COMP2100 Lab 1 - Technical Documentation

Completed by Quinn Parent for Barett Olsen in COMP2100.

Table of Contents:

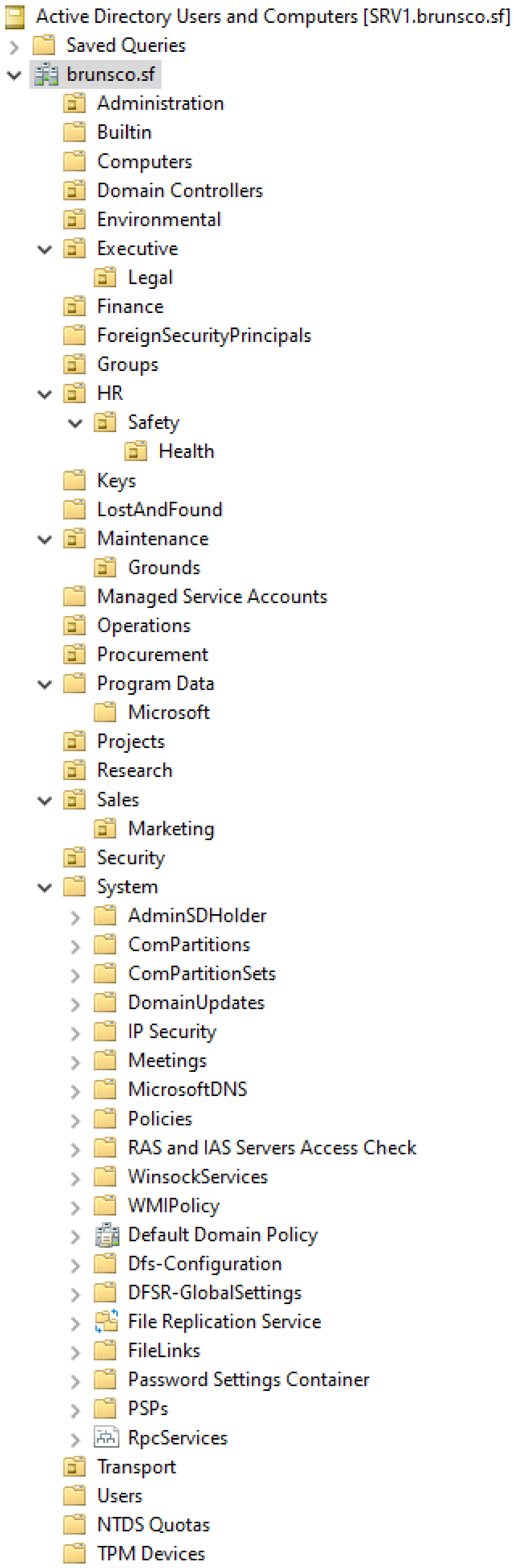
- Project Overview
  - AD Structure
    - AD Usernames and Convention
    - AD Groups and Convention
    - AD GPOs
  - DNS
  - DHCP
  - Firewall and Ports
  - File Services
    - Shares
    - Distributed Files System
    - Data Deduplication
  - VM Information

Project Overview

The goal of this project was to reclaim and redocument Burnsco Industries technical infrastructure. This was done by entering the environment with an observational perspective to record all basic infrastructure information, then with a continuation of making the environment more functional by utilizing file shares and data deduplication.

AD Structure

The active directory structure is split into multiple OUs that contain the business' departments. Some OUs contain teams within the department. Each OU contains users pertaining to that department or team.



