Original task was to create setup Windows Server VMs, promote them to DCs, create new domain and perform initial configuration. All other created VMs must be added to the domain.

Table of Contents

Portfolio 1

Observations

First of all, three VMs with Windows Server were created and configured. IP addresses, DNS address and server names were set, time server and connectivity were checked (Figure 1). Other Windows Server machines were configured analogically.

After that, Active Directory Domain Controller role was installed, server was promoted to the DC and was added to a new domain (Figure 2). AD DC role was also installed on the second server. Last was promoted to the DC and added to the existing domain. Third server will be used for backups in the future.

One VM with Windows 10 was created. It was only necessary to configure IP address, DNS and workstation name in order to join the domain.

Another three VMs with Linux were created: two servers and one workstation. After network configuration, LDAP, Kerberos, NTP client and other required modules were installed. Now, it is possible to join Linux machines to the domain (Figure 3, Figure 4).

Apache Server was installed on one of the Linux machines. HTTP port was opened in the firewall and corresponding record was added to the DNS on the DC. Domain now has Web server (Figure 5).

On every Windows machine C:/ drives were made shared. On every Linux machine Samba package was installed and configured. Now Windows machines are able to access files on Linux machines. In order to mount Windows shared folders, CIFS utilities were installed on every Linux machine. After all described manipulations, each machine can access files on any other machine. Examples of that are shown on (Figure 6, Figure 7).

Records from Users and Computer service are shown on (Figure 8, Figure 9). Topology schematic looks like this (Figure 10).

DHCP role was installed on both DC servers. After that, DHCP was configured on one of the domain controllers. It can be seen on (Figure 11).

On the Windows workstation DHCP can be easily enabled in the network adapters settings. On the Linux workstation, corresponding ifcfg file must be edited. To be more specific, *BOOTPROTO=DHCP* and *ONBOOT=yes* lines must be added. Also, in the DHCP properties on the DC, “Always dynamically update DNS records” and "Dynamically update DNS records for DHCP clients that do not request updates" options must be selected.

In the end, DNS records look like this (Figure 12). Name resolutions example can be seen on (Figure 13, Figure 14).

Root account on Linux machines was disabled via SSH. Instead, Administrator account was added to the wheel group. VMs description is shown in (Table 1).

Table 1. VMs description

VM Name	OS	Memory	Disk Space	Admin account	VM function	IP address
WINSRV1-SB-8569394	Windows server 2016	4 GB	40 GB	Administrator Secret55	Domain Controller, DNS and DHCP server	10.174.68.10/24
WINSRV2-SB-8569394	Windows server 2016	4 GB	40 GB	Administrator Secret55	Domain Controller, DNS and DHCP server	10.174.68.11/24
LINSRV1-SB-8569394	CentOS 7	1 GB	8 GB	Administrator Root Secret55	Web-Server	10.174.68.12/24
LINSRV2-SB-8569394	CentOS 7	1 GB	8 GB	Administrator Root Secret55	Reserved for future use	10.174.68.13/24
WINWS-SB-8569394	Windows 10	2 GB	32 GB	Administrator Secret55	Workstation	10.174.68.40/24
LINWS-SB-8569394	CentOS 7	1 GB	4 GB	Administrator Root Secret55	Workstation	10.174.68.41/24
BACKSRV-SB-8569394	Windows Server 2016	4 GB	40 GB	Administrator Secret55	Server for backups	10.174.68.30/24

