`Implementing IPAM

Eli Chang

MSSA Cohort #2

Lab Summary 5

2/13/2020

Implementing IPAM

IP Address Management (IPAM) helps deploy, manage, and monitor the IP address space in a network. Also, it helps manage the DHCP Server and DNS Server roles. The company wants to control the networking environment effectively and efficiently. IPAM would help reduce the complexity in the environment.

There are multiple locations, such as London, Sydney, and Toronto. The IPAM server should be a domain member and single-purpose server because if IPAM installed on a DNS or DHCP server, it would not be able to detect other DNS or DHCP servers on the network. LON-SVR2 becomes an IPAM server for the company.

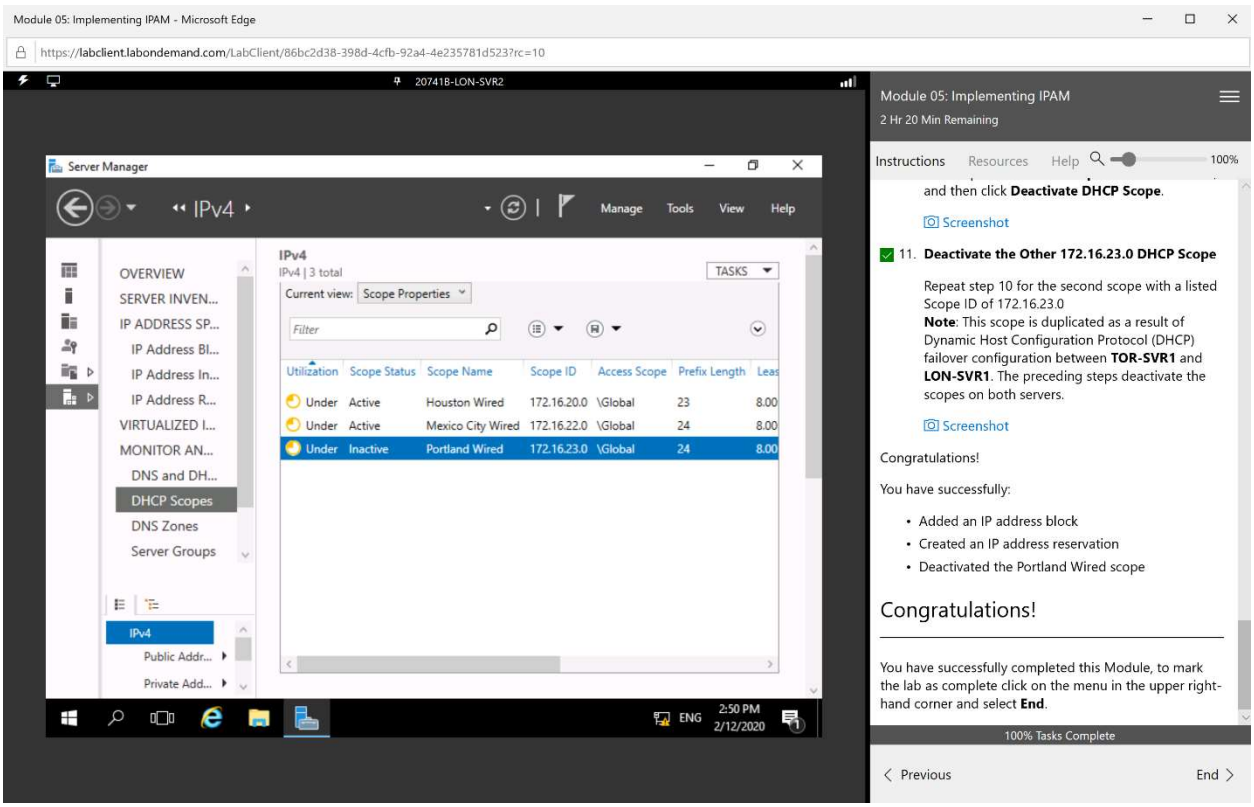
The administrators could view and manage an IP address space by using IP address blocks, IP address ranges, IP addresses, IP address inventory, and IP address range groups. In the lab, there are two options to manage the IP address space, such as IP address blocks and IP address ranges. Also, the admin could monitor the IP address by using DHCP and DNS servers, DHCP scopes, DNS zone monitoring, and server groups.

It is crucial to configure IPAM discovery for servers so that the administrators could find which servers they would manage with IPAM. In the London head office, there are two servers: LON-DC1 and LON-SVR1. LON-DC1 has three servers: a domain controller, DHCP, and DNS; LON-SVR1 has DHCP and DNS servers. In the Toronto regional office, there is a DHCP server, and the Sydney office has a domain controller and DNS server. The IPAM server will manage these eight servers in London.

There are three GPOs created in the IPAM to assign DHCP servers and DNS servers to the managed servers. After setting DHCP and DNS to managed in the GPO allows IPAM to

monitor, manage, and collect information from the managed DHCP and DNS servers on the network.

IP address blocks are to create and allocate IP address ranges to DHCP so that the option maps IP address ranges to the blocks automatically based on the boundaries of the range. The start IP address is 172.16.18.0; the end IP address is 172.16.18.255. Within this range of the IP address, the requests from the hosts will be rejected. In the end, the DHCP scope for the Portland wired scope is deactivated to delete as a duplicate, resulting in DHCP failover between TOR-SVR1 and LON-SVR1.


Module 05: Implementing IPAM - Microsoft Edge
https://labclient.labondemand.com/LabClient/86bc2d38-398d-4cfb-92a4-4e235781d523?rc=10
20741B-LON-SVR2
Server Manager
IPv4
Manage
Tools
View
Help
OVERVIEW
SERVER INVEN...
IP ADDRESS SP...
IP Address Bl...
IP Address In...
IP Address R...
VIRTUALIZED I...
MONITOR AN...
DNS and DH...
DHCP Scopes
DNS Zones
Server Groups
IPv4
Public Addr...
Private Add...
IPv4
IPv4 | 3 total
TASKS
Current view: Scope Properties
Filter
Utilization
Scope Status
Scope Name
Scope ID
Access Scope
Prefix Length
Under Active Houston Wired 172.16.20.0 \Global 23 8.00
Under Active Mexico City Wired 172.16.22.0 \Global 24 8.00
Under Inactive Portland Wired 172.16.23.0 \Global 24 8.00
ENG
2:50 PM
2/12/2020
Module 05: Implementing IPAM
2 Hr 20 Min Remaining
Instructions
Resources
Help
100%
and then click Deactivate DHCP Scope.
Screenshot
11. Deactivate the Other 172.16.23.0 DHCP Scope
Repeat step 10 for the second scope with a listed Scope ID of 172.16.23.0
Note: This scope is duplicated as a result of Dynamic Host Configuration Protocol (DHCP) failover configuration between TOR-SVR1 and LON-SVR1. The preceding steps deactivate the scopes on both servers.
Screenshot
Congratulations!
You have successfully:
Added an IP address block
Created an IP address reservation
Deactivated the Portland Wired scope
Congratulations!
You have successfully completed this Module, to mark the lab as complete click on the menu in the upper right-hand corner and select End.
100% Tasks Complete
Previous
End