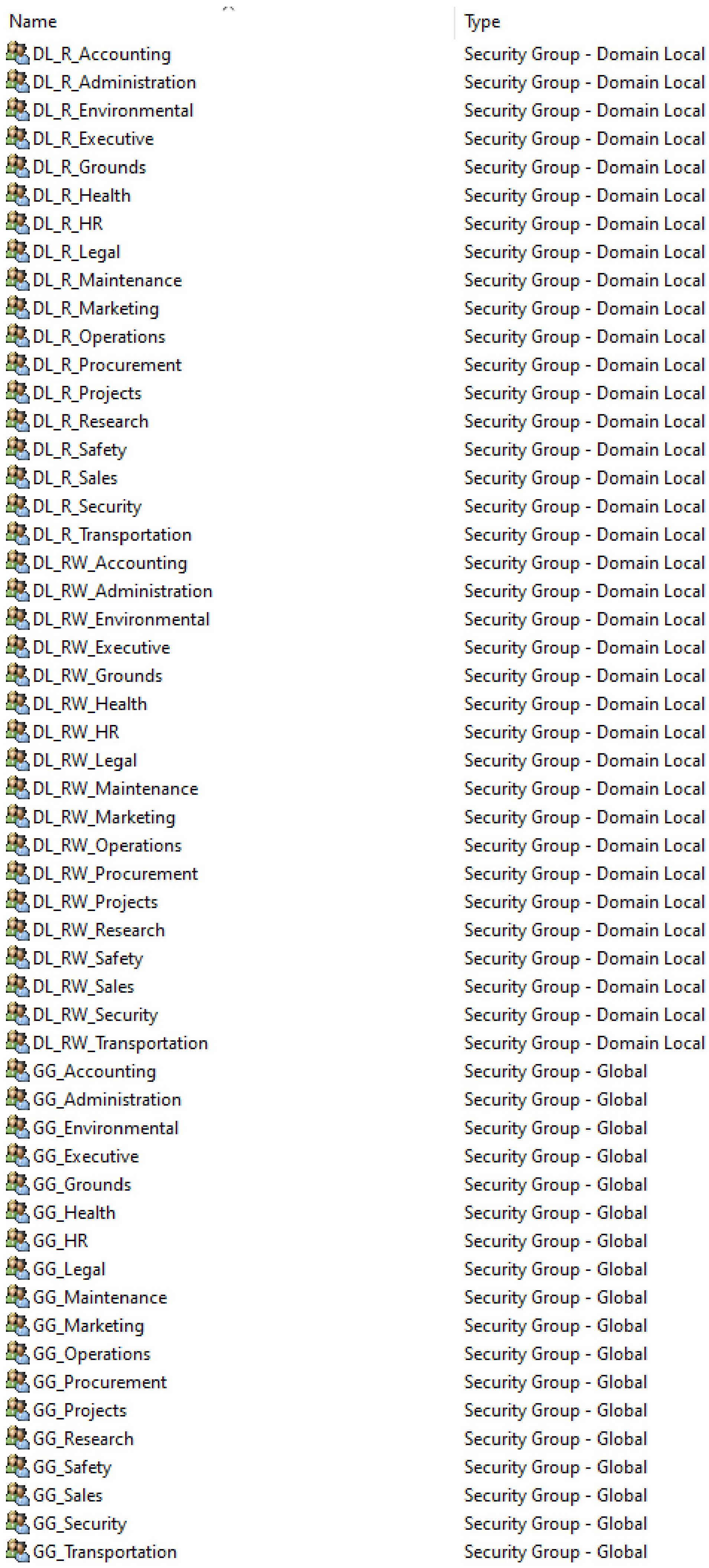
```
Active Directory Users and Computers [SRV1.brunsco.sf]
> Saved Queries
v brunsco.sf
    Administration
    Builtin
    Computers
    Domain Controllers
    Environmental
  v Executive
      Legal
    Finance
    ForeignSecurityPrincipals
    Groups
  v HR
    v Safety
        Health
    Keys
    LostAndFound
  v Maintenance
      Grounds
    Managed Service Accounts
    Operations
    Procurement
  v Program Data
      Microsoft
    Projects
    Research
  v Sales
      Marketing
    Security
  v System
    > AdminSDHolder
    > ComPartitions
    > ComPartitionSets
    > DomainUpdates
    > IP Security
    > Meetings
    > MicrosoftDNS
    > Policies
    > RAS and IAS Servers Access Check
    > WinsockServices
    > WMIPolicy
    > Default Domain Policy
    > Dfs-Configuration
    > DFSR-GlobalSettings
    > File Replication Service
    > FileLinks
    > Password Settings Container
    > PSPs
    > RpcServices
    Transport
    Users
    NTDS Quotas
    TPM Devices
```