Screenshots

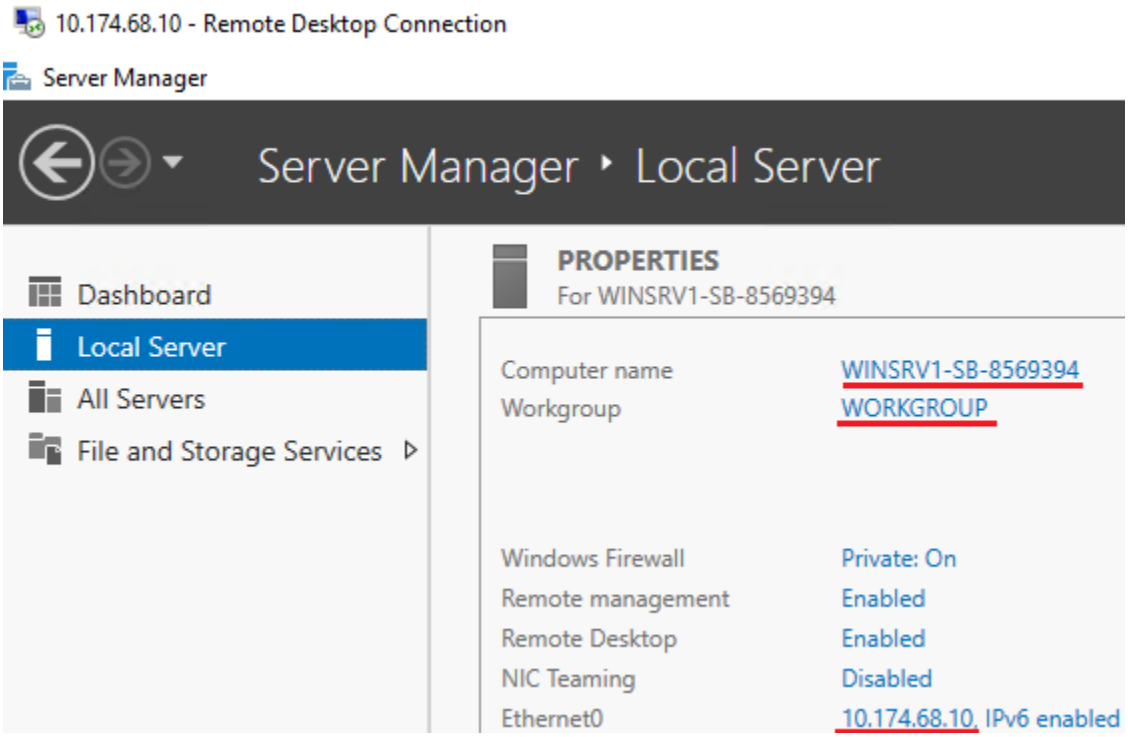

Figure 1. Windows server after initial configuration

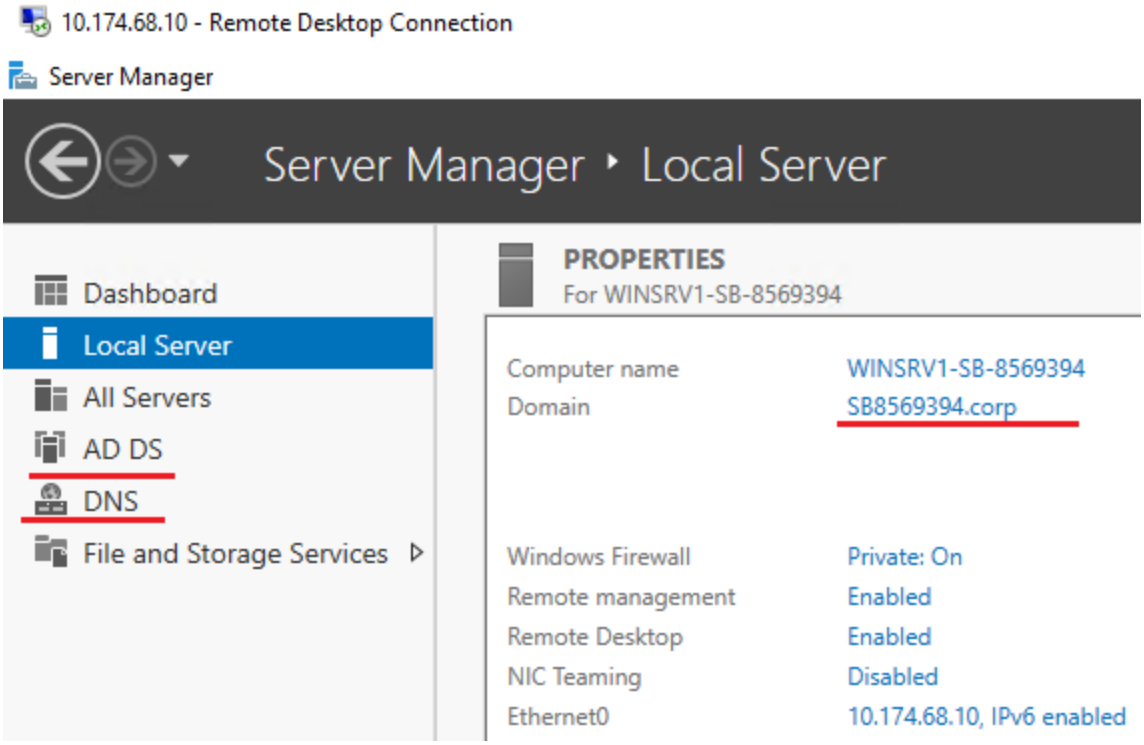

Figure 2. Server was promoted to DC

```
[root@LINSRV1-SB-8569394 ~]# realm list
[root@LINSRV1-SB-8569394 ~]# ip address show dev ens192
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:56:b5:e7:68 brd ff:ff:ff:ff:ff:ff
    inet 10.174.68.12/24 brd 10.174.68.255 scope global noprefixroute ens192
       valid_lft forever preferred_lft forever
    inet6 fe80::55fb:2207:472:dd3a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Figure 3. Linux configuration before joining the domain

