS` to the application for both calls.
51. Similarly, the application calls PAM through `pam_open_session`.
52. PAM queries `pam_vas3`.
53. `pam_vas3` asks `vasd` through the IPC to create a login session for the user.
54. `vasd` fills the `~<user>/.vas_logon_server` file with the server name.
55. `vasd` runs VGP to apply any user policies if configured so.
56. `pam_vas3` returns `PAM_SUCCESS` to PAM.
57. PAM returns `PAM_SUCCESS` to the application.
58. The application starts the user's shell, which then sets up their environment.
59. The OS/shell calls NSS getgroups for the user's group memberships.
60. NSS reads `/etc/nsswitch.conf` and processes the `group: files vas4` entry.
61. NSS queries `nss_files`, which reads `etc/group` and adds no groups if no local groups contain the user.
62. NSS queries `nss_vas4`.
63. `nss_vas4` queries `vasd` to compute the user's group memberships.

64. `vasd` reads the group memberships from the local cache and returns them.
65. `nss_vas4` returns the memberships to NSS.
66. The shell uses the groups to set the process space group memberships.
67. The OS presents the shell to the application.
68. The application presents the shell to the user, and they are now logged in.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Glossary

A

access control
A set of procedures performed by hardware, software, and administrators to monitor access, identify users requesting access, record access attempts, and grant or deny access. Compare with authorization. See also ACL.

Access Control List (ACL)
A set of data that informs a computer's operating system which permissions, or access rights, that each user or group has to a specific system object, such as a directory or file. Each object has a unique security attribute that identifies which users have access to it, and the ACL is a list of each object and user access privileges such as read, write, or execute.

ACE
Acronym for Access Control Entry.

ACL
Acronym for Access Control List.

ACL Filtering
Access Control Lists can be applied to Group Policy objects that determine whether or not the policy will be applied on a system.

Active Directory
Microsoft's network directory service for computers.

ADAM
Active Directory Application Mode, a Windows 2003 service in which LDAP runs as a user service rather than as a system service.

ADSI
Active Directory Services Interface, an editor (browser), scripting language, and so on.

ADUC
Active Directory Users and Computers (ADUC) is a Microsoft Management Console snap-in that you use to administer Active Directory (AD). You can manage objects (users, computers), Organizational Units (OU), and their attributes.

affinity
With respect to a directory, the organization of the accounts relies on properties they have in common. This similarity may be due to departmental structure or geographical location of the people that use the accounts.

ARC4
See RC4.

ARCFOUR
See RC4.

ARS
ActiveRoles Server is a product installed on a Windows server that uses SQL Server for configuring data and publishing itself as a connection point object within Active Directory. It is a cross-platform, roles-based provisioning system that allows additional attributes to be stored for an object. For example, ARS can put a newly hired engineer into all the appropriate groups on all platforms relevant to their job description.

authentication
Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially (or is registered by someone else), using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password. The weakness in this system for transactions that are significant (such as the exchange of money) is that passwords can often be stolen, accidentally revealed, or forgotten. Logically, authentication precedes authorization (although they may often seem to be combined).

authoritative source
In migrating identities from disparate NIS domains, identities from the first source repository are migrated without any changes to their internal identity (ID) and the first repository becomes the authoritative source. In case of ID conflict or mismatch, IDs in all remaining sources are changed to match those in the first source.

authorization
Authorization is the process of giving someone permission to do or have something. In multi-user computer systems, a system administrator defines for the system which users are allowed access to the system and what privileges of use (such as access to which file directories, hours of access, amount of allocated storage space, and so on). Assuming that someone has logged in to a computer operating system or application, the system or application may want to identify what resources the user can be given during this session. Thus, authorization is sometimes seen as both the preliminary setting up of permissions by a system administrator and the actual checking of the permission values that have been set up when a user is getting access. Logically, authorization is preceded by authentication.

B

Block Inheritance
When Block Inheritance is set on a GPO link, all GPOs above the link level are excluded from GPO processing unless the GPO is enforced.

C

CAC
Common Access Card, a smart card issued by the United States Department of Defense (DoD) for active-duty military, civilian employees and contractors.

canonical name
Essentially the distinguished name in reverse; generally, a software-internal representation, such as acme.com/engineering/jim.

CIFS
Common Internet File System, a Microsoft technology. See also SMB.

CN
Common Name, a component of a distinguished name (DN).

COM
Component Object Model, a Microsoft technology that enables components to communicate, used by developers to create reusable software components, link components together to build applications, and take advantage of Windows services like Active Directory.

credential
A proof of qualification or competence attached to a user or session, an object verified during an authentication transaction. In Kerberos parlance, a message containing the random key along with a service name and the user's long-term key.