AD Usernames and Convention

The username convention for modern Burnsco Industries logon is as follows: `<Last Name><First Name>@brunsco.sf`, an example of which would be: `SimpsonBart@brunsco.sf`. The user logon for pre-Windows 2000 is as follows: `BRUNSCO\<First Name><First 4 letters of Last Name>`, an example of which would be: `BRUNSCO\BartSimp`.

AD Groups and Convention

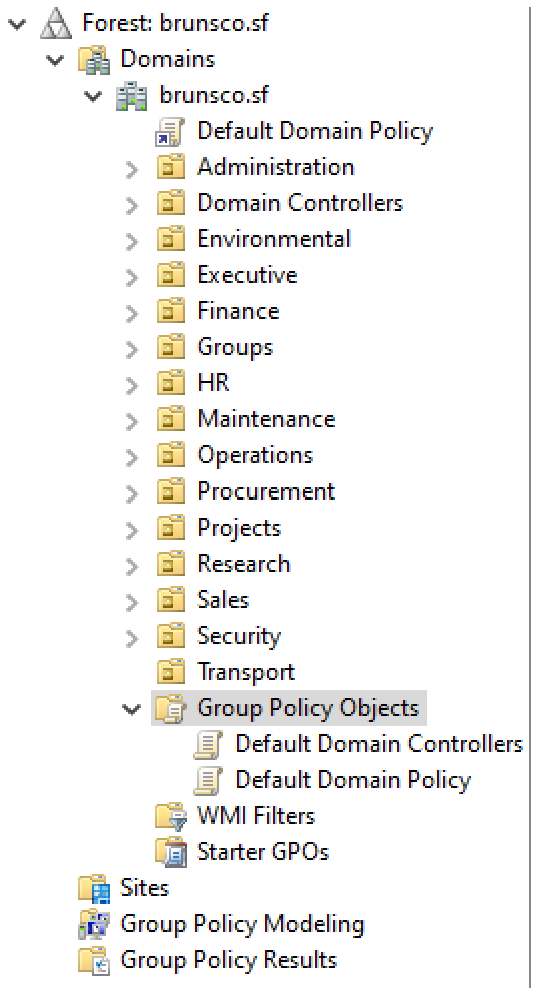
Active Directory groups are setup with a name scheme as follows: For domain local groups: `DL_<Permissions>_<Department>`, an example of such would be: `DL_R_Accounting` which is a domain local read only group for the accounting department. For global groups: `GG_<Department>`, an example of which would be: `GG_Operations` which is a global group for the operations department.