```
[root@LINSRV1-SB-8569394 ~]# realm join SB8569394.corp --user=Administrator
Password for Administrator:
[root@LINSRV1-SB-8569394 ~]# realm list
SB8569394.corp
  type: kerberos
  realm-name: SB8569394.CORP
  domain-name: sb8569394.corp
  configured: kerberos-member
```

Figure 4. Linux machine now is in the domain

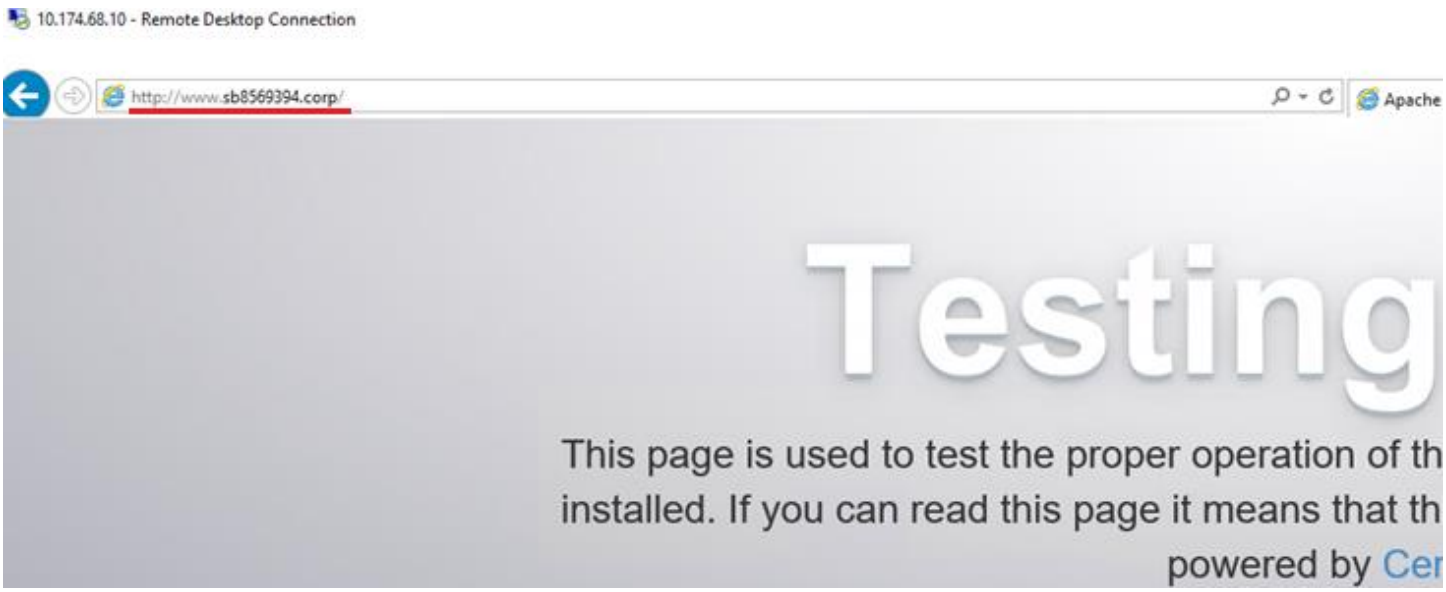

Figure 5. Accessing web server