D

DC
Domain Controller.

DES
Data Encryption Standard is a cypher selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976. It is characterized by a relatively short key length (56 bits) and is considered less secure for many application environments than some alternatives.

disconnected authentication
Provisory authentication based on prior login and used in case of network failure. The maximum duration of a stored password hash is configurable.

DN
Distinguished Name.

domain
In Active Directory, a centrally-managed group of computers.

domain controller (DC)
The server that responds to security authentication requests in the Active Directory domain.

DSE
Directory-specific entry in an LDAP environment.

E

Enforced
If a GPO is enforced, then it will be applied regardless of block inheritance settings.

F

firewall
A piece of hardware, software, or both that sets rules about what network traffic can cross it. These rules can focus on the protocols used by the traffic and ports in use. Authentication Services, for instance, requires a set of ports by which it implements its services. Those ports must not be blocked. However, if a host has access to Active Directory, to its domain controllers, and so on, then the ports needed by Authentication Service are open. For Authentication Services specifically, this means 88 (TCP/UDP for Kerberos ticket services), 389 (LDAP queries and ping), 464 (TCP/UDP for Kerberos passwords), and 3268 (TCP for Global Catalog access); optionally, 53 (UDP for DNS SRV records) and 123 (UDP for time-synchronization with Active Directory). For Authentication Services Group Policy, port 445 (TCP for Microsoft DS).

forest
The collection of all objects and their attributes and rules in Active Directory. It is named "forest" because it holds one or more trust-linked trees, allowing users in one domain to access resources in another domain.

FQDN
Fully Qualified Domain Name; a domain name specified exhaustively, such as somehost.example.com.

FSMO
Flexible Single Master Operations; a multi-master-enabled database such as Active Directory that provides the flexibility of allowing changes at any domain controller in the enterprise, but also gives rise to the possibility of conflicts and the need to resolve them, especially for certain tasks. Collectively, FSMO tasks are used where standard data transfer and update methods on multiple peer domain controllers are ill-adapted to multi-master replication, for example: schema update and modification domain naming (addition or removal of domains in the

forest), relative ID assignment (including SIDs), infrastructure (security) maintenance (including GUIDs, SIDs, and reference object DN in cross-domain references), and PDC emulation. These tasks are handled in a single master model by Windows 2000/2003.

G

GC
Global Catalog.

GECOS
(also in lower case) A field in the Unix /etc/passwd file that contains general information about the user including things like full name, telephone number, and so on, depending completely on the host implementation.

gid
group identity, standard C library object, represented by gid_t, identifying a group.

GID
Group identity; broad term referring to the underlying number that identifies a group of users or other objects in a directory service.

GPMC
Group Policy Management Console; a Microsoft tool.

GPO
Group Policy Object; an actual directory object tied to system volume instance. The group policy object is a collection of settings that define what a system looks like and how it behaves for a defined group of users. A GPO is created, using the Group Policy Management Console when there are such settings. GPOs are associated with a container such as a site, domain, or organizational unit (OU). GPOs are very powerful and can be used to distribute software and updates such as Tivoli (IBM). See also group policy.

group policy
A Microsoft technology that reduces the cost of supporting Windows users by providing centralized management of computers and user in Active Directory. Group Policy controls various aspects of an object including security policy, software installation, login, folder redirection, and software settings. Such policies are stored on group policy objects (GPOs).

GSS
Generic Security Service; security services provided atop underlying, alternative cryptographic mechanisms such as Kerberos. According to RFC 2744, the GSS API allows a caller application to authenticate a principal identity associated with a peer application to delegate rights to another peer, and to apply security services such as confidentiality and integrity on a per-message basis.

GUID
Globally Unique Identifier; a number, address, or other cookie used to represent an object uniquely in a directory service, file system, and so on. In Active Directory, the GUID is a unique, unchanging 128-bit string used for search and replication.

J

joining
Describes the action of a Unix or Linux workstation being incorporated into an Active Directory domain by means of the vastool join command.

K

KDC
The Key Distribution Center in Kerberos. Part of a cryptosystem to reduce the intrinsic risk of exchanging keys, basically consisting of the authentication server (AS) and the ticket-granting server (TGS).

Kerberized application
A software application that requires or performs Kerberos authentication.

Kerberos
A computer network authentication protocol that proves the identity of intercommunicating points on an insecure network like a LAN or the Internet in a secure manner. Guards against eavesdropping and replay attacks.