Name	Type
DL_R_Accounting	Security Group - Domain Local
DL_R_Administration	Security Group - Domain Local
DL_R_Environmental	Security Group - Domain Local
DL_R_Executive	Security Group - Domain Local
DL_R_Grounds	Security Group - Domain Local
DL_R_Health	Security Group - Domain Local
DL_R_HR	Security Group - Domain Local
DL_R_Legal	Security Group - Domain Local
DL_R_Maintenance	Security Group - Domain Local
DL_R_Marketing	Security Group - Domain Local
DL_R_Operations	Security Group - Domain Local
DL_R_Procurement	Security Group - Domain Local
DL_R_Projects	Security Group - Domain Local
DL_R_Research	Security Group - Domain Local
DL_R_Safety	Security Group - Domain Local
DL_R_Sales	Security Group - Domain Local
DL_R_Security	Security Group - Domain Local
DL_R_Transportation	Security Group - Domain Local
DL_RW_Accounting	Security Group - Domain Local
DL_RW_Administration	Security Group - Domain Local
DL_RW_Environmental	Security Group - Domain Local
DL_RW_Executive	Security Group - Domain Local
DL_RW_Grounds	Security Group - Domain Local
DL_RW_Health	Security Group - Domain Local
DL_RW_HR	Security Group - Domain Local
DL_RW_Legal	Security Group - Domain Local
DL_RW_Maintenance	Security Group - Domain Local
DL_RW_Marketing	Security Group - Domain Local
DL_RW_Operations	Security Group - Domain Local
DL_RW_Procurement	Security Group - Domain Local
DL_RW_Projects	Security Group - Domain Local
DL_RW_Research	Security Group - Domain Local
DL_RW_Safety	Security Group - Domain Local
DL_RW_Sales	Security Group - Domain Local
DL_RW_Security	Security Group - Domain Local
DL_RW_Transportation	Security Group - Domain Local
GG_Accounting	Security Group - Global
GG_Administration	Security Group - Global
GG_Environmental	Security Group - Global
GG_Executive	Security Group - Global
GG_Grounds	Security Group - Global
GG_Health	Security Group - Global
GG_HR	Security Group - Global
GG_Legal	Security Group - Global
GG_Maintenance	Security Group - Global
GG_Marketing	Security Group - Global
GG_Operations	Security Group - Global
GG_Procurement	Security Group - Global
GG_Projects	Security Group - Global
GG_Research	Security Group - Global
GG_Safety	Security Group - Global
GG_Sales	Security Group - Global
GG_Security	Security Group - Global
GG_Transportation	Security Group - Global

AD GPOs

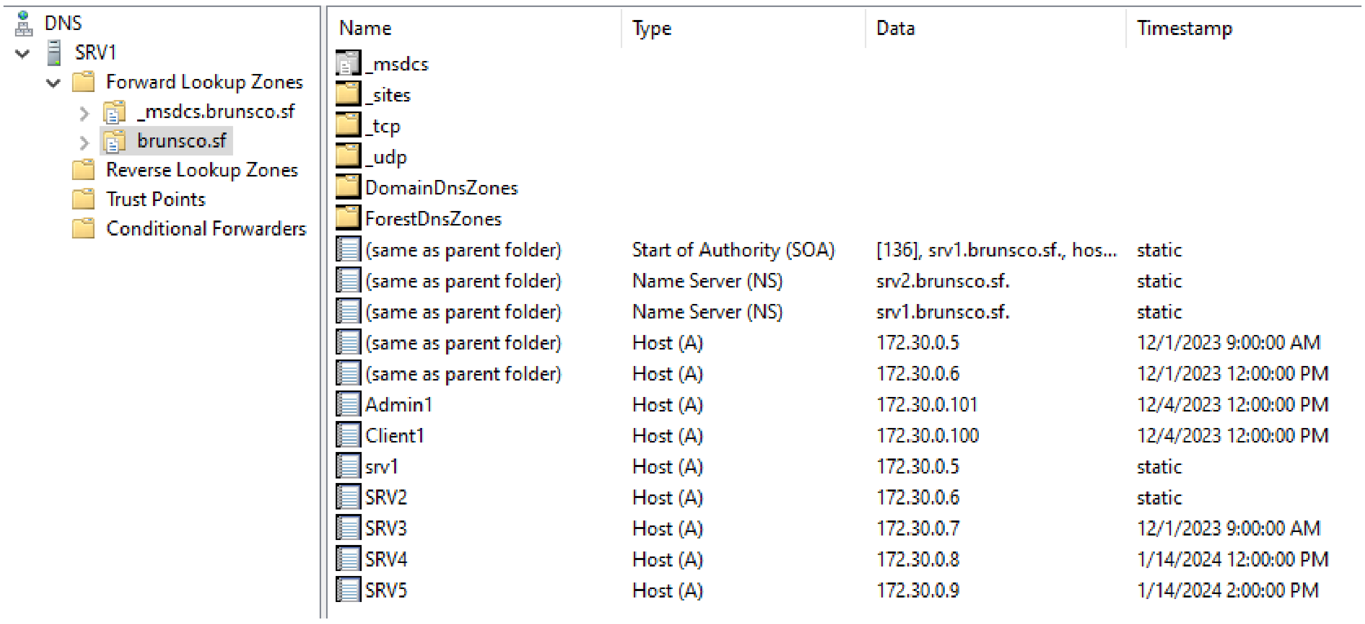
The Group Policy Management window shows no signs of change from the two default policies created upon the domain being created. The two default policies being the `Default Domain Controllers` policy which is only applied to the Domain Controllers OU, and the `Default Domain Policy` which is applied to all OUs.



