Kerberos Infrastructure HOWTO

V. Alex Brennen

vab@cryptnet.net

2004-05-29

Diario delle Revisioni

Revisione 2.0.0 2004-05-28 Revisionato da: VAB
Conversion to DocBook XML. General Content Updates, including incorporation of Technical and Metadata/M

Revisione 1.0.3 2003-04-01 Revisionato da: VAB
Minor Updates, Minor Corrections, Additional links added.

Revisione 1.0.2 2002-09-13 Revisionato da: VAB
Minor Updates, Minor Corrections, Added 8.6, Additional links added.

Revisione 1.0.1 2002-07-15 Revisionato da: VAB
Minor Updates, Fixes.

Revisione 1.0.0 2002-06-13 Revisionato da: VAB
Initial Release.

Questo documento descrive il progetto e la configurazione di una infrastruttura Kerberos per la gestione dell'autenticazione su GNU/Linux. Illustra in dettaglio i passi da seguire, secondo le buone prassi, per installare un server o un software basato su Kerberos e per effettuare la conversione dei sistemi preesistenti; risponde inoltre alle domande più frequenti.

Traduzione di Lorenzo Vaina *work [at] vaina [dot] it*

Revisione della traduzione a cura di Marco Curreli *marcocurreli [at] tiscali [dot] it*

1. A proposito di questo documento

1.1. Informazioni generali

Questo documento è pubblicato all'indirizzo:
http://cryptnet.net/fdp/admin/kerby-infra/en/kerby-infra.html

1.2. Traduzioni

Al momento questo documento è disponibile nelle seguenti lingue:

- [en (http://cryptnet.net/fdp/admin/kerby-infra/en/kerby-infra.html)] English
- [it (http://www.pluto.it/ildp/howto/kerberos-infrastructure)] Italiano

Se conoscete una traduzione o intendete tradurlo in un'altra lingua informatemi (mailto:vab@cryptnet.net) in modo che io possa distribuire la traduzione o riferirla con un link.

1.3. Contributi e ringraziamenti

- V. Alex Brennen (http://cryptnet.net/people/vab/) (VAB (http://cryptnet.net/people/vab/)) `<vab (at) cryptnet.net>` (Autore principale)
- Nickolai Zeldovich (http://kolya.net/) `<kolya (at) zepa.net>` (Suggerimenti e correzioni tecniche)

1.4. Feedback

Per favore inviate le vostre aggiunte, commenti, correzioni e critiche a questo indirizzo di posta elettronica: `<vab@cryptnet.net>`.

2. Una vista di insieme dell'infrastruttura di Kerberos

2.1. Introduzione a Kerberos

Kerberos è un sistema di autenticazione sviluppato dal MIT nell'ambito del progetto Athena. Kerberos usa la crittografia e una terza parte fidata, un arbitro, per eseguire l'autenticazione in maniera sicura attraverso una rete non sicura. In particolare Kerberos usa dei ticket cifrati per evitare di trasmettere le password come testo in chiaro attraverso la rete; Kerberos si basa sul protocollo di Needham e Schroeder.

Adesso sono in uso due versioni di kerberos: la 4 e la 5. Le versioni dalla 1 alla 3 erano versioni interne di sviluppo e non sono mai state pubblicate; la versione 4 ha alcune lacune di sicurezza a non dovrebbe più essere usata. Questo documento tratta soltanto di Kerberos 5, definito nel RFC1510 (http://cryptnet.net/mirrors/rfcs/rfc1510.txt).

La locuzione Infrastruttura Kerberos si riferisce alla configurazione del software, del server e del client che permettono a un amministratore di usare il protocollo Kerberos per realizzare l'autenticazione sulla rete. Precisamente, l'infrastruttura kerberos consiste nel software Kerberos stesso, in alcuni server di autenticazione ridondanti posti in sicurezza, in un deposito centralizzato di account e password e nei sistemi configurati per usare Kerberos come protocollo di autenticazione. Questo documento permetterà di apprendere i passi necessari per installare, configurare e distribuire una tale infrastruttura.

2.2. I benefici di Kerberos

Chi non ha confidenza col protocollo kerberos potrebbe non aver chiaro quali siano i benefici che comporta distribuirlo sulla rete; comunque tutti gli amministratori hanno confidenza con i problemi che Kerberos dovrebbe mitigare. Alcuni di questi problemi sono l'intercettazione della password in transito sulla rete (sniffing), la lettura abusiva del file o del database delle password (stealing), e gli sforzi che si devono sostenere per mantenere un vasto numero di database degli account.

Un' infrastruttura kerberos distribuita in modo appropriato costituisce un buon punto di partenza per la soluzione dei problemi cui si è accennato e aumenta la sicurezza dell'organizzazione. L'uso di Kerberos evita che le password siano trasmesse in chiaro sulla rete; inoltre il sistema centralizza le informazioni sulle credenziali semplificandone la gestione e la manutenzione. Infine l'utilizzo di Kerberos evita di dover conservare le password localmente sulla macchina, riducendo la probabilità che la compromissione di una singola macchina comporti ulteriori violazioni.

Riassumendo, in una grande impresa i benefici di Kerberos si tradurranno in minori costi amministrativi attraverso una gestione più semplice di account e password e attraverso il miglioramento nella sicurezza della rete. In un ambiente più piccolo i benefici più evidenti sono costituiti dalla scalabilità dell'infrastruttura di autenticazione e dal miglioramento della sicurezza della rete.

2.3. Come funziona Kerberos

Il protocollo di autenticazione Kerberos usa un segreto condiviso e una terza parte fidata, con ruolo di arbitro, per convalidare l'identità dei client, che possono essere utenti, server o programmi. La terza parte fidata è un server chiamato Key Distribution Center (KDC) che esegue i dèmoni Kerberos. Il segreto condiviso è la password dell'utente trasformata in chiave crittografica; per i server e i sistemi software è generata una chiave casuale.