Kerberos authentication
An authentication system developed at the Massachusetts Institute of Technology (MIT). Kerberos is designed to enable two parties to exchange private information across an otherwise open network. It works by assigning a unique key, called a ticket, to each user that logs on to the network. The ticket is then embedded in messages to identify the sender of the message.

keytab
A file containing authentication credentials used, usually in place of a password, for authentication.

L

LAM
Loadable Authentication Module, IBM's precursor to PAM on the AIX (Unix) operating system. Authentication Services provides a LAM-based implementation on AIX. LAMs are configured in /usr/lib/security/methods.cfg.

LDIF
LDAP Data Interchange Format. See also Lightweight Directory Access Protocol (LDAP).

libvas
Prefix associated with Authentication Services runtime libraries and interfaces.

Lightweight Directory Access Protocol (LDAP)
A software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. LDAP is a "lightweight" version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network.

M

Mapped Users
Mapped User allows Authentication Services to authenticate against Active Directory while taking identity and Unix attributes from local files. It is implemented by replacing the 'x' placeholder in /etc/passwd with the user principal name (UPN) (Linux and Unix only), or by creating a local-to-AD user map file and specifying the location of that file in /etc/opt/quest/vas/vas.conf (Linux, Unix, or Mac).

MIIS
Microsoft Identity Integration Server; a server that manages the flow of data between all connected data sources and automates the process of updating identity information (for example, of employees, and so on) in the implementing environment.

MMC
Microsoft Management Console, for which Authentication Services has a snap-in used when browsing users or groups and getting their properties.

N

NAS
Network-Attached Storage; file-level data storage connected, often remote, but not appearing as a local volume/disk. This is in opposition to SAN.

Native Mode
Native Active Directory mode refers to a network being serviced completely by either Windows 2000 or Windows 2003 servers, but not both. If servers from both versions are present, the services offered can only be a common subset of the two. If all servers are running Windows 2003 Server, then all the features that this operating system offers over its predecessor are available. Not being in native mode has ramifications for various components, that is, local groups are not added to the PAC of the Kerberos ticket; group membership is not available.

NIS
Network Information Services; a Unix client-server directory service protocol, originally Sun Microsystems' "Yellow Pages." It provides centralized control over many types of network objects including users, groups, and network services like printers. NIS arose as a solution to each Unix host having its own /etc/passwd and

groups files as the resident authority on users and groups when these notions needed to be extended over a network. NIS domains are flat (no hierarchy), use no authentication and the NIS map files are limited to 1024 bytes in size.

nscd
Name service caching daemon; provides a cache for the most common name service request on Linux and Unix from the passwd, group, and hosts databases through standard C library interfaces including getpwnam, getpwuid, getgrnam, getgrgid, gehostbyname, and others. The configuration file is /etc/nscd.conf.

NSS
Name Service Switch; interface to nsswitch.conf that controls how look-ups are done for users (/etc/passwd), groups (/etc/grps), hosts (/etc/hosts), and so on. For example, getpwnam goes through NSS, which is extensible and configurable (just as is PAM), to reach variably passwd, vasd, NIS, or LDAP.

NTP
Network Time Protocol, as implemented by a server that keeps time on the network and is accessible to other nodes for the purpose of all keeping the same notion of time.

O

Organizational Unit (OU)
An Active Directory container object used within domains. An organizational unit is a logical container into which users, groups, computers, and other organizational units are placed. It can contain objects only from its parent domain. An organizational unit is the smallest scope to which a group policy object can be linked, or over which administrative authority can be delegated.

OU
Organization Unit. See also Personality container.

Override
If a GPO specifies a policy and another GPO further down in the GPO application chain is allowed to overwrite the previously specified policy, then the policy supports override.

P

PAC
Privileged Attribute Certificates, used by Kerberized applications for fine-grained access control to services, a feature of Microsoft's Kerberos implementation.

PAM
Pluggable Authentication Module; an architecture and shared libraries created by Sun Microsystems for the Solaris operating system that permits intervention into and specialization of the authentication process. PAMs are configured in /etc/pam.conf or in individual files off /etc/pam.d/.

PDC

Primary Domain Controller; an NT concept, emulated on Windows 2000/2003, that performs a number of crucial tasks in an enterprise including time synchronization, password replication, recording of password failures, account lock-out, and modification or creation of GPOs.

Personality container

An Active Directory organization unit (OU) designated to contain user and group personalities. Unix clients specify a Unix personality container (vastool join -p) in order to join the domain in Unix Personality Management (UPM) mode.

Personality scope

Consists of a primary Personality container, along with any secondary Personality containers. Only the Personalities, Active Directory users, and Active Directory groups that reside within that Personality scope will be usable on the Unix system.