- Forest: brunsco.sf
  - Domains
    - brunsco.sf
      - Default Domain Policy
      - Administration
      - Domain Controllers
      - Environmental
      - Executive
      - Finance
      - Groups
      - HR
      - Maintenance
      - Operations
      - Procurement
      - Projects
      - Research
      - Sales
      - Security
      - Transport
      - Group Policy Objects
        - Default Domain Controllers
        - Default Domain Policy
      - WMI Filters
      - Starter GPOs
  - Sites
  - Group Policy Modeling
  - Group Policy Results

DNS

The DNS roles is setup on both SRV1 and SRV2, the two DCs for this domain. SRV1 is set as the primary DNS server for all other servers on the network, SRV2 uses itself as its secondary. The DNS forwarders are set to `10.11.8.8` and `10.11.4.4`, the Ultracloud ISP network DNS servers, on both SRV1 and SRV2.

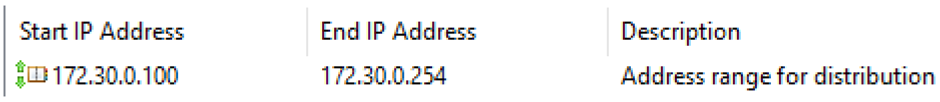


- DNS
  - SRV1
    - Forward Lookup Zones
      - _msdcs.brunsco.sf
      - brunsco.sf
    - Reverse Lookup Zones
    - Trust Points
    - Conditional Forwarders

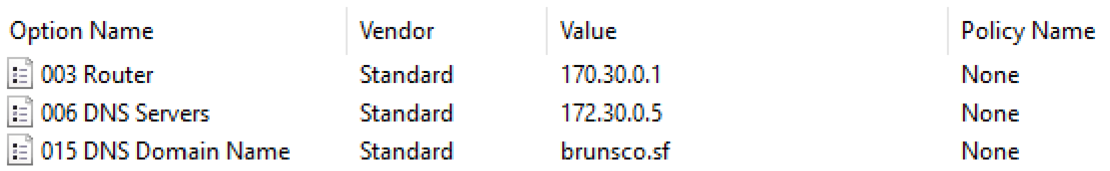
Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[136], srv1.brunsco.sf., hos...	static
(same as parent folder)	Name Server (NS)	srv2.brunsco.sf.	static
(same as parent folder)	Name Server (NS)	srv1.brunsco.sf.	static
(same as parent folder)	Host (A)	172.30.0.5	12/1/2023 9:00:00 AM
(same as parent folder)	Host (A)	172.30.0.6	12/1/2023 12:00:00 PM
Admin1	Host (A)	172.30.0.101	12/4/2023 12:00:00 PM
Client1	Host (A)	172.30.0.100	12/4/2023 12:00:00 PM
srv1	Host (A)	172.30.0.5	static
SRV2	Host (A)	172.30.0.6	static
SRV3	Host (A)	172.30.0.7	12/1/2023 9:00:00 AM
SRV4	Host (A)	172.30.0.8	1/14/2024 12:00:00 PM
SRV5	Host (A)	172.30.0.9	1/14/2024 2:00:00 PM

DHCP

SRV1 is the only DHCP server on the network, with a single IPv4 scope setup. The scope is on the `172.30.0.0/24` network with a range from `172.30.0.100` - `172.30.0.254`. The scope options are configured to give `172.30.0.1` for default gateway, and `172.30.0.5` for DNS server, as well as `brunsco.sf` as domain name.



