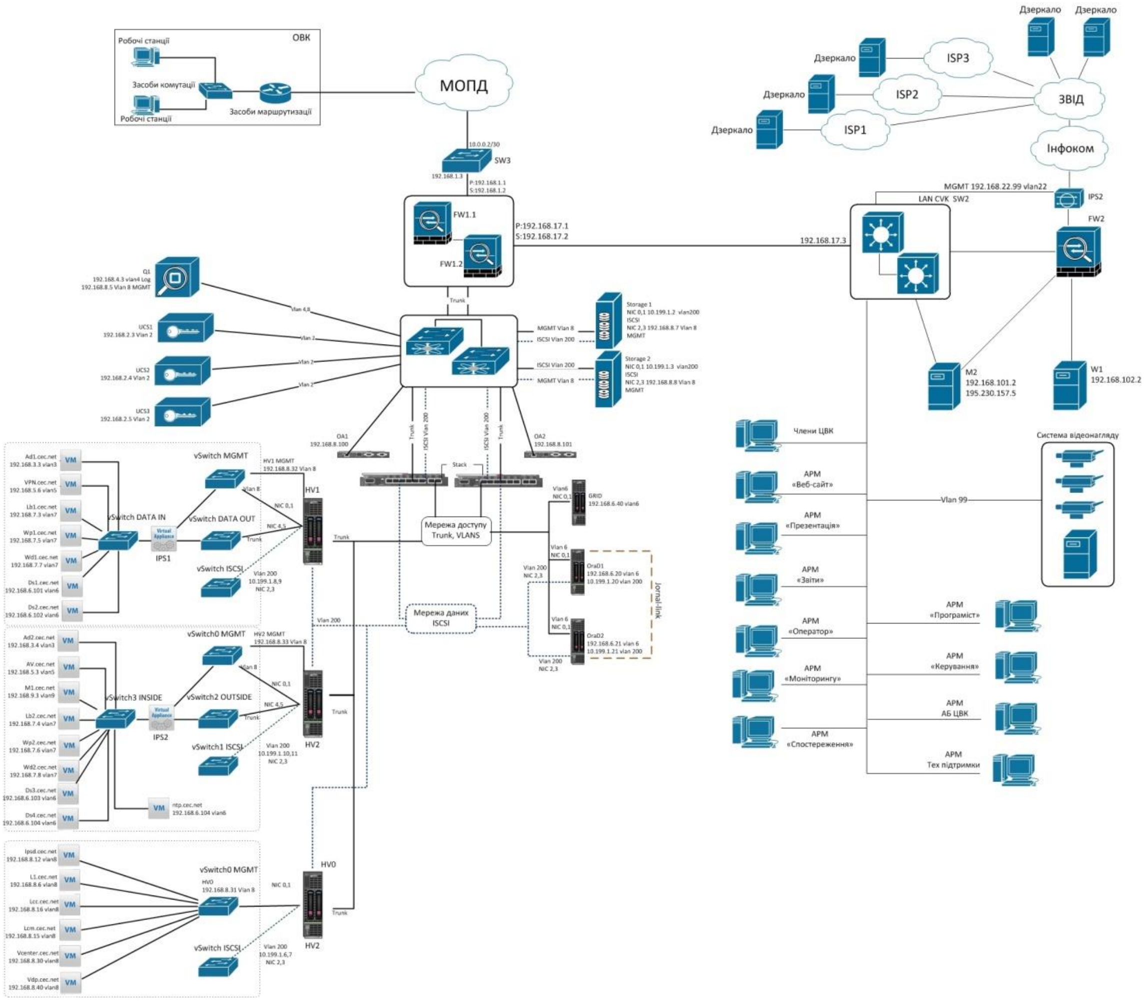
Взломали сеть ЦИК через 0-day уязвимость в Cisco ASA.

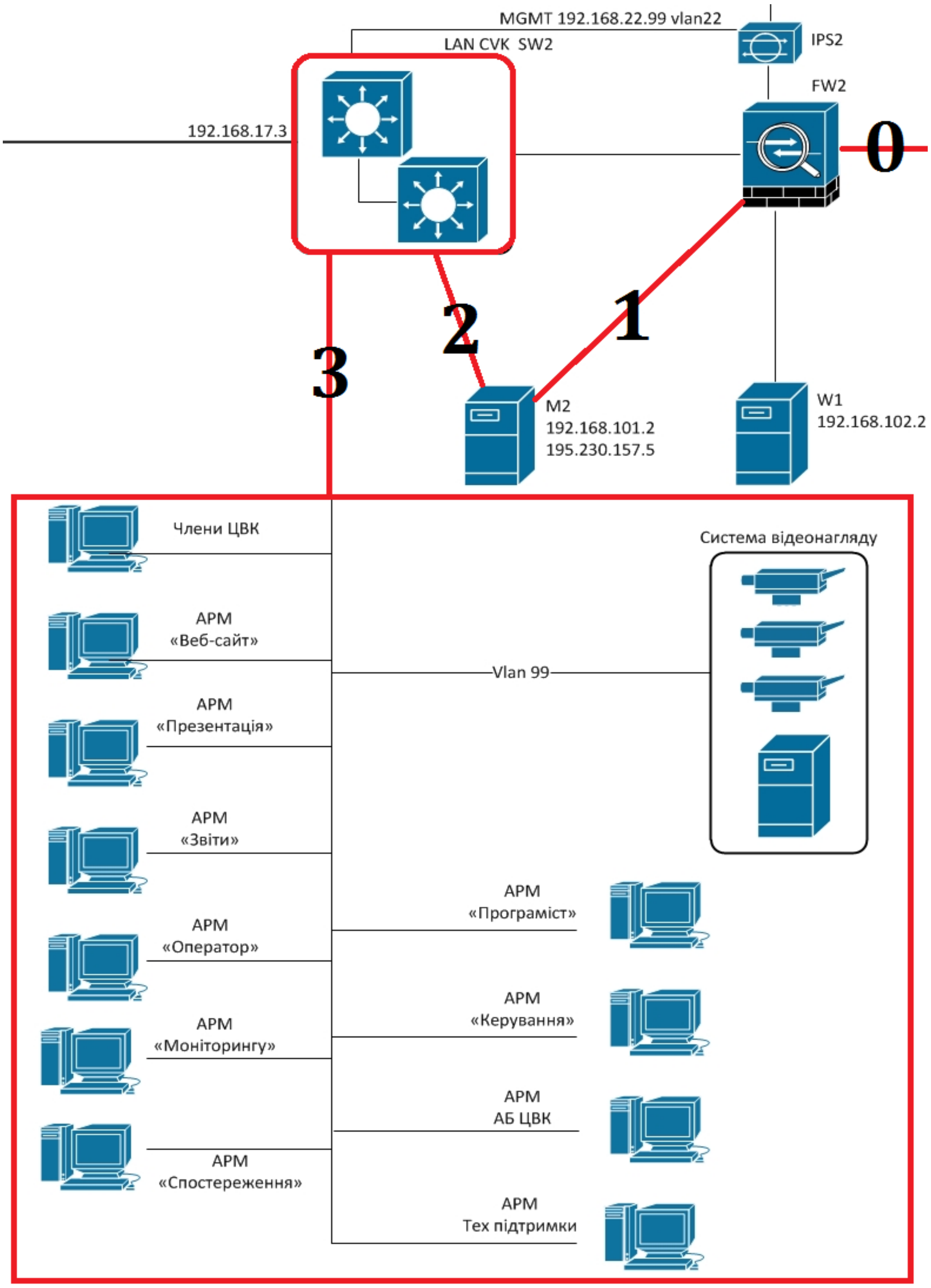
Карта взломанной сети ЦИК Украины:



Сеть состоит из 3 подсетей:

1. User LAN + DMZ;
2. Server & Storage LAN;
3. Удаленные клиентские машины.

**UserLAN + DMZ**



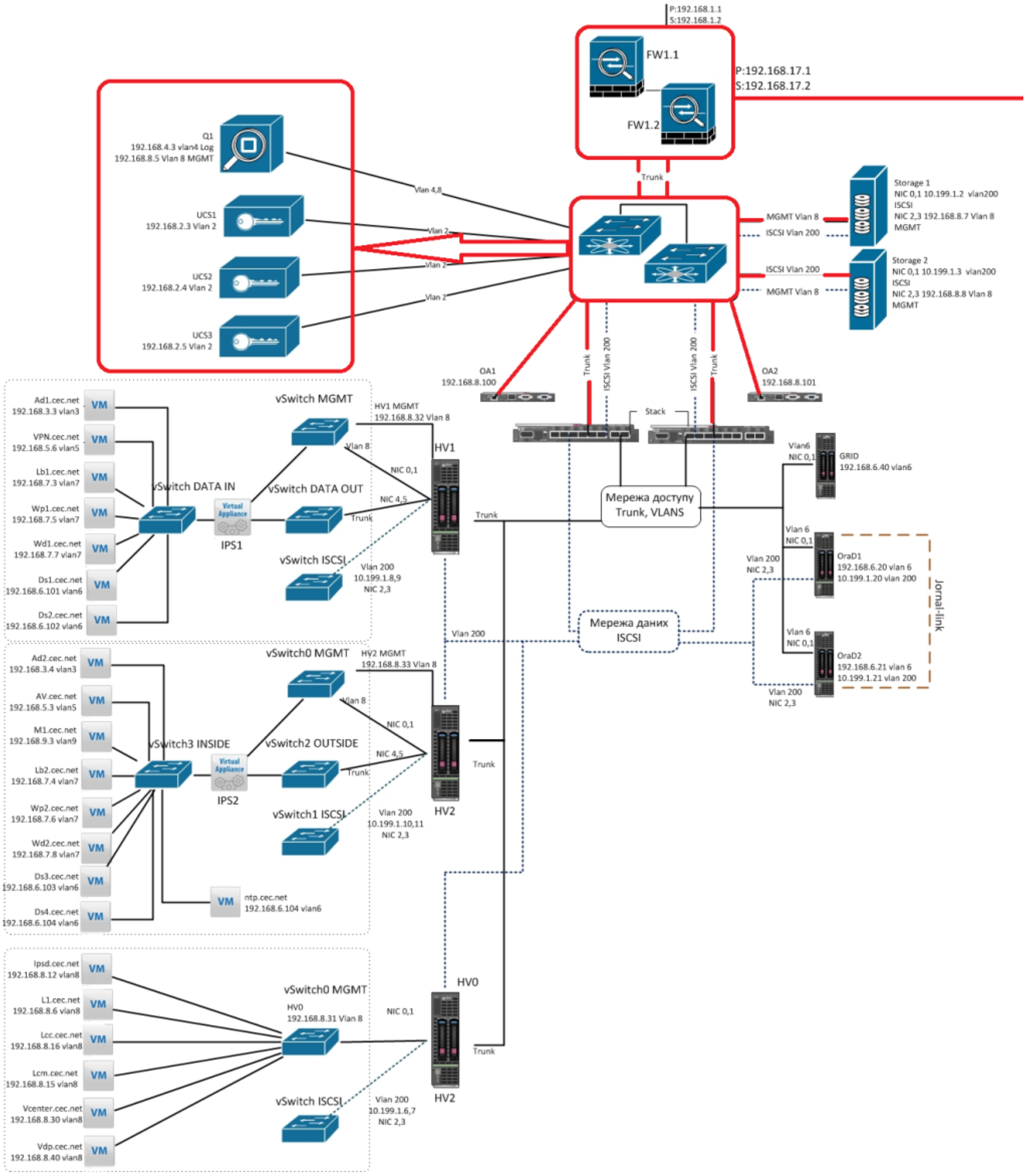
Эта подсеть состоит из ASA FW2, центрального коммутатора с резервированием и пользовательских машин. Прослушивая трафик на CiscoASA, получили доступ к внутренним ресурсам сети, в частности, к серверам с адресами 192.168.101.2 (M2) и 192.168.102.2 (W1). Судя по настройкам ASA, сервер M2 – почтовый, а W2–WEB.

```
access-list M2_access_in extended permit  tcp object-group M2 any4 eq smtp
object network DMZ-M2
nat (M2,outside) static 195.230.157.5 service tcp smtp smtp
object network DMZ-WEB
nat (W2,outside) static 195.230.157.53 service tcp www www
```

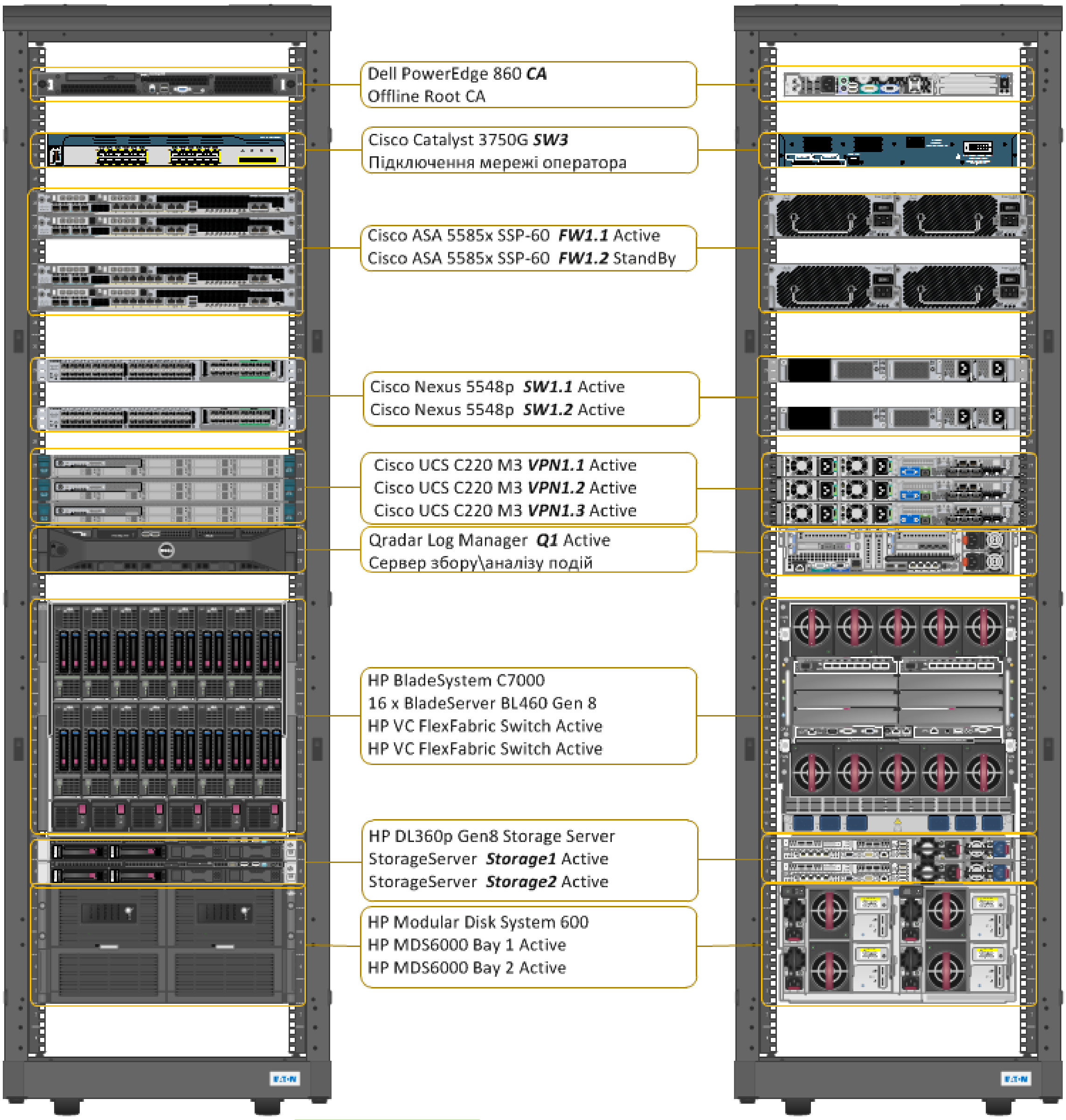
По всей видимости, то, что в настройках обозначено какW2, на схеме обозначено как W1.

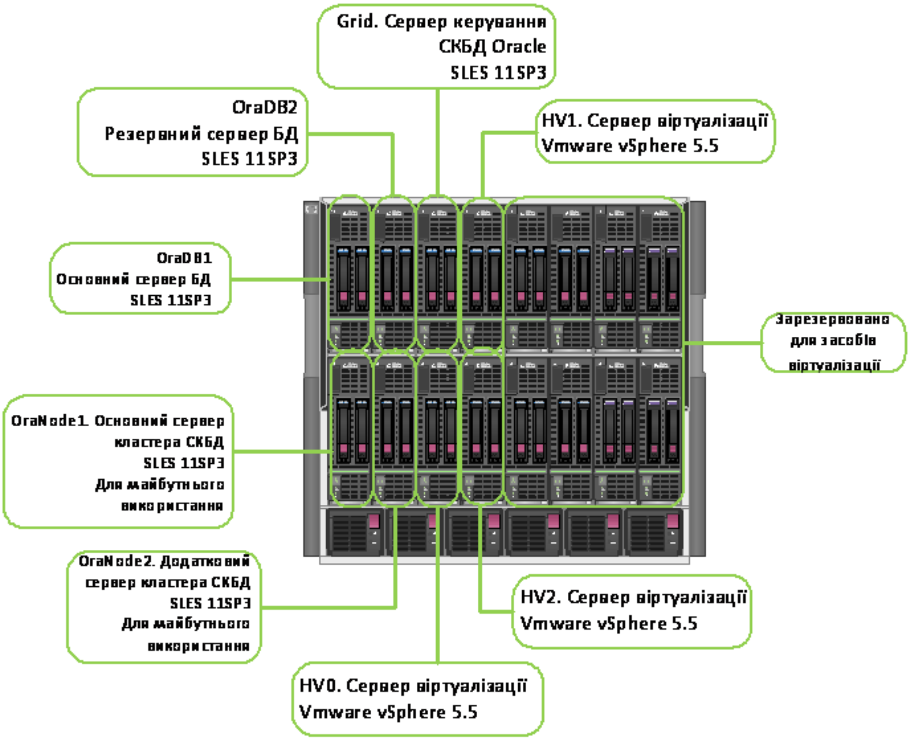
В почте выловили логины и пароли, среди которых были пароли администраторов. Эти учетные данные подошли к серверам M2 и W1 во внутренней сети User LAN и Server LAN.

