# Design and Implementation for Active Directory

Statement of Work

Prepared for

Prepared by

Date: February 28, 2020

Version: 1.0



# Table of contents

[INTRODUCTION 1](#_TOC_250014)

1. [PROJECT OBJECTIVES AND SCOPE 1](#_TOC_250013)
   1. [OBJECTIVES 1](#_TOC_250012)
   2. [AREAS IN SCOPE 1](#_TOC_250011)
      1. [General project scope 1](#_TOC_250010)
      2. [Software products and technologies 3](#_TOC_250009)
      3. [Environments 5](#_TOC_250008)
   3. [AREAS OUT OF SCOPE 5](#_TOC_250007)
2. [PROJECT APPROACH AND TIMELINE 7](#_TOC_250006)
   1. [APPROACH 7](#_TOC_250005)
      1. [Assess Phase 7](#_TOC_250004)
      2. [Enable Phase 9](#_TOC_250003)
   2. [TIMELINE 10](#_TOC_250002)
3. [PROJECT ORGANIZATION 11](#_TOC_250001)
   1. [PROJECT ROLES AND RESPONSIBILITIES 11](#_TOC_250000)

This **‘Design and Implementation for Active Directory (DIAD)’** Statement of Work (SOW) and any exhibits, appendices, schedules, and attachments to it are made with accordance to the Master SOW (**Modern Workplace for Spin-Off**). Each chapter in the Master SOW applies to this document.

# Introduction

# Project objectives and scope

## Objectives

The objective of this project is to deploy a new Active Directory Domain Services (AD DS) environment for . This new AD DS environment will serve as a production directory service that provides authentication and authorization services across a variety of Technologies’ resources. This objective will be met by using the following principles:

* + - Designed by using the latest Microsoft-recommended practices
    - Built by employing the latest security recommendations

## Areas in scope

### General project scope

Microsoft will support the customer in the following areas: .

|  |  |  |
| --- | --- | --- |
| **Area** | **Description** | **Assumptions** |
| Design Workshops | Microsoft will lead up to four (4) design workshops to determine specific configuration elements for the AD DS deployment. | All required personnel will attend these meetings.  Decisions will be made during the meetings, so the final design can be completed. |
| Domain controller deployment (on- premises) | Microsoft will deploy up to four (4) AD DS domain controllers within the production network environment for the new forest. | Physical hardware or virtual machines are available on the production network and have been built per the specifications that are outlined in the design document for this project. |
| Domain Name Service (DNS) | Configure a single Active Directory integrated DNS forward lookup zone to serve as the primary namespace for this AD DS deployment. | It is assumed that will provide an Internet- resolvable DNS namespace that is a subzone of their current DNS |

|  |  |  |
| --- | --- | --- |
| **Area** | **Description** | **Assumptions** |
|  |  | namespace to serve as the AD DS DNS namespace. |
| Site structure | Configure Active Directory Sites and Services to model the ’ IP subnets as it relates to their network infrastructure. | It is assumed that has a complete listing of all IP subnets that will participate within this new AD DS environment and this list will be given to Microsoft to configure AD DS. |
| Secure Domain Group Policy object (GPO) | A GPO will be deployed that will replace the Default Domain Policy using Microsoft recommended security baselines. | will provide input into the Account Policies portion of this GPO. |
| Secure Domain Controller GPO | A GPO will be deployed that will replace the Default Domain Controllers Policy using Microsoft recommended security baselines. | The settings that are applied within this GPO will remain unchanged. |
| Organizational unit (OU) configuration | A predetermined OU structure will be applied to this configuration which is based upon the tier model for Active Directory Domain Services administration. | The recommended OU structure that is provided as a part of this deployment will remain unchanged. |
| Administrative delegations | An administrative OU model will be deployed following the recommended model for isolating resources per security tiers. This design provides recommendations for Tier 0 (AD service, Services administrators and Domain Controllers) and isolation of this tier with Tier 1 (servers) and Tier 2 (workstations). The detailed delegation model for Tier 1 and Tier 2 is out of scope and should be provided by a following project. | The “Admin” OU model and corresponding delegations as a part of this deployment will remain unchanged. |
| Windows Server 2016 image | Configure a single server image for one (1) hardware model or type   * One server image for Windows Server 2016 will be prepared with the Microsoft Deployment Toolkit (MDT). |  |

|  |  |  |
| --- | --- | --- |
| **Area** | **Description** | **Assumptions** |
|  | This is time-boxed to four (4) days. |  |
| Windows Server 2016 deployment | Deploy of up to one (1) Windows Server 2016 | The Customer will have the server hardware ready before the start of the project. |
| Tier 0 WSUS Server | Built a dedicated Tier 0 WSUS server via MDT | Dedicated WSUS (based on Windows Server 2016 Standard SKU) server for patching Tier 0 Domain Controllers and Tier 0 PAWs. |
| Windows Event log forwarding (WEF) | Domain Controller WEF configuration | Forward specific events (max. 30 events specified by the customer) to a destination specified by the customer. The destination must be compatible with WEF. |
| AD Migration conceptional work | Conceptional work for migration from existing AD to new AD environment | Microsoft will help the customer to develop a migration concept. |

### Software products and technologies

The products and technology that are listed in the following table are required for project execution. is responsible for obtaining all identified licenses and products.