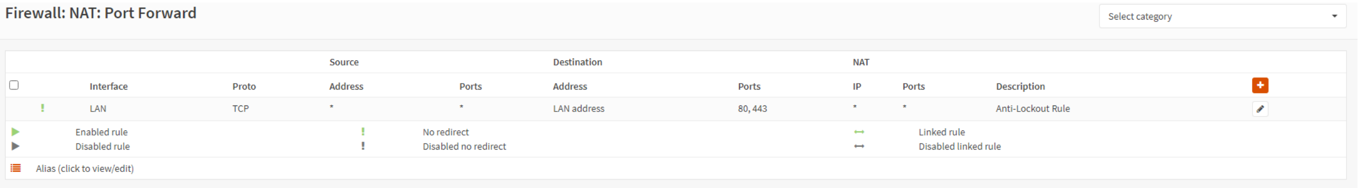
Start IP Address	End IP Address	Description
172.30.0.100	172.30.0.254	Address range for distribution



Option Name	Vendor	Value	Policy Name
003 Router	Standard	170.30.0.1	None
006 DNS Servers	Standard	172.30.0.5	None
015 DNS Domain Name	Standard	brunsco.sf	None

Firewall and Ports

The firewall is an OPNsense firewall that has a LAN and a WAN port. The WAN port is getting a DHCP address from the ISP network, and is set to `10.10.64.10/20` currently with the default gateway being `10.10.79.254`. The LAN port is configured as the default gateway for the network at `172.30.0.1`. The only port forwarding that has been setup on the firewall is the default `Anti-Lockout Rule` that allows any traffic in to the `172.30.0.1` address through port `80 (HTTP)` and `443 (HTTPS)`.



Firewall: NAT: Port Forward

				Source		Destination		NAT			
□		Interface	Proto	Address	Ports	Address	Ports	IP	Ports	Description	+
	!	LAN	TCP	*	*	LAN address	80, 443	*	*	Anti-Lockout Rule	✎

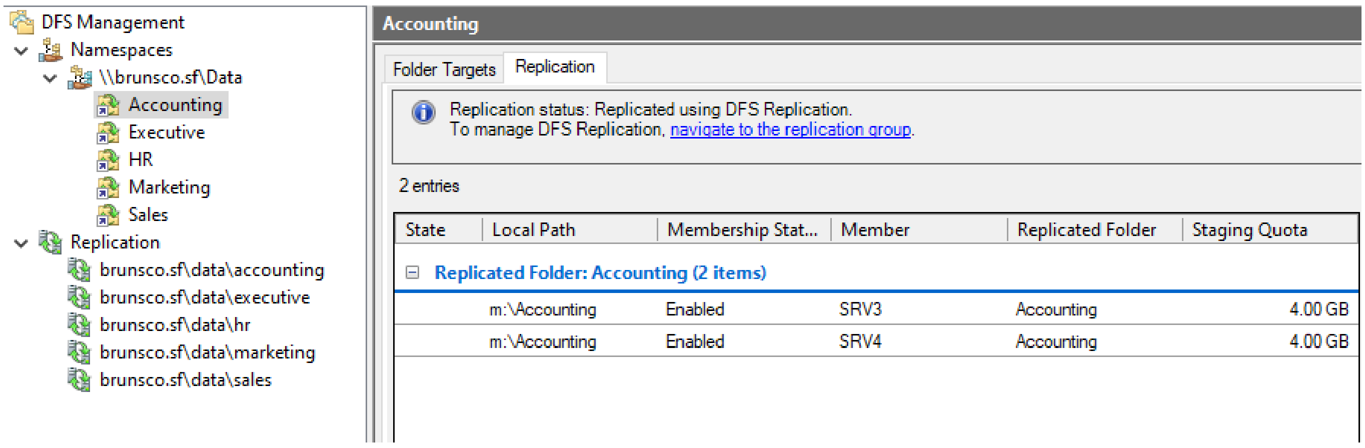
▶ Enabled rule ! No redirect ⟷ Linked rule
▶ Disabled rule ! Disabled no redirect ⟷ Disabled linked rule
☰ Alias (click to view/edit)

