Интеграция приобретенных в 2024 рабочих станций учебного класса CMT B5-2007 с сетью Skoltech

Конфигурация учебного класса

1. Число рабочих станций, добавленных CMT в октябре 2024: **21**.
2. Host ОС: **Debian 12.7**.
3. Виртуализация: desktop virualization, гипервизор **VirtualBox**.
4. Гостевые ОС: **Windows 10 Enterprise**.
5. «Интеграция» на первом уровне OSI (обжатие 21 патчкорда) выполнена силами CMT.

Вопросы по интеграции на втором и третьем уровнях

Частично эти вопросы фигурировали в созданных мной tickets, здесь обобщение.

Аутентификация рабочих станций средствами 802.1x

Для wired-аутентификации использовалась учетная запись «*cmt_netservice*». На основе информации из Skoltech Wiki была реализована аутентификация средствами *wpa_supplicant* и *systemd* (подсистема *NetworkManager* на хостовых ОС установлена, но не используется).

Выделение IP-адресов

Выявлено, что различным рабочим станциям (очевидно, с различными MAC-адресами проводного Ethernet-интерфейса) при аутентификации с одной и той же учетной записью могут выдаваться совпадающие IP-адреса (но могут и различные). Подобная ситуация не приемлема.

Более того, с учетом требования организации удаленного доступа как к хостовым, так и к гостевым ОС, потребуется привязка MAC-адресов к IP-адресам. Такая привязка может быть сделана только силами IT Department. Список MAC-адресов, отсортированный по именам хостов (*2007stud01*...*2007stud20*, *teacher2007*) и – возможно – гостевых ОС (*2007stud01v*...*2007stud20v*, *teacher2007v*) я предоставлю.

Интеграция гостевых ОС Windows с сетью Skoltech зависит от режима виртуализации сети на каждом из хостов. Штатная функциональность VirtualBox допускает 2 основных режима виртуализации сети.

В одном из способов на каждом из хостов средствами VirtualBox создается транслятор сетевых адресов (NAT), гостевая ОС «невидима» для сети Skoltech и на ней не требуется выполнять

802.1x-аутентификацию. Доступ к сервисам гостевой ОС (например, к её RDP-серверу) может быть организован только средствами DSTNAT в составе VirtualBox. Недостатком является необходимость в некоторых случаях использовать нестандартные номера портов на IP-адресе хостовой ОС (в частности, на хостовых ОС также запущен RDP-сервер, и порт 3389 придется менять либо на хостовой ОС, либо на гостевой). Достоинство способа – нет необходимости расширять пул выделяемых IP-адресов на гостевые ОС.

При использовании другого способа средствами VirtualBox на каждом из хостов создается сетевой мост, гостевая ОС отправляет ARP-запросы в сеть Skoltech, получает (после 802.1x-аутентификации) от DHCP-сервера сети Skoltech необходимую информацию (IP-адрес и др.) Достоинство – гостевая ОС видима из сети Skoltech по своему IP-адресу, допустимо бесконфликтно использовать стандартные номера портов сервисов гостевой ОС. Недостаток – необходимость расширения пула IP-адресов на гостевые ОС.

Для рабочих станций, размещенных в помещении B5-2007, DHCP-сервер Skoltech выдает адреса из подсети 10.16.74.0/24, которая, *предположительно*, уже перегружена хостами.

Лучше, если выбор способа реализации (собственно реализация осуществляется силами CMT) будет выполнен сотрудниками IT Department.

Интеграция гостевых ОС с MS AD DS Skoltech

Выполняется стандартными для Windows средствами, требуется наличие представителя IT Department, с учетной записью администратора домена.

Интеграция хостовых ОС с MS AD DS Skoltech

Требует сотрудничества представителя CMT (меня) и представителя IT Department, обладающего учетной записью администратора домена.

Последнее обусловлено тем, что до идентификации и аутентификации администратора домена на стадии ввода хоста в домен MS AD DS Skoltech требуется выполнение подготовительных работ, включающих:

- реализацию **идентификации** (LDAP-сервер в составе MS AD DS Skoltech);
- реализацию **аутентификации** (Kerberos-сервер в составе MS AD DS Skoltech);
- реализацию **авторизации** (средствами MS AD совместно со средствами ОС Linux рабочей станции учебного класса).

Конкретные этапы подготовительных работ будут различными в зависимости от выбора администратора хостовых ОС Linux (штатные LDAP- и Kerberos клиенты ОС Linux + подсистема PAM; winbind в составе Samba; sssd; sssd + realmd и пр.)

Мой выбор как администратора хостовых ОС зависит, в частности, от предварительной информации о MS AD DS Skoltech. В этой связи имеется ряд вопросов (см. последний раздел.)

DNS-серверы Skoltech

DHCP-сервер Skoltech (по крайней мере, для хостов подсети 10.16.74.0/24) выдает два IP-адреса DNS-серверов: 10.16.32.100 и 10.17.11.100. Как и следовало ожидать, оба этих DNS-сервера являются рекурсивными:

$ dig @10.17.11.100 intel.com

```
;; ANSWER SECTION:
intel.com.      50  IN  A   13.91.95.74
```

Оба этих сервера (как и DNS-сервер 10.17.11.200, также рекурсивный) корректно отвечают на запросы SRV-записей MS AD DS, например:

$ dig @10.17.11.100 -t SRV _ldap._tcp.skoltech.ru

```
;; ANSWER SECTION:
_ldap._tcp.skoltech.ru. 600 IN  SRV 0 100 389
    srv-dc-04.skoltech.ru.
_ldap._tcp.skoltech.ru. 600 IN  SRV 0 100 389
    srv-dc-03.skoltech.ru.
;; ADDITIONAL SECTION:
srv-dc-04.skoltech.ru.  3600    IN  A   10.17.11.100
srv-dc-03.skoltech.ru.  3600    IN  A   10.17.11.200
```

$ dig @10.17.11.200 -t SRV _ldap._tcp.dc._msdcs.skoltech.ru

```
;; ANSWER SECTION:
_ldap._tcp.dc._msdcs.skoltech.ru. 600 IN SRV    0 100 389
    srv-dc-01.skoltech.ru.
_ldap._tcp.dc._msdcs.skoltech.ru. 600 IN SRV    0 100 389
    srv-dc-04.skoltech.ru.
_ldap._tcp.dc._msdcs.skoltech.ru. 600 IN SRV    0 100 389
    srv-dc-03.skoltech.ru.
;; ADDITIONAL SECTION:
srv-dc-01.skoltech.ru.  3600    IN  A   10.17.11.100
srv-dc-04.skoltech.ru.  3600    IN  A   10.17.11.100
srv-dc-03.skoltech.ru.  3600    IN  A   10.17.11.200
```

Выбор DNS-сервера и имя домена MS AD Skoltech

1. **Вопрос**: ***следует ли доверить выбор*** **DNS-*сервера, отвечающего на запросы*** **MS AD DS, *серверу*** **DHCP Skoltech, *или же предпочтительным будет фиксированный выбор*** **DNS-*сервера*****?**
2. **Вопрос**: ***в моих запросах SRV-записей был указан фиктивный домен*** **MS AD «SKOLTECH.RU»; *очевидно, что имя домена*** **MS AD Skoltech (*и соответствующий Kerberos realm*) *будет уровнем ниже. Каково имя домена*** **MS AD Skoltech?**