VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

GENERAL NOTIFICATION SYSTEM FOR FREEIPA

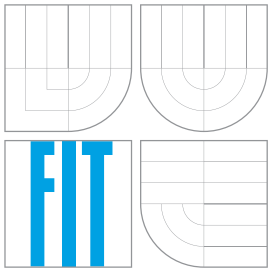
SEMESTRÁLNÍ PROJEKT
TERM PROJECT

AUTOR PRÁCE
AUTHOR

Bc. PETR KUBÁT

BRNO 2015

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

OBECNÝ NOTIFIKAČNÍ SYSTÉM PRO PROJEKT FREEIPA

GENERAL NOTIFICATION SYSTEM FOR FREEIPA

SEMESTRÁLNÍ PROJEKT
TERM PROJECT

AUTOR PRÁCE
AUTHOR

Bc. PETR KUBÁT

VEDOUCÍ PRÁCE
SUPERVISOR

Mgr. ADAM ROGALEWICZ, Ph.D.

BRNO 2015

Abstrakt

Výtah (abstrakt) práce v českém jazyce.

Abstract

Výtah (abstrakt) práce v anglickém jazyce.

Klíčová slova

LDAP, Active Directory, FreeIPA, Kerberos, DNS, Dogtag

Keywords

LDAP, Active Directory, FreeIPA, Kerberos, DNS, Dogtag

Citace

Petr Kubát: General Notification System for FreeIPA, semestrální projekt, Brno, FIT VUT v Brně, 2015

General Notification System for FreeIPA

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením pana Mgr. Adama Rogalewicze, Ph.D.

.....
Petr Kubát
December 28, 2015

Poděkování

Rád bych poděkoval hlavně panu Petru Špačkovi za jeho trpělivost pri odborném vedení práce.

Contents

Chapter 1

FreeIPA

FreeIPA (where IPA stands for Identity, Policy and Audit) is an open-source security management solution sponsored by Red Hat aimed primarily at Linux and Unix machines[12].

The project itself combines a number of various existing open-source technologies to achieve the goal of providing centralized authentication and authorization, as well as storing important account information like users or group memberships. FreeIPA also aims to provide easy management and setup of a domain controller which would otherwise be very difficult by using the same components on your own.

In this chapter I will briefly introduce some of the components FreeIPA uses and describe the architecture of the resulting FreeIPA server solution.

1.1 Directory Server

FreeIPA's directory service is the foundation of the whole solution as it stores various information on behalf of all of FreeIPA's components. It also plays a big role in authentication and authorization using Kerberos which will be presented in the next section.

The LDAP protocol[11] is used as a means of communication with the server and the data itself is stored in a Directory Information Tree (DIT) which is a tree-like data structure.

LDAP provides several operations to use with the server[11]:

- **add, delete, modify:** These operations add, remove and modify the data contained in the DIT.
- **search, compare:** The search and compare operations are used in querying the DIT for specific information.
- **bind, unbind, abandon:** These operations can be used to authenticate to the directory, terminating the connection or abandoning a previously sent request entirely, respectively.
- **extended operations:** New operations that are not a part of the original protocol.

The actual LDAP compatible server is implemented using the 389 Directory Server project[4].

1.2 Kerberos

Kerberos[10] is a network authentication protocol that uses symmetric encryption using a pre-shared key to authenticate the client to a network service (and vice versa) via an insecure connection using a trusted third party service called a Key Distribution Center (KDC).
The resulting communication is secure because no secret keys are transported over the network in plaintext format as the KDC already contains a database of credentials for users and services in the Kerberos realm.

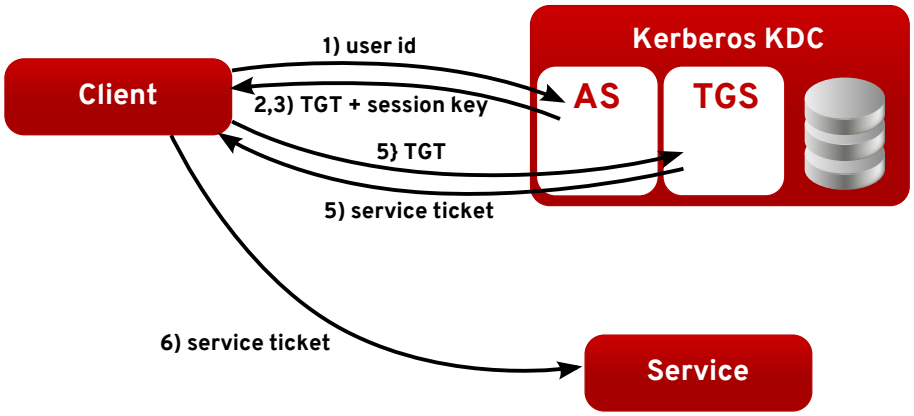


Figure 1.1: Kerberos authentication process.

The process of authenticating the user to a network service is shown in figure 1.1 and can be described in these steps:

1. The user sends his principal name (an unique identifier) to the KDC's Authentication Server (AS) via a plaintext request.

2. The AS then checks the database to make sure the user exists and sends back a randomly generated session key to be used to encrypt communication with another service called a Ticket-Granting Service (TGS) encrypted with the user's secret key.

3. The AS also generates a set of credentials called a Ticket-Granting Ticket (TGT) which includes the previously generated session key and is encrypted by the secret key of the TGS.

4. After recieving the first message the client decrypts it using his secret key. This is the only time the user's key is actually used. The TGT which the client can't decrypt himself is saved in a cache on the client's side to be used later to setup a session with the TGS. At this point the user is authenticated to the Kerberos realm and doesn't have to input his secret key again for a set amount of time (commonly 10-24 hours).

5. When the user wants to authenticate agains a service in the Kerberos realm he just has to ask the TGS to send him a ticket.