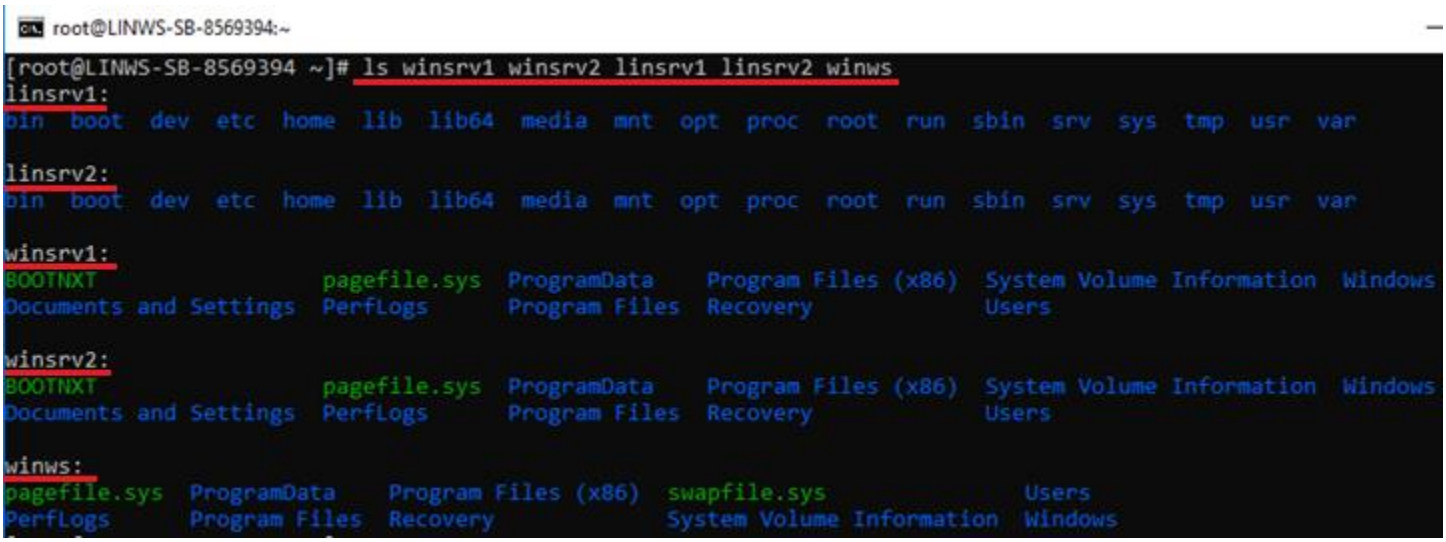

Figure 6. Accessing shared folders from Linux machine

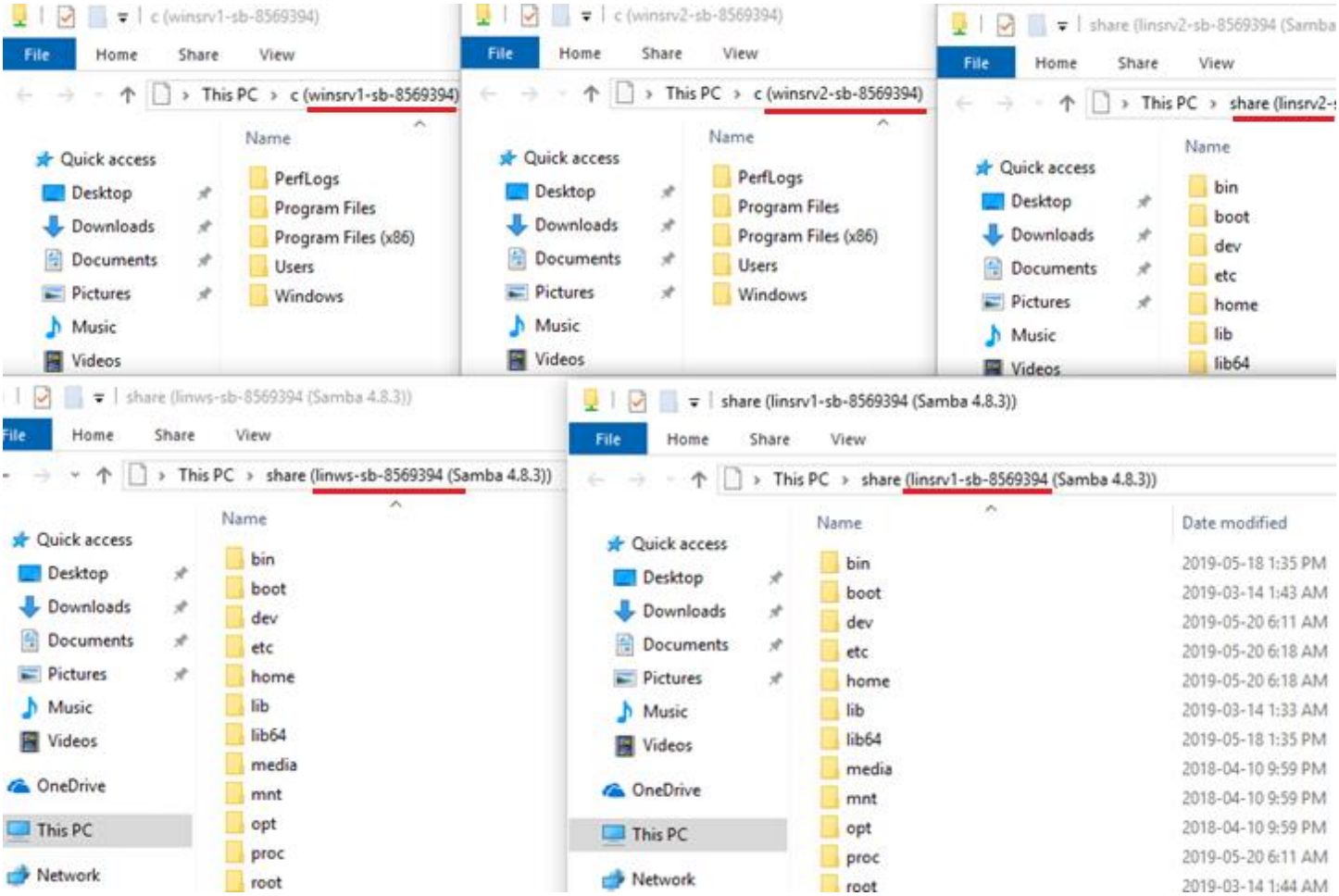

Figure 7. Accessing shared folders from Windows machine

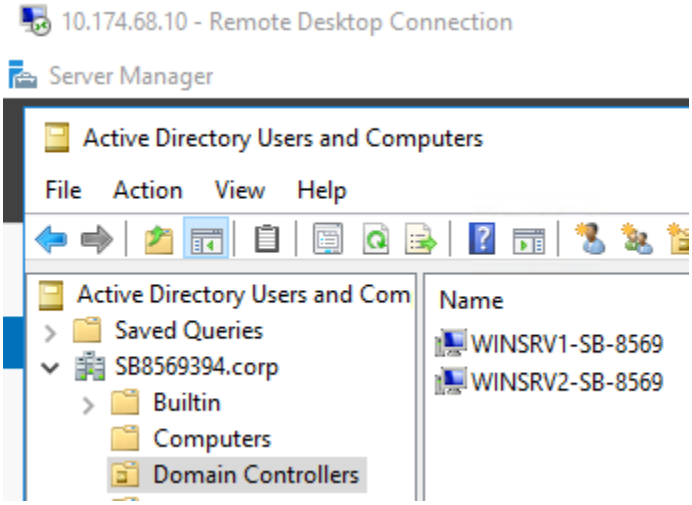

