

Single sign-on with Kerberos and LDAP

Wouter Verhelst

LOADays 2011

- Network authentication

Kerberos?

- Network authentication
- Written by MIT in 1980's, as part of Project Athena

Kerberos?

- Network authentication
- Written by MIT in 1980's, as part of Project Athena
- picky about network setup

Kerberos?

- Network authentication
- Written by MIT in 1980's, as part of Project Athena
- picky about network setup
- Common implementations: MIT krb5, Heimdal

Kerberos?

- Network authentication
- Written by MIT in 1980's, as part of Project Athena
- picky about network setup
- Common implementations: MIT krb5, Heimdal, Microsoft Active Directory

Kerberos?

- Network authentication
- Written by MIT in 1980's, as part of Project Athena
- picky about network setup
- Common implementations: MIT krb5, Heimdal, Microsoft Active Directory

<http://web.mit.edu/Kerberos>

Kerberos?

- Network authentication
- Written by MIT in 1980's, as part of Project Athena
- picky about network setup
- Common implementations: MIT krb5, Heimdal, Microsoft Active Directory

<http://web.mit.edu/Kerberos>

- Lightweight Directory Access Protocol

- Lightweight Directory Access Protocol
- "lightweight"

- Lightweight Directory Access Protocol
- "lightweight" – hah.

- Lightweight Directory Access Protocol
- "lightweight" – hah.
- Directory

- Lightweight Directory Access Protocol
- "lightweight" – hah.
- Directory
- Common implementation : OpenLDAP

- Lightweight Directory Access Protocol
- "lightweight" – hah.
- Directory
- Common implementations: OpenLDAP

- Lightweight Directory Access Protocol
- "lightweight" – hah.
- Directory
- Common implementations: OpenLDAP, Microsoft Active Directory

- Lightweight Directory Access Protocol
- "lightweight" – hah.
- Directory
- Common implementations: OpenLDAP, Microsoft Active Directory (almost)

- Lightweight Directory Access Protocol
- "lightweight" – hah.
- Directory
- Common implementations: OpenLDAP, Microsoft Active Directory (almost)

Authentication vs Authorization

- Authentication: allowing someone to prove they are who they say they are.

Authentication vs Authorization

- Authentication: allowing someone to prove they are who they say they are.
- Authorization: deciding whether users, based on their authentication credentials, are allowed to do certain things

Authentication vs Authorization

- Authentication: allowing someone to prove they are who they say they are.
- Authorization: deciding whether users, based on their authentication credentials, are allowed to do certain things
- Kerberos does authentication only; LDAP can be used for both.

Authentication vs Authorization

- Authentication: allowing someone to prove they are who they say they are.
- Authorization: deciding whether users, based on their authentication credentials, are allowed to do certain things
- Kerberos does authentication only; LDAP can be used for both.

- Realm

- Realm
- Principal

- Realm
- Principal
- Ticket

- Realm
- Principal
- Ticket
- KDC

- Realm
- Principal
- Ticket
- KDC
- TGT

- Realm
- Principal
- Ticket
- KDC
- TGT

Anatomy of a kerberos principal

host/samba.grep.be@GREP.BE

- host: primary

Anatomy of a kerberos principal

host/samba.grep.be@GREP.BE

- host: primary
- samba.grep.be: instance

Anatomy of a kerberos principal

host/samba.grep.be@GREP.BE

- host: primary
- samba.grep.be: instance
- GREP.BE: realm

Kerberos has certain requirements...

- no clock skew (use ntp)

Kerberos has certain requirements...

- no clock skew (use ntp)
- reverse lookups must make sense for servers

Kerberos has certain requirements...

- no clock skew (use ntp)
- reverse lookups must make sense for servers
- optionally, announce realm and kdc's through DNS (reduces setup on clients).

Kerberos has certain requirements...

- no clock skew (use ntp)
- reverse lookups must make sense for servers
- optionally, announce realm and kdc's through DNS (reduces setup on clients).