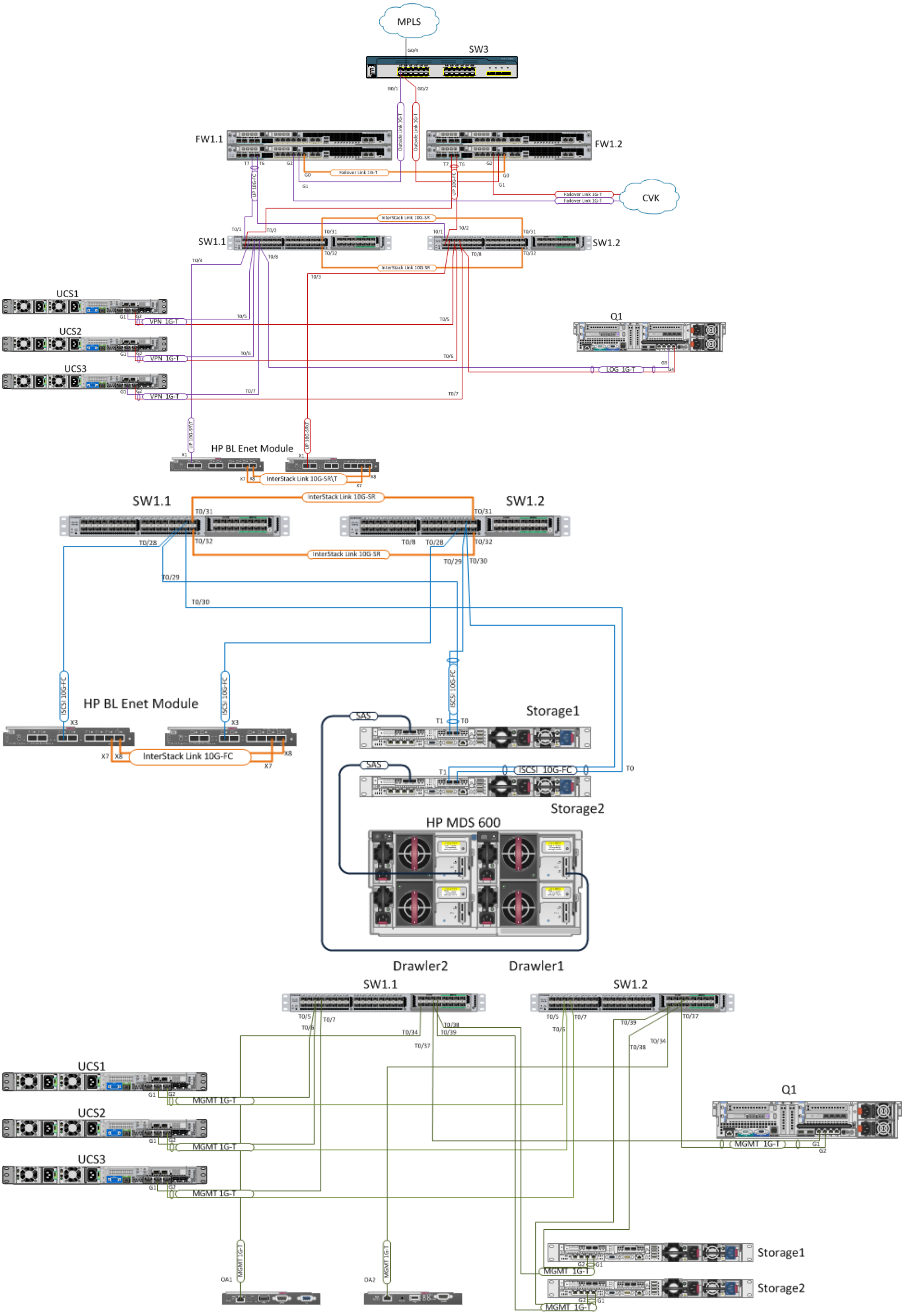
## Server&Storage LAN



В этом сегменте стоят CiscoNexus, развернута система хранения и система виртуализации. Второй сегмент состоит из двух корзин блэйд-серверов (OA 1,2) и файловых хранилищ (Storage 1,2).


Dell PowerEdge 860 ***CA***
Offline Root CA
Cisco Catalyst 3750G ***SW3***
Підключення мережі оператора
Cisco ASA 5585x SSP-60 ***FW1.1*** Active
Cisco ASA 5585x SSP-60 ***FW1.2*** StandBy
Cisco Nexus 5548p ***SW1.1*** Active
Cisco Nexus 5548p ***SW1.2*** Active
Cisco UCS C220 M3 ***VPN1.1*** Active
Cisco UCS C220 M3 ***VPN1.2*** Active
Cisco UCS C220 M3 ***VPN1.3*** Active
Qradar Log Manager ***Q1*** Active
Сервер збору\аналізу подій
HP BladeSystem C7000
16 x BladeServer BL460 Gen 8
HP VC FlexFabric Switch Active
HP VC FlexFabric Switch Active
HP DL360p Gen8 Storage Server
StorageServer ***Storage1*** Active
StorageServer ***Storage2*** Active
HP Modular Disk System 600
HP MDS6000 Bay 1 Active
HP MDS6000 Bay 2 Active


Grid. Сервер керування
СКБД Oracle
SLES 11SP3
OraDB2
Резервний сервер БД
SLES 11SP3
HV1. Сервер віртуалізації
Vmware vSphere 5.5
OraDB1
Основний сервер БД
SLES 11SP3
Зарезервовано
для засобів
віртуалізації
OraNode1. Основний сервер
кластера СКБД
SLES 11SP3
Для майбутнього
використання
OraNode2. Додатковий
сервер кластера СКБД
SLES 11SP3
Для майбутнього
використання
HV2. Сервер віртуалізації
Vmware vSphere 5.5
HV0. Сервер віртуалізації
Vmware vSphere 5.5

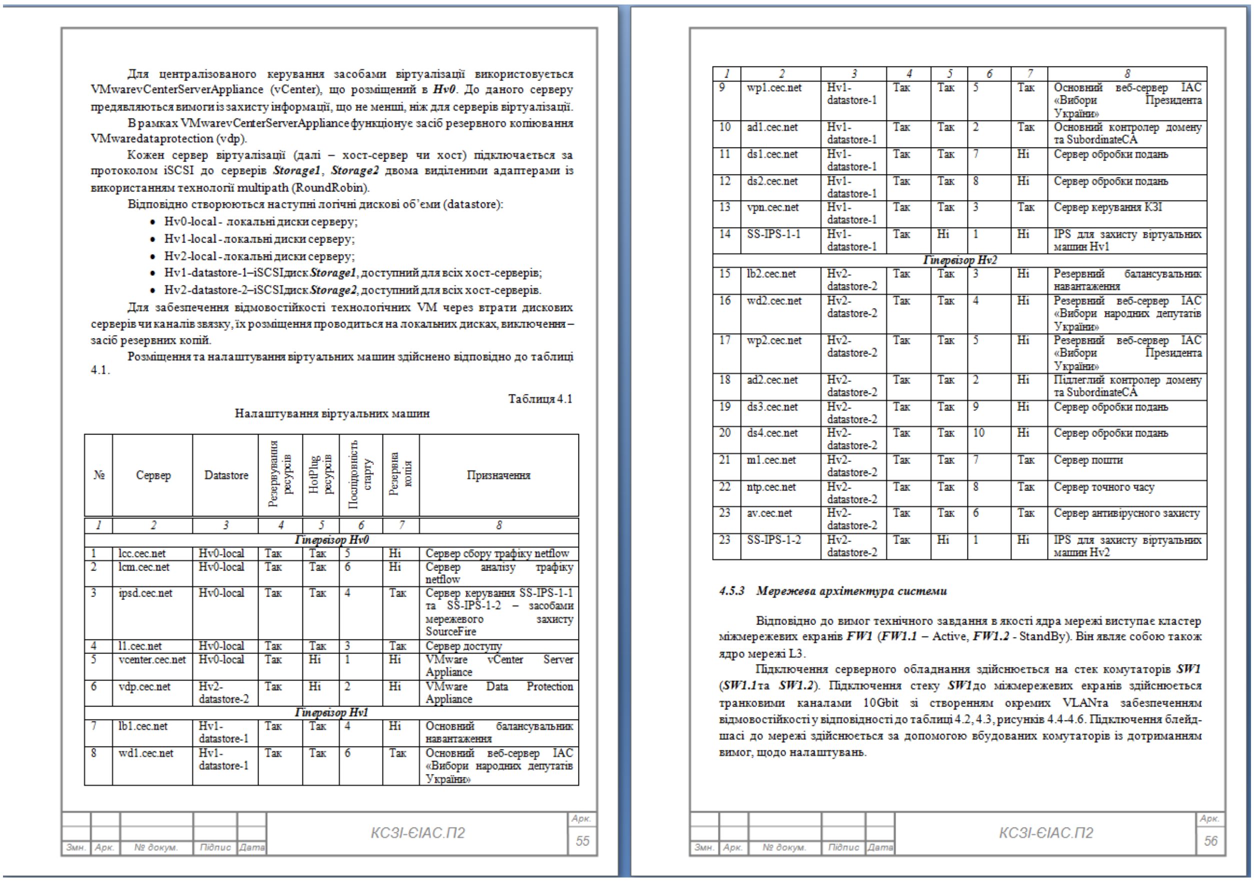

MPLS
SW3
G0/4
G0/1
G0/2
Outside Link 1G-T
Outside Link 1G-T
FW1.1
FW1.2
T7
T6
G2
G0
G1
Failover Link 1G-T
UP 10G-FC
UP 10G-FC
Failover Link 1G-T
Failover Link 1G-T
CVK
InterStack Link 10G-SR
T0/1
T0/2
T0/31
T0/32
T0/3
T0/8
SW1.1
SW1.2
InterStack Link 10G-SR
UCS1
UCS2
UCS3
G1
G2
VPN 1G-T
VPN 1G-T
VPN 1G-T
T0/5
T0/6
T0/7
Q1
G3
G4
LOG 1G-T
UP 10G-SR\T
UP 10G-SR\T
HP BL Enet Module
X1
X7
X8
InterStack Link 10G-SR\T
SW1.1
SW1.2
InterStack Link 10G-SR
T0/31
T0/32
T0/28
T0/29
T0/30
T0/8
InterStack Link 10G-SR
ISCSI 10G-FC
ISCSI 10G-FC
ISCSI 10G-FC
HP BL Enet Module
X3
X7
X8
InterStack Link 10G-FC
SAS
SAS
T1
T0
Storage1
ISCSI 10G-FC
Storage2
HP MDS 600
Drawler2
Drawler1
SW1.1
SW1.2
T0/5
T0/6
T0/7
T0/34
T0/37
T0/38
T0/39
UCS1
UCS2
UCS3
G1
G2
MGMT 1G-T
MGMT 1G-T
MGMT 1G-T
Q1
MGMT 1G-T
MGMT 1G-T
MGMT 1G-T
OA1
OA2
Storage1
Storage2
MGMT 1G-T
MGMT 1G-T

На входе в эту подсеть стоит ASA. Доступ к ней получили через ту же багу.

Конфигурация ниже. По ней видно, что доступ к основным узлам второй подсети (AD, Oracle и др.) открыт для админов. Именно с этих машин и пошли дальше.

```
access-listLAN_CVK_access_in extended permit tcp object-group Supportobject-group DBobject-group DB_admin_ports
access-listLAN_CVK_access_in extended  permit icmp object-group Support object-group DBecho
access-listLAN_CVK_access_in extended  permit tcp object-group Support object-group L1eq 3389
access-listLAN_CVK_access_in extended  permit icmp object-group Support object-group M1echo
access-listLAN_CVK_access_in extended  permit tcp object-group Support object-group M1eq https
access-listLAN_CVK_access_in extended  permit tcp object-group Support object-group ADeq domain
access-listLAN_CVK_access_in extended  permit udp object-group Support object-group ADeq domain
access-listLAN_CVK_access_in extended  permit tcp object-group Support object-group DSeq 3389
access-listLAN_CVK_access_in extended  permit ip object-group Support object-group L1
access-listLAN_CVK_access_in extended  permit ip object-group Support object-group AD
access-listLAN_CVK_access_in extended  permit ip object-group Support object-group M1
access-listLAN_CVK_access_in extended  permit tcp object-group Support object-group M1eq imap4
access-listLAN_CVK_access_in extended  permit tcp object-group Support object-group M1eq pop3
access-listLAN_CVK_access_in extended  permit tcp object-group Support object-group M1eqsmtp
access-listLAN_CVK_access_in extended  permit tcp object-group Support object-group M1eq www
```

Вся структура и назначение узлов сети очень подробно описана в ТЗ, которое удалось вытащить у сисадминов ЦИКа.



Для централізованого керування засобами віртуалізації використовується VMwarevCenterServerAppliance (vCenter), що розміщений в ***Hv0***. До даного серверу предявляються вимоги із захисту інформації, що не менші, ніж для серверів віртуалізації.

В рамках VMwarevCenterServerAppliance функціонує засіб резервного копіювання VMwaredataprotection (vdp).

Кожен сервер віртуалізації (далі – хост-сервер чи хост) підключається за протоколом iSCSI до серверів ***Storage1***, ***Storage2*** двома виділеними адаптерами із використанням технології multipath (RoundRobin).

Відповідно створюються наступні логічні дискові об’єми (datastore):

- Hv0-local - локальні диски серверу;
- Hv1-local - локальні диски серверу;
- Hv2-local - локальні диски серверу;
- Hv1-datastore-1–iSCSIдиск ***Storage1***, доступний для всіх хост-серверів;
- Hv2-datastore-2–iSCSIдиск ***Storage2***, доступний для всіх хост-серверів.

Для забезпечення відмовостійкості технологічних VM через втрати дискових серверів чи каналів звязку, їх розміщення проводиться на локальних дисках, виключення – засіб резервних копій.

Розміщення та налаштування віртуальних машин здійснено відповідно до таблиці 4.1.

Таблиця 4.1

Налаштування віртуальних машин

| № | Сервер | Datastore | Резервування ресурсів | HotPlug ресурсів | Послідовність старту | Резервна копія | Призначення |
|---|---|---|---|---|---|---|---|
| *1* | *2* | *3* | *4* | *5* | *6* | *7* | *8* |
| ***Гіпервізор Hv0*** | | | | | | | |
| 1 | lcc.cec.net | Hv0-local | Так | Так | 5 | Ні | Сервер сбору трафіку netflow |
| 2 | lcm.cec.net | Hv0-local | Так | Так | 6 | Ні | Сервер аналізу трафіку netflow |
| 3 | ipsd.cec.net | Hv0-local | Так | Так | 4 | Так | Сервер керування SS-IPS-1-1 та SS-IPS-1-2 – засобами мережевого захисту SourceFire |
| 4 | l1.cec.net | Hv0-local | Так | Так | 3 | Так | Сервер доступу |
| 5 | vcenter.cec.net | Hv0-local | Так | Ні | 1 | Ні | VMware vCenter Server Appliance |
| 6 | vdp.cec.net | Hv2-datastore-2 | Так | Ні | 2 | Ні | VMware Data Protection Appliance |
| ***Гіпервізор Hv1*** | | | | | | | |
| 7 | lb1.cec.net | Hv1-datastore-1 | Так | Так | 4 | Ні | Основний балансувальник навантаження |
| 8 | wd1.cec.net | Hv1-datastore-1 | Так | Так | 6 | Так | Основний веб-сервер ІАС «Вибори народних депутатів України» |
| 9 | wp1.cec.net | Hv1-datastore-1 | Так | Так | 5 | Так | Основний веб-сервер ІАС «Вибори Президента України» |
| 10 | ad1.cec.net | Hv1-datastore-1 | Так | Так | 2 | Так | Основний контролер домену та SubordinateCA |
| 11 | ds1.cec.net | Hv1-datastore-1 | Так | Так | 7 | Ні | Сервер обробки подань |
| 12 | ds2.cec.net | Hv1-datastore-1 | Так | Так | 8 | Ні | Сервер обробки подань |
| 13 | vpn.cec.net | Hv1-datastore-1 | Так | Так | 3 | Так | Сервер керування КЗІ |
| 14 | SS-IPS-1-1 | Hv1-datastore-1 | Так | Ні | 1 | Ні | IPS для захисту віртуальних машин Hv1 |
| ***Гіпервізор Hv2*** | | | | | | | |
| 15 | lb2.cec.net | Hv2-datastore-2 | Так | Так | 3 | Ні | Резервний балансувальник навантаження |
| 16 | wd2.cec.net | Hv2-datastore-2 | Так | Так | 4 | Ні | Резервний веб-сервер ІАС «Вибори народних депутатів України» |
| 17 | wp2.cec.net | Hv2-datastore-2 | Так | Так | 5 | Ні | Резервний веб-сервер ІАС «Вибори Президента України» |
| 18 | ad2.cec.net | Hv2-datastore-2 | Так | Так | 2 | Ні | Підлеглий контролер домену та SubordinateCA |
| 19 | ds3.cec.net | Hv2-datastore-2 | Так | Так | 9 | Ні | Сервер обробки подань |
| 20 | ds4.cec.net | Hv2-datastore-2 | Так | Так | 10 | Ні | Сервер обробки подань |
| 21 | m1.cec.net | Hv2-datastore-2 | Так | Так | 7 | Так | Сервер пошти |
| 22 | ntp.cec.net | Hv2-datastore-2 | Так | Так | 8 | Так | Сервер точного часу |
| 23 | av.cec.net | Hv2-datastore-2 | Так | Так | 6 | Так | Сервер антивірусного захисту |
| 23 | SS-IPS-1-2 | Hv2-datastore-2 | Так | Ні | 1 | Ні | IPS для захисту віртуальних машин Hv2 |