6. The user then authenticates to the chosen service using this ticket without the need for his secret key.

As the security of the Kerberos protocol is partly based on the time stamps of tickets, all of the clients and services in the realm have to be properly synchronized time-wise. To achieve this goal the Network Time Protocol is used in the FreeIPA project.
FreeIPA's KDC is implemented using the MIT Kerberos[8] open source software and FreeIPA also provides its own KDC data backend called ipa-kdb which is used to both read and write user information to FreeIPA's LDAP directory service[14].

1.3 DNS

Even though it would be possible to access network services located in a FreeIPA domain directly using their IP addresses, it is much more easier to do so using domain names.
The Domain Name System (DNS)[9] is distributed naming system, that translates domain names, which can be easily memorized by humans, into IP addresses using special name servers. As such if one wants to access a network service or a webpage he doesn't have to remember its IP address, only the IP address of the name server (which is stored localy on the client machine) and the domain name of the service/webpage.
The domain name space resembles a tree structure, each node having a label that designates a part of its domain name, while the full domain name of the node can be built by concatenating this label with the domain name of its parent node.
The name space is divided into zones starting at the root of the tree structure with child nodes of the root node called top-level domains (TLD). These zones can contain one or several domains, each domain served by one or several name servers, and can be divided into additional zones if deemed necessary.
The DNS server in FreeIPA uses a enhanced BIND name server which allows FreeIPA to store data into a LDAP directory[15]. However using FreeIPA's integrated DNS server is optional and as such the project can be used with a different third party DNS server if so desired.

1.4 FreeIPA Architecture

1.5 Extending FreeIPA

1.5.1 Extending the Framework

1.5.2 Extending the Directory Server

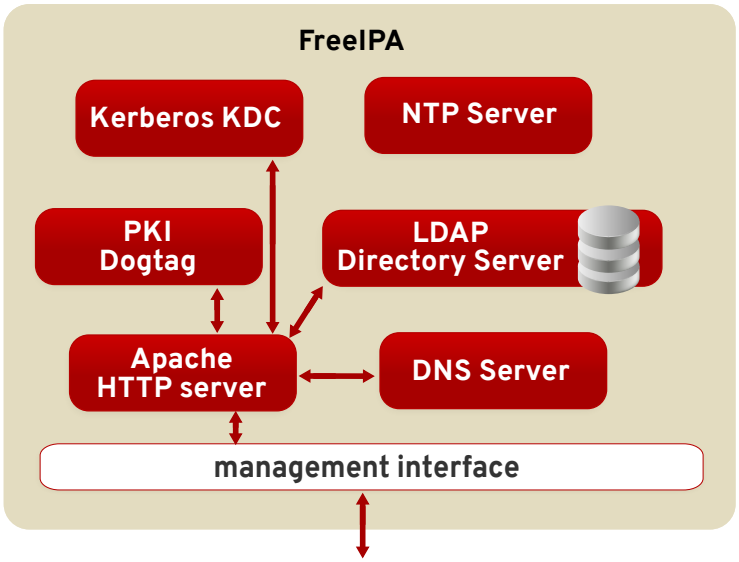


Figure 1.2: FreeIPA server architecture.

Chapter 2

Active Directory

Chapter 3

Analyze

Chapter 4

Conclusion

Bibliography

[1] dbus. [online], [cit. 2015-12-12]. http://www.freedesktop.org/wiki/Software/dbus/.

[2] Alexander Bokovoy. *Extending FreeIPA*, 2011. https://abbra.fedorapeople.org/freeipa-extensibility.pdf.

[3] Dogtag. Dogtag Certificate System. [online], [cit. 2015-12-12]. http://pki.fedoraproject.org/.

[4] Red Hat. 389 Directory Server. [online], [cit. 2015-12-12]. http://directory.fedoraproject.org/.

[5] Brian W. Kernigihan and Dennis M. Ritchie. *Programovacďž˝ jazyk C*. Computer Press, first edition, 2008. ISBN 80-251-0897-X.

[6] Microsoft. Event Tracing. [online], [cit. 2015-12-12]. https://msdn.microsoft.com/en-us/library/bb968803%28v=vs.85%29.aspx.

[7] Microsoft. Overview of Change Tracking Techniques. [online], [cit. 2015-12-12]. https://msdn.microsoft.com/en-us/library/ms677625%28v=vs.85%29.aspx.

[8] MIT. Kerberos: The Network Authentication Protocol. [online], [cit. 2015-12-12]. http://web.mit.edu/kerberos/.

[9] P. Mockapetris. Domain Names - Implementation and Speci

cation, RFC 1035. [online], November 1987 [cit. 2015-12-27]. https://tools.ietf.org/html/rfc1035.

[10] C. Neuman, T. Yu, S. Hartman, and K. Raeburn. The Kerberos Network Authentication Service (V5), RFC 4120. [online], July 2005 [cit. 2015-12-25]. https://tools.ietf.org/html/rfc4120.

[11] J. Sermersheim. Lightweight Directory Access Protocol (LDAP): The Protocol, RFC 4511. [online], June 2006 [cit. 2015-12-12]. https://tools.ietf.org/html/rfc4511.

[12] The FreeIPA Team. About FreeIPA. [online], [cit. 2015-12-12]. http://www.freeipa.org/page/About.

[13] The FreeIPA Team. bind-dyndb-ldap. [online], [cit. 2015-12-12]. https://fedorahosted.org/bind-dyndb-ldap/.

[14] The FreeIPA Team. Kerberos. [online], [cit. 2015-12-25]. https://www.freeipa.org/page/Kerberos.

[15] The FreeIPA Team. DNS. [online], [cit. 2015-12-27].
https://www.freeipa.org/page/DNS.