In Kerberos gli utenti sono detti "principal"; il KDC conserva un database dei principal e delle chiavi segrete che essi usano per autenticarsi. In Kerberos la conoscenza della chiave segreta è considerata una valida dimostrazione di identità, perciò il server Kerberos è affidabile per autenticare ogni client nei confronti di ogni altro client. Con Kerberos l'autenticazione è ottentuta senza trasmettere alcuna password in chiaro attraverso la rete. Nel seguito sarà spiegata la corrispondenza fra il protocollo Kerberos e il software Kerberos in GNU Linux.

Il KDC esegue i due importanti dèmoni Kerberos kadmind e krb5kdc. Una convenzione di denominazione in GNU Linux prevede che i processi il cui nome inizia per "k" siano attinenti al kernel o eseguiti nello spazio del kernel; invece krb5kdc e kadmind sono eseguiti in spazio utente.

kadmind è il demone amministrativo di Kerberos; kadmind si usa attraverso il programma kadmin per la manutenzione del database dei principal e la configurazione dei criteri. Se si sceglie di non permettere il login remoto tramite ssh sulla macchina Kerberos, kadmin consente l'amministrazione remota dei componenti Kerberos del server.

krb5kdc è la bestia da soma del server Kerberos, vestendo il ruolo di terza parte fidata nel processo di autenticazione. Quando un utente vuole autenticarsi presso un sistema o un servizio, chiede un ticket al KDC. Un ticket è un datagramma che contiene l'identità del client, una chiave di sessione, una marcatura oraria e altre indicazioni; il datagramma è cifrato con la chiave segreta del server.

Descrivendo il processo più in dettaglio, esso inizia con la richiesta di autenticazione che è trasmessa al demone krb5kdc. Quest'ultimo, ricevuta la richiesta, cerca il client, cioè il principal, nel database dei principal per autenticarlo; legge la chiave segreta del client nel database e cifra un ticket speciale detto Ticket Granting Ticket (TGT), che invia al client. Il client riceve il TGT cifrato che contiene una chiave di sessione; se il client conosce la password (la chiave segreta che è conservata nel database dei principal) può decifrare il TGT, quindi lo cifra con la chiave di sessione, che è contenuta nel TGT stesso, per presentarlo a un Ticket Granting Service (TGS). Il TGS rilascia un ulteriore Ticket che consentirà al client di ottenere l'autenticazione presso uno specifico sistema o servizio.

L'autenticazione sicura si realizza tramite l'uso di ticket cifrati che possono essere decifrati soltanto se il client conosce la chiave segreta. Il ticket contiene informazioni sull'orario per prevenire attacchi di replica, che consistono in rappresentazioni fraudolente di un ticket rilasciato precedentemente, per ottenere un accesso illecito.

2.4. Compromissione dell'infrastruttura Kerberos

Il primo modo in cui un aggressore può tentare di compromettere un'infrastruttura Kerberos è attaccando il server Kerberos; se l'aggressore riuscisse a ottenere un accesso di root al KDC egli avrebbe accesso al database delle password cifrate dei principal. In questo modo l'aggressore potrebbe accedere anche al software Kerberos e ai file di configurazione e modificarli per fare in modo che il sistema consenta delle autenticazioni che non dovrebbero avere successo.

Tra gli altri metodi per attaccare l'infrastruttura di Kerberos vanno citati gli attacchi di replica (replay attack) e i tentativi di indovinare la password (password guessing attack). Un attacco di replica si esplica intercettando o acquisendo altrimenti un ticket Kerberos e utilizzandolo fraudolentemente per tentare di ottenere l'autenticazione. Per provare a indovinare la password si possono intercettare dei ticket Kerberos sulla rete per decifrarli mediante un attacco di forza bruta.

Un aggressore può sfruttare le vulnerabilità del software vetusto ancora presente nell'infrastruttura; per esempio sono noti parecchi problemi con la versione 4 di Kerberos il più importante dei quali è una fondamentale debolezza nel protocollo usato per la crittografia. Il progetto di Kerberos versione 4 contempla l'uso di DES in modalità normale che permette a un aggressore di intercettare e modificare il testo cifrato del ticket senza lasciare tracce. Per prevenire questi attacchi Kerberos è stato modificato nella versione 5 che usa triple DES in modalità Cipher Block Chaining (CBC).

Trattando della robustezza della versione 4 di Kerberos è importante notare anche che parecchie implementazioni soffrono di vulnerabilità di superamento del buffer (buffer overflow). Le implementazioni di riferimento di Kerberos versione 5 hanno riparato le vulnerabilità di superamento del buffer presenti nella versione 4 ma le distribuzioni della versione 5 generalmente forniscono programmi che consentono la compatibilità all'indietro e supportano le applicazioni preesistenti progettate per Kerberos 4; si ritiene che il codice compatibile presente nella versione 5 sia ancora vulnerabile agli attacchi di buffer overflow.

Quindi, visti i problemi del protocollo della versione 4 e le potenziali vulnerabilità di superamento del buffer, è meglio non supportare né usare Kerberos versione 4.

Riassumendo, da questa descrizione su come sia possibile compromettere un'infrastruttura Kerberos, si comprende che la sicurezza dello stesso server Kerberos è un'esigenza prioritaria; bisogna poi eseguire software Kerberos aggiornato e restare vigili scegliendo buone password e predisponendo buoni criteri per le password.