### ***4.5.3 Мережева архітектура системи***

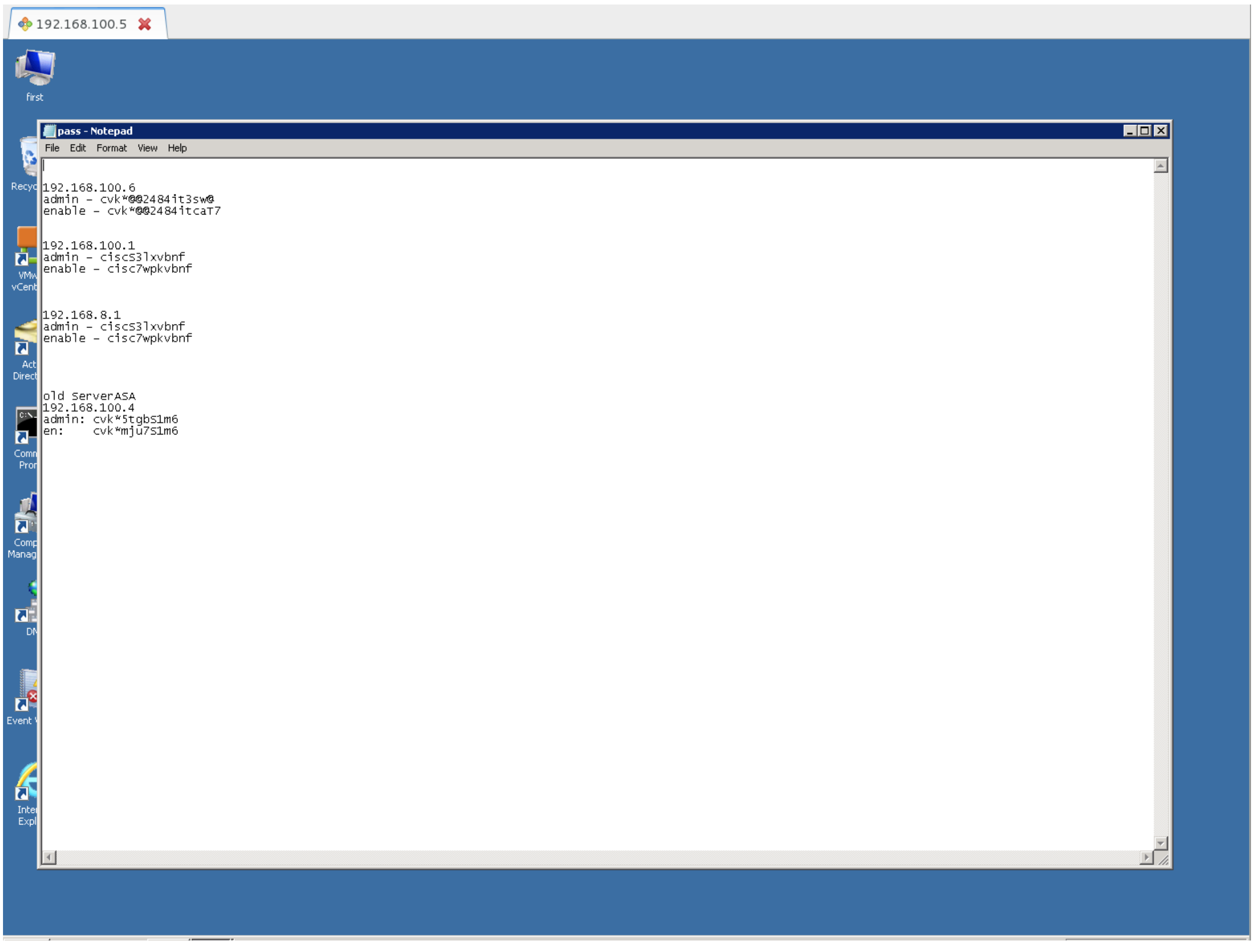
Відповідно до вимог технічного завдання в якості ядра мережі виступає кластер міжмережевих екранів ***FW1*** (***FW1.1*** – Active, ***FW1.2*** - StandBy). Він являє собою також ядро мережі L3.

Підключення серверного обладнання здійснюється на стек комутаторів ***SW1*** (***SW1.1***та ***SW1.2***). Підключення стеку ***SW1***до міжмережевих екранів здійснюється транковими каналами 10Gbit зі створенням окремих VLANта забезпеченням відмовостійкості у відповідності до таблиці 4.2, 4.3, рисунків 4.4-4.6. Підключення блейд-шасі до мережі здійснюється за допомогою вбудованих комутаторів із дотриманням вимог, щодо налаштувань.

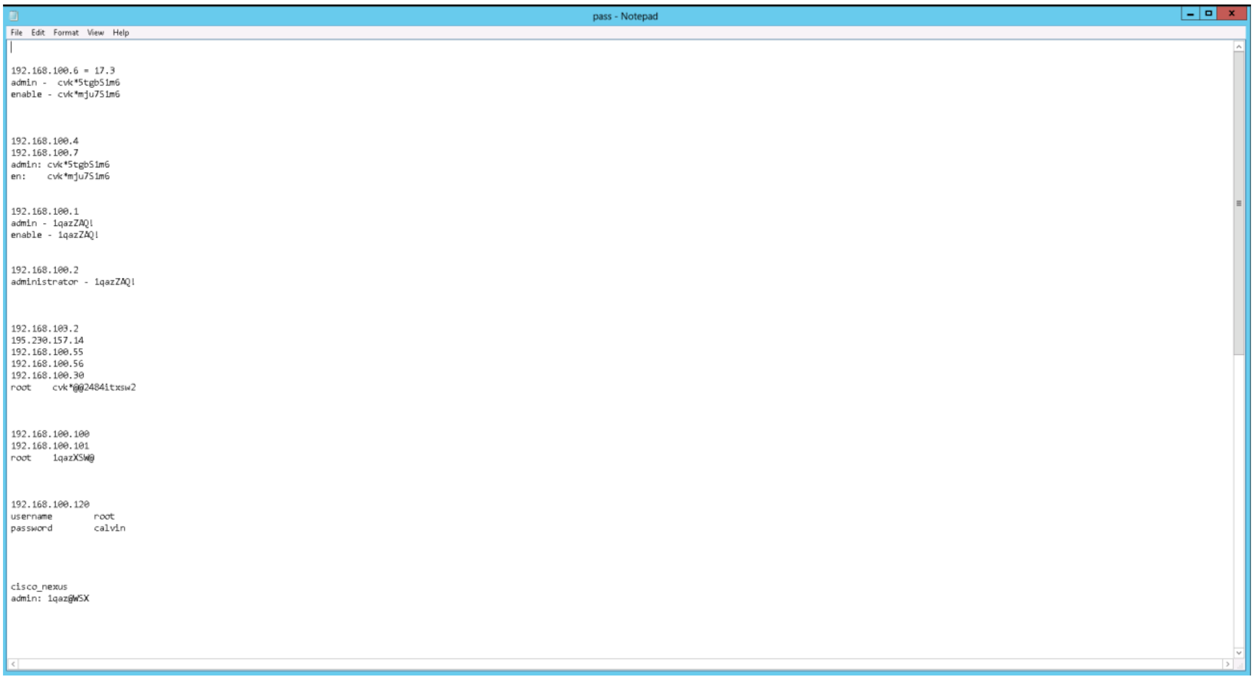
Змн. Арк. № докум. Підпис Дата КСЗІ-ЄІАС.П2 Арк. 55

Змн. Арк. № докум. Підпис Дата КСЗІ-ЄІАС.П2 Арк. 56

P.S. Особая благодарность чудо-админам, хранящим данные по доступу к узлам сети в текстовых файлах на рабочем столе, за увлекательный квест.

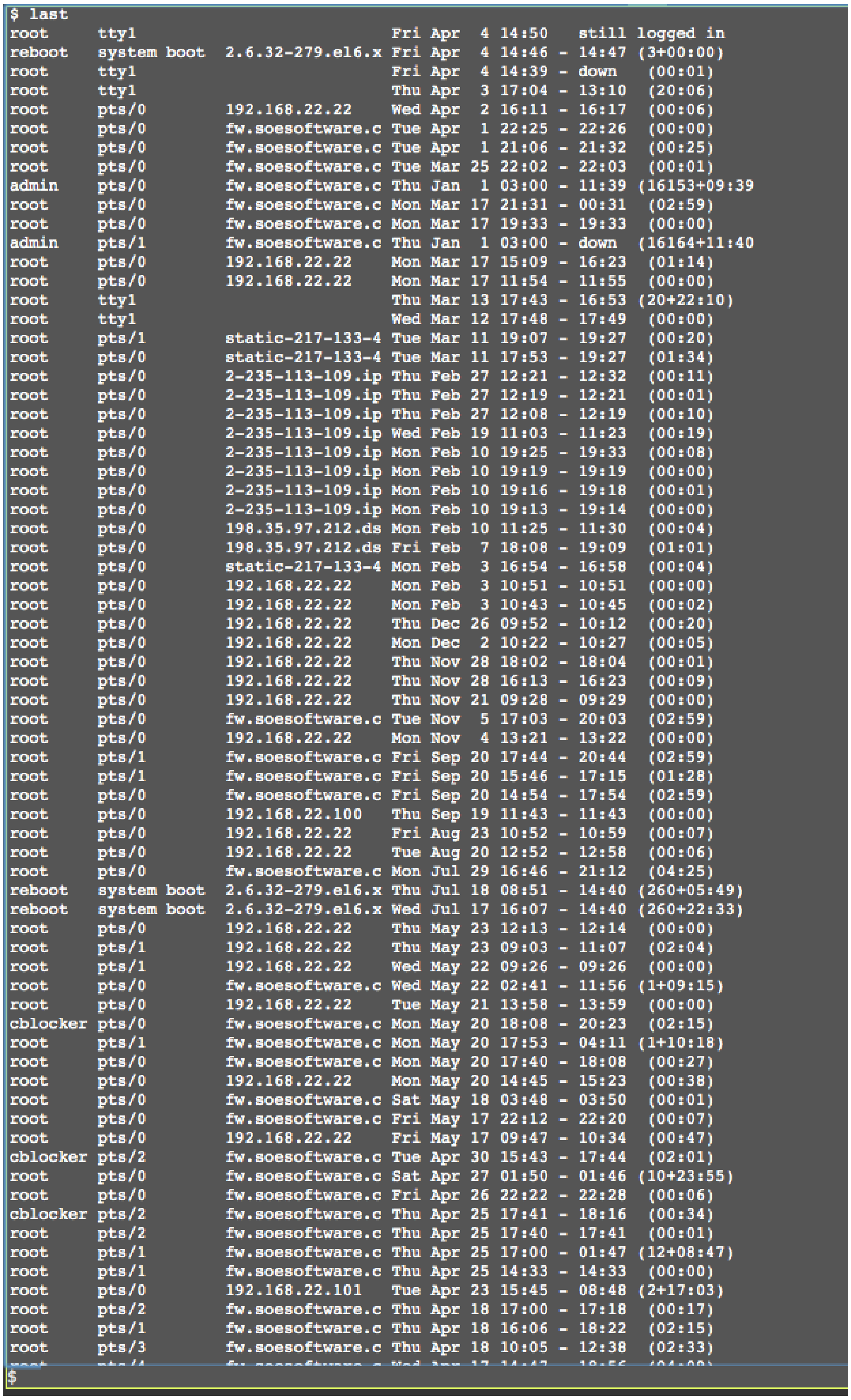


```
192.168.100.6
admin – cvk*@@2484it3sw@
enable – cvk*@@2484itcaT7


192.168.100.1
admin – ciscS3lxvbnf
enable – cisc7wpkvbnf



192.168.8.1
admin – ciscS3lxvbnf
enable – cisc7wpkvbnf




old ServerASA
192.168.100.4
admin: cvk*5tgbS1m6
en:    cvk*mju7S1m6
```

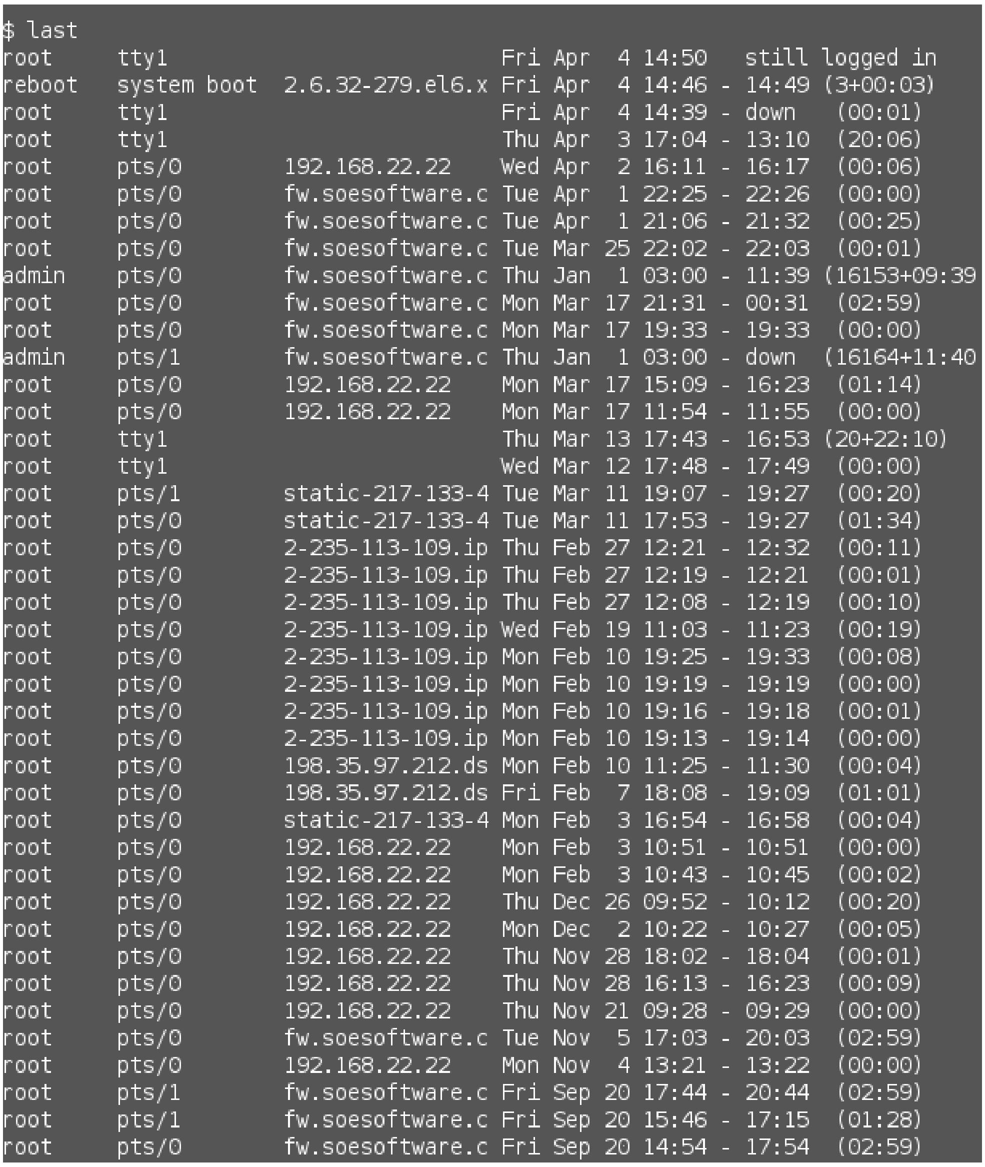


```
192.168.100.6 = 17.3
admin -  cvk*5tgbS1m6
enable - cvk*mju7S1m6



192.168.100.4
192.168.100.7
admin: cvk*5tgbS1m6
en:    cvk*mju7S1m6


192.168.100.1
admin - 1qazZAQ!
enable - 1qazZAQ!


192.168.100.2
administrator - 1qazZAQ!



192.168.103.2
195.230.157.14
192.168.100.55
192.168.100.56
192.168.100.30
root    cvk*@@2484itxsw2



192.168.100.100
192.168.100.101
root    1qazXSW@



192.168.100.120
username        root
password        calvin




cisco_nexus
admin: 1qazWSX
```

