# Active Directory Health Check Guide

This document outlines the proper commands to run for checking the health of Active Directory (AD), the expected outputs for a healthy environment, and steps to take if AD is not healthy.

## 1. Commands to Check AD Health

### a. Replication Health Check

Command: `repadmin /replsummary`  
Expected Output: The replication summary should show zero errors under the 'Largest Delta' and 'Fails' columns.

If errors are present:  
- Investigate specific errors using `repadmin /showrepl`.  
- Check DNS settings and ensure all domain controllers are properly synchronized.

### b. Domain Controller Diagnostics

Command: `dcdiag`  
Expected Output: All tests should pass without any errors or warnings. The output should end with 'DC diagnosis test passed'.  
If errors occur:  
- Review the failed test sections in the output for more details.  
- Use targeted tests (e.g., `dcdiag /test:<TestName>`) to troubleshoot specific issues.

### c. Replication Topology

Command: `repadmin /showrepl`  
Expected Output: No errors in the replication status for any domain controller.  
If issues are found:  
- Ensure all domain controllers can resolve each other's names.  
- Check for network connectivity issues.

### d. DNS Health Check

Command: `dcdiag /test:DNS`  
Expected Output: DNS tests should pass without errors.  
If DNS errors occur:  
- Verify DNS server configurations.  
- Ensure domain controllers have the correct DNS settings.

### e. Netlogon Service

Command: `nltest /dsgetdc:<DomainName>`  
Expected Output: Returns information about the domain controller for the specified domain.  
If the domain controller is not found:  
- Restart the Netlogon service.  
- Check network connectivity and DNS resolution.

## 2. Actions for an Unhealthy Active Directory

If any issues are identified during the health checks, follow these steps to troubleshoot and resolve them:

### a. Replication Issues

- Run `repadmin /syncall` to force synchronization.  
- Check event logs for replication errors on the affected domain controllers.  
- Verify time synchronization across all domain controllers.

### b. DNS Issues

- Verify that all domain controllers are using the correct DNS settings.  
- Restart the DNS server service on the affected domain controllers.  
- Clear the DNS cache using `ipconfig /flushdns` and restart the Netlogon service.

### c. Domain Controller Connectivity

- Ensure the domain controllers can communicate with each other over the network.  
- Test connectivity using `ping` and `nslookup` commands.  
- Check firewall settings to ensure required ports are open.

### d. Rebuilding AD Database

- As a last resort, rebuild the Active Directory database by restarting the domain controller in Directory Services Restore Mode (DSRM) and using the `ntdsutil` command to perform repairs.

### f. Full Diagnostic Check

Command: `dcdiag /c /v /f:<logfile>`  
Expected Output: A comprehensive diagnostic log will be generated, including verbose output for all tests.  
- Replace `<logfile>` with the path and name of the file where you want to save the output.  
If errors are found:  
- Review the log file for detailed information about the failed tests.  
- Use the specific test names provided in the log to run targeted diagnostics (e.g., `dcdiag /test:<TestName>`).  
- Address the errors based on the information provided, focusing on areas like replication, DNS, or connectivity.