File Services

SRV1 through SRV4 are all configured to have the file server role enabled. SRV3 and SRV4 are the two main file servers, being noted as FS1 and FS2 respectively internally. Both SRV3 and SRV4 have the DFS replica role enabled, and SRV3 acts as the DFS Namespace.

Distributed Files System

SRV3 is the DFS Namespace and one of two DFS Replica servers, SRV4 is the other. `Accounting`, `Executive`, `HR`, `Marketing`, and `Sales` are departments that have DFS enabled for redundancy of files. They can be accessed by going to: `\\SRV3\Data\<department>`, or going directly to `M:\<department>` on either SRV3 or SRV4. SRV3 is the primary member for replication in a full mesh topology.



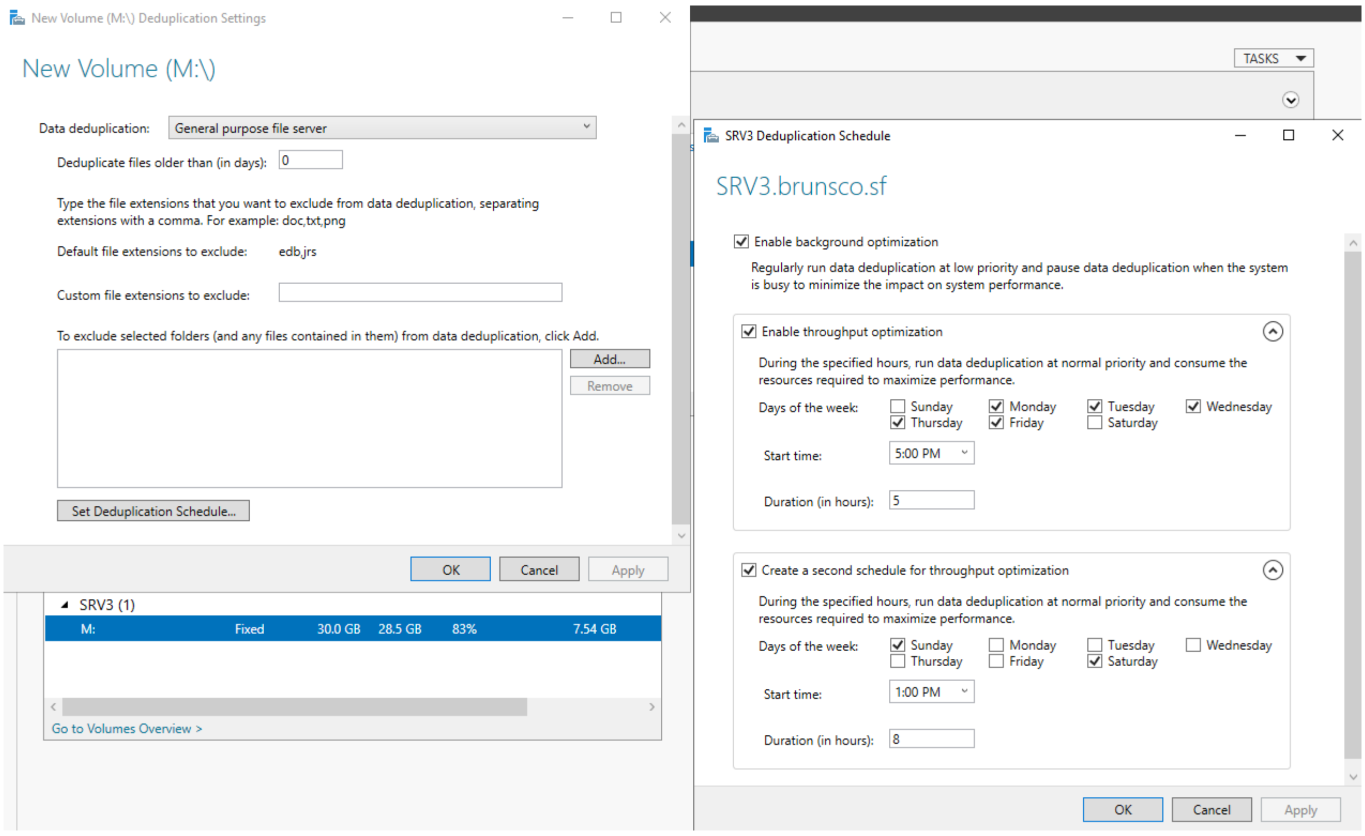
Replication status: Replicated using DFS Replication.
To manage DFS Replication, navigate to the replication group.

