Securing OpenStack with FreeIPA

Adam Young
Senior Software Engineer
April 18, 2013

Subject Matter

- Securing OpenStack Services
- Kerberos
- LDAP
- X509 Certificate
- Identity Management
- AMQP
- Database

Audience Composition Survey

- Python Coders?
- System Administrators?
- Know Kerberos?
- Know LDAP?
- Worked with FreeIPA?

Audience Composition Survey Cont

ere because you thought there was going to be fre

Agenda

- Securing the base
- About FreeIPA
- Technical details
- Looking forward

SECURING THE BASE

My Nightmare

- “Sure you can run your code on my computer
- In a virtual machine.”
- Hypervisor Exploit
- Escalation of Privileges
- Infects other Services
- Infects Virtual Machines
- All My Base Are Belong to You

OpenStack Architecture

OpenStack Architecture

Defense in Depth

What OpenStack Requires

- “Physical” Hosts for Services
- Identity Management
  - Σ Single Sign On
  - Σ Access Control/Minimize authority
- Secure Communication
  - Σ Encrypt on the Wire
  - Σ Certificate Management
  - Σ HTTPS
  - Σ AMQP
  - Σ Data Storage

Cloud Identity Management

“Physical” Layer

- May actually be virtual
- Allocated Machines
  - (at least) One per OpenStack API
    - Yes, you can consolidate some
  - AMQP
  - PostgreSQL
  - Several for Nova Compute
  - Several with disk for Swift
  - Administering > 10 servers.

FreeIPA

FreeIPA

- Integrated Identity and Authentication solution for Linux/UNIX networked environments.
- Open Source components
- Standard Protocols
- Ease of
  - Σ Management
  - Σ Automation of installation
  - Σ Configuration tasks.
- In RHEL as ipa-server etc...

Components

- (MIT) Kerberos
- Directory Server (LDAP, 389)
- Certificate Authority (Dogtag)
- Domain Name Server (BIND)
- System Security Services Daemon (SSSD)

Identity

freeIPA
identity | policy | audit

- User
- Groups
- Hosts
- Hostgroups
- Services
- Keytabs and Certificates
- DNS

Policy

- Access Control Lists (ACL)
- Host Based Access Control
  - Σ System Security Services Daemon (SSSD)
- SUDO
- Automount
- SELinux User Maps
- Cross Domain Trusts

MIT Kerberos

- Authentication
- Multiple Protocols
- 2 Way Verification
- Cross Domain Trusts
- Ticket Policy
- Wire Encryption (SASL)
- New: DIR: Credential Caches
  Σ Multiple KDCs/TGTs

TECHNICAL DETAILS

Mapping FreeIPA to OpenStack

- Kerberos SSO for “Physical Layer”
  - Σ Authentication between components
- Encrypting AMQP
- Certificate management for HTTPS
- LDAP provider for Keystone
- Kerberos to Keystone
  - Σ Apache with mod_auth_krb5

General Approach

- Install FreeIPA Server
- Install ipa-client on each machine and enroll
- Service keytab/credentials cache
- Set up Service
- Test with command line tools
- Set up SSL
  - Certmonger...

Certmonger

which attempts to simplify interaction with certifying authorities (CAs) on networks which use public-

otify early

new certificate via FreeIPA

rage

Service Choices

- Fedora 18 for Development
- PostgreSQL
  - Shared instance
  - Clustered? Replicated?
- Qpid
- Apache HTTPD
- 389 Directory Server
- Network Security Services (NSS)
- CYRUS-SASL

Keystone

- Cron for TGTs (UGLY!)
  - KRB5CCNAME=FILE:/tmp/krb5cc_$UID
  - kinit keystone -k -t /var/kerberos/krb5/user/$UID/client.keytab"
- SQLAlchemy URL
  - connection = postgresql://pg.openstack.freeipa.org/keystone?krbsrvname=postgres

Keystone: HTTPD

- mod_auth_krb5
- REMOTE_USER
- LDAP Backend for Identity
  - Kerberos for internal
  - Simple Bind for Keystone User requires code change for some operations
- Keytab for httpd service and user

Qpid

- /etc/sasl2/qpidd.conf
  - mech_list: GSSAPI
- /etc/qpidd.conf
  - /cluster-mechanism=GSSAPI
  - auth=yes
  - realm=OPENSTACK.FREEIPA.ORG
- Keytab and credential cache
- SELinux updates via audit2allow
- python-saslwrapper python-amqplib for clients

LOOKING FORWARD

Looking Forward

- Automatic credentials refresh
- Apache HTTPD
- Kerberize Horizon
- Authorization Data in Service Tickets
- Kerberos over HTTP

Looking Forward

- Access Control List Delegation
  - Enrollment, Group, DNS
  - No Admin LDAP operations
- Centralized SUDO/Rootwrap
- SSH Keys
- Encryption Keys

Documentation

org/page/Documentation

org/books/0.20/AMQP-Messaging-Broker-CPP-Book/html/chap-Messaging_User_

t.org/wiki/Getting_started_with_OpenStack_on_Fedora

e.org/qpid/rasc.html

sql.org/docs/devel/static/auth-methods.html

people.org/repos/openstack/openstack-grizzly/fedora-openstack-grizzly.repo

redhat®