3. Installazione e configurazione

3.1. Descrizione generale della configurazione della macchina

Questa sezione del documento descrive l'installazione e la configurazione delle macchine e del software che svolge il ruolo di KDC. È possibile intervenire con aggiustamenti sulle configurazioni suggerite ma saranno presentati alcuni punti chiave che è importante tenere a mente quando si configura il KDC e anche se si sceglie di praticare una strategia di configurazione alternativa è necessario aver compreso il materiale che viene presentato quì.

Le macchine eseguono il demone Kerberos e conservano le password e le informazioni sui criteri, perciò è molto importante per la salvaguardia della rete che questi server siano messi in sicurezza. Bisognerà prendere ogni misura possibile per scongiurare la compromissione di questi server; le raccomandazioni per la sicurezza contenute in questa sezione rivestono fondamentale importanza.

La raccomandazione principale è di usare macchine dedicate per erogare il servizio KDC di kerberos; l'hardware dovrà essere inaccessibile alle minacce materiali e anche il sistema GNU Linux andrà rinforzato il più possibile. Dalla compromissione del KDC deriverebbe la compromissione dell'intera infrastruttura Kerberos.

3.2. Hardware

Il servizio Kerberos non ha grosse richieste riguardo all'hardware e ha capacità di ridondanza, quindi l'hardware del server può essere esiguo. Per i server Kerberos che ho distribuito ho usato macchine con un processore Pentium III e due dischi in RAID 1 hardware, sufficienti per svolgere da quaranta a centomila autenticazioni al giorno. Anche se il server può essere dotato di schede di rete ridondanti, bisogna evitare di tenerle attive entrambe contemporaneamente perché Kerberos scrive l'indirizzo IP del KDC nei ticket e se durante il processo di autenticazione il client contatta il KDC attraverso interfacce multiple possono insorgere difficoltà.

È importante evidenziare che il servizio Kerberos andrebbe eseguito su hardware dedicato. Riservare una macchina a Kerberos significa che soltanto gli amministratori di Kerberos avranno bisogno di accedere a quella macchina e che sulla macchina non saranno in esecuzione altri servizi, salvo probabilmente SSH. Tutte le password degli utenti saranno conservate presso i server Kerberos, quindi sarà bene limitare il più possibile l'accesso fisico alle macchine interessate; usando hardware riservato a Kerberos sarà più semplice adempiere a questo requisito, magari chiudendo il server con la sua console in un proprio armadio.

Per approfittare della capacità nativa di Kerberos di fornire ridondanza bisogna avere almeno due macchine che funzionano da KDC. Kerberos è progettato per essere distribuito con un server principale (master) e uno o più server secondari (slave); non c'è limite al numero di secondari.

3.3. Installazione di GNU Linux

Installando GNU Linux su server dedicati all'esecuzione dei servizi kerberos si percorreranno ulteriori passi per garantirne la sicurezza.

Per prima cosa si installerà soltanto il software assolutamente necessario per il servizio Kerberos, costituito dal sistema operativo di base e dai pacchetti Kerberos, escludendo X e qualunque applicazione grafica. SSH è opzionale e andrà installato se si desidera poter amministrare i server a distanza; del resto i server saranno parecchio più sicuri se si permetterà di accedervi soltanto mediante il terminale collegato direttamente ad essi.

In un sistema GNU Linux basato su Fedora Core, il servizio kerberos è fornito dai pacchetti:

```
krb5-server
krb5-libs
```

La documentazione e le librerie di sviluppo non andranno installate sul KDC perché non si intende usare questa macchina per altre attività che non siano l'espletamento del servizio KDC.

Nel passo successivo ci si accerterà che non vi siano porte aperte oltre a quelle necessarie e che tutti gli aggiornamenti di sicurezza siano stati applicati. Il procedimento per controllare quali aggiornamenti di sicurezza vanno applicati dipende dal programma di gestione dei pacchetti in uso. Per determinare su quali porte la macchina è in ascolto si può usare il comando netstat; per esempio su una macchina che ha in esecuzione soltanto ssh, si leggerà:

```
bash$ netstat -an | grep -i listen | less
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
```

Infine si dovrà configurare il server in modo che possano accedervi soltanto i server che devono comunicare con lui per esigenze di autenticazione, editando i file `/etc/hosts.allow` and `/etc/hosts.deny` insieme al file `iptables`.

3.4. La scelta del realm

I nomi dei realm [domini di protezione] sono sensibili alle maiuscole e devono esere unici sulla rete; è buona pratica usare come nome del realm il nome del dominio di secondo livello scritto in lettere maiuscole. Se si sta configurando Kerberos soltanto per una sottorete anziché per la rete intera, si potrebbe usare un nome di dominio figlio da far corrispondere alla sottorete.

Quando si sceglie la topologia dei realm si deve prendere in considerazione l'assetto complessivo dell'organizzazione; se si hanno uffici remoti o sottogruppi indipendenti è bene che essi appartengano a un realm separato. La topologia dei realm di Kerberos deve riflettere la topologia del sistema di gestione e non la struttura fisica della rete.

Infine si dovrà tener presente l'esistenza di sistemi preesistenti, come distribuzioni precedenti di Kerberos o raggruppamenti di rete che si intende mantenere (per esempio domini di Windows NT).

Se si installa Kerberos in una rete che ne ospita già una distribuzione, nella rete globale o in una sottorete, bisogna evitare una collisione di nomi. Il caso più comune in cui succede di distribuire kerberos in un ambiente in cui è già stato installato precedentemente è dove esiste un cluster IBM SP; la soluzione migliore è creare appositamente per il cluster SP un realm con un nome di dominio almeno di terzo livello e usare un nome di dominio di secondo livello per il realm Kerberos principale.