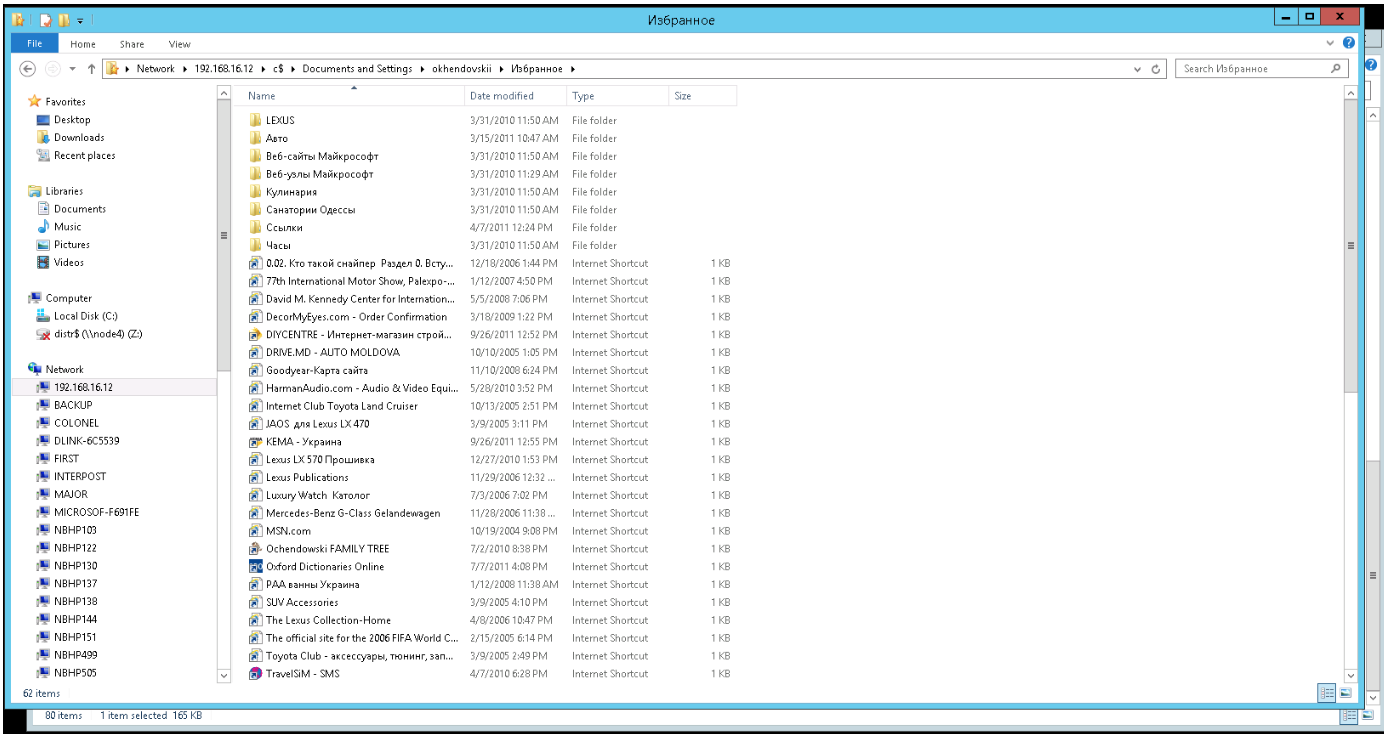
Судя по истории подключений, американская компания SOESoftware продолжает осуществлять непосредственное управление волеизъявлением народа Украины, оставив для себя полный (!!!) доступ к ключевым узлам сети ЦИК (см. ниже скриншоты с логами подключений):



```
$ last
root     tty1                          Fri Apr  4 14:50   still logged in
reboot   system boot  2.6.32-279.el6.x Fri Apr  4 14:46 - 14:47 (3+00:00)
root     tty1                          Fri Apr  4 14:39 - down   (00:01)
root     tty1                          Thu Apr  3 17:04 - 13:10  (20:06)
root     pts/0        192.168.22.22    Wed Apr  2 16:11 - 16:17  (00:06)
root     pts/0        fw.soesoftware.c Tue Apr  1 22:25 - 22:26  (00:00)
root     pts/0        fw.soesoftware.c Tue Apr  1 21:06 - 21:32  (00:25)
root     pts/0        fw.soesoftware.c Tue Mar 25 22:02 - 22:03  (00:01)
admin    pts/0        fw.soesoftware.c Thu Jan  1 03:00 - 11:39 (16153+09:39
root     pts/0        fw.soesoftware.c Mon Mar 17 21:31 - 00:31  (02:59)
root     pts/0        fw.soesoftware.c Mon Mar 17 19:33 - 19:33  (00:00)
admin    pts/1        fw.soesoftware.c Thu Jan  1 03:00 - down  (16164+11:40
root     pts/0        192.168.22.22    Mon Mar 17 15:09 - 16:23  (01:14)
root     pts/0        192.168.22.22    Mon Mar 17 11:54 - 11:55  (00:00)
root     tty1                          Thu Mar 13 17:43 - 16:53 (20+22:10)
root     tty1                          Wed Mar 12 17:48 - 17:49  (00:00)
root     pts/1        static-217-133-4 Tue Mar 11 19:07 - 19:27  (00:20)
root     pts/0        static-217-133-4 Tue Mar 11 17:53 - 19:27  (01:34)
root     pts/0        2-235-113-109.ip Thu Feb 27 12:21 - 12:32  (00:11)
root     pts/0        2-235-113-109.ip Thu Feb 27 12:19 - 12:21  (00:01)
root     pts/0        2-235-113-109.ip Thu Feb 27 12:08 - 12:19  (00:10)
root     pts/0        2-235-113-109.ip Wed Feb 19 11:03 - 11:23  (00:19)
root     pts/0        2-235-113-109.ip Mon Feb 10 19:25 - 19:33  (00:08)
root     pts/0        2-235-113-109.ip Mon Feb 10 19:19 - 19:19  (00:00)
root     pts/0        2-235-113-109.ip Mon Feb 10 19:16 - 19:18  (00:01)
root     pts/0        2-235-113-109.ip Mon Feb 10 19:13 - 19:14  (00:00)
root     pts/0        198.35.97.212.ds Mon Feb 10 11:25 - 11:30  (00:04)
root     pts/0        198.35.97.212.ds Fri Feb  7 18:08 - 19:09  (01:01)
root     pts/0        static-217-133-4 Mon Feb  3 16:54 - 16:58  (00:04)
root     pts/0        192.168.22.22    Mon Feb  3 10:51 - 10:51  (00:00)
root     pts/0        192.168.22.22    Mon Feb  3 10:43 - 10:45  (00:02)
root     pts/0        192.168.22.22    Thu Dec 26 09:52 - 10:12  (00:20)
root     pts/0        192.168.22.22    Mon Dec  2 10:22 - 10:27  (00:05)
root     pts/0        192.168.22.22    Thu Nov 28 18:02 - 18:04  (00:01)
root     pts/0        192.168.22.22    Thu Nov 28 16:13 - 16:23  (00:09)
root     pts/0        192.168.22.22    Thu Nov 21 09:28 - 09:29  (00:00)
root     pts/0        fw.soesoftware.c Tue Nov  5 17:03 - 20:03  (02:59)
root     pts/0        192.168.22.22    Mon Nov  4 13:21 - 13:22  (00:00)
root     pts/1        fw.soesoftware.c Fri Sep 20 17:44 - 20:44  (02:59)
root     pts/1        fw.soesoftware.c Fri Sep 20 15:46 - 17:15  (01:28)
root     pts/0        fw.soesoftware.c Fri Sep 20 14:54 - 17:54  (02:59)
root     pts/0        192.168.22.100   Thu Sep 19 11:43 - 11:43  (00:00)
root     pts/0        192.168.22.22    Fri Aug 23 10:52 - 10:59  (00:07)
root     pts/0        192.168.22.22    Tue Aug 20 12:52 - 12:58  (00:06)
root     pts/0        fw.soesoftware.c Mon Jul 29 16:46 - 21:12  (04:25)
reboot   system boot  2.6.32-279.el6.x Thu Jul 18 08:51 - 14:40 (260+05:49)
reboot   system boot  2.6.32-279.el6.x Wed Jul 17 16:07 - 14:40 (260+22:33)
root     pts/0        192.168.22.22    Thu May 23 12:13 - 12:14  (00:00)
root     pts/1        192.168.22.22    Thu May 23 09:03 - 11:07  (02:04)
root     pts/1        192.168.22.22    Wed May 22 09:26 - 09:26  (00:00)
root     pts/0        fw.soesoftware.c Wed May 22 02:41 - 11:56 (1+09:15)
root     pts/0        192.168.22.22    Tue May 21 13:58 - 13:59  (00:00)
cblocker pts/0        fw.soesoftware.c Mon May 20 18:08 - 20:23  (02:15)
root     pts/1        fw.soesoftware.c Mon May 20 17:53 - 04:11 (1+10:18)
root     pts/0        fw.soesoftware.c Mon May 20 17:40 - 18:08  (00:27)
root     pts/0        192.168.22.22    Mon May 20 14:45 - 15:23  (00:38)
root     pts/0        fw.soesoftware.c Sat May 18 03:48 - 03:50  (00:01)
root     pts/0        fw.soesoftware.c Fri May 17 22:12 - 22:20  (00:07)
root     pts/0        192.168.22.22    Fri May 17 09:47 - 10:34  (00:47)
cblocker pts/2        fw.soesoftware.c Tue Apr 30 15:43 - 17:44  (02:01)
root     pts/0        fw.soesoftware.c Sat Apr 27 01:50 - 01:46 (10+23:55)
root     pts/0        fw.soesoftware.c Fri Apr 26 22:22 - 22:28  (00:06)
cblocker pts/2        fw.soesoftware.c Thu Apr 25 17:41 - 18:16  (00:34)
root     pts/2        fw.soesoftware.c Thu Apr 25 17:40 - 17:41  (00:01)
root     pts/1        fw.soesoftware.c Thu Apr 25 17:00 - 01:47 (12+08:47)
root     pts/1        fw.soesoftware.c Thu Apr 25 14:33 - 14:33  (00:00)
root     pts/0        192.168.22.101   Tue Apr 23 15:45 - 08:48 (2+17:03)
root     pts/2        fw.soesoftware.c Thu Apr 18 17:00 - 17:18  (00:17)
root     pts/1        fw.soesoftware.c Thu Apr 18 16:06 - 18:22  (02:15)
root     pts/3        fw.soesoftware.c Thu Apr 18 10:05 - 12:38  (02:33)
root     pts/4        fw.soesoftware.c Wed Apr 17 14:47 - 18:56  (04:09)
$
```



```
$ last
root     tty1                          Fri Apr  4 14:50   still logged in
reboot   system boot  2.6.32-279.el6.x Fri Apr  4 14:46 - 14:49 (3+00:03)
root     tty1                          Fri Apr  4 14:39 - down   (00:01)
root     tty1                          Thu Apr  3 17:04 - 13:10  (20:06)
root     pts/0        192.168.22.22    Wed Apr  2 16:11 - 16:17  (00:06)
root     pts/0        fw.soesoftware.c Tue Apr  1 22:25 - 22:26  (00:00)
root     pts/0        fw.soesoftware.c Tue Apr  1 21:06 - 21:32  (00:25)
root     pts/0        fw.soesoftware.c Tue Mar 25 22:02 - 22:03  (00:01)
admin    pts/0        fw.soesoftware.c Thu Jan  1 03:00 - 11:39 (16153+09:39
root     pts/0        fw.soesoftware.c Mon Mar 17 21:31 - 00:31  (02:59)
root     pts/0        fw.soesoftware.c Mon Mar 17 19:33 - 19:33  (00:00)
admin    pts/1        fw.soesoftware.c Thu Jan  1 03:00 - down  (16164+11:40
root     pts/0        192.168.22.22    Mon Mar 17 15:09 - 16:23  (01:14)
root     pts/0        192.168.22.22    Mon Mar 17 11:54 - 11:55  (00:00)
root     tty1                          Thu Mar 13 17:43 - 16:53 (20+22:10)
root     tty1                          Wed Mar 12 17:48 - 17:49  (00:00)
root     pts/1        static-217-133-4 Tue Mar 11 19:07 - 19:27  (00:20)
root     pts/0        static-217-133-4 Tue Mar 11 17:53 - 19:27  (01:34)
root     pts/0        2-235-113-109.ip Thu Feb 27 12:21 - 12:32  (00:11)
root     pts/0        2-235-113-109.ip Thu Feb 27 12:19 - 12:21  (00:01)
root     pts/0        2-235-113-109.ip Thu Feb 27 12:08 - 12:19  (00:10)
root     pts/0        2-235-113-109.ip Wed Feb 19 11:03 - 11:23  (00:19)
root     pts/0        2-235-113-109.ip Mon Feb 10 19:25 - 19:33  (00:08)
root     pts/0        2-235-113-109.ip Mon Feb 10 19:19 - 19:19  (00:00)
root     pts/0        2-235-113-109.ip Mon Feb 10 19:16 - 19:18  (00:01)
root     pts/0        2-235-113-109.ip Mon Feb 10 19:13 - 19:14  (00:00)
root     pts/0        198.35.97.212.ds Mon Feb 10 11:25 - 11:30  (00:04)
root     pts/0        198.35.97.212.ds Fri Feb  7 18:08 - 19:09  (01:01)
root     pts/0        static-217-133-4 Mon Feb  3 16:54 - 16:58  (00:04)
root     pts/0        192.168.22.22    Mon Feb  3 10:51 - 10:51  (00:00)
root     pts/0        192.168.22.22    Mon Feb  3 10:43 - 10:45  (00:02)
root     pts/0        192.168.22.22    Thu Dec 26 09:52 - 10:12  (00:20)
root     pts/0        192.168.22.22    Mon Dec  2 10:22 - 10:27  (00:05)
root     pts/0        192.168.22.22    Thu Nov 28 18:02 - 18:04  (00:01)
root     pts/0        192.168.22.22    Thu Nov 28 16:13 - 16:23  (00:09)
root     pts/0        192.168.22.22    Thu Nov 21 09:28 - 09:29  (00:00)
root     pts/0        fw.soesoftware.c Tue Nov  5 17:03 - 20:03  (02:59)
root     pts/0        192.168.22.22    Mon Nov  4 13:21 - 13:22  (00:00)
root     pts/1        fw.soesoftware.c Fri Sep 20 17:44 - 20:44  (02:59)
root     pts/1        fw.soesoftware.c Fri Sep 20 15:46 - 17:15  (01:28)
root     pts/0        fw.soesoftware.c Fri Sep 20 14:54 - 17:54  (02:59)
```

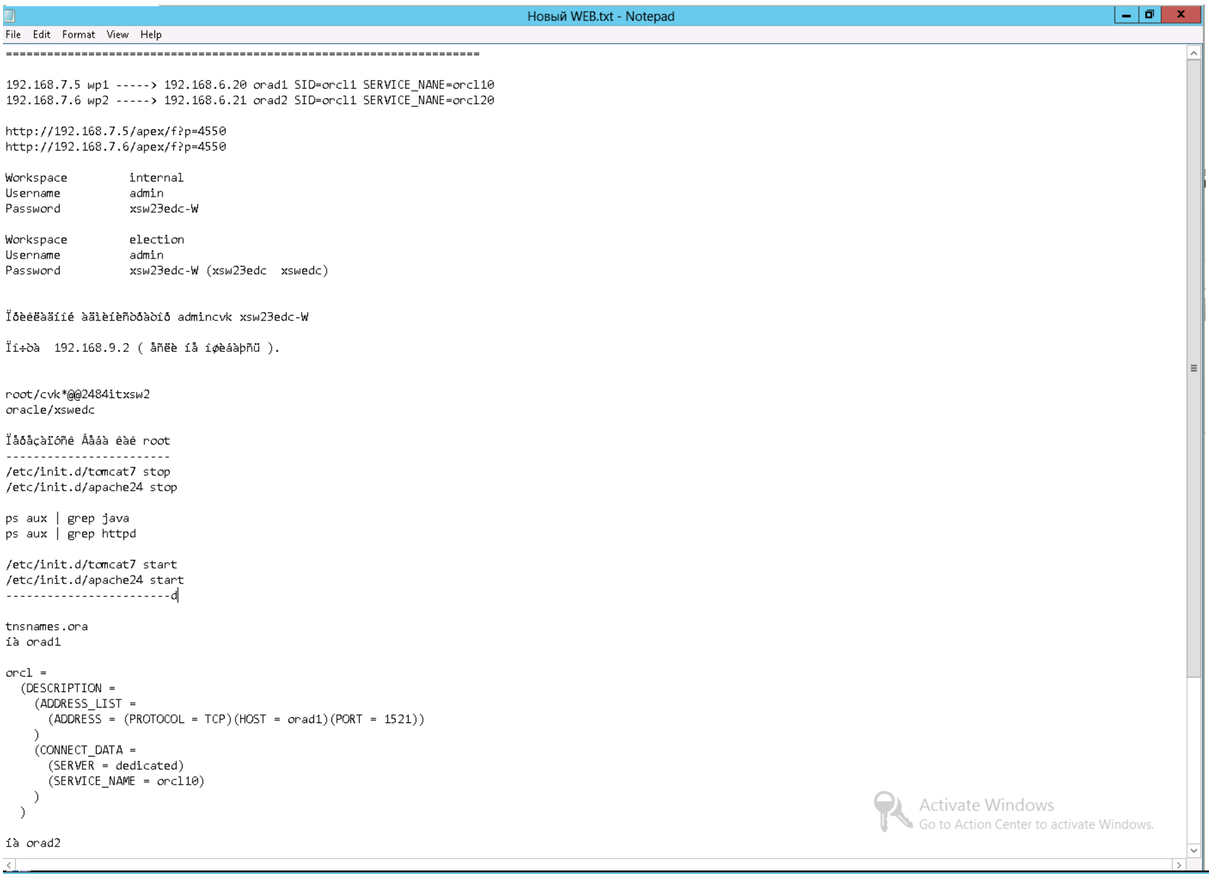


Network ▸ 192.168.16.12 ▸ c$ ▸ Documents and Settings ▸ okhendovskii ▸ Избранное ▸