- `_kerberos.grep.be. 86400 IN TXT "GREP.BE"`

- `_kerberos.grep.be. 86400 IN TXT "GREP.BE"`
- `_kerberos._udp.grep.be. 86400 IN SRV 0 0 88
samba.grep.be.`

- `_kerberos.grep.be. 86400 IN TXT "GREP.BE"`
- `_kerberos._udp.grep.be. 86400 IN SRV 0 0 88
samba.grep.be.`
- `_kerberos-adm._tcp.grep.be. 86400 IN SRV 0 0 749
samba.grep.be.`

- `_kerberos.grep.be. 86400 IN TXT "GREP.BE"`
- `_kerberos._udp.grep.be. 86400 IN SRV 0 0 88
samba.grep.be.`
- `_kerberos-adm._tcp.grep.be. 86400 IN SRV 0 0 749
samba.grep.be.`
- `_kpasswd.grep.be. 86400 IN SRV 0 0 464 samba.grep.be.`

- `_kerberos.grep.be. 86400 IN TXT "GREP.BE"`
- `_kerberos._udp.grep.be. 86400 IN SRV 0 0 88
samba.grep.be.`
- `_kerberos-adm._tcp.grep.be. 86400 IN SRV 0 0 749
samba.grep.be.`
- `_kpasswd.grep.be. 86400 IN SRV 0 0 464 samba.grep.be.`

Setting up a kerberos realm

- Debian packages: krb5-admin-server, krb5-kdc

Setting up a kerberos realm

- Debian packages: krb5-admin-server, krb5-kdc
- RedHat: krb5-server

Setting up a kerberos realm

- Debian packages: krb5-admin-server, krb5-kdc
- RedHat: krb5-server
- kdb5_util create

Setting up a kerberos realm

- Debian packages: krb5-admin-server, krb5-kdc
- RedHat: krb5-server
- kdb5_util create (or: krb5_newrealm)

Setting up a kerberos realm

- Debian packages: krb5-admin-server, krb5-kdc
- RedHat: krb5-server
- kdb5_util create (or: krb5_newrealm)
- kadmin.local: addprinc *user/admin*

Setting up a kerberos realm

- Debian packages: krb5-admin-server, krb5-kdc
- RedHat: krb5-server
- kdb5_util create (or: krb5_newrealm)
- kadmin.local: addprinc *user/admin*
- Start kadmin and kdc services

Setting up a kerberos realm

- Debian packages: krb5-admin-server, krb5-kdc
- RedHat: krb5-server
- kdb5_util create (or: krb5_newrealm)
- kadmin.local: addprinc *user/admin*
- Start kadmin and kdc services
- use kadmin (with newly created admin user) to add more principals

Setting up a kerberos realm

- Debian packages: krb5-admin-server, krb5-kdc
- RedHat: krb5-server
- kdb5_util create (or: krb5_newrealm)
- kadmin.local: addprinc *user/admin*
- Start kadmin and kdc services
- use kadmin (with newly created admin user) to add more principals

Congratulations! You have a realm!

Setting up a kerberos realm

- Debian packages: krb5-admin-server, krb5-kdc
- RedHat: krb5-server
- kdb5_util create (or: krb5_newrealm)
- kadmin.local: addprinc *user/admin*
- Start kadmin and kdc services
- use kadmin (with newly created admin user) to add more principals

Congratulations! You have a realm!

Using the kerberos realm

- kinit/kdestroy
- klist

Using the kerberos realm

- kinit/kdestroy
- klist
- pam_krb5.so
- sshd: GSSAPIAuthentication yes

- GSSAPI

- GSSAPI: "GSSAPI is just a funny name for Kerberos v5" – Peter Palfrader

- GSSAPI: "GSSAPI is just a funny name for Kerberos v5" – Peter Palfrader
- SASL: IMAP (dovecot, evolution, thunderbird, offlineimap, mutt, ...)