In questo documento si utilizzerà un esempio che aiuterà a illustrare il disegno e la configurazione di un'infrastruttura. Soggetto dell'esempio sarà una mitica università fondata per educare le persone ai contenuti liberi e per compiere ricerche sull'argomento, l'Università GNU di Dublino in Irlanda.

L'esempio comprende due server Kerberos usati per autenticare gli studenti e il corpo docente. Il nome di dominio dell'università è gnud.ie quindi per il realm Kerberos si userà GNUD.IE.

3.5. Configurazione del software Kerberos

Adesso è necessario configurare Kerberos, creare un amministratore, determinare un criterio di sicurezza e inizializzare il database dei principal di Kerberos.

Il primo passaggio consiste nell'editare il file di configurazione `/etc/krb5.conf`. In questo file si imposta il realm, si estende la definizione del realm specificando i server kerberos e infine si imposta il dominio del realm. Nell'esempio il contenuto del file è il seguente:

```
default_realm = GNUD.IE

[realms]
 GNUD.IE = {
  kdc = kerberos1.gnud.ie:88
  kdc = kerberos2.gnud.ie:88
  admin_server = kerberos1.gnud.ie:749
  default_domain = gnud.ie
 }

[domain_realm]
 .gnud.ie = GNUD.IE
 gnud.ie = GNUD.IE
```

Il database di Kerberos si crea e inizializza con il comando:

```
{Kerberos1}bash# /usr/Kerberos/sbin/kdb5_util create -s
```

Il flag *-s* fa in modo che il KDC crei un file riservato per autenticare sé stesso; si usa il flag *-r* per specificare un realm. Quando si crea un nuovo database è necessario specificare il realm soltanto se nel file `krb5.conf` sono definiti più realm.

A questo punto Kerberos domanderà di predisporre una master password per il database; è molto importante non dimenticarla. Non sarà possibile compiere alcuna azione amministrativa sul server se non si ricorderà la master password.

Ora è necessario editare il file delle acl [access control list] sul KDC per concedere l'accesso come amministratore. Normalmente questo file si trova in `/var/Kerberos/krb5kdc/kadm5.acl`. Può essere necessario specificarne la posizione nel file `kdc.conf`, il cui percorso è precisato nel file `/etc/krb5.conf` ed ha come valore predefinito `/var/Kerberos/krb5kdc/kdc.conf`. Considerando l'esempio dell'Università GNU di Dublino si dovrà modificare il file delle acl perché contenga la riga:

```
*/admin@GNUD.IE     *
```

Questa impostazione significa che a ogni account che termina con un /admin nel realm *GNUD.IE* sono concessi tutti i diritti d'accesso.

Una volta impostato l'accesso per gli utenti amministratori bisogna creare tali utenti; questo si fa utilizzando il comando kadmin.local, impartito da una shell di root sul KDC e usando il suo sottocomando addprinc. Di solito il nome dell'account amministrativo è *admin*; nell'esempio della Università GNU di Dublino è scritto come:

```
{Kerberos1}bash# /usr/Kerberos/sbin/kadmin.local -q "addprinc admin/admin"
```

Sul server andranno eseguiti i dèmoni krb5kdc e kadmin. Se è necessario potrà essere eseguito anche krb524 per fornire la compatibilità con i client Kerberos 4. Tuttavia prima di far partire krb524 si rammenti l'avvertimento riguardante le debolezze nella sicurezza di Kerberos 4 e ci si accerti di avere davvero bisogno di questa funzionalità. Sui KDC si possono configurare i dèmoni krb5kdc e kadmin per avviarsi automaticamente, tramite il comando chkconfig.

```
{Kerberos1}bash# /sbin/chkconfig krb5kdc on
{Kerberos1}bash# /sbin/chkconfig kadmin on
```

Alternativamente si possono avviare manualmente, impartendo i comandi:

```
{Kerberos1}bash# /etc/rc.d/init.d/krb5kdc start
{Kerberos1}bash# /etc/rc.d/init.d/kadmin start
```

Questo è sufficiente per ottenere un KDC funzionante.

3.6. Creazione dei principal

Si crea un principal di Kerberos per un utente con il comando:

```
{Kerberos1}bash# kadmin.local
{Kerberos1}kadmin.local: addprinc <username>
```

Se Kerberos deve supportare un vasto numero di account, si può scrivere uno script per creare i principal in massa.

4. Sincronizzazione del tempo

4.1. L'importanza della sincronia temporale

La sicurezza di Kerberos è basata anche sui time stamp dei ticket perciò è d'importanza critica che gli orologi dei sever kerberos siano regolati con accuratezza. Come è stato discusso nell'introduzione a kerberos, i ticket hanno una scadenza breve per prevenire attacchi di forza bruta e attacchi di replica.

Permettendo agli orologi di subire scostamenti si rende la rete vulnerabile a questi attacchi. A causa dell'importanza della sincronia degli orologi nella sicurezza del protocollo Kerberos, se gli orologi non sono sincronizzati entro un ragionevole intervallo Kerberos presenta errori fatali e smette di funzionare. I client che tentino di autenticarsi da una macchina con un orologio non accurato falliranno il tentativo di autenticazione presso il KDC a causa della differenza di ora con il suo orologio.

4.2. Introduzione a NTP

Per sincronizzare l'orario fra i server è disponibile il protocollo NTP (Network Time Protocol); esistono molti server NTP pubblici utilizzabili per la sincronizzazione. NTP può sincronizzare gli orologi dei client al millisecondo sulla LAN ed entro decine di millisecondi attraverso una WAN. I server NTP sono divisi in strati (stratum). I server NTP primari sono classificati come stratum 1; essi non devono essere usati per sincronizzare le macchine perché sono in numero esiguo. I server pubblici dello stratum 2 sono disponibili per la sinconizzazione dei client e a loro volta si sincronizzano con i server pubblici stratum 1. Si imposteranno i server Kerberos per interrogare tre server stratum 2 usando NTP. Questa (http://support.ntp.org/bin/view/Servers/StratumTwoTimeServers) è una lista di server pubblici dello stratum 2 [aggiornato dal traduttore].