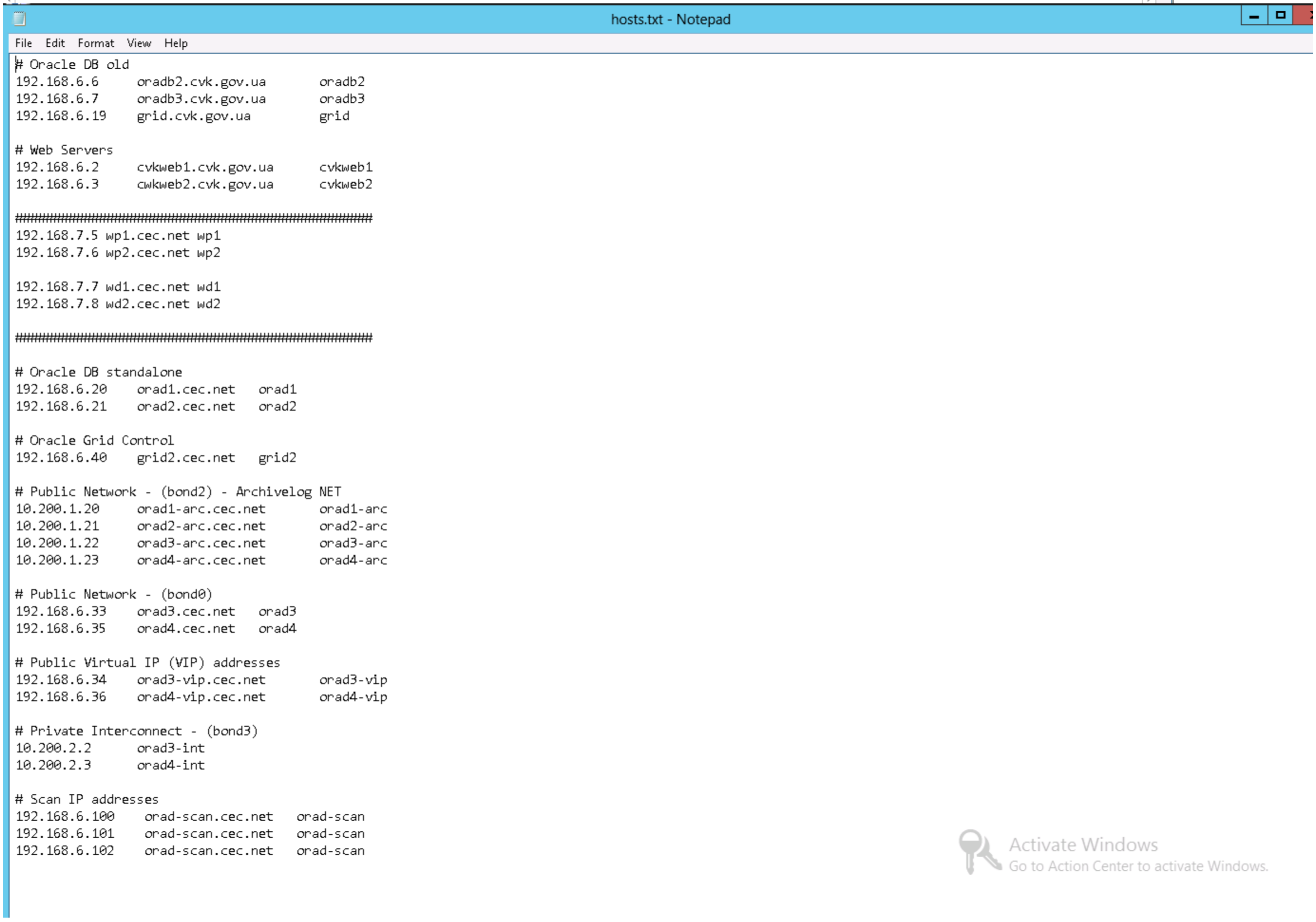
| Name | Date modified | Type | Size |
|---|---|---|---|
| LEXUS | 3/31/2010 11:50 AM | File folder | |
| Авто | 3/15/2011 10:47 AM | File folder | |
| Веб-сайты Майкрософт | 3/31/2010 11:50 AM | File folder | |
| Веб-узлы Майкрософт | 3/31/2010 11:29 AM | File folder | |
| Кулинария | 3/31/2010 11:50 AM | File folder | |
| Санатории Одессы | 3/31/2010 11:50 AM | File folder | |
| Ссылки | 4/7/2011 12:24 PM | File folder | |
| Часы | 3/31/2010 11:50 AM | File folder | |
| 0.02. Кто такой снайпер Раздел 0. Всту... | 12/18/2006 1:44 PM | Internet Shortcut | 1 KB |
| 77th International Motor Show, Palexpo-... | 1/12/2007 4:50 PM | Internet Shortcut | 1 KB |
| David M. Kennedy Center for Internation... | 5/5/2008 7:06 PM | Internet Shortcut | 1 KB |
| DecorMyEyes.com - Order Confirmation | 3/18/2009 1:22 PM | Internet Shortcut | 1 KB |
| DIYCENTRE - Интернет-магазин строй... | 9/26/2011 12:52 PM | Internet Shortcut | 1 KB |
| DRIVE.MD - AUTO MOLDOVA | 10/10/2005 1:05 PM | Internet Shortcut | 1 KB |
| Goodyear-Карта сайта | 11/10/2008 6:24 PM | Internet Shortcut | 1 KB |
| HarmanAudio.com - Audio & Video Equi... | 5/28/2010 3:52 PM | Internet Shortcut | 1 KB |
| Internet Club Toyota Land Cruiser | 10/13/2005 2:51 PM | Internet Shortcut | 1 KB |
| JAOS для Lexus LX 470 | 3/9/2005 3:11 PM | Internet Shortcut | 1 KB |
| KEMA - Украина | 9/26/2011 12:55 PM | Internet Shortcut | 1 KB |
| Lexus LX 570 Прошивка | 12/27/2010 1:53 PM | Internet Shortcut | 1 KB |
| Lexus Publications | 11/29/2006 12:32 ... | Internet Shortcut | 1 KB |
| Luxury Watch Католог | 7/3/2006 7:02 PM | Internet Shortcut | 1 KB |
| Mercedes-Benz G-Class Gelandewagen | 11/28/2006 11:38 ... | Internet Shortcut | 1 KB |
| MSN.com | 10/19/2004 9:08 PM | Internet Shortcut | 1 KB |
| Ochendowski FAMILY TREE | 7/2/2010 8:38 PM | Internet Shortcut | 1 KB |
| Oxford Dictionaries Online | 7/7/2011 4:08 PM | Internet Shortcut | 1 KB |
| PAA ванны Украина | 1/12/2008 11:38 AM | Internet Shortcut | 1 KB |
| SUV Accessories | 3/9/2005 4:10 PM | Internet Shortcut | 1 KB |
| The Lexus Collection-Home | 4/8/2006 10:47 PM | Internet Shortcut | 1 KB |
| The official site for the 2006 FIFA World C... | 2/15/2005 6:14 PM | Internet Shortcut | 1 KB |
| Toyota Club - аксессуары, тюнинг, зап... | 3/9/2005 2:49 PM | Internet Shortcut | 1 KB |
| TravelSiM - SMS | 4/7/2010 6:28 PM | Internet Shortcut | 1 KB |

62 items

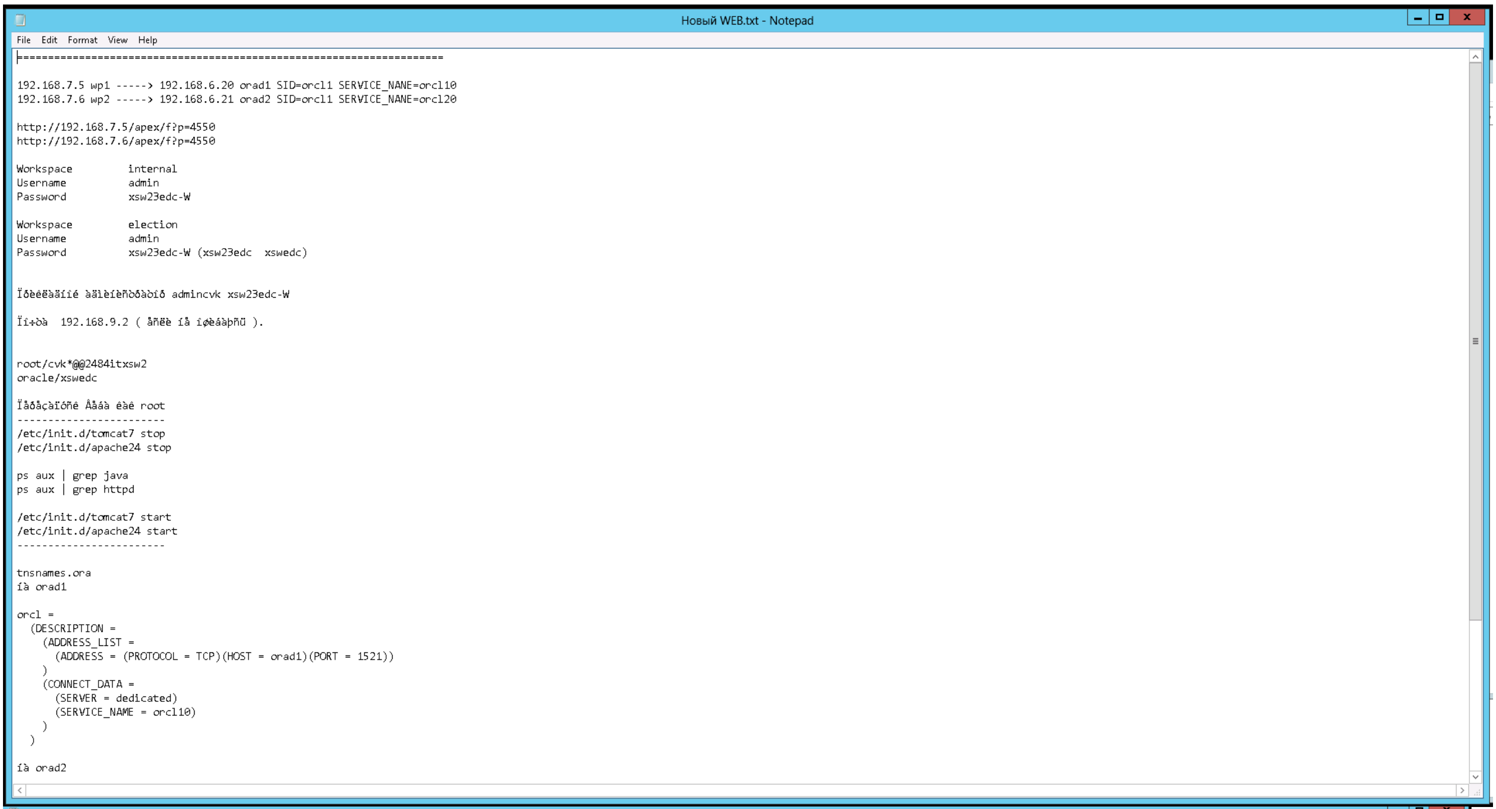
80 items  1 item selected  165 KB


Новый WEB.txt - Notepad
File Edit Format View Help
Activate Windows
Go to Action Center to activate Windows.

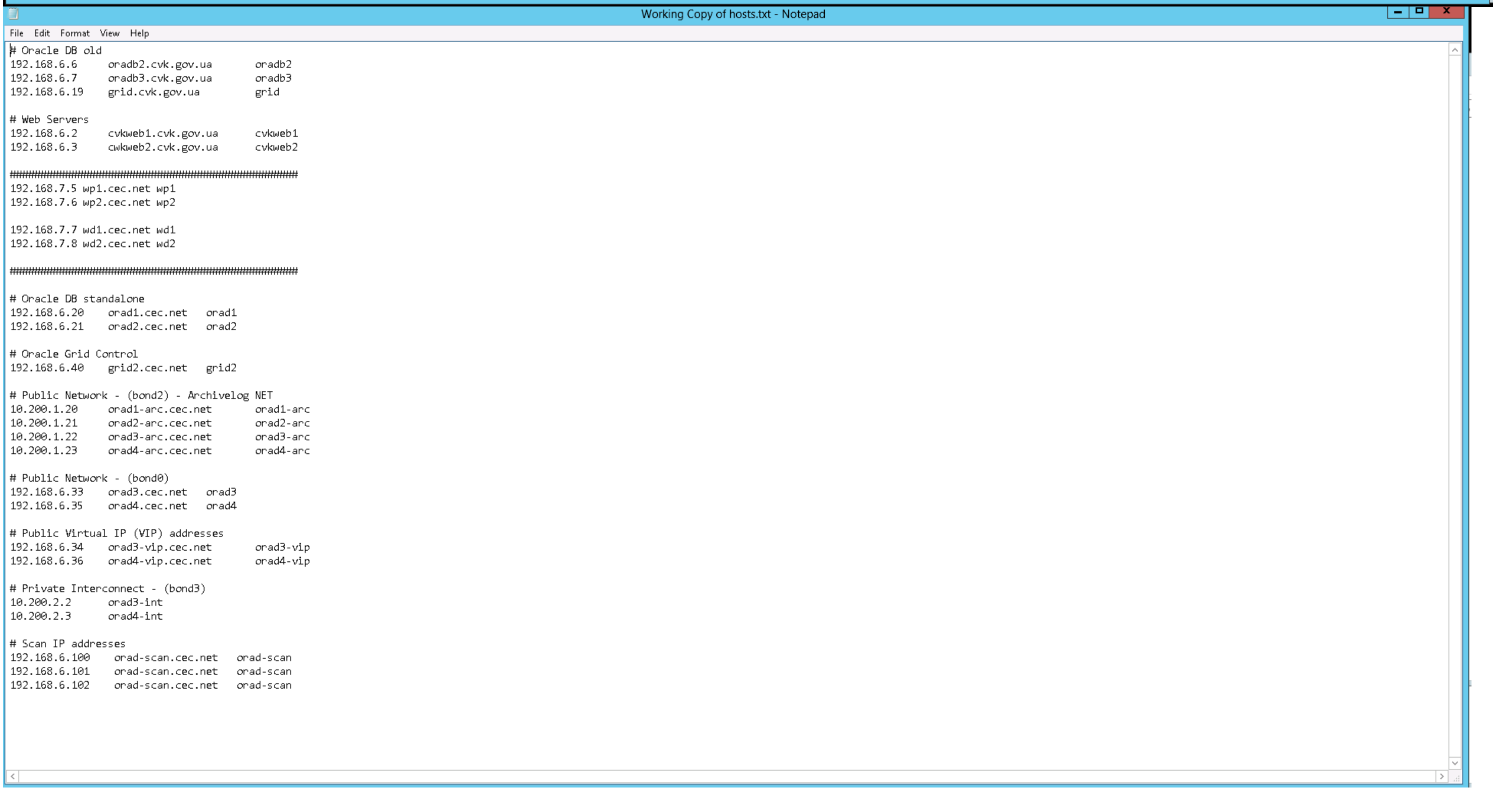
```
=====================================================================

192.168.7.5 wp1 -----> 192.168.6.20 orad1 SID=orcl1 SERVICE_NANE=orcl10
192.168.7.6 wp2 -----> 192.168.6.21 orad2 SID=orcl1 SERVICE_NANE=orcl20

http://192.168.7.5/apex/f?p=4550
http://192.168.7.6/apex/f?p=4550

Workspace         internal
Username          admin
Password          xsw23edc-W

Workspace         election
Username          admin
Password          xsw23edc-W (xsw23edc  xswedc)


Ïðèêëàäíîé àäìèíèñòðàòîð admincvk xsw23edc-W

Ïî÷òà  192.168.9.2 ( åñëè íå íøèáàþñü ).


root/cvk*@@2484itxsw2
oracle/xswedc

Ïåðåçàïóñê Âåáà èàê root
------------------------
/etc/init.d/tomcat7 stop
/etc/init.d/apache24 stop

ps aux | grep java
ps aux | grep httpd

/etc/init.d/tomcat7 start
/etc/init.d/apache24 start
------------------------d

tnsnames.ora
íà orad1

orcl =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = orad1)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVER = dedicated)
      (SERVICE_NAME = orcl10)
    )
  )

íà orad2
```


hosts.txt - Notepad
File Edit Format View Help
Activate Windows
Go to Action Center to activate Windows.

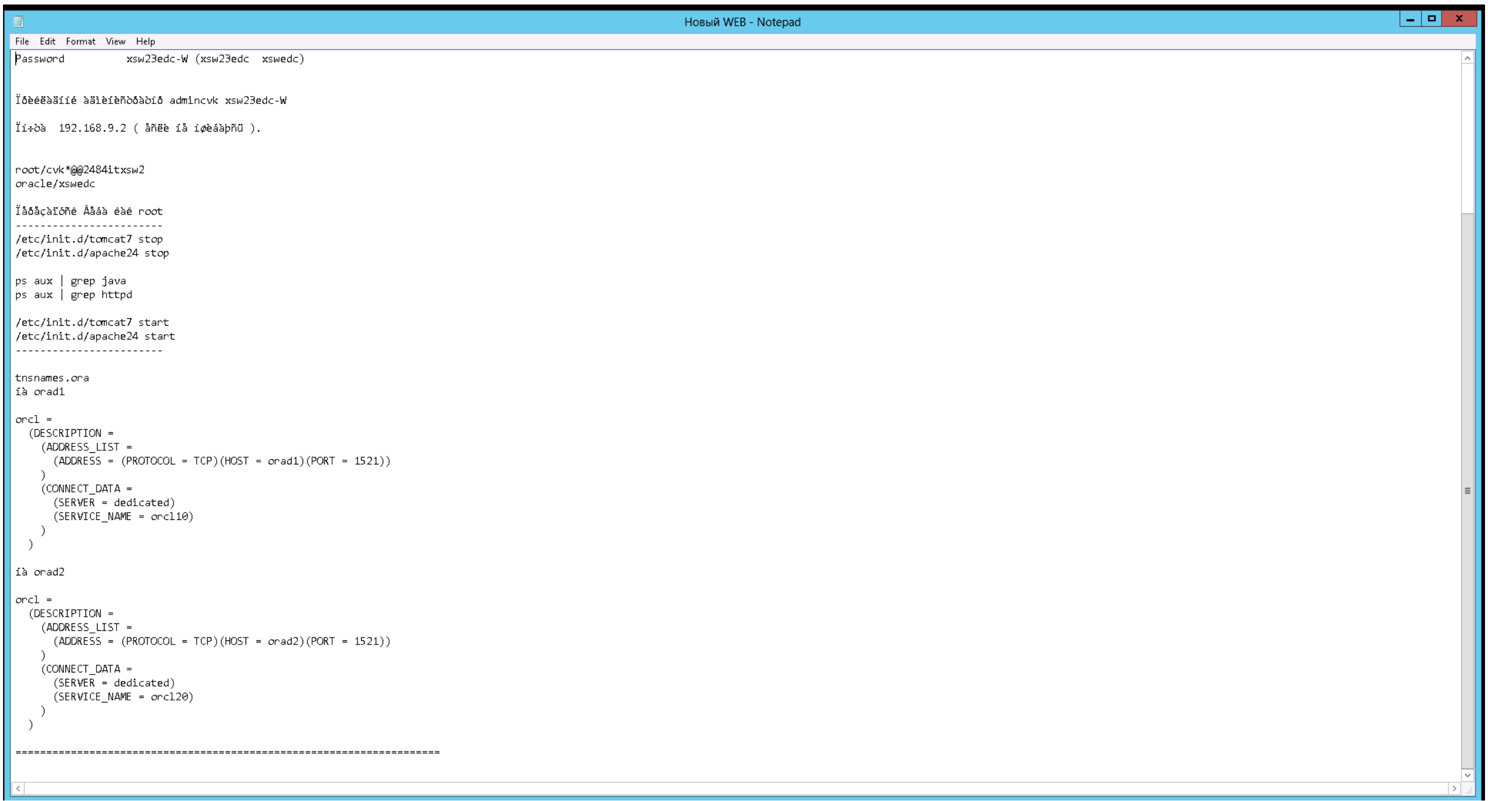
```
# Oracle DB old
192.168.6.6     oradb2.cvk.gov.ua       oradb2
192.168.6.7     oradb3.cvk.gov.ua       oradb3
192.168.6.19    grid.cvk.gov.ua         grid

# Web Servers
192.168.6.2     cvkweb1.cvk.gov.ua      cvkweb1
192.168.6.3     cwkweb2.cvk.gov.ua      cvkweb2

################################################
192.168.7.5 wp1.cec.net wp1
192.168.7.6 wp2.cec.net wp2

192.168.7.7 wd1.cec.net wd1
192.168.7.8 wd2.cec.net wd2

################################################

# Oracle DB standalone
192.168.6.20    orad1.cec.net   orad1
192.168.6.21    orad2.cec.net   orad2

# Oracle Grid Control
192.168.6.40    grid2.cec.net   grid2

# Public Network - (bond2) - Archivelog NET
10.200.1.20     orad1-arc.cec.net       orad1-arc
10.200.1.21     orad2-arc.cec.net       orad2-arc
10.200.1.22     orad3-arc.cec.net       orad3-arc
10.200.1.23     orad4-arc.cec.net       orad4-arc

# Public Network - (bond0)
192.168.6.33    orad3.cec.net   orad3
192.168.6.35    orad4.cec.net   orad4

# Public Virtual IP (VIP) addresses
192.168.6.34    orad3-vip.cec.net       orad3-vip
192.168.6.36    orad4-vip.cec.net       orad4-vip

# Private Interconnect - (bond3)
10.200.2.2      orad3-int
10.200.2.3      orad4-int

# Scan IP addresses
192.168.6.100    orad-scan.cec.net   orad-scan
192.168.6.101    orad-scan.cec.net   orad-scan
192.168.6.102    orad-scan.cec.net   orad-scan
```