- GSSAPI: "GSSAPI is just a funny name for Kerberos v5" – Peter Palfrader
- SASL: IMAP (dovecot, evolution, thunderbird, offlineimap, mutt, ...)
- SASL: LDAP (openldap – beware circular dependency)

- GSSAPI: "GSSAPI is just a funny name for Kerberos v5" – Peter Palfrader
- SASL: IMAP (dovecot, evolution, thunderbird, offlineimap, mutt, ...)
- SASL: LDAP (openldap – beware circular dependency)
- SASL: ...

- GSSAPI: "GSSAPI is just a funny name for Kerberos v5" – Peter Palfrader
- SASL: IMAP (dovecot, evolution, thunderbird, offlineimap, mutt, ...)
- SASL: LDAP (openldap – beware circular dependency)
- SASL: ...
- HTTP: Negotiate authentication (mod_auth_kerb, gecko-browsers, internet explorer, google chrome for windows (*not* chrome for Linux, yet), webkit, ...)

- GSSAPI: "GSSAPI is just a funny name for Kerberos v5" – Peter Palfrader
- SASL: IMAP (dovecot, evolution, thunderbird, offlineimap, mutt, ...)
- SASL: LDAP (openldap – beware circular dependency)
- SASL: ...
- HTTP: Negotiate authentication (mod_auth_kerb, gecko-browsers, internet explorer, google chrome for windows (*not* chrome for Linux, yet), webkit, ...)
- NFS: sec=gss/krb5, sec=gss/krb5i, sec=gss/krb5p

- GSSAPI: "GSSAPI is just a funny name for Kerberos v5" – Peter Palfrader
- SASL: IMAP (dovecot, evolution, thunderbird, offlineimap, mutt, ...)
- SASL: LDAP (openldap – beware circular dependency)
- SASL: ...
- HTTP: Negotiate authentication (mod_auth_kerb, gecko-browsers, internet explorer, google chrome for windows (*not* chrome for Linux, yet), webkit, ...)
- NFS: sec=gss/krb5, sec=gss/krb5i, sec=gss/krb5p
- ...

- GSSAPI: "GSSAPI is just a funny name for Kerberos v5" – Peter Palfrader
- SASL: IMAP (dovecot, evolution, thunderbird, offlineimap, mutt, ...)
- SASL: LDAP (openldap – beware circular dependency)
- SASL: ...
- HTTP: Negotiate authentication (mod_auth_kerb, gecko-browsers, internet explorer, google chrome for windows (*not* chrome for Linux, yet), webkit, ...)
- NFS: sec=gss/krb5, sec=gss/krb5i, sec=gss/krb5p
- ...

- Debian packages: slapd

Setting up LDAP

- Debian packages: slapd
- RedHat packages: openldap-servers

Setting up LDAP

- Debian packages: slapd
- RedHat packages: openldap-servers
- Create slapd.conf (see tutorial, or use Debian)

Setting up LDAP

- Debian packages: slapd
- RedHat packages: openldap-servers
- Create slapd.conf (see tutorial, or use Debian)
- slapadd to add initial directory tree.

Setting up LDAP

- Debian packages: slapd
- RedHat packages: openldap-servers
- Create slapd.conf (see tutorial, or use Debian)
- slapadd to add initial directory tree.
- objectClass required for unix accounts: posixUser, posixGroup, shadowAccount

Setting up LDAP

- Debian packages: slapd
- RedHat packages: openldap-servers
- Create slapd.conf (see tutorial, or use Debian)
- slapadd to add initial directory tree.
- objectClass required for unix accounts: posixUser, posixGroup, shadowAccount
- libnss_ldap.so

Setting up LDAP

- Debian packages: slapd
- RedHat packages: openldap-servers
- Create slapd.conf (see tutorial, or use Debian)
- slapadd to add initial directory tree.
- objectClass required for unix accounts: posixUser, posixGroup, shadowAccount
- libnss_ldap.so
- pam_mkhome.so

Setting up LDAP

- Debian packages: slapd
- RedHat packages: openldap-servers
- Create slapd.conf (see tutorial, or use Debian)
- slapadd to add initial directory tree.
- objectClass required for unix accounts: posixUser, posixGroup, shadowAccount
- libnss_ldap.so
- pam_mkhome.so