**IMPLEMENTATION OF DNS INFRASTRUCTURE AND WEB SERVER FARM FACILITY FOR LARGE SCALE ORGANIZATION USING APACHE, PHP, NFS, ND MYSQL)**

Name

Date

**IMPLEMENTATION OF DNS INFRASTRUCTURE AND WEB SERVER FARM FACILITY FOR LARGE SCALE ORGANIZATION USING APACHE, PHP, NFS, ND MYSQL)**

**Section-1: DNS Deployment**

* To deploy DNS using BIND9 and integrate it into the Netplan configuration, you'll typically follow a series of steps. Below is a general guide, assuming you are setting up a DNS server for the domain "unn.co.uk". Please adapt the steps based on your specific needs and configurations:

**DNS Setup and Configurations**

1. **Primary DNS Server**
2. **Network Configuration**

**Install BIND9:**

sudo apt update

sudo apt install bind9

**Configure BIND9:**

Edit the BIND configuration file as shown below:

*sudo nano /etc/bind/named.conf.options*



* Save the changes and exit the text editor (in nano, you can do this by pressing Ctrl + X, then Y to confirm, and Enter).
* After saving the named.conf.local file, you need to restart the BIND9 service to apply the changes:
* *sudo systemctl restart bind9*
* Now, BIND9 will use the configurations specified in the named.conf.local file for the zones "unn.co.uk," "tech.co.uk," and "staff.unn.co.uk."
* Please ensure that the paths and filenames match the ones you used when creating the zone files and named.conf.local file.

**Configure DNS forwarders (optional):**

*options {*

 *// ...*

 *forwarders {*

 *8.8.8.8;*

 *8.8.4.4;*

 *};*

 *// ...*

*};*

**Create DNS Zones:**

* Edit the zone files. For example:

sudo nano /etc/bind/named.conf.local

Add zone configurations:

bind

zone "unn.co.uk" {

 type master;

 file "/etc/bind/zones/unn.co.uk.db";

};

zone "170.168.192.in-addr.arpa" {

 type master;

 file "/etc/bind/zones/170.168.192.db";

};

**Add DNS Zones**

*$TTL 604800*

*@ IN SOA ns1.unn.co.uk. admin.unn.co.uk. (*

 *2023011701 ; Serial*

 *604800 ; Refresh*

 *86400 ; Retry*

 *2419200 ; Expire*

 *604800 ) ; Negative Cache TTL*

;

@ IN NS ns1.unn.co.uk.

; Add other DNS records (A, CNAME, MX, etc.)

**Create Reverse Zone File:**

*sudo nano /etc/bind/zones/170.168.192.db*

***Add reverse DNS records:***

*$TTL 604800*

*@ IN SOA ns1.unn.co.uk. admin.unn.co.uk. (*

 *2023011701 ; Serial*

 *604800 ; Refresh*

 *86400 ; Retry*

 *2419200 ; Expire*

 *604800 ) ; Negative Cache TTL*

*;*

*@ IN NS ns1.unn.co.uk.wwwwwwwwww11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111 vgt; Add PTR records for reverse DNS lookup*

Edit the Netplan configuration file.

Add DNS configuration:



**Restart Services**

* *sudo systemctl restart bind9*
* *sudo netplan apply*
* You must configure the DNS options in the /etc/bind/named.conf.options file. Open the file with a text editor, for example using nano:
* *sudo nano /etc/bind/named.conf.options*
* Now, add or modify the relevant configurations:

*options {*

 *directory "/var/cache/bind";*

 *// Enable DNSSEC validation*

 *dnssec-validation auto;*

 *// Primary DNS Server 1 (use your actual IP address)*

 *forwarders {*

 *192.168.101.26; // Replace with the IP address of your first DNS server*

 *};*

 *// Primary DNS Server 2 (use a different IP address)*

 *forwarders {*

 *192.168.101.27; // Replace with the IP address of your second DNS server*

 *};*

 *// Other options...*

*};*

* Save the changes and exit the text editor (in nano, you can do this by pressing Ctrl + X, then Y to confirm, and Enter).
* After saving the named.conf.options file, restart the BIND9 service to apply the changes:
* *sudo systemctl restart bind9*

**Zone Distribution:**

* To configure zone distribution for the domains unn.co.uk, tech.co.uk, and staff.unn.co.uk, you need to create separate zone files for each domain. Below are the steps and configurations for the BIND9 named.conf.local file, assuming you are following a standard setup with separate zone files:
* *sudo nano /etc/bind/named.conf.local*
* Add the zone configurations for unn.co.uk, tech.co.uk, and staff.unn.co.uk as shown below.

*// unn.co.uk zone*

*zone "unn.co.uk" {*

 *type master;*

 *file "/etc/bind/zones/db.unn.co.uk"; // Adjust the path accordingly*

*};*

// Primary DNS Server 1

*zone "unn.co.uk" {*

 *type master;*

 *file "/etc/bind/zones/db.unn.co.uk"; // Adjust the path accordingly*

*};*

*zone "tech.co.uk" {*

 *type master;*

 *file "/etc/bind/zones/db.tech.co.uk"; // Adjust the path accordingly*

*};*

*// Primary DNS Server 2*

*zone "unn.co.uk" {*

 *type master;*

 *file "/etc/bind/zones/db.unn.co.uk"; // Adjust the path accordingly*

*};*

*zone "tech.co.uk" {*

 *type master;*

 *file "/etc/bind/zones/db.tech.co.uk"; // Adjust the path accordingly*

*};*

*// tech.co.uk zone*

*zone "tech.co.uk" {*

 *type master;*

 *file "/etc/bind/zones/db.tech.co.uk"; // Adjust the path accordingly*

*};*

*// staff.unn.co.uk zone*

*zone "staff.unn.co.uk" {*

 *type master;*

 *file "/etc/bind/zones/db.staff.unn.co.uk"; // Adjust the path accordingly*

*};*

* After making these changes, save the file and restart BIND9:

sudo systemctl restart bind9

* To configure BIND9 for secondary servers, slave zones, and subdomains, follow these steps:
1. **Modify /etc/bind/named.conf.local**:

// Secondary DNS Servers

zone "unn.co.uk" {

 type slave;

 masters { IP\_OF\_PRIMARY\_SERVER\_1; IP\_OF\_PRIMARY\_SERVER\_2; }; // Replace with actual IP addresses

 file "/etc/bind/zones/db.unn.co.uk"; // Adjust the path accordingly

};

zone "tech.co.uk" {

 type slave;

 masters { IP\_OF\_PRIMARY\_SERVER\_1; IP\_OF\_PRIMARY\_SERVER\_2; }; // Replace with actual IP addresses

 file "/etc/bind/zones/db.tech.co.uk"; // Adjust the path accordingly

};

zone "staff.unn.co.uk" {

 type slave;

 masters { IP\_OF\_PRIMARY\_SERVER\_1; IP\_OF\_PRIMARY\_SERVER\_2; }; // Replace with actual IP addresses

 file "/etc/bind/zones/db.staff.unn.co.uk"; // Adjust the path accordingly

};

* **Create or modify zone files accordingly**:
* Create /etc/bind/zones/db.staff.unn.co.uk for the "staff.unn.co.uk" zone.
* **Restart BIND9**:

*sudo systemctl restart bind9*

* These configurations set up secondary DNS servers that act as backups for the primary servers. The slave zones for "unn.co.uk" and "tech.co.uk" are synchronized from the primary servers. The "staff.unn.co.uk" zone is a slave, synchronized from the secondary servers. Adjust the configurations based on your specific requirements and server setup. Ensure that firewalls are configured to allow DNS traffic, and regularly monitor DNS logs for errors or unauthorized queries.

SERVER CONFIGURATIONS

* For configuring the network on Primary DNS Server 1 (192.168.155.25), you can use the Netplan utility in Ubuntu. Here is an example configuration for the /etc/netplan/10-cloud-init.yaml file:



* After making these changes, save the file and apply the configuration using:

*sudo netplan apply*

* **Network Configuration (/etc/netplan/10-cloud-init.yaml):**



**Main Configurations**

1. **Primary and Master Zones:** The configuration defines three primary DNS zones – "unn.co.uk," "tech.co.uk," and a slave zone "staff.unn.co.uk." The primary zones contain authoritative data and are stored in respective zone files. The "staff.unn.co.uk" zone is configured as a slave, synchronized from the secondary servers.
2. **Zone Distribution:** The primary servers (192.168.101.28 and 192.168.101.29) are responsible for authoritative data in the "unn.co.uk" and "tech.co.uk" zones. The "staff.unn.co.uk" zone is maintained as a slave, synchronized from the primary servers. Secondary servers act as backups, holding slave zones synchronized from the primary servers, ensuring fault tolerance.
3. **Subdomain Specification:** The zone files specify subdomains such as "web," "www," and "ftp." These subdomains help organize and manage various services within each primary zone. It's essential to maintain firewall configurations allowing DNS traffic and regularly monitor DNS logs for errors or unauthorized queries.



1. B
2. **Unauthorized Access to Zone Data:**
	* *Explanation:* Inadequate limitations on DNS servers may result in complete access to zone data.
	* *Impact:* Malicious actors can obtain crucial DNS data through unauthorized access, compromising the confidentiality of sensitive information.
3. **Zone Poisoning and Data Manipulation:**
	* *Explanation:* Unrestricted zone transfers pose a risk, potentially leading to data integrity breaches.
	* *Impact:* The integrity of data within the DNS zone could be compromised, allowing for manipulation and unauthorized modifications.
4. **Amplification Attacks:**
	* *Explanation:* Unrestricted zones can be exploited for DNS amplification attacks, generating large responses for minimal requests.
	* *Impact:* Such attacks can significantly impact network performance, causing congestion and potentially leading to service disruptions.
5. **Resource Utilization:**
	* *Explanation:* Uncontrolled zone transmissions can escalate demand and resource usage.
	* *Impact:* Excessive bandwidth consumption may hamper overall network performance, affecting the efficiency of data transmission.
6. **Denial-of-Service (DoS) Attacks:**
	* *Explanation:* Floods of zone transfer requests can overwhelm the primary server, depleting its resources.
	* *Impact:* Resource exhaustion can result in a denial of DNS service, disrupting the availability of DNS resolution for legitimate users.
7. **Increased Attack Surface:**
	* *Explanation:* Unrestricted transfers expose DNS system information publicly.
	* *Impact:* Knowledge gained through such exposure increases the server's vulnerability, providing attackers with insights that could be exploited for further security breaches.
8. **Failure to Comply with Best Practices:**
	* *Explanation:* Prohibiting zone transfers is a fundamental security practice.
	* *Impact:* Neglecting security requirements increases the risk of potential attacks, emphasizing the importance of adherence to best practices for a robust DNS infrastructure.