Figure 8. Domain controllers

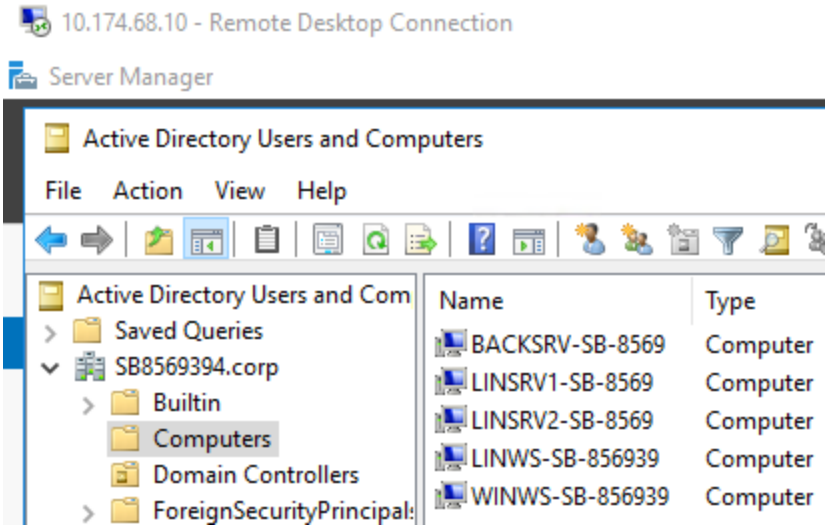

Figure 9. Domain computers

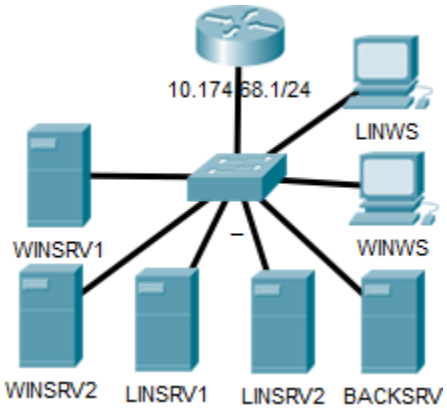

Figure 10. Topology

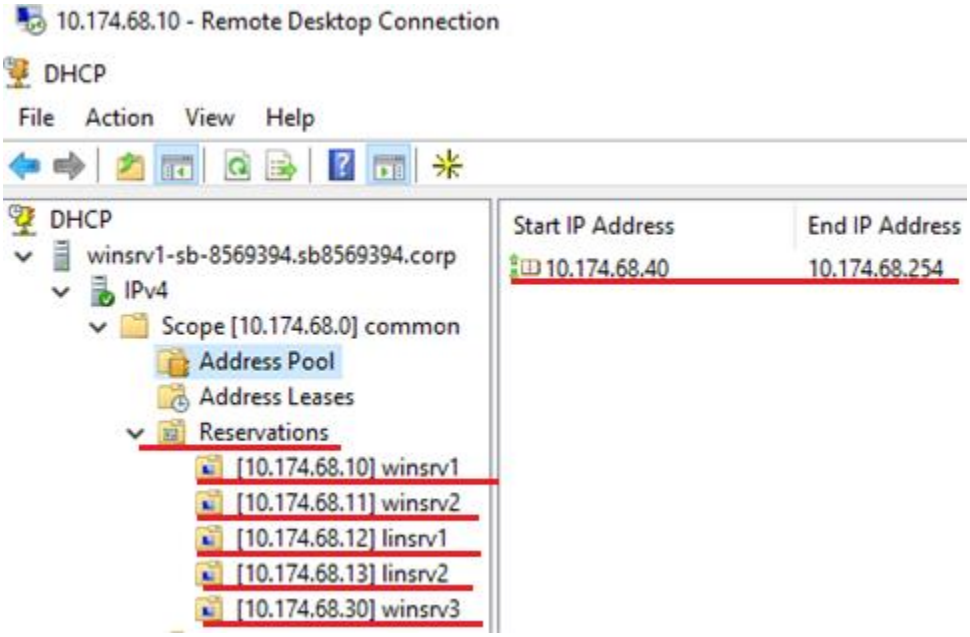