4.3. Installazione e configurazione di NTP

Per abilitare NTP in GNU Linux è necessario installare il pacchetto NTP ed editare il file di configurazione, che per impostazione predefinita è `/etc/ntp.conf`. I valori della configurazione di default sono accettabili; bisogna soltanto aggiungere i server che si intende usare per sincronizzare l'orario. Non è necessario usare l'autenticazione ma si può farlo per aumentare la sicurezza; andrà usata se si utilizzano i server NTP della LAN. Quì c'è un esempio di file di configurazione per l'Università GNU di Dublino: `ntp.conf (http://cryptnet.net/fdp/admin/kerby-infra/en/ntp.conf)`.

Per ottenere l'effettiva sincronizzazione si imposta un job di cron:

```
30 * * * * /usr/sbin/ntpdate -s
```

Se i sistemi si trovano dietro un firewall si userà *-su* invece che soltanto *-s*. L'argomento *-u* indica a ntpdate di usare porte non privilegiate per la connessione in uscita ai server stratum 2.

5. Replica del server Kerberos

5.1. Descrizione della replica

Kerberos è stato progettato per permettere l'implementazione di un cluster di replica in configurazione master e slave. Un cluster Kerberos può consistere in qualunque numero di host; si raccomanda di schierarne almeno due: un master che funziona come server principale e almeno uno slave che resta disponibile come backup del master. I server master e slave sono anche detti rispettivamente server primario e server secondario.

Kerberos conserva tutte le sue informazioni, relative agli account e ai criteri, in database applicativi; la distribuzione del software Kerberos comprende programmi per replicare, o copiare, questi dati sugli altri server.

Le applicazioni client Kerberos sono progettate per tentare l'autenticazione sui server secondari se il server primario è indisponibile, quindi in caso di guasto non è necessario alcun provvedimento aggiuntivo per spostare il servizio di autenticazione di Kerberos sul server di backup. Invece le funzioni di amministrazione di Kerberos non sono interessate dal failover automatico.

In caso di guasto del server primario, kadmind diventa indisponibile, quindi le funzioni di amministrazione non saranno utilizzabili finché il server primario non sarà riparato o sostituito. In particolare durante un guasto al server primario non si potranno effettuare la gestione dei principal, la creazione e la sostituzione delle chiavi.

5.2. Implementazione

Per avviare la replica si impartisce il comando kprop sul master KDC; si può anche pianificarne l'esecuzione come job di cron per mantenere il database dei principal sincronizzato fra i server.

Nell'impostazione della replica innanzitutto si configurano le ACL per kpropd; il file delle ACL di kpropd per impostazione predefinita si trova nel percorso: `/var/Kerberos/krb5kdc/kpropd.acl`. Nell'esempio esso conterrà le righe:

```
host/kerberos1.gnud.ie@GNUD.IE
host/kerberos2.gnud.ie@GNUD.IE
```

Il file `kpropd.acl` può esistere soltanto sui server Kerberos secondari; nei sistemi GNU Linux derivati da Fedora, kadmin non viene eseguito su un server Kerberos su cui sia presente il file `/var/Kerberos/krb5kdc/kpropd.acl`.

Dopo di questo si devono creare le chiavi di host per i server Kerberos master e slave:

```
{Kerberos1}bash# kadmin.local
{Kerberos1}kadmin.local:  addprinc -randkey host/kerberos1.gnud.ie
{Kerberos1}kadmin.local:  addprinc -randkey host/kerberos2.gnud.ie
```

Le chiavi devono essere estratte nel file keytab: si tratta di un portachiavi che contiene le chiavi crittografiche che servono per autenticarsi presso il KDC. L'estrazione delle chiavi nel keytab si ottiene con il sottocomando ktadd:

```
{Kerberos1}kadmin.local:  ktadd host/kerberos1.gnud.ie
{Kerberos1}kadmin.local:  ktadd host/kerberos2.gnud.ie
```

Infine sarà necessario copiare il keytab sul server slave in modo che questo abbia le chiavi necessarie per procedere all'autenticazione.

```
{Kerberos2}bash# scp root@kerberos1.gnud.ie:/etc/krb5.keytab /etc
```

Questa linea inserita nel crontab del master server Kerberos sincronizza i database dei principal ogni quindici minuti:

```
15 * * * * /usr/local/bin/krb5prop.sh
```

Questo è il contenuto dello script `krb5prop.sh`:

```
#!/bin/sh

/usr/Kerberos/sbin/kdb5_util dump /var/Kerberos/krb5kdc/slave_datatrans

/usr/Kerberos/sbin/kprop -f /var/Kerberos/krb5kdc/slave_datatrans kerberos2.gnud.ie > /de
```

Questo comando, impartito manualmente, restituisce qualcosa di simile a quel che segue:

```
{Kerberos1}bash# /usr/Kerberos/sbin/kdb5_util dump /var/Kerberos/krb5kdc/slave_datatrans
{Kerberos1}bash# /usr/Kerberos/sbin/kprop -d -f /var/Kerberos/krb5kdc/slave_datatrans ker
3234 bytes sent.
Database propagation to kerberos2.gnud.ie: SUCCEEDED
{Kerberos1}bash#
```

Il server slave sincronizzerà il database dei principal con il server master.

5.3. Manutenzione

Una volta che siano stati impostati i job di cron, la propagazione dei principal sarà automatica e non richiederà alcuna manutenzione; al momento di un guasto del KDC primario non sarà necessario un intervento umano, a meno che il guasto non duri molto tempo.