PKI

Public Key Infrastructure; a way to ensure secure transactions over the wire; an arrangement providing for third-party vetting of user identities typically placing any keys within a certificate. Not yet a standard; there are myriad implementations.

POSIX

Portable Operating System Interface; the open operating interface standard accepted worldwide. It is produced by IEEE and recognized by ISO and ANSI.

principal

In Kerberos, this is basically a simple account including name, password, and other information stored in the database and encrypted using a master key.

provisioning

The process of providing customers or clients with accounts, the appropriate access to those accounts, all the rights associated with those accounts, and all of the resources necessary to manage the accounts. When used in reference to a client, provisioning can be thought of as a form of customer service.

R

RC4

(pronounced "arcfour") A stream cipher in such popular protocols as secure sockets layer (SSL). RC4 generates a pseudo random stream of bits XOR'd with the clear-text password, for example. RC4 is more secure than DES.

realm

A Kerberos term that usually maps to an Active Directory domain, not because they are the same thing, but because for implementation, it is a natural alignment.

S

Samba

A free software implementation of Microsoft's networking protocol that runs on *nix systems and is capable of integrating with an Active Directory (Windows) domain as either a primary domain controller or as a domain member. See also SMB.

SAN

Storage Area Network; an architecture for attaching remote storage devices (disk arrays, tape libraries, optical jukeboxes, and so on) to servers in such a way that to the operating system these appear as locally attached. This is in opposition to NAS where it is clear that the storage is remote.

Sarbanes Oxley Act (SOX)

Reference to legislation enacted in response to recent and spectacular financial scandals, to protect shareholders and the general public from accounting errors and fraudulent practices. The act is administered by the Securities and Exchange Commission, which sets deadlines for compliance and publishes rules on requirements. SOX defines which records are to be stored and for how long. It also affects IT departments whose job it is to store electronic records.

SAS

Safeguard Authentication Services.

schema master

A domain controller that holds the schema operations master role in Active Directory. The schema master performs write operations to the directory schema and replicates updates to all other domain controllers in the forest. At any time, the schema master role can be assigned to only one domain controller in the forest.

Secure Sockets Layer (SSL)

The Secure Sockets Layer (SSL) is a commonly used protocol for managing the security of message transmission on the Internet. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most web server products. Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers, becoming the de facto standard until evolving into Transport Layer Security (TLS). The sockets part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public/private key encryption system from RSA, which also includes the use of a digital certificate.

security principal

An entity that can be positively identified and verified by means of a technique known as authentication.

Simple and Protected GSS-API Negotiation Mechanism (SPNEGO)
A GSSAPI mechanism that allows the secure negotiation of the mechanism to be used by two different GSSAPI implementations. In essence, SPNEGO defines a universal but separate mechanism, solely for the purpose of negotiating the use of other security mechanisms. SPNEGO itself does not define or provide authentication or data protection, although it can allow negotiators to determine if the negotiation has been subverted, once a mechanism is established.

Single Sign-On (SSO)
An authentication process in a client/server relationship where the user, or client, can enter one name and password and have access to more than one application or access to a number of resources within an enterprise. Single sign-on removes the need for the user to enter further authentications when switching between applications.

SMB
Server Message Block; a protocol that exists primarily for trust relationships, the concept upon which NetBIOS is based and hence, used by DOS and Windows. The message format is used for sharing files, directories and devices. CIFS (Common Internet File System) is a synonym for SMB. See also Samba.

T

Tattooing
When files or settings are left on the system after group policy has been un-applied, the files and settings are said to be tattooed. Unless otherwise documented a policy should remove all associated settings and files when the policy is unlinked. A policy that supports non-tattooing will not leave any files or settings behind after it is un-applied.

TGS
Ticket-granting server, part of a key-distribution server (KDC).

TGT
Ticket-granting ticket, the initial ticket given by the Kerberos authentication server permitting the TGS to be contacted

Ticket
A voucher that isn't easily forged and proves that the bearer has properly applied for authentication to a service. In Kerberos parlance, a message containing a random key, the same one that was passed in the credential, plus the user's name, the whole being encrypted using the service's long-term key. Tickets obviate the inconvenience of using a password in that they can be supplied to different services rather than performing separate authentication of the password with each service. See credential.

U

UID
User identity, broad term referring to the underlying number that identifies a user in a directory.

V

VAS
Vintela Authentication Services.

vas.conf
Configuration file on the path /etc/opt/quest/vas/vas.conf that is Authentication Services' equivalent (and more) to Kerberos' krb5.conf.

vasd
The name of the Autentication Service daemon.

VGP
Quest Group Policy, Unix group policy product.