Figure 11. DHCP configuration

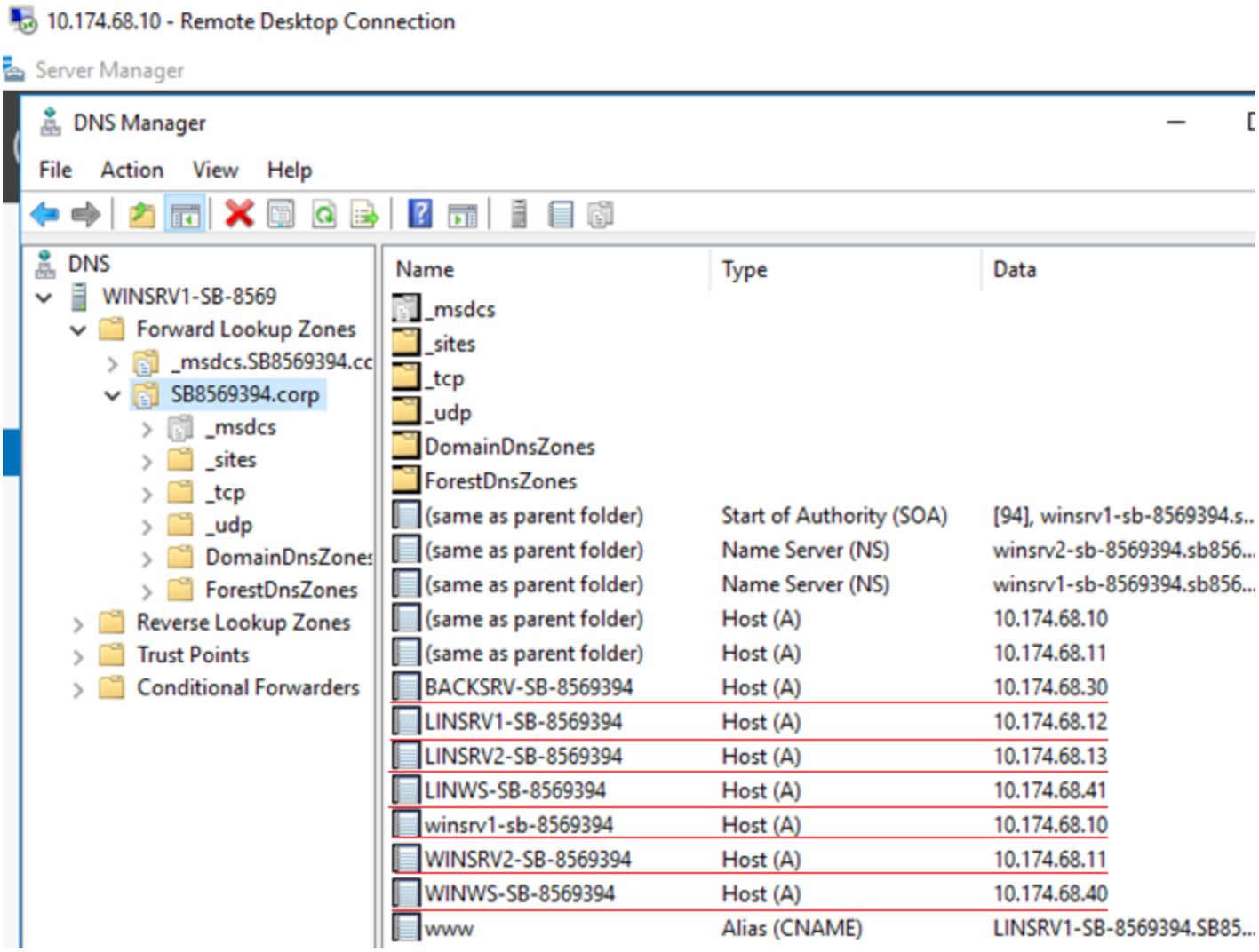

Figure 12. DNS records

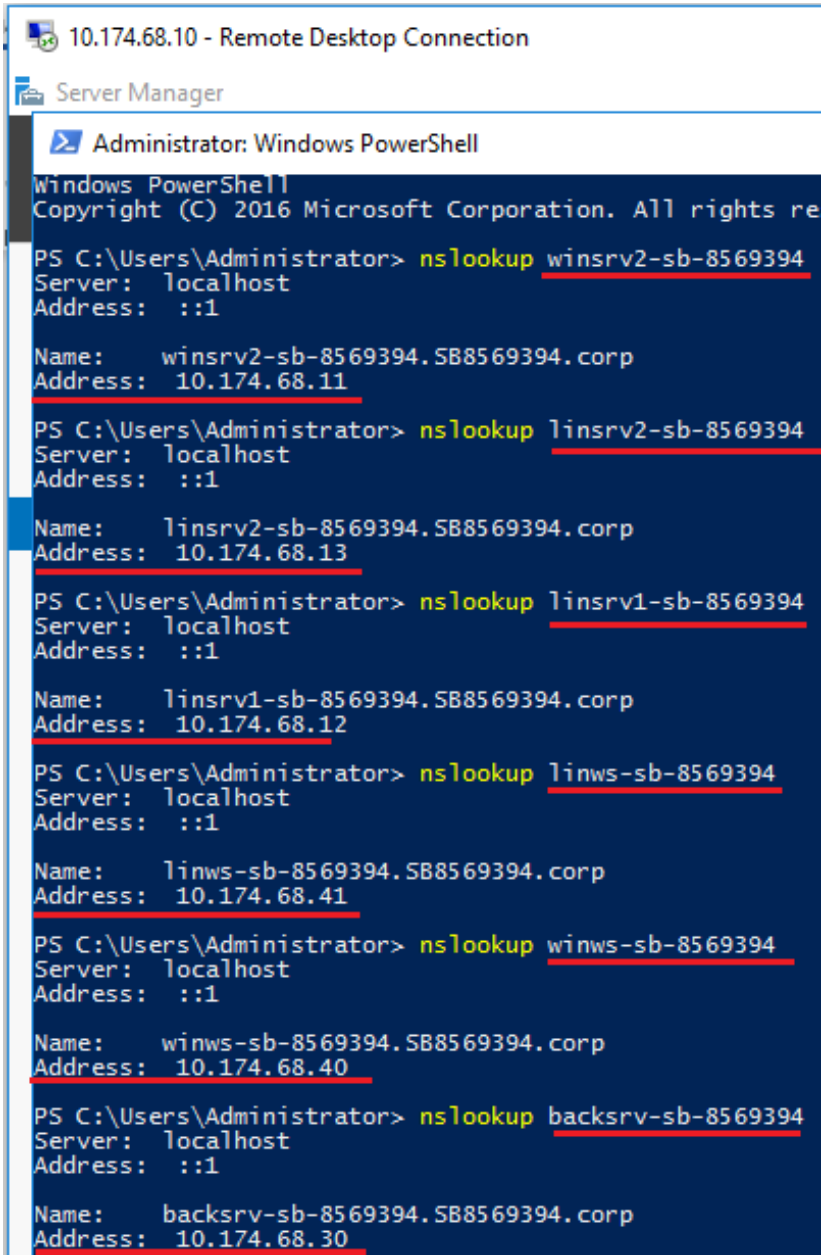

Figure 13. Name resolution example on Windows machine