6. Configurazione dei client

6.1. Configurazione generale dei client GNU Linux

Le distribuzioni di Kerberos per GNU Linux comprendono un pacchetto client che contiene tutto il software e i file di configurazione necessari per configurare una macchina GNU Linux capace di effettuare l'autenticazione Kerberos su un KDC. Nei sistemi basati su Fedora e suoi derivati si tratta del pacchetto *krb5-workstation*. Perché il sistema possa usare Kerberos per l'autenticazione, anche con l'utilizzo delle applicazioni compatibili, Kerberos deve essere configurato su di esso.

La configurazione consiste nell'editare il file `/etc/krb5.conf`, dove si specifica il realm, i KDC, il server amministrativo, il logging, il dominio predefinito, e le informazioni sul KDC; andrà modificato anche il file `kdc.conf`, la posizione del quale può essere specificata nel file `krb5.conf`; il percorso predefinito è `/var/Kerberos/krb5kdc/kdc.conf`. Il file `kdc.conf` contiene informazioni sul criterio dell'algoritmo di crittografia applicato nel realm.

Sul sistema che si vuole abilitare a effettuare l'autenticazione con Kerberos si devono immettere le medesime informazioni di configurazione che sono state scritte nel file `/etc/krb5.conf` del KDC. Si consultino anche i file di configurazione di esempio per l'università GNU di Dublino: `krb5.conf` (`http://cryptnet.net/fdp/admin/kerby-infra/en/krb5.conf`) e `kdc.conf` (`http://cryptnet.net/fdp/admin/kerby-infra/en/kdc.conf`).

A questo punto è possibile provare l'autenticazione di Kerberos, usando il comando kinit:

```
bash$ kinit <username>
```

Se l'autenticazione non riesce si può cercare una descrizione della causa del fallimento nei file del registro di sistema del client e nel file log di KDC nel KDC su cui si tenta di autenticarsi. Durante l'indagine sui problemi di autenticazione può essere d'aiuto avere un terminale aperto che esegue il comando *tail -f* sul file log di KDC. Nell'esempio di `krb5.conf` la posizione del file di registro del KDC è `/var/log/Kerberos/krb5kdc.log`.

6.2. PAM

La tecnologia PAM, o moduli di autenticazione inseribili (Pluggable Authentication Modules), che è inclusa in molte distribuzioni di GNU Linux, si integra con Kerberos tramite il modulo pam_krb5. Per utilizzare l'autenticazione Kerberos con PAM si deve installare il modulo pam_krb5 e modificare i file di configurazione di PAM.

Con il modulo pam_krb5 vengono installati dei file di configurazione esemplificativi, che si trovano in `/usr/share/doc/pam_krb5-1.55/pam.d`. La modifica fondamentale che è necessario inserire per permettere ai servizi controllati da PAM di autenticarsi con Kerberos è di questo tipo:

```
auth       required     /lib/security/pam_krb5.so use_first_pass
```

6.3. Il server web Apache

Si può utilizzare Kerberos come meccanismo di autenticazione per il server web Apache; tale funzionalità è fornita dal modulo mod_auth_kerb, mediante il quale è possibile impostare Kerberos come tipo di autenticazione per le occorrenze del controllo di accesso nel file `httpd.conf`. Si noti che questo non è il meccanismo di autenticazione ideale quando si usa kerberos, perché i ticket sono conservati nel server web anziché nella macchina client; peraltro se la finalità è di implementare una soluzione di accesso a un solo stadio o di consolidare gli account questa soluzione è praticabile. mod_auth_kerb può supportare Kerberos 4 ma questo documento non ne tratta, in considerazione delle debolezze nella sicurezza della versione 4 del protocollo.

Il sito di mod_auth_kerb si trova all'indirizzo http://modauthkerb.sourceforge.net/. Si raccomanda di usare il protocollo HTTPS per l'accesso ai siti che usano mod_auth_kerb, perché esso usa l'autenticazione di base che trasmette i dati in codifica base64 ed è semplice tradurli in testo in chiaro. È importante che le credenziali di autenticazione siano cifrate con SSL per garantire che il nome utente e la password siano protette mentre sono trasmesse al server web.

Si riportano i passaggi necessari per compilare Apache con il modulo mod_auth_krb.

```
bash$ export 'LIBS=-L/usr/Kerberos/lib -lkrb5 -lcrypto -lcom_err'
bash$ export 'CFLAGS=-DKRB5 -DKRB_DEF_REALM=\\\"GNUD.IE\\\"'
bash$ export 'INCLUDES=-I/usr/Kerberos/include'
bash$ mkdir apache_x.x.x/src/modules/kerberos
bash$ cp mod_auth_kerb-x.x.x.c apache_x.x.x/src/modules/kerberos
bash$ ./configure --prefix=/home/httpd --add-module=src/modules/Kerberos/mod_auth_kerb.c
bash$ make
bash$ make install
```

È consigliabile collaudare Apache per verificarne il buon funzionamento; quando si dispone di una copia sicuramente funzionante di Apache con SSL abilitato, si può modificare il file `httpd.conf` per fornire l'autenticazione kerberos per una directory.

Il frammento che segue è un esempio che abilita l'autenticazione Kerberos 5 per una directory attraverso il modulo mod_auth_kerb:

```
<Directory "/home/httpd/htdocs/content">
   AllowOverride None
   AuthType KerberosV5
   AuthName "Kerberos Login"
   KrbAuthRealm GNUD.IE
   require valid-user
</Directory>
```

6.4. Microsoft Windows

La compatibilità fra lo standard Kerberos del MIT e la versione Microsoft è limitata, a causa della imperfetta implementazione dello standard Kerberos da parte di Microsoft. Quì (http://www.microsoft.com/windows2000/techinfo/planning/security/kerbsteps.asp) è disponibile un documento pubblicato da Microsoft che descrive in che modo e con che limiti la versione viziata di Kerberos prodotta da Microsoft può operare insieme con quella standard.