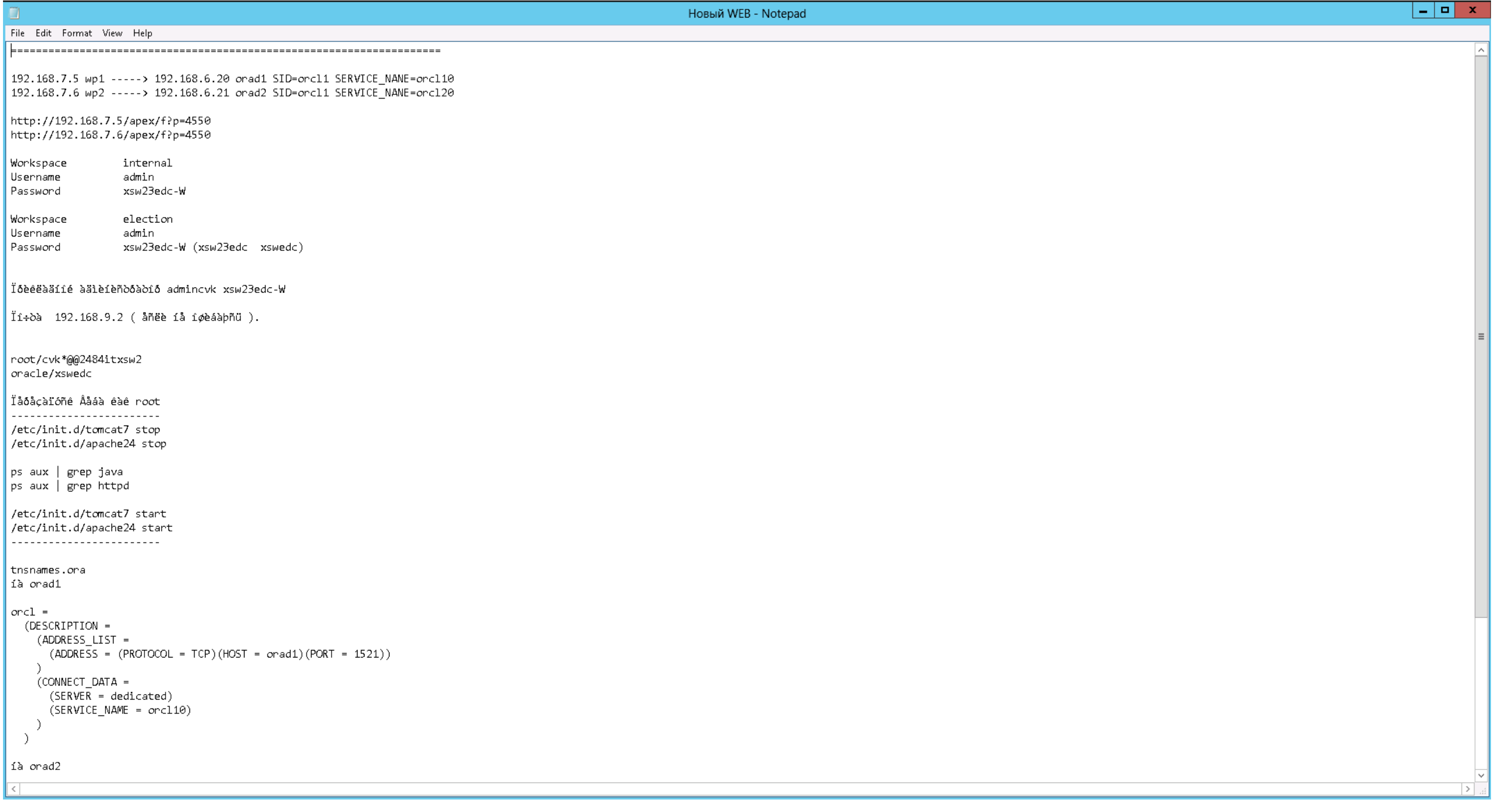
```
=====================================================================

192.168.7.5 wp1 -----> 192.168.6.20 orad1 SID=orcl1 SERVICE_NANE=orcl10
192.168.7.6 wp2 -----> 192.168.6.21 orad2 SID=orcl1 SERVICE_NANE=orcl20

http://192.168.7.5/apex/f?p=4550
http://192.168.7.6/apex/f?p=4550

Workspace        internal
Username         admin
Password         xsw23edc-W

Workspace        election
Username         admin
Password         xsw23edc-W (xsw23edc  xswedc)


Ïðèêëàäíîé àäìèíèñòðàòîð admincvk xsw23edc-W

Ïî÷òà  192.168.9.2 ( åñëè íå îøèáàþñü ).


root/cvk*@@2484itxsw2
oracle/xswedc

Ïåðåçàïóñê Âåáà èàê root
------------------------
/etc/init.d/tomcat7 stop
/etc/init.d/apache24 stop

ps aux | grep java
ps aux | grep httpd

/etc/init.d/tomcat7 start
/etc/init.d/apache24 start
------------------------

tnsnames.ora
íà orad1

orcl =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = orad1)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVER = dedicated)
      (SERVICE_NAME = orcl10)
    )
  )

íà orad2
```


Working Copy of hosts.txt - Notepad
File Edit Format View Help

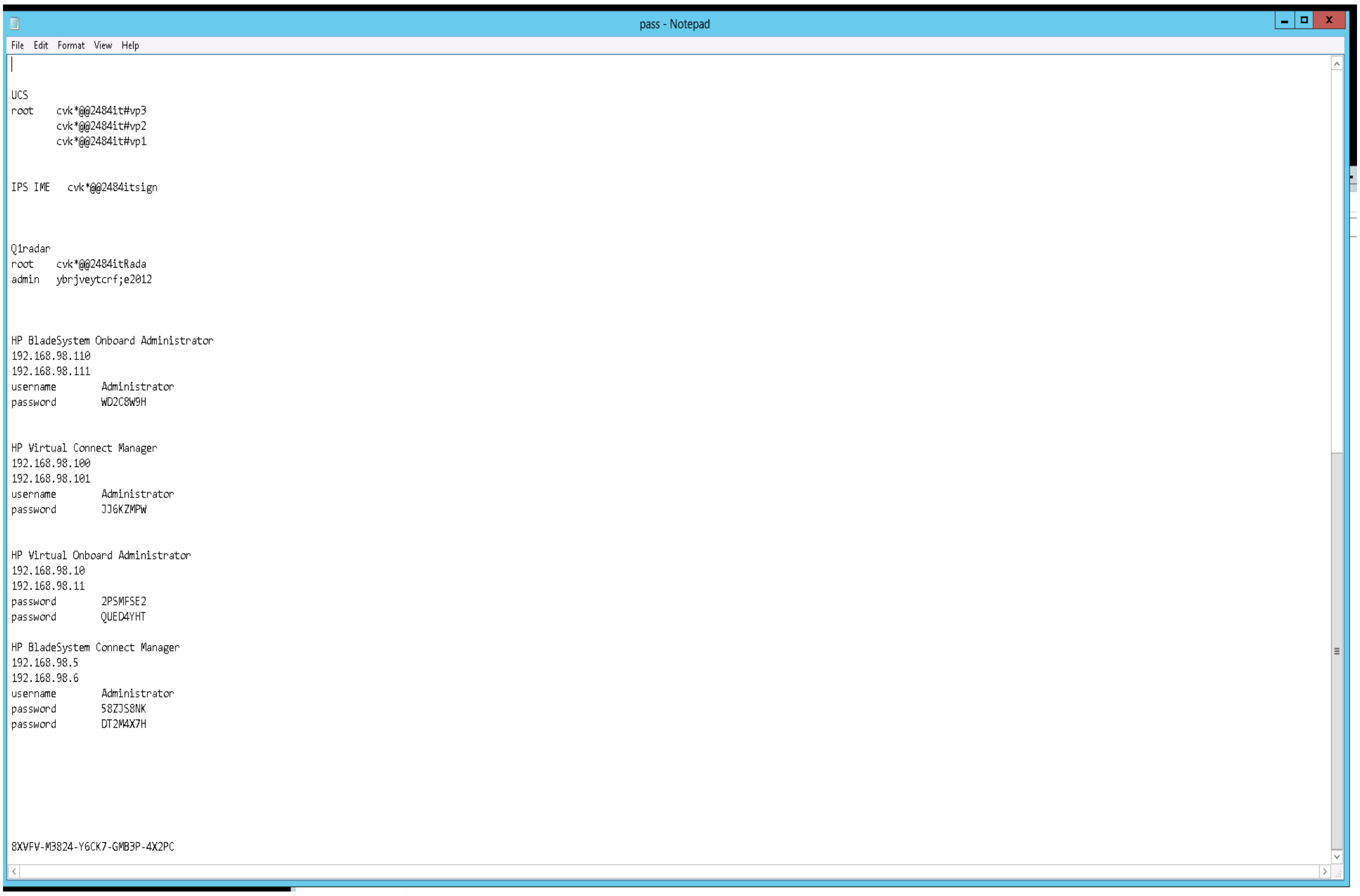
```
# Oracle DB old
192.168.6.6     oradb2.cvk.gov.ua       oradb2
192.168.6.7     oradb3.cvk.gov.ua       oradb3
192.168.6.19    grid.cvk.gov.ua         grid

# Web Servers
192.168.6.2     cvkweb1.cvk.gov.ua      cvkweb1
192.168.6.3     cwkweb2.cvk.gov.ua      cvkweb2

###############################################
192.168.7.5 wp1.cec.net wp1
192.168.7.6 wp2.cec.net wp2

192.168.7.7 wd1.cec.net wd1
192.168.7.8 wd2.cec.net wd2

###############################################

# Oracle DB standalone
192.168.6.20    orad1.cec.net   orad1
192.168.6.21    orad2.cec.net   orad2

# Oracle Grid Control
192.168.6.40    grid2.cec.net   grid2

# Public Network - (bond2) - Archivelog NET
10.200.1.20     orad1-arc.cec.net       orad1-arc
10.200.1.21     orad2-arc.cec.net       orad2-arc
10.200.1.22     orad3-arc.cec.net       orad3-arc
10.200.1.23     orad4-arc.cec.net       orad4-arc

# Public Network - (bond0)
192.168.6.33    orad3.cec.net   orad3
192.168.6.35    orad4.cec.net   orad4

# Public Virtual IP (VIP) addresses
192.168.6.34    orad3-vip.cec.net       orad3-vip
192.168.6.36    orad4-vip.cec.net       orad4-vip

# Private Interconnect - (bond3)
10.200.2.2      orad3-int
10.200.2.3      orad4-int

# Scan IP addresses
192.168.6.100    orad-scan.cec.net   orad-scan
192.168.6.101    orad-scan.cec.net   orad-scan
192.168.6.102    orad-scan.cec.net   orad-scan
```



```
Password          xsw23edc-W (xsw23edc  xswedc)


Ïðèêëàäíîé àäìèíèñòðàòîð admincvk xsw23edc-W

Ïî÷òà  192.168.9.2 ( åñëè íå îøèáàþñü ).


root/cvk*@@2484itxsw2
oracle/xswedc

Ïåðåçàïóñê Âåáà êàê root
------------------------
/etc/init.d/tomcat7 stop
/etc/init.d/apache24 stop

ps aux | grep java
ps aux | grep httpd

/etc/init.d/tomcat7 start
/etc/init.d/apache24 start
------------------------

tnsnames.ora
íà orad1

orcl =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = orad1)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVER = dedicated)
      (SERVICE_NAME = orcl10)
    )
  )

íà orad2

orcl =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = orad2)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVER = dedicated)
      (SERVICE_NAME = orcl20)
    )
  )

=====================================================================
```

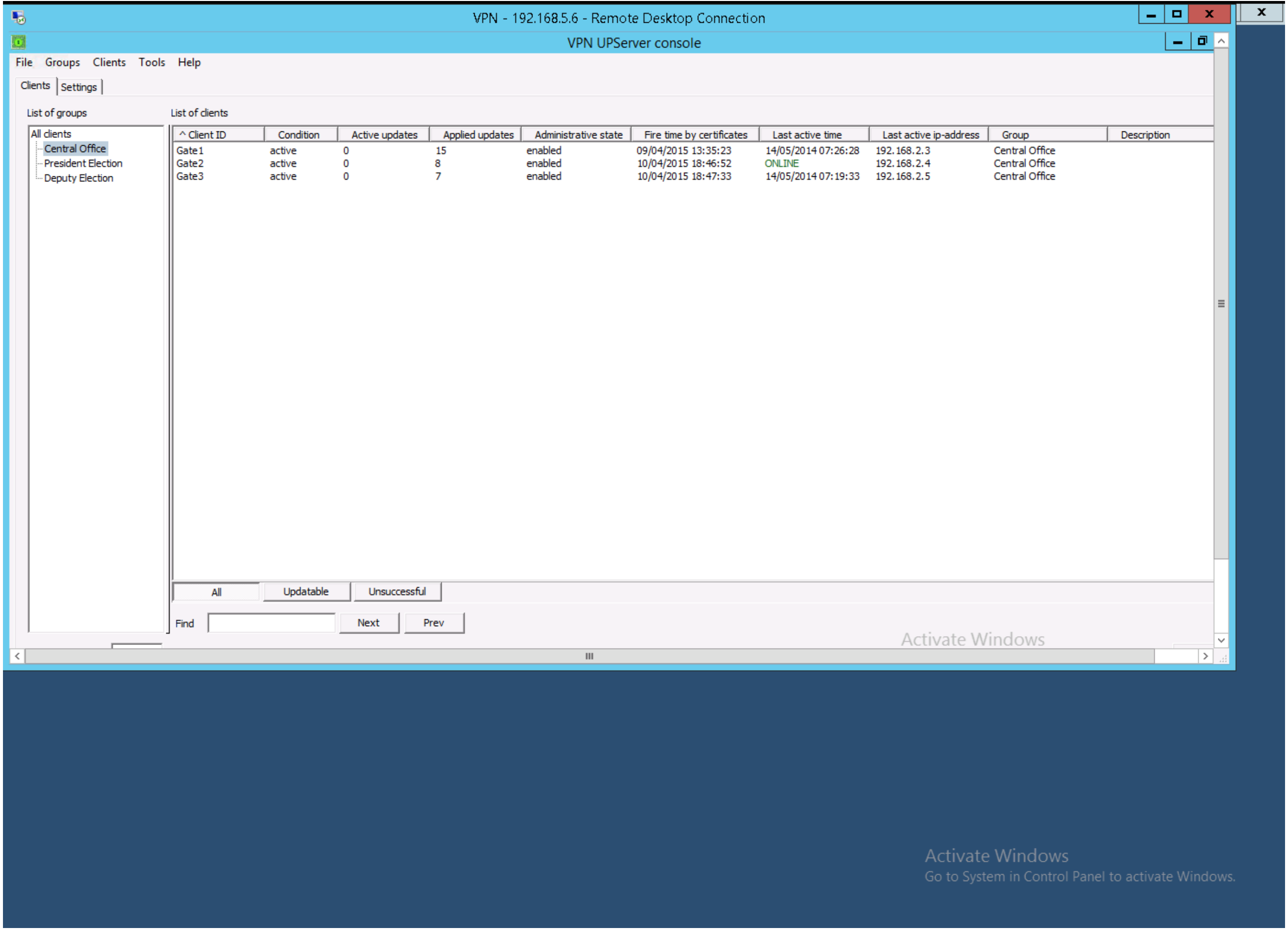


```
=====================================================================

192.168.7.5 wp1 -----> 192.168.6.20 orad1 SID=orcl1 SERVICE_NANE=orcl10
192.168.7.6 wp2 -----> 192.168.6.21 orad2 SID=orcl1 SERVICE_NANE=orcl20

http://192.168.7.5/apex/f?p=4550
http://192.168.7.6/apex/f?p=4550

Workspace         internal
Username          admin
Password          xsw23edc-W

Workspace         election
Username          admin
Password          xsw23edc-W (xsw23edc  xswedc)


Ïðèêëàäíîé àäìèíèñòðàòîð admincvk xsw23edc-W

Ïî÷òà  192.168.9.2 ( åñëè íå îøèáàþñü ).


root/cvk*@@2484itxsw2
oracle/xswedc

Ïåðåçàïóñê Âåáà êàê root
------------------------
/etc/init.d/tomcat7 stop
/etc/init.d/apache24 stop

ps aux | grep java
ps aux | grep httpd

/etc/init.d/tomcat7 start
/etc/init.d/apache24 start
------------------------

tnsnames.ora
íà orad1

orcl =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = orad1)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVER = dedicated)
      (SERVICE_NAME = orcl10)
    )
  )

íà orad2
```