2 entries

State	Local Path	Membership Stat...	Member	Replicated Folder	Staging Quota
⊟ Replicated Folder: Accounting (2 items)					
	m:\Accounting	Enabled	SRV3	Accounting	4.00 GB
	m:\Accounting	Enabled	SRV4	Accounting	4.00 GB

Data Deduplication

Data deduplication was configured on SRV3 on the `M:` volume to maximize utilization. The deduplication settings are as follows: `General purpose file server`, deduplication of files older than `0 days`, there are two throughput optimization schedules: `weekdays, 5 hours after 5:00pm` and `weekends, 8 hours after 1:00pm`.



New Volume (M:\)

Data deduplication: General purpose file server

Deduplicate files older than (in days): 0

Type the file extensions that you want to exclude from data deduplication, separating extensions with a comma. For example: doc,txt,png

Default file extensions to exclude: edb,jrs

Custom file extensions to exclude:

To exclude selected folders (and any files contained in them) from data deduplication, click Add.

SRV3 (1)

M:	Fixed	30.0 GB	28.5 GB	83%	7.54 GB

SRV3.brunsco.sf

☑ Enable background optimization

Regularly run data deduplication at low priority and pause data deduplication when the system is busy to minimize the impact on system performance.

☑ Enable throughput optimization

During the specified hours, run data deduplication at normal priority and consume the resources required to maximize performance.

Days of the week: □ Sunday ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday □ Saturday

Start time: 5:00 PM

Duration (in hours): 5

☑ Create a second schedule for throughput optimization

During the specified hours, run data deduplication at normal priority and consume the resources required to maximize performance.

Days of the week: ☑ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday ☑ Saturday

Start time: 1:00 PM

Duration (in hours): 8

VM Information

There are seven virtual machines. Five servers, `SRV1` - `SRV5`, one admin workstation, `Admin1`, and one firewall, `FW`. All the servers are running on Windows Server 2022, version 21H2. The admin workstation is running on Windows 10, version 22H2. The firewall is running on OPNsense 23.7-amd64. All VMs are running with `4GB of RAM`, `1 processor`, and `80GB virtual disks`. Each VM has a NIC assigned to `VMNET15`. The firewall has an additional NIC of `VMNET1` where it is directly patched into the ISP network. SRV3 and SRV4 have two extra disks that are `30GB`, SRV3 has an additional `500GB` drive for data. SRV5 has been given an additional `10GB` and `100GB` drive for a future lab.