

Active Directory Health Check

Overview

Active Directory is a cornerstone of the security of your network. The health check process gathers key data about the health and security of your Active Directory environment. A Ravenswood consultant will analyze the data and prepare a detailed report based on hundreds of best practices and known issues. Based on this report, we will review key findings and make recommendations on remediation. Optionally, you may choose to re-run the health check again at a later date to check progress towards remediation.

Key Outcomes

- ✓ Identify areas to improve the configuration and security posture of AD
- ✓ Gain industry best practices from decades of combined AD design, operations, and remediation experience
- ✓ Get insight from consultants that focus on enterprise AD everyday
- ✓ Actionable remediation recommendations prioritized by severity
- ✓ Operational recommendations to improve reliability and security

Approach

Each health check takes the following approach:



Scope

Health checks are run on a per-forest basis with a focus on technical findings and operational processes.

The technical analysis focuses on the key areas below:

- Administrative roles and security
- Back-up and restore
- Domain controller configuration
- Domain and forest configuration
- DNS configuration
- FSMO roles
- Group Policy usage
- High availability
- Logging
- Replication
- Server performance
- Sites and subnets

Data collected about these areas serves as the primary input to the report generation

Timeline

Depending on the size and complexity of your AD environment, the health check process typically takes from 2 – 4 weeks to complete.

You may optionally elect to add a recurring health check service to check progress on a periodic basis.