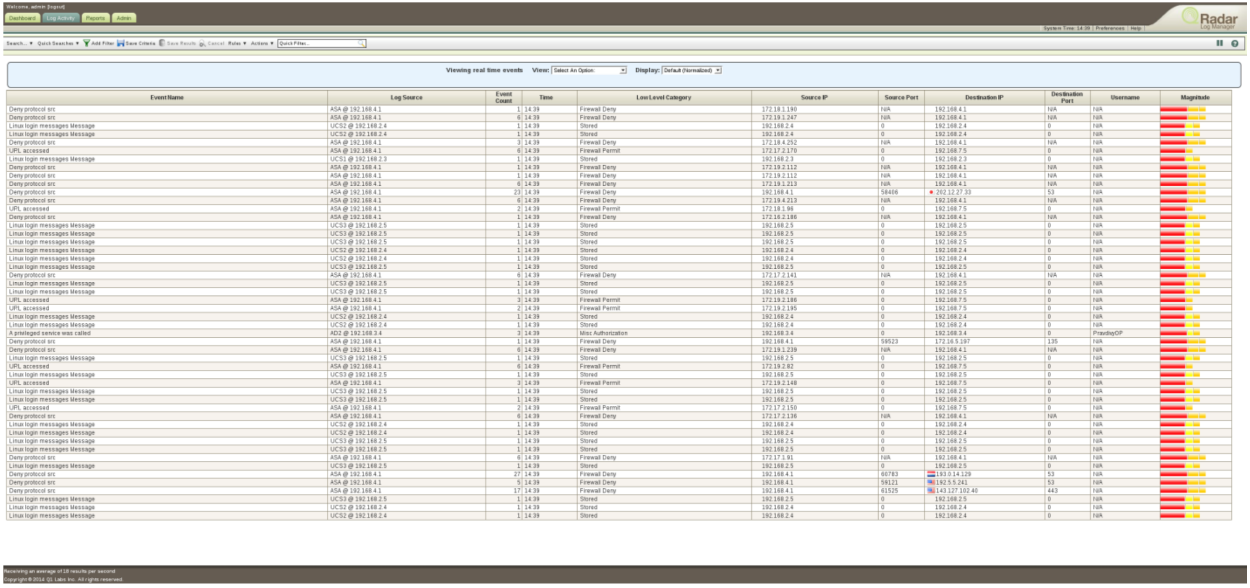
```
UCS
root    cvk*@@2484it#vp3
        cvk*@@2484it#vp2
        cvk*@@2484it#vp1


IPS IME   cvk*@@2484itsign



Q1radar
root    cvk*@@2484itRada
admin   ybrjveytcrf;e2012



HP BladeSystem Onboard Administrator
192.168.98.110
192.168.98.111
username        Administrator
password        WD2C8W9H


HP Virtual Connect Manager
192.168.98.100
192.168.98.101
username        Administrator
password        JJ6KZMPW


HP Virtual Onboard Administrator
192.168.98.10
192.168.98.11
password        2PSMFSE2
password        QUED4YHT

HP BladeSystem Connect Manager
192.168.98.5
192.168.98.6
username        Administrator
password        58ZJS8NK
password        DT2M4X7H







8XVFV-M3824-Y6CK7-GMB3P-4X2PC
```

Странно, что при этом операционная система не активирована(**!!!**):



| ^ Client ID | Condition | Active updates | Applied updates | Administrative state | Fire time by certificates | Last active time | Last active ip-address | Group | Description |
|---|---|---|---|---|---|---|---|---|---|
| Gate1 | active | 0 | 15 | enabled | 09/04/2015 13:35:23 | 14/05/2014 07:26:28 | 192.168.2.3 | Central Office | |
| Gate2 | active | 0 | 8 | enabled | 10/04/2015 18:46:52 | ONLINE | 192.168.2.4 | Central Office | |
| Gate3 | active | 0 | 7 | enabled | 10/04/2015 18:47:33 | 14/05/2014 07:19:33 | 192.168.2.5 | Central Office | |

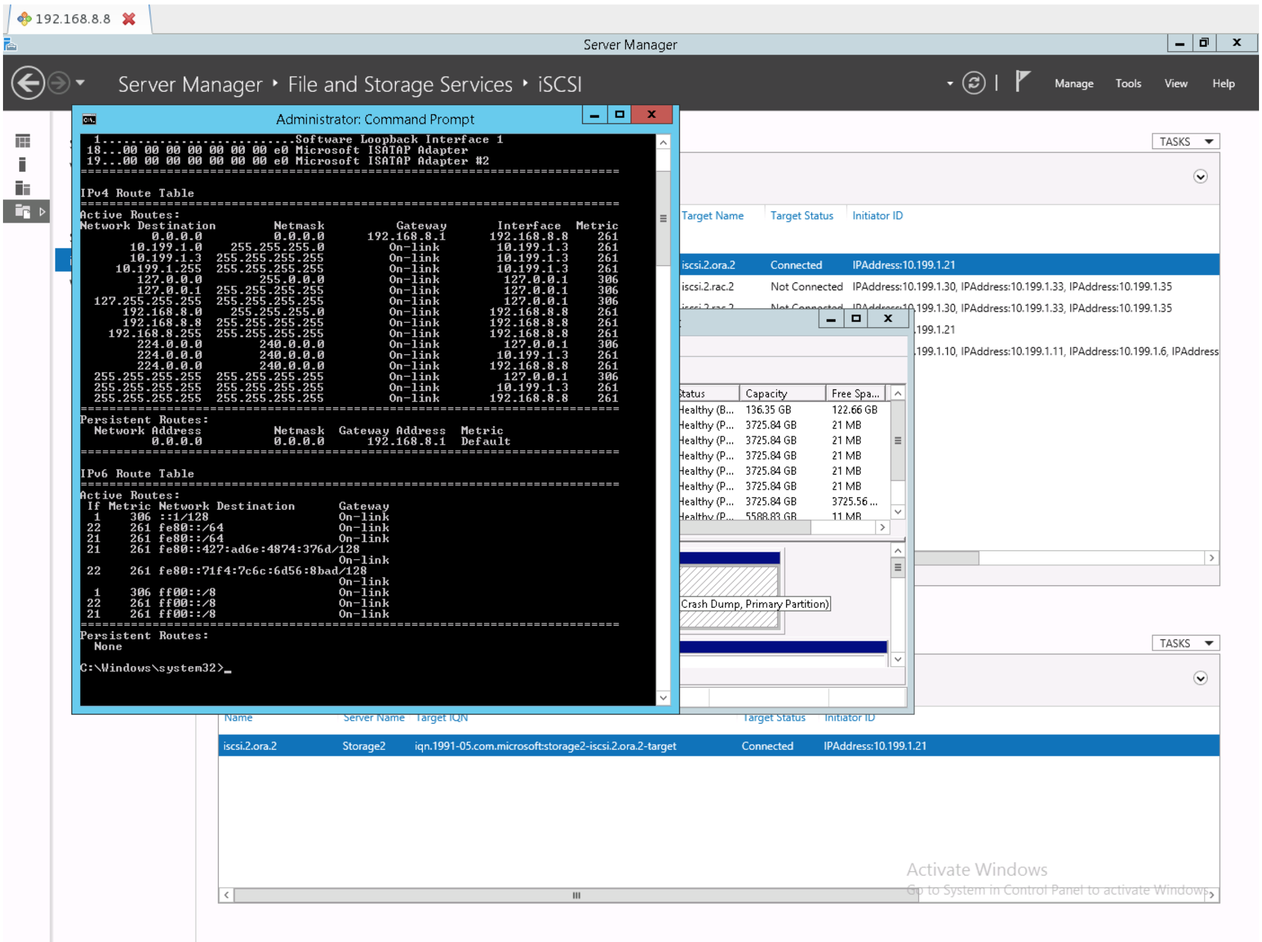
Activate Windows
Go to System in Control Panel to activate Windows.



Viewing real time events   View: Select An Option:   Display: Default (Normalized)

| Event Name | Log Source | Event Count | Time | Low Level Category | Source IP | Source Port | Destination IP | Destination Port | Username | Magnitude |
|---|---|---|---|---|---|---|---|---|---|---|
| Deny protocol src | ASA @ 192.168.4.1 | 1 | 14:39 | Firewall Deny | 172.18.1.190 | N/A | 192.168.4.1 | N/A | N/A | 🟥🟨 |
| Deny protocol src | ASA @ 192.168.4.1 | 6 | 14:39 | Firewall Deny | 172.19.1.247 | N/A | 192.168.4.1 | N/A | N/A | 🟥🟨 |
| Linux login messages Message | UCS2 @ 192.168.2.4 | 1 | 14:39 | Stored | 192.168.2.4 | 0 | 192.168.2.4 | 0 | N/A | 🟥🟨 |
| Linux login messages Message | UCS2 @ 192.168.2.4 | 1 | 14:39 | Stored | 192.168.2.4 | 0 | 192.168.2.4 | 0 | N/A | 🟥🟨 |
| Deny protocol src | ASA @ 192.168.4.1 | 3 | 14:39 | Firewall Deny | 172.18.4.252 | N/A | 192.168.4.1 | N/A | N/A | 🟥🟨 |
| URL accessed | ASA @ 192.168.4.1 | 6 | 14:39 | Firewall Permit | 172.17.2.170 | 0 | 192.168.7.5 | 0 | N/A | 🟥🟨 |
| Linux login messages Message | UCS1 @ 192.168.2.3 | 1 | 14:39 | Stored | 192.168.2.3 | 0 | 192.168.2.3 | 0 | N/A | 🟥🟨 |
| Deny protocol src | ASA @ 192.168.4.1 | 1 | 14:39 | Firewall Deny | 172.19.2.112 | N/A | 192.168.4.1 | N/A | N/A | 🟥🟨 |
| Deny protocol src | ASA @ 192.168.4.1 | 1 | 14:39 | Firewall Deny | 172.19.2.112 | N/A | 192.168.4.1 | N/A | N/A | 🟥🟨 |
| Deny protocol src | ASA @ 192.168.4.1 | 6 | 14:39 | Firewall Deny | 172.19.1.213 | N/A | 192.168.4.1 | N/A | N/A | 🟥🟨 |
| Deny protocol src | ASA @ 192.168.4.1 | 23 | 14:39 | Firewall Deny | 192.168.4.1 | 58406 | 202.12.27.33 | 53 | N/A | 🟥🟨 |
| Deny protocol src | ASA @ 192.168.4.1 | 6 | 14:39 | Firewall Deny | 172.19.4.213 | N/A | 192.168.4.1 | N/A | N/A | 🟥🟨 |
| URL accessed | ASA @ 192.168.4.1 | 2 | 14:39 | Firewall Permit | 172.18.1.96 | 0 | 192.168.7.5 | 0 | N/A | 🟥🟨 |
| Deny protocol src | ASA @ 192.168.4.1 | 1 | 14:39 | Firewall Deny | 172.16.2.186 | N/A | 192.168.4.1 | N/A | N/A | 🟥🟨 |
| Linux login messages Message | UCS3 @ 192.168.2.5 | 1 | 14:39 | Stored | 192.168.2.5 | 0 | 192.168.2.5 | 0 | N/A | 🟥🟨 |
| Linux login messages Message | UCS3 @ 192.168.2.5 | 1 | 14:39 | Stored | 192.168.2.5 | 0 | 192.168.2.5 | 0 | N/A | 🟥🟨 |
| Linux login messages Message | UCS3 @ 192.168.2.5 | 1 | 14:39 | Stored | 192.168.2.5 | 0 | 192.168.2.5 | 0 | N/A | 🟥🟨 |
| Linux login messages Message | UCS2 @ 192.168.2.4 | 1 | 14:39 | Stored | 192.168.2.4 | 0 | 192.168.2.4 | 0 | N/A | 🟥🟨 |
| Linux login messages Message | UCS2 @ 192.168.2.4 | 1 | 14:39 | Stored | 192.168.2.4 | 0 | 192.168.2.4 | 0 | N/A | 🟥🟨 |
| Linux login messages Message | UCS3 @ 192.168.2.5 | 1 | 14:39 | Stored | 192.168.2.5 | 0 | 192.168.2.5 | 0 | N/A | 🟥🟨 |
| Deny protocol src | ASA @ 192.168.4.1 | 6 | 14:39 | Firewall Deny | 172.17.2.141 | N/A | 192.168.4.1 | N/A | N/A | 🟥🟨 |
| Linux login messages Message | UCS3 @ 192.168.2.5 | 1 | 14:39 | Stored | 192.168.2.5 | 0 | 192.168.2.5 | 0 | N/A | 🟥🟨 |
| Linux login messages Message | UCS3 @ 192.168.2.5 | 1 | 14:39 | Stored | 192.168.2.5 | 0 | 192.168.2.5 | 0 | N/A | 🟥🟨 |
| URL accessed | ASA @ 192.168.4.1 | 3 | 14:39 | Firewall Permit | 172.19.2.186 | 0 | 192.168.7.5 | 0 | N/A | 🟥🟨 |
| URL accessed | ASA @ 192.168.4.1 | 2 | 14:39 | Firewall Permit | 172.19.2.195 | 0 | 192.168.7.5 | 0 | N/A | 🟥🟨 |
| Linux login messages Message | UCS2 @ 192.168.2.4 | 1 | 14:39 | Stored | 192.168.2.4 | 0 | 192.168.2.4 | 0 | N/A | 🟥🟨 |
| Linux login messages Message | UCS2 @ 192.168.2.4 | 1 | 14:39 | Stored | 192.168.2.4 | 0 | 192.168.2.4 | 0 | N/A | 🟥🟨 |
| A privileged service was called | AD2 @ 192.168.3.4 | 3 | 14:39 | Misc Authorization | 192.168.3.4 | 0 | 192.168.3.4 | 0 | PravdivyOP | 🟥🟨 |
| Deny protocol src | ASA @ 192.168.4.1 | 1 | 14:39 | Firewall Deny | 192.168.4.1 | 59523 | 172.16.5.197 | 135 | N/A | 🟥🟨 |
| Deny protocol src | ASA @ 192.168.4.1 | 6 | 14:39 | Firewall Deny | 172.19.1.239 | N/A | 192.168.4.1 | N/A | N/A | 🟥🟨 |
| Linux login messages Message | UCS3 @ 192.168.2.5 | 1 | 14:39 | Stored | 192.168.2.5 | 0 | 192.168.2.5 | 0 | N/A | 🟥🟨 |
| URL accessed | ASA @ 192.168.4.1 | 6 | 14:39 | Firewall Permit | 172.19.2.82 | 0 | 192.168.7.5 | 0 | N/A | 🟥🟨 |
| Linux login messages Message | UCS3 @ 192.168.2.5 | 1 | 14:39 | Stored | 192.168.2.5 | 0 | 192.168.2.5 | 0 | N/A | 🟥🟨 |
| URL accessed | ASA @ 192.168.4.1 | 3 | 14:39 | Firewall Permit | 172.19.2.148 | 0 | 192.168.7.5 | 0 | N/A | 🟥🟨 |
| Linux login messages Message | UCS3 @ 192.168.2.5 | 1 | 14:39 | Stored | 192.168.2.5 | 0 | 192.168.2.5 | 0 | N/A | 🟥🟨 |
| Linux login messages Message | UCS3 @ 192.168.2.5 | 1 | 14:39 | Stored | 192.168.2.5 | 0 | 192.168.2.5 | 0 | N/A | 🟥🟨 |
| URL accessed | ASA @ 192.168.4.1 | 2 | 14:39 | Firewall Permit | 172.17.2.150 | 0 | 192.168.7.5 | 0 | N/A | 🟥🟨 |
| Deny protocol src | ASA @ 192.168.4.1 | 6 | 14:39 | Firewall Deny | 172.17.2.136 | N/A | 192.168.4.1 | N/A | N/A | 🟥🟨 |
| Linux login messages Message | UCS2 @ 192.168.2.4 | 1 | 14:39 | Stored | 192.168.2.4 | 0 | 192.168.2.4 | 0 | N/A | 🟥🟨 |
| Linux login messages Message | UCS2 @ 192.168.2.4 | 1 | 14:39 | Stored | 192.168.2.4 | 0 | 192.168.2.4 | 0 | N/A | 🟥🟨 |
| Linux login messages Message | UCS3 @ 192.168.2.5 | 1 | 14:39 | Stored | 192.168.2.5 | 0 | 192.168.2.5 | 0 | N/A | 🟥🟨 |
| Linux login messages Message | UCS3 @ 192.168.2.5 | 1 | 14:39 | Stored | 192.168.2.5 | 0 | 192.168.2.5 | 0 | N/A | 🟥🟨 |
| Deny protocol src | ASA @ 192.168.4.1 | 6 | 14:39 | Firewall Deny | 172.17.1.91 | N/A | 192.168.4.1 | N/A | N/A | 🟥🟨 |
| Linux login messages Message | UCS3 @ 192.168.2.5 | 1 | 14:39 | Stored | 192.168.2.5 | 0 | 192.168.2.5 | 0 | N/A | 🟥🟨 |
| Deny protocol src | ASA @ 192.168.4.1 | 27 | 14:39 | Firewall Deny | 192.168.4.1 | 60783 | 193.0.14.129 | 53 | N/A | 🟥🟨 |
| Deny protocol src | ASA @ 192.168.4.1 | 5 | 14:39 | Firewall Deny | 192.168.4.1 | 59121 | 192.5.5.241 | 53 | N/A | 🟥🟨 |
| Deny protocol src | ASA @ 192.168.4.1 | 17 | 14:39 | Firewall Deny | 192.168.4.1 | 61525 | 143.127.102.40 | 443 | N/A | 🟥🟨 |
| Linux login messages Message | UCS3 @ 192.168.2.5 | 1 | 14:39 | Stored | 192.168.2.5 | 0 | 192.168.2.5 | 0 | N/A | 🟥🟨 |
| Linux login messages Message | UCS2 @ 192.168.2.4 | 1 | 14:39 | Stored | 192.168.2.4 | 0 | 192.168.2.4 | 0 | N/A | 🟥🟨 |
| Linux login messages Message | UCS2 @ 192.168.2.4 | 1 | 14:39 | Stored | 192.168.2.4 | 0 | 192.168.2.4 | 0 | N/A | 🟥🟨 |

Receiving an average of 18 results per second
Copyright © 2014 Q1 Labs Inc. All rights reserved.

