Централизованное управление системами на базе GNU/Linux

Кривушин Михаил

17 мая 2008 г.

Краткое описание сети

Задачи выполняемые сетью

- розничная сеть, множество филиалов
- основная задача сети - торговые операции на терминальных серверах
- необходим обмен документами
- развернут домен Active Directory, требуется интеграция

Два этапа внедрения

- Thinstation Linux - тонкие клиенты
- Kubuntu - полноценное десктоп окружение

Вступление

Составляющие эффективного управления информационными системами

- централизованная аутентификация
- хранение и репликация сетевой информации
- управление конфигурацией на элементах системы

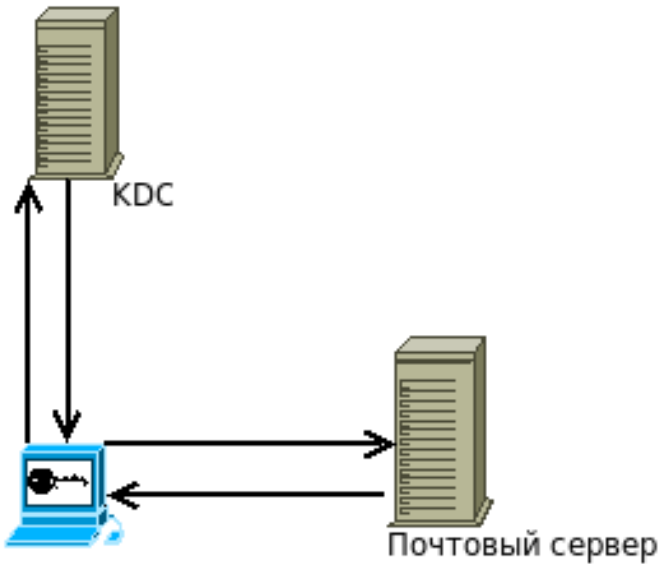
Технологии

- Kerberos - аутентификация
- Каталог LDAP - хранение и репликация
- Cfengine - управление конфигурацией

Kerberos, описание протокола

- разработан в МИТ для проекта Athena
- построен на криптографии с симметричным ключом
- разрабатывался в основном для клиент-сервисной модели, предоставляет взаимную аутентификацию
- Инфраструктура требует доверенной третьей стороны - KDC (Key Distribution Center, центр распределения ключей).

Kerberos - служба аутентификации



Процесс аутентификации

Краткое введение в протокол

- Для аутентификации пользователь запрашивает у KDC билет
- Билет включает в себя случайный ключ, зашифрованый ключом пользователя, и его копию, зашифрованную ключом сервиса
- TGT - билет для получения билетов

Поддержка различными приложениями

Поддерживается

- Squid, CUPS
- Apache, Subversion, Firefox
- NFSv4, Samba, OpenAFS
- Cyrus IMAP, Exim, KMail
- IPSEC (Racoon)
- Telnet, SSH

Не поддерживается

- в реализациях XMPP (Jabber)
- в mount.cifs

Особенности настройки

Настройки сетевой инфраструктуры

- Обязательная настройка NTP
- Настройка прямой и обратной зон DNS

Поддержка ключа системы

- Heimdal KCM
- K5start
- Cron или Cfengine

Нерешенные проблемы

- Отсутствует возможность получить TGT по запросу сервиса
- Нет реализации Read Only KDC

Взаимодействие с Active Directory

Доступ из Linux к AD среде

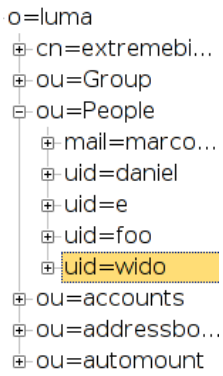
- дружба доменов - прозрачная аутентификация
- отображение имен - авторизация
- libsmbclient - доступ к сетевым ресурсам

Доступ из AD к Linux сервисам

- дружба доменов
- Winbind для энумерации пользователей
- Samba

Каталог LDAP, хранилище сетевой информации

- Lightweight Directory Access Protocol, протокол доступа к каталогу
- Позволяет искать по каталогу, изменять, добавлять и удалять записи
- хорошо подходит для хранения записей, у которых не все атрибуты обязательны для заполнения, или могут включаться несколько раз



Пример записи

```
dn: cn=users,dc=realm,dc=tld
objectClass: posixGroup
cn: users
gidNumber: 7003
memberUid: mkrivushin
memberUid: szaitsev
```

Поддержка LDAP приложениями

Со стороны серверов

- DNS
- DHCP
- Apache
- Squid

Рабочие станции

- Авторизационная информация
- Адресная книга
- Информация о сервисах

Авторизация, NSS Service

Использование LDAP для хранения авторизационной информации

- libnss-ldap - оригинальный пакет от PADL, требуется билет для каждого пользователя/демона
- libnss-ldapd - разделение библиотеки на сервер и клиент - ключ требуется только одному пользователю/демону
- syslog - не рекомендуется использовать стандартный Syslog демон
- nssupdate-db - кеширование на случай недоступности LDAP сервера

LDAP, программное обеспечение

Реализации

- OpenLDAP
- FedoraDS, средства конфигурирования в комплекте
- ApacheDS, помимо LDAP предоставляет интегрированные DNS, Kerberos

Средства управления

- PHPLDAPAdmin
- Luma, LDAPAdmin
- ldif + скрипты

Репликация

Модели репликации

- Мастер/реплики
- Равноправные мастер-сервера

OpenLDAP и репликация

- Syncrepl, новый механизм репликации в 2.4
- Поддерживается GSSAPI

Конфигурирование

Два типа инструментов для конфигурирования нескольких машин

- посылающие одновременно пользовательский ввод нескольким машинам, ClusterSSH
- системы с поддержкой конфигурации, Cfengine, Puppet, Bcfg2.

ClusterSSH

- Используется для передачи ввода в несколько сеансов одновременно
- Изначально разработан для управления кластерами
- Наиболее удобен для очень похожих систем

Системы с поддержкой конфигурации

Периодически проверяют все условия на которые настроены.

Возможные условия

- наличие определенной строки в файле,
- разрешения на доступ,
- состояние процесса (запущен/нет),
- установлен ли пакет
- и тд.

Краткое сравнение Cfengine и Puppet

- Puppet поддерживает шаблоны для создания файлов
- Cfengine предоставляет продвинутые средства для редактирования файлов
- Пакеты Puppet предоставляют однообразное конфигурирование для различных систем
- Cfengine требует знания особенностей конкретной среды

Распространение конфигурационной информации

Сравнение методов

- Cfengine и Puppet используют свои собственные протоколы, безопасность основана на парах ключей. Нет поддержки kerberos, сложности с репликацией
- Хранение в LDAP. Репликация уже настроена, GSSAPI

SCFL

LDAP $\longrightarrow SCFL \longrightarrow Cfengine$

Ссылки

- http://www.ixbt.com/comm/kerberos5.shtml
- http://openldap.org
- http://www.h5l.org
- http://deepwalker.blogspot.com