7. La programmazione con Kerberos

7.1. L'API di Kerberos

Le librerie di sviluppo di Kerberos permettono di abilitare qualsiasi applicazione all'autenticazione con Kerberos. Sono due le librerie principali, una di uso generale usata per la semplice autenticazione e una libreria di amministrazione utile per svolgere funzioni amministrative quali le operazioni sui principal. Nei sistemi GNU Linux derivati da Fedora, il pacchetto rpm `krb5-devel` contiene le librerie di sviluppo e la documentazione. Una descrizione dell'API per queste librerie si trova nella documentazione di kerberos, inclusa nella maggior parte delle distribuzioni; nei derivati di Fedora si installa nel percorso: `/usr/share/doc/krb5-devel-1.2.2/api`.

La documentazione è nel formato LaTeX; per consultarla si devono generare da essa i file dvi che poi possono leggersi con il programma xdvi. Per far ciò si usano i comandi:

```
bash$ cd /usr/share/doc/krb5-devel-x.x.x/api/
bash$ su
bash# make
bash# (^d)
bash$ xdvi library.dvi
```

A. Fonti di approfondimento

A.1. Collegamenti a documenti pertinenti

- Kerberos V5 Installation Guide (http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.6/doc/install_toc.html)

- Kerberos V5 UNIX User's Guide (http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.6/doc/user-guide_toc.html)
- Kerberos V5 System Administrator's Guide (http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.6/doc/admin_toc.html)
- Upgrading to Kerberos V5 from Kerberos V4 (http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.6/doc/krb425_toc.html)
- Kerberos FAQ (http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html)
- Designing an Authentication System: a Dialog in Four Scenes (http://web.mit.edu/kerberos/www/dialogue.html)
- How To Kerberize Your Site (http://www.ornl.gov/~jar/HowToKerb.html)
- The Moron's Guide to Kerberos (http://www.isi.edu/gost/brian/security/kerberos.html)
- AFS FAQ (http://www.angelfire.com/hi/plutonic/afs-faq.html)
- The Kerberos 5 API (http://cryptnet.net/mirrors/docs/krb5api.html)
- The Kerberos 5 Admin API (http://cryptnet.net/mirrors/docs/krb5adm_api.html)

A.2. Siti web di interesse

- MIT Kerberos Website (http://web.mit.edu/kerberos/www/)
- The NTP Distribution Website (http://www.ntp.org/)
- List of Public Stratum 2 NTP Servers (http://www.eecis.udel.edu/~mills/ntp/clock2b.html)
- OpenAFS Website (http://www.openafs.org/)
- Heimdal Kerberos Website (http://www.pdc.kth.se/heimdal/)
- The Crypto Publishing Project (http://www.crypto-publish.org/) (Unrestricted source for Kerberos source code)
- SESAME (http://www.cosic.esat.kuleuven.ac.be/sesame/) (Secure European System for Applications in a Multi-vendor Environment)

A.3. RFC sull'argomento

- RFC2744: Generic Security Service API Version 2: C-bindings (http://cryptnet.net/mirrors/rfcs/rfc2744.txt)
- RFC2743: Generic Security Service Application Program Interface, Version 2 Update 1 (http://cryptnet.net/mirrors/rfcs/rfc2743.txt)
- RFC2712: Addition of Kerberos Cipher Suites to Transport Layer Security (TLS) (http://cryptnet.net/mirrors/rfcs/rfc2712.txt)
- RFC2078: Generic Security Service Application Program Interface, Version 2 (http://cryptnet.net/mirrors/rfcs/rfc2078.txt)

- RFC1964: The Kerberos Version 5 GSS-API Mechanism (http://cryptnet.net/mirrors/rfcs/rfc1964.txt)
- RFC1510: The Kerberos Network Authentication Service (V5) (http://cryptnet.net/mirrors/rfcs/rfc1510.txt)
- RFC1509: Generic Security Service API : C-bindings (http://cryptnet.net/mirrors/rfcs/rfc1509.txt)
- RFC1508: Generic Security Service Application Program Interface (http://cryptnet.net/mirrors/rfcs/rfc1508.txt)
- RFC1411: Telnet Authentication: Kerberos Version 4 (http://cryptnet.net/mirrors/rfcs/rfc1411.txt)
- RFC1305: Network Time Protocol (Version 3) Specification, Implementation and Analysis (http://cryptnet.net/mirrors/rfcs/rfc1305.txt)
- RFC1119: Network Time Protocol (Version 2) Specification and Implementation (http://cryptnet.net/mirrors/rfcs/rfc1119.txt)
- RFC1059: Network Time Protocol (Version 1) Specification and Implementation (http://cryptnet.net/mirrors/rfcs/rfc1059.txt)
- RFC958: Network Time Protocol (NTP) (http://cryptnet.net/mirrors/rfcs/rfc958.txt)

A.4. Altri riferimenti

- [Applied Cryptography] Second Edition, Bruce Schneier [ISBN: 0-471-11709-9 (http://www.amazon.com/exec/obidos/tg/detail/-/0471117099/qid%3D1085516723/sr%3D11-1/ref%3Dsr%5F11%5F1/103-3431487-6727030?v=glance)]

A.5. Risorse aggiuntive

- The Kerberos Authentication System Mailing List (http://mailman.mit.edu/mailman/listinfo/kerberos)
- The Kerberos Authentication System Mailing List Archives (http://mailman.mit.edu/pipermail/kerberos/)
- comp.protocols.kerberos (news:comp.protocols.kerberos) UseNet Newsgroup

A.6. Imprese che forniscono consulenza specializzata su Kerberos

- Cybersafe, Ltd. (http://www.cybersafe.ltd.uk/)
- e-TechServices.com, Inc. (http://www.e-techservices.com/solutions/kerberos/) IBM Business Partner

Glossario dei termini

ASN.1

Abstract Syntax Notation One [notazione sintattica astratta uno]. ASN.1 è una notazione usata per descrivere messaggi, come sequenze di componenti. ASN.1 è utilizzata per rappresentare il contenuto dei datagrammi di Kerberos; la sua conoscenza è utile soltanto agli sviluppatori di applicativi.