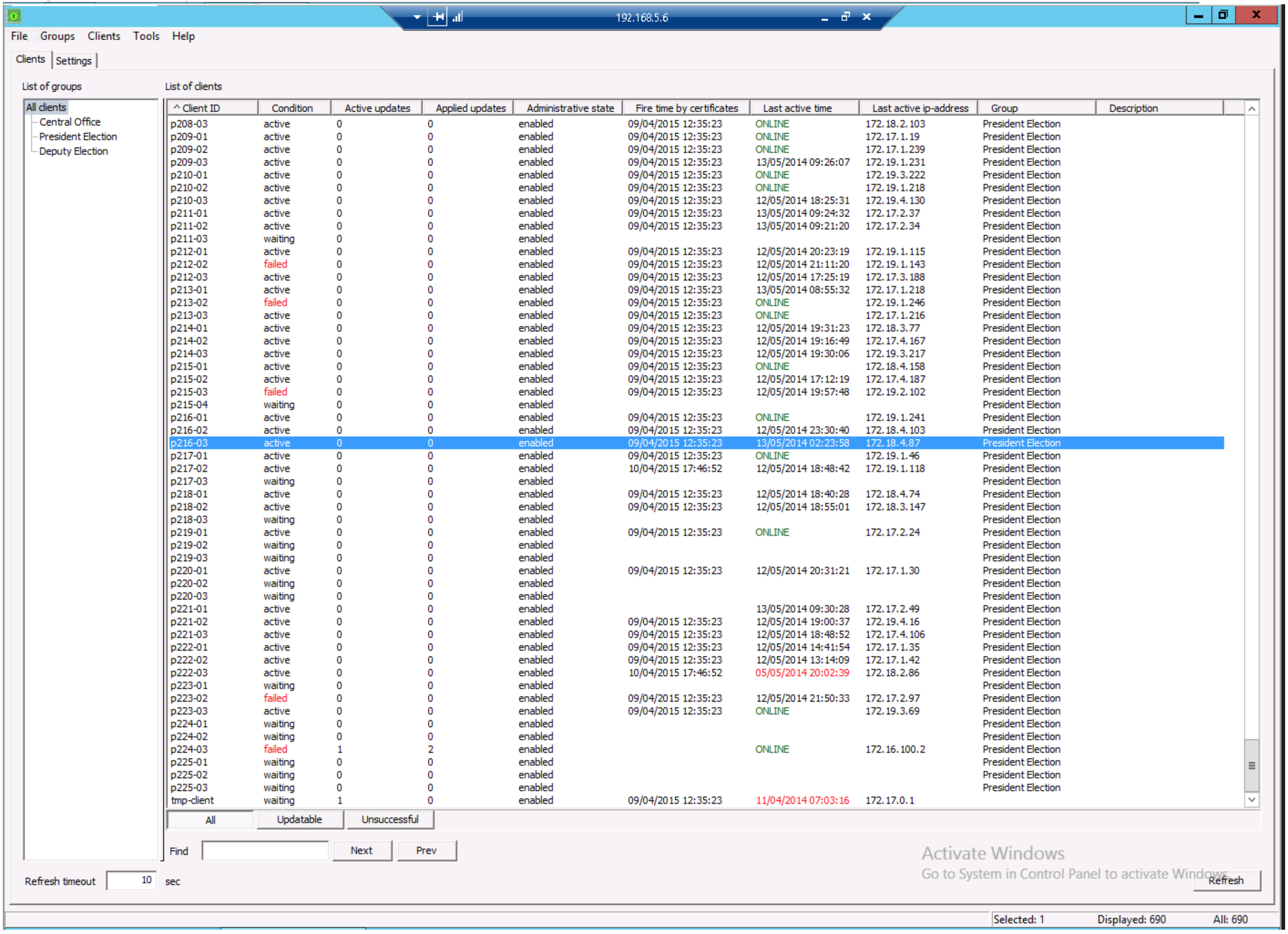

192.168.8.8
Server Manager
Server Manager ‣ File and Storage Services ‣ iSCSI
Manage
Tools
View
Help
Administrator: Command Prompt
TASKS
TASKS
Crash Dump, Primary Partition)
Activate Windows
Go to System in Control Panel to activate Windows.

```
  1...........................Software Loopback Interface 1
 18...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 19...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.8.1     192.168.8.8    261
       10.199.1.0    255.255.255.0         On-link       10.199.1.3    261
       10.199.1.3  255.255.255.255         On-link       10.199.1.3    261
     10.199.1.255  255.255.255.255         On-link       10.199.1.3    261
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link        127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link        127.0.0.1    306
      192.168.8.0    255.255.255.0         On-link      192.168.8.8    261
      192.168.8.8  255.255.255.255         On-link      192.168.8.8    261
    192.168.8.255  255.255.255.255         On-link      192.168.8.8    261
        224.0.0.0        240.0.0.0         On-link        127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link       10.199.1.3    261
        224.0.0.0        240.0.0.0         On-link      192.168.8.8    261
  255.255.255.255  255.255.255.255         On-link        127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link       10.199.1.3    261
  255.255.255.255  255.255.255.255         On-link      192.168.8.8    261
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0      192.168.8.1  Default
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    306 ::1/128                  On-link
 22    261 fe80::/64                On-link
 21    261 fe80::/64                On-link
 21    261 fe80::427:ad6e:4874:376d/128
                                    On-link
 22    261 fe80::71f4:7c6c:6d56:8bad/128
                                    On-link
  1    306 ff00::/8                 On-link
 22    261 ff00::/8                 On-link
 21    261 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None

C:\Windows\system32>_
```

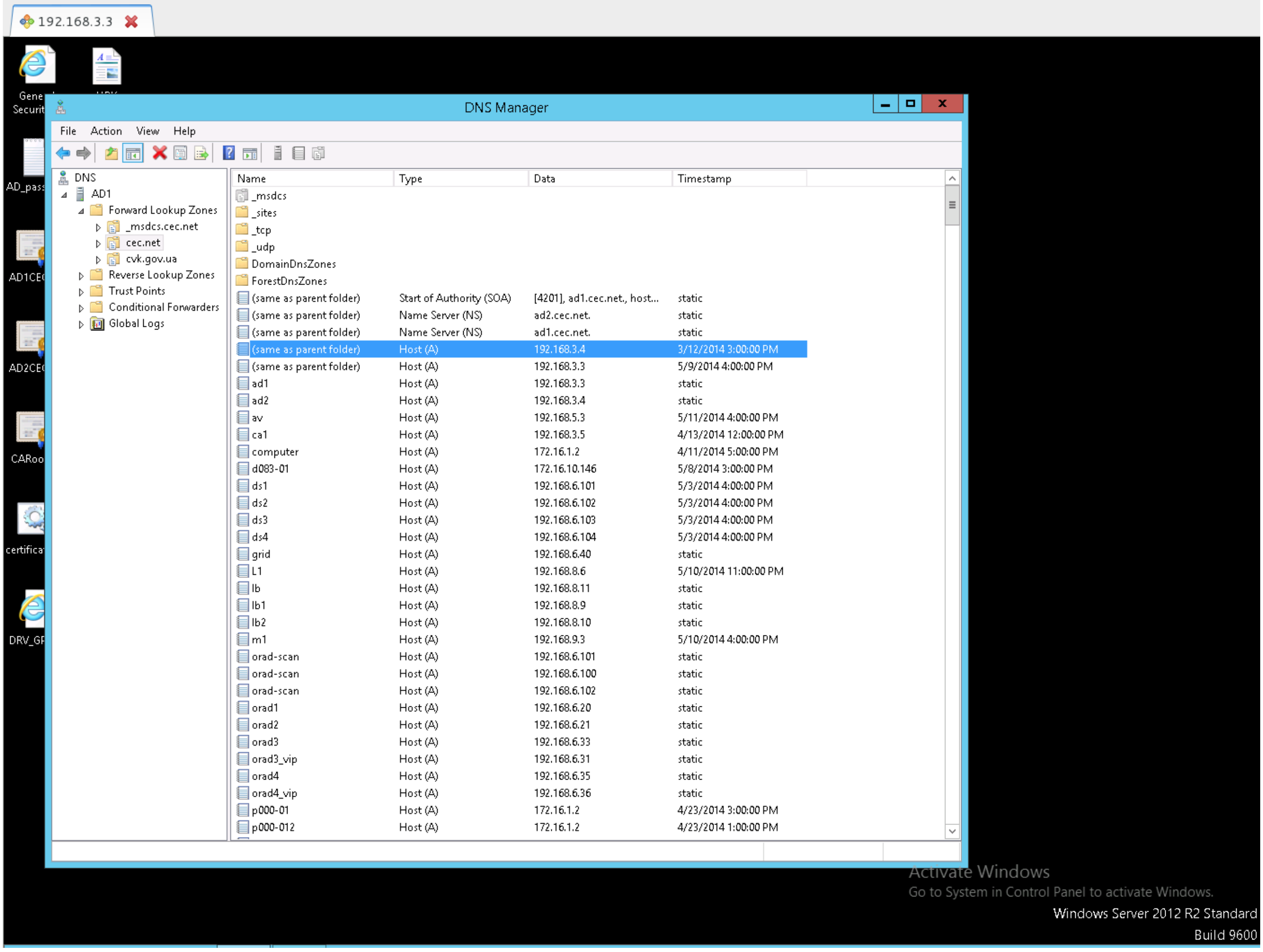
| Target Name | Target Status | Initiator ID |
|---|---|---|
| iscsi.2.ora.2 | Connected | IPAddress:10.199.1.21 |
| iscsi.2.rac.2 | Not Connected | IPAddress:10.199.1.30, IPAddress:10.199.1.33, IPAddress:10.199.1.35 |
| iscsi.2.rac.2 | Not Connected | IPAddress:10.199.1.30, IPAddress:10.199.1.33, IPAddress:10.199.1.35 |
| | | .199.1.21 |
| | | .199.1.10, IPAddress:10.199.1.11, IPAddress:10.199.1.6, IPAddress |

| Status | Capacity | Free Spa... |
|---|---|---|
| Healthy (B... | 136.35 GB | 122.66 GB |
| Healthy (P... | 3725.84 GB | 21 MB |
| Healthy (P... | 3725.84 GB | 21 MB |
| Healthy (P... | 3725.84 GB | 21 MB |
| Healthy (P... | 3725.84 GB | 21 MB |
| Healthy (P... | 3725.84 GB | 21 MB |
| Healthy (P... | 3725.84 GB | 3725.56 ... |
| Healthy (P... | 5588.83 GB | 11 MB |

| Name | Server Name | Target IQN | Target Status | Initiator ID |
|---|---|---|---|---|
| iscsi.2.ora.2 | Storage2 | iqn.1991-05.com.microsoft:storage2-iscsi.2.ora.2-target | Connected | IPAddress:10.199.1.21 |



| ^ Client ID | Condition | Active updates | Applied updates | Administrative state | Fire time by certificates | Last active time | Last active ip-address | Group | Description |
|---|---|---|---|---|---|---|---|---|---|
| p208-03 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | ONLINE | 172.18.2.103 | President Election | |
| p209-01 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | ONLINE | 172.17.1.19 | President Election | |
| p209-02 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | ONLINE | 172.17.1.239 | President Election | |
| p209-03 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | 13/05/2014 09:26:07 | 172.19.1.231 | President Election | |
| p210-01 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | ONLINE | 172.19.3.222 | President Election | |
| p210-02 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | ONLINE | 172.19.1.218 | President Election | |
| p210-03 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | 12/05/2014 18:25:31 | 172.19.4.130 | President Election | |
| p211-01 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | 13/05/2014 09:24:32 | 172.17.2.37 | President Election | |
| p211-02 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | 13/05/2014 09:21:20 | 172.17.2.34 | President Election | |
| p211-03 | waiting | 0 | 0 | enabled | | | | President Election | |
| p212-01 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | 12/05/2014 20:23:19 | 172.19.1.115 | President Election | |
| p212-02 | failed | 0 | 0 | enabled | 09/04/2015 12:35:23 | 12/05/2014 21:11:20 | 172.19.1.143 | President Election | |
| p212-03 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | 12/05/2014 17:25:19 | 172.17.3.188 | President Election | |
| p213-01 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | 13/05/2014 08:55:32 | 172.17.1.218 | President Election | |
| p213-02 | failed | 0 | 0 | enabled | 09/04/2015 12:35:23 | ONLINE | 172.19.1.246 | President Election | |
| p213-03 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | ONLINE | 172.17.1.216 | President Election | |
| p214-01 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | 12/05/2014 19:31:23 | 172.18.3.77 | President Election | |
| p214-02 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | 12/05/2014 19:16:49 | 172.17.4.167 | President Election | |
| p214-03 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | 12/05/2014 19:30:06 | 172.19.3.217 | President Election | |
| p215-01 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | ONLINE | 172.18.4.158 | President Election | |
| p215-02 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | 12/05/2014 17:12:19 | 172.17.4.187 | President Election | |
| p215-03 | failed | 0 | 0 | enabled | 09/04/2015 12:35:23 | 12/05/2014 19:57:48 | 172.19.2.102 | President Election | |
| p215-04 | waiting | 0 | 0 | enabled | | | | President Election | |
| p216-01 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | ONLINE | 172.19.1.241 | President Election | |
| p216-02 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | 12/05/2014 23:30:40 | 172.18.4.103 | President Election | |
| p216-03 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | 13/05/2014 02:23:58 | 172.18.4.87 | President Election | |
| p217-01 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | ONLINE | 172.19.1.46 | President Election | |
| p217-02 | active | 0 | 0 | enabled | 10/04/2015 17:46:52 | 12/05/2014 18:48:42 | 172.19.1.118 | President Election | |
| p217-03 | waiting | 0 | 0 | enabled | | | | President Election | |
| p218-01 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | 12/05/2014 18:40:28 | 172.18.4.74 | President Election | |
| p218-02 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | 12/05/2014 18:55:01 | 172.18.3.147 | President Election | |
| p218-03 | waiting | 0 | 0 | enabled | | | | President Election | |
| p219-01 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | ONLINE | 172.17.2.24 | President Election | |
| p219-02 | waiting | 0 | 0 | enabled | | | | President Election | |
| p219-03 | waiting | 0 | 0 | enabled | | | | President Election | |
| p220-01 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | 12/05/2014 20:31:21 | 172.17.1.30 | President Election | |
| p220-02 | waiting | 0 | 0 | enabled | | | | President Election | |
| p220-03 | waiting | 0 | 0 | enabled | | | | President Election | |
| p221-01 | active | 0 | 0 | enabled | | 13/05/2014 09:30:28 | 172.17.2.49 | President Election | |
| p221-02 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | 12/05/2014 19:00:37 | 172.19.4.16 | President Election | |
| p221-03 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | 12/05/2014 18:48:52 | 172.17.4.106 | President Election | |
| p222-01 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | 12/05/2014 14:41:54 | 172.17.1.35 | President Election | |
| p222-02 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | 12/05/2014 13:14:09 | 172.17.1.42 | President Election | |
| p222-03 | active | 0 | 0 | enabled | 10/04/2015 17:46:52 | 05/05/2014 20:02:39 | 172.18.2.86 | President Election | |
| p223-01 | waiting | 0 | 0 | enabled | | | | President Election | |
| p223-02 | failed | 0 | 0 | enabled | 09/04/2015 12:35:23 | 12/05/2014 21:50:33 | 172.17.2.97 | President Election | |
| p223-03 | active | 0 | 0 | enabled | 09/04/2015 12:35:23 | ONLINE | 172.19.3.69 | President Election | |
| p224-01 | waiting | 0 | 0 | enabled | | | | President Election | |
| p224-02 | waiting | 0 | 0 | enabled | | | | President Election | |
| p224-03 | failed | 1 | 2 | enabled | | ONLINE | 172.16.100.2 | President Election | |
| p225-01 | waiting | 0 | 0 | enabled | | | | President Election | |
| p225-02 | waiting | 0 | 0 | enabled | | | | President Election | |
| p225-03 | waiting | 0 | 0 | enabled | | | | President Election | |
| tmp-client | waiting | 1 | 0 | enabled | 09/04/2015 12:35:23 | 11/04/2014 07:03:16 | 172.17.0.1 | | |



| Name | Type | Data | Timestamp |
|---|---|---|---|
| _msdcs | | | |
| _sites | | | |
| _tcp | | | |
| _udp | | | |
| DomainDnsZones | | | |
| ForestDnsZones | | | |
| (same as parent folder) | Start of Authority (SOA) | [4201], ad1.cec.net., host... | static |
| (same as parent folder) | Name Server (NS) | ad2.cec.net. | static |
| (same as parent folder) | Name Server (NS) | ad1.cec.net. | static |
| (same as parent folder) | Host (A) | 192.168.3.4 | 3/12/2014 3:00:00 PM |
| (same as parent folder) | Host (A) | 192.168.3.3 | 5/9/2014 4:00:00 PM |
| ad1 | Host (A) | 192.168.3.3 | static |
| ad2 | Host (A) | 192.168.3.4 | static |
| av | Host (A) | 192.168.5.3 | 5/11/2014 4:00:00 PM |
| ca1 | Host (A) | 192.168.3.5 | 4/13/2014 12:00:00 PM |
| computer | Host (A) | 172.16.1.2 | 4/11/2014 5:00:00 PM |
| d083-01 | Host (A) | 172.16.10.146 | 5/8/2014 3:00:00 PM |
| ds1 | Host (A) | 192.168.6.101 | 5/3/2014 4:00:00 PM |
| ds2 | Host (A) | 192.168.6.102 | 5/3/2014 4:00:00 PM |
| ds3 | Host (A) | 192.168.6.103 | 5/3/2014 4:00:00 PM |
| ds4 | Host (A) | 192.168.6.104 | 5/3/2014 4:00:00 PM |
| grid | Host (A) | 192.168.6.40 | static |
| L1 | Host (A) | 192.168.8.6 | 5/10/2014 11:00:00 PM |
| lb | Host (A) | 192.168.8.11 | static |
| lb1 | Host (A) | 192.168.8.9 | static |
| lb2 | Host (A) | 192.168.8.10 | static |
| m1 | Host (A) | 192.168.9.3 | 5/10/2014 4:00:00 PM |
| orad-scan | Host (A) | 192.168.6.101 | static |
| orad-scan | Host (A) | 192.168.6.100 | static |
| orad-scan | Host (A) | 192.168.6.102 | static |
| orad1 | Host (A) | 192.168.6.20 | static |
| orad2 | Host (A) | 192.168.6.21 | static |
| orad3 | Host (A) | 192.168.6.33 | static |
| orad3_vip | Host (A) | 192.168.6.31 | static |
| orad4 | Host (A) | 192.168.6.35 | static |
| orad4_vip | Host (A) | 192.168.6.36 | static |
| p000-01 | Host (A) | 172.16.1.2 | 4/23/2014 3:00:00 PM |
| p000-012 | Host (A) | 172.16.1.2 | 4/23/2014 1:00:00 PM |