```
[administrator@SB8569394.corp@LINSRV1-SB-8569394 ~]$ nslookup winsrv1-sb-8569394.sb8569394.corp
Server:         10.174.68.10
Address:        10.174.68.10#53

Name:   winsrv1-sb-8569394.sb8569394.corp
Address: 10.174.68.10

[administrator@SB8569394.corp@LINSRV1-SB-8569394 ~]$ nslookup winsrv2-sb-8569394.sb8569394.corp
Server:         10.174.68.10
Address:        10.174.68.10#53

Name:   winsrv2-sb-8569394.sb8569394.corp
Address: 10.174.68.11

[administrator@SB8569394.corp@LINSRV1-SB-8569394 ~]$ nslookup linsrv2-sb-8569394.sb8569394.corp
Server:         10.174.68.10
Address:        10.174.68.10#53

Name:   linsrv2-sb-8569394.sb8569394.corp
Address: 10.174.68.13

[administrator@SB8569394.corp@LINSRV1-SB-8569394 ~]$ nslookup winws-sb-8569394.sb8569394.corp
Server:         10.174.68.10
Address:        10.174.68.10#53

Name:   winws-sb-8569394.sb8569394.corp
Address: 10.174.68.40

[administrator@SB8569394.corp@LINSRV1-SB-8569394 ~]$ nslookup linws-sb-8569394.sb8569394.corp
Server:         10.174.68.10
Address:        10.174.68.10#53

Name:   linws-sb-8569394.sb8569394.corp
Address: 10.174.68.41

[administrator@SB8569394.corp@LINSRV1-SB-8569394 ~]$ nslookup backsrv-sb-8569394.sb8569394.corp
Server:         10.174.68.10
Address:        10.174.68.10#53

Name:   backsrv-sb-8569394.sb8569394.corp
Address: 10.174.68.30
```

Figure 14. Name resolution example on Linux machine

Reflections

Risk analysis and recovery planning cannot be performed completely in this case since, since all the work was done in laboratory conditions. However, some issues can be mentioned now.

From security point of view, all the VMs now have only their host-based firewalls with default configuration. All firewall should be configured properly and, in addition to them, another firewall should be installed on the border of the network.

Directory controllers with DNS and DHCP servers must not share one physical machine. If one physical machine goes down due to, for instance, hardware failure the second will still be up and running. Backup server should also be running on a separate machine because of the same reason. All physical servers should be powered by uninterruptable supply. Network connection should also be redundant, maybe using Round Robin methodology. Physical access to the last ones should also be restricted. And the last point here is server room location must also be considered properly.

DHCP roles were installed on both DCs, however, it was configured only on the one of them. This gap should be fixed to make DHCP service redundant.

There is a web-server in the domain. It does not perform any logic and data manipulation now, nevertheless if it changes in the future, another instance of web-server should be ready to up and run. Maybe, even both instances should be running with load balancing configured. And if web-server manipulates customer data, the database must be backed up.

In this case, root account on Linux machines was disabled for SSH, however in the real environment the administrator and root accounts on all the machines should be completely locked. Instead, separate accounts for every user-admin should be created. This will increase accountability.