Authenticator

Un record che contiene informazioni che possono essere esibite nell'evidenza che sono state generate di recente usando la chiave di sessione nota soltanto al client e al server. (Definizione da RFC1510 (http://cryptnet.net/mirrors/rfcs/rfc1510.txt))

Credenziali

Un ticket per il server e una chiave di sessione che è utilizzata per autenticare il principal.

Cross-Realm Authentication [autenticazione trasversale ai realm]

Kerberos può consentire a un KDC di un realm di autenticare un principal in un altro realm se esiste un segreto condiviso da entrambi i realm; questa autenticazione tra i realm è detta cross-realm authentication.

Data Encryption Standard [DES]

Un algoritmo di cifratura che è stato l'algoritmo ufficiale del Governo degli Stati Uniti, sviluppato dall'IBM con la collaborazione della NSA. L'algoritmo è un cifrario a blocchi fissi di sedici caratteri che usa un blocco di 64 bit e una chiave di 56 bit.

Forwardable Ticket [Ticket inoltrabile]

Un ticket concesso dal KDC che consente agli utenti di richiedere ticket addizionali con indirizzi IP differenti; in pratica si tratta di un TGT che permette ai principal autenticati di ottentere ticket validi per altre macchine aggiuntive.

Generic Security Services Application Programming Interface [GSS-API]

Un insieme di associazioni del linguaggio C che fornisce servizi di sicurezza alla funzione chiamante; l'API può essere implementata su vari sistemi di crittografia, fra i quali Kerberos.

Key Distribution Center [KDC]

La macchina e il software che riveste il ruolo di arbitro di fiducia nel protocollo Kerberos.

Kerberos

Un protocollo di autenticazione che si appoggia a una terza parte fidata (arbitro) per l'autenticazione dei client in una rete TCP IP. Il protocollo è stato progettato in modo che sulla rete siano trasmessi ticket cifrati anziché password in chiaro, garantendo l'autenticazione sicura attraverso la rete.

Kerberize

[Neologismo americano che si è preferito tradurre con circumlocuzioni, essendo poco in uso l'omologo italiano. - NdT] (verbo transitivo) L'azione di modificare un sistema, un servizio o un programma in maniera che utilizzi Kerberos per l'autenticazione. (aggettivo kerberized) Un sistema, servizio o programma che supporta l'autenticazione attraverso Kerberos.

Network Time Protocol [NTP]

Un protocollo usato per sincronizzare gli orologi dei computer e dei router in internet.

Postdatable ticket [Ticket postdatato]

In Kerberos 5, un ticket che non è valido inizialmente e che lo diventerà in futuro; i ticket Kerberos normali sono validi dal momento della richiesta a quello della scadenza.

Preauthentication

Autenticazione aggiuntiva che ha luogo prima che un KDC conceda un TGT a un principal; un esempio può essere la soddisfazione dei requisiti di un sistema biometrico.

Principal

Un utente o server per il quale il KDC conserva una chiave segreta nel proprio database.

Proxiable Ticket [Ticket per procura]

In Kerberos 5, un ticket che permette di richiedere un TGT per un indirizzo IP alternativo.

Realm

L'ambito della distribuzione di Kerberos; precisamente, il dominio dell'organizzazione per cui il KDC è considerato di fiducia e può autenticare i principal.

Renewable Ticket [Ticket Rinnovabile]

In Kerberos 5, un ticket con una durata di rinnovo in aggiunta alla durata ordinaria del ticket. I ticket rinnovabili possono essere usati per acquisire ulteriori ticket dal KDC finché sono validi; i ticket rinnovati possono essere richiesti fino alla scadenza di rinnovo del ticket rinnovabile originario.

Salt

Un seme usato nella cifratura delle password per aumentare il numero dei risultati che è possibile ottenere come testo cifrato a partire dallo stesso testo in chiaro; l'uso del seme è una misura che protegge le password cifrate dagli attacchi del dizionario.

Stash File

Il file dove sono conservate le chiavi segrete.

Ticket

Un messaggio formato dall'identità del client, una chiave di sessione, un riferimento temporale e altre informazioni, tutte cifrate con la chiave segreta del server; è usato per costruire il procedimento di autenticazione.

Ticket Granting Service [TGS]

Un servizio che è autorizzato e organizzato per rilasciare ticket ai client dopo che essi hanno ricevuto un Ticket Granting Ticket (TGT).

Ticket Granting Ticket [TGT]

Un ticket contentente una chiave di sessione utilizzabile per la comunicazione fra i client e il KDC.

Transitive Cross-Realm Authentication

In Kerberos 5, la possibilità di formare una catena di fiducia attraverso i realm in modo che se un principal nel realm X ha bisogno di autenticare un principal nel realm Z, non è necessario che il KDC del realm X condivida un segreto con il realm Z, se entrambi condividono un segreto con il realm Y; quest'ultimo funge da intermediario nel percorso di fiducia.

Triple DES

Una variante di DES che cifra i dati tre volte con DES, usando due chiavi differenti.