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

RÁCE Mgr. ADAM ROGALEWICZ, Ph.D.

SUPERVISOR

BRNO 2015

Δ	h	:+:	ra	\mathbf{kt}
$\overline{}$	IJ) L.I	_	n L

Výtah (abstrakt) práce v českém jazyce.

Abstract

Výtah (abstrakt) práce v anglickém jazyce.

Klíčová slova

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

Keywords

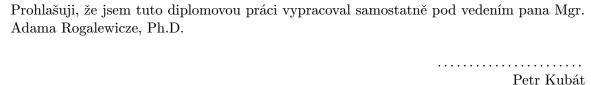
LDAP, Active Directory, FreeIPA, Kerberos, DNS, Dogtag

Citace

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

General Notification System for FreeIPA

Prohlášení



December 20, 2015

Poděkování

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

Tato práce vznikla jako školní dílo na Vysokém učení technickém v Brně, Fakultě informačních technologií. Práce je chráněna autorským zákonem a její užití bez udělení oprávnění autorem je nezákonné, s výjimkou zákonem definovaných případů.

[©] Petr Kubát, 2015.

Contents

1	FreeIPA				
	1.1 Directory Server				
	1.2 Kerberos				
	1.3 DNS				
	1.4 Dogtag				
	1.5 FreeIPA Architecture				
2	Active Directory				
3	Analyze				
4	Conclusion				

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[10].

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 is built using the 389 Directory Server[4] and is used to store various information 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[9] is used as a means of communication with the 389 DS 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[9]:

- 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.

- 1.2 Kerberos
- 1.3 DNS
- 1.4 Dogtag
- 1.5 FreeIPA Architecture

Active Directory

Analyze

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. *Programovací 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] J. Sermersheim. Lightweight Directory Access Protocol (LDAP): The Protocol, RFC 4511. [online], June 2006 [cit. 2015-12-12]. https://tools.ietf.org/html/rfc4511.
- [10] The FreeIPA Team. About FreeIPA. [online], [cit. 2015-12-12]. http://www.freeipa.org/page/About.
- [11] The FreeIPA Team. bind-dyndb-ldap. [online], [cit. 2015-12-12]. https://fedorahosted.org/bind-dyndb-ldap/.