==

CATEGORY: DNS

==

DNS operations directly affect name resolution, service availability, and security posture. These SOPs ensure every DNS action performed through RDAM Script Wizard is controlled, auditable, and aligned with enterprise standards.

SOP 1 – Get DNS A Record

Script Name: Get DNS A Record **Category:** DNS **Version:** 1.0 **Approved By:** IT Operations / Security

1. Purpose

This script retrieves an IPv4 A record from a DNS zone. It provides a standardized, auditable method for verifying DNS entries, supporting troubleshooting, inventory, and validation of name-to-IP mappings.

2. Scope

- **Systems:** Domain-joined systems with DNS management tools.
- **Zones:** AD-integrated or standard primary zones.
- **Authorized Personnel:**
    - Network engineers
    - Domain Admins
    - Helpdesk Tier-2/3
    - Application support teams

3. Definitions

- **A Record:** DNS record mapping a hostname to an IPv4 address.
- **Zone:** DNS namespace (e.g., contoso.com).
- **FQDN:** Fully Qualified Domain Name.

4. Preconditions

- Operator must have read access to DNS zones.
- DNS server must be reachable.
- Zone must exist.
- Hostname must be valid.

5. Required Inputs

- **Zone Name** (e.g., contoso.com)
- **Record Name** (e.g., server01)

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for zone and record name.
    - Validate non-empty and valid DNS label format.
2. **DNS Server Resolution**
    - Identify authoritative DNS server for the zone.
    - If server unreachable, abort and log.
3. **Record Query**
    - Query DNS for the A record.
    - If multiple A records exist, return all.
4. **Output Formatting**
    - Present:
        - FQDN
        - IPv4 address
        - TTL
        - Timestamp (if available)
5. **Logging**
    - Log zone, record name, operator, timestamp.

7. Expected Output

- A structured result showing the A record(s) for the hostname.

8. Post-Execution Validation

- Operator may verify using nslookup or Resolve-DnsName.

9. Error Handling

- Zone not found
- Record not found
- DNS server unreachable
- Access denied

10. Security Considerations

- DNS data may reveal internal infrastructure; restrict access.
- Avoid querying sensitive hostnames without business justification.

11. Audit Logging Requirements

- Operator ID
- Zone
- Record name
- Timestamp
- Success/Failure

12. Organizational Benefit Statement

This script provides a consistent, auditable method for retrieving DNS A records, improving troubleshooting efficiency and reducing misconfiguration risk.

SOP 2 – Add DNS A Record

Script Name: Add DNS A Record **Category:** DNS

1. Purpose

This script creates a new A record in a DNS zone, mapping a hostname to an IPv4 address. It ensures DNS additions are performed safely, consistently, and with full auditability.

2. Scope

- AD-integrated or primary DNS zones
- Used by network, server, and application teams

3. Definitions

- **A Record:** Maps hostname → IPv4 address.
- **Create Operation:** Adding a new DNS entry.

4. Preconditions

- Operator must have write permissions to the DNS zone.
- Hostname must not conflict with existing records (unless overwrite allowed).
- IP address must be valid and assigned per network standards.
- Action must align with approved change request.

5. Required Inputs

- Zone name
- Record name
- IPv4 address
- Optional: TTL value

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for zone, hostname, and IP.
    - Validate hostname format and IP address syntax.
2. **DNS Server Resolution**
    - Identify authoritative DNS server.
3. **Conflict Check**
    - Query for existing A record.
    - If record exists and overwrite not allowed, abort.
4. **Record Creation**
    - Add A record to zone with specified IP and TTL.
5. **Post-Creation Verification**
    - Requery DNS to confirm record exists.
    - Validate FQDN resolves correctly.
6. **Logging**

    - Log zone, hostname, IP, operator, timestamp.

7. Expected Output

- Confirmation that the A record was successfully created.

8. Post-Execution Validation

- Operator may test resolution using nslookup or Resolve-DnsName.
- Application teams may validate connectivity.

9. Error Handling

- Invalid IP address
- Hostname conflict
- Zone not found
- Access denied
- DNS server unreachable

10. Security Considerations

- Incorrect DNS entries can cause outages; ensure approvals.
- Avoid creating records for unauthorized hosts.
- DNS poisoning risks require strict access control.

11. Audit Logging Requirements

- Operator ID
- Zone
- Hostname
- IP address
- Timestamp
- Result

12. Organizational Benefit Statement

This script ensures DNS entries are created in a controlled, auditable manner, reducing risk of outages and ensuring consistent name resolution across the enterprise.

SOP 3 – Remove DNS A Record

Script Name: Remove DNS A Record **Category:** DNS

1. Purpose

This script deletes an existing A record from a DNS zone. It supports decommissioning, cleanup, and correction of invalid DNS entries.

2. Scope

- AD-integrated or primary DNS zones
- Used by network, server, and security teams

3. Definitions

- **Record Removal:** Deleting a DNS entry so it no longer resolves.

4. Preconditions

- Operator must have write access to the DNS zone.
- Record must exist.
- Removal must be authorized (e.g., decommissioning, cleanup).

5. Required Inputs

- Zone name
- Record name

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for zone and hostname.
2. **DNS Server Resolution**
    - Identify authoritative DNS server.
3. **Record Lookup**
    - Query DNS for the A record.
    - If not found, return informational message.
4. **Removal Confirmation**
    - Script may require explicit confirmation depending on policy.

5. **Record Deletion**
    - Remove A record from zone.
6. **Post-Removal Verification**
    - Requery DNS to confirm record no longer exists.
    - Validate hostname no longer resolves.
7. **Logging**
    - Log zone, hostname, operator, timestamp.

7. Expected Output

- Confirmation that the A record was removed.

8. Post-Execution Validation

- Operator may test resolution to ensure record is gone.
- Application teams may validate service behavior.

9. Error Handling

- Record not found
- Access denied
- Zone not found
- DNS server unreachable

10. Security Considerations

- Removing DNS entries may break services; ensure approvals.
- DNS cleanup should follow decommissioning procedures.

11. Audit Logging Requirements

- Operator ID
- Zone
- Hostname
- Timestamp
- Result

12. Organizational Benefit Statement

This script provides a safe, auditable method for removing DNS entries, reducing stale records and improving name resolution accuracy across the enterprise.