This project will rely upon functionality that is provided as a part of either the Datacenter or Standard edition of Windows Server 2016. Between those two options, the edition that will be used is solely up to and the requirements of their AD DS deployment. The following table provides additional detail about the required software for this project.

The standard domain controller installation that will be provided includes the following software prerequisites.

**Important note:** unless otherwise agreed to in the work order, temporarily appoints Microsoft to act as its agent for the limited purpose of supporting and agreeing to the user terms of any click-through license agreement that accompanies the software (Microsoft or non-Microsoft) that is listed in this SOW or the work order and is included within the test and development environments. can read these terms by clicking the About box in the toolbar ribbon for the specific product at [www.microsoft.com](http://www.microsoft.com/) or by requesting a copy from the Microsoft Delivery Manager.

Unless otherwise agreed to in writing in the work order, temporarily entitles Microsoft to act as its agent for the download of the required software. With this authority, Microsoft can apply the known-good media process to download and validate the required software and can compile the software into a specific disk image structure that can be used to build an MDT server or provide a known good build ISO.

|  |  |  |
| --- | --- | --- |
| **Product and technology item** | **Version** | **Ready by** |
| Windows Server 2016 | Datacenter or Standard | Prior to Enable phase |

The following software packages will be required for the solution and are available as Internet downloads at no cost. Microsoft will provide a text file with packages, versions, and their respective download locations. A script will be provided to help download the required files.

|  |  |
| --- | --- |
| **Name** | **Provided Through** |
| Microsoft BgInfo (from the Sysinternals Suite) | Scripted download |
| Microsoft Assessment and Deployment Kit | Scripted download |
| Windows Management Framework | Scripted download |
| Microsoft Report Viewer | Scripted download |
| Microsoft Deployment Toolkit | Scripted download |
| Microsoft .NET Framework | Scripted download |
| Microsoft Attack Surface Analyzer | Scripted download |
| Microsoft Enhanced Mitigation Experience Toolkit | Scripted download |
| Microsoft Network Monitor | Scripted download |
| Microsoft Message Analyzer | Scripted download |
| Remote Server Administration Tools for Windows | Scripted download |
| Microsoft Local Administrator Password Solution | Scripted download |
| TCPView for Windows (from the Sysinternals Suite) | Scripted download |
| Microsoft Process Explorer (from the Sysinternals Suite) | Scripted download |
| Microsoft Process Monitor (from the Sysinternals Suite) | Scripted download |
| Microsoft Deployment Toolkit (MDT) | Scripted download |
| Microsoft PsTools (from the Sysinternals Suite) | Scripted download |
| Microsoft security baseline templates | Scripted download |
| Administrative templates for Windows 10 | Scripted download |

**Note:** The use of Windows Defender is recommended as the antivirus solution for the new AD DS environment. might choose to use their own antivirus software. However, because domain controllers are managed as Tier 0 resources, and the existing antivirus infrastructure also manages other tiers (1 and 2), a new Tier 0–specific antivirus infrastructure would need to be deployed to adequately support the new, in-scope AD DS environment. This new antivirus infrastructure would need to be governed as a Tier 0 resource and managed accordingly, possibly adding overhead.

### Environments

The following environments will be required to cooperate the project.

|  |  |  |  |
| --- | --- | --- | --- |
| **Environment** | **Location** | **Responsibility** | **Ready by** |
| Development/Test | Dedicated Secure Room | Customer | Prior to Enable phase |
| Production | Secure Datacenter | Customer | Prior to Enable phase |

## Areas out of scope

Any area not explicitly included in the Areas in scope section is out of scope for Microsoft during this project. Areas out of scope for this project are listed in the following table.

|  |  |  |
| --- | --- | --- |
|  | **Note:** This project uses a preconfigured AD DS deployment that follows recommended practices. Any changes to the default configuration, aside from those listed as in-scope, are considered out of scope for this project. | |
| **Area** | | **Description** |
| Additional AD DS delegations or DS Access Control Lists | | This project provides a default AD DS administrative delegation model for managing Tier 0 resources. Placeholder roles are provided for Tier 1 and Tier  2. The detailed delegation model for Tier 1 and Tier 2 is out of scope. Changes or additions to this default model are considered out of scope for this project. |
| Additional AD DS domain controller installation or configuration | | This project has been scoped for the deployment of up to four (4) AD DS domain controllers. The deployment of domain controllers beyond this number is considered out of scope for this project. |
| Additional Group Policy Design, Configuration or Implementation | | This project will provide two new GPO’s which will override the existing Default Domain and Default Domain Controllers GPO objects which will be based on SCM templates. Additional GPOs for managing general |

|  |  |
| --- | --- |
| **Area** | **Description** |
|  | workstations, servers (computer), or user-related objects are out of scope for this project. |
| Additional Testing, including UAT and application testing | This project will perform system testing to validate that the new AD DS environment has been built per the specifications that are listed in the design document for this project. Any additional testing is considered out of scope for this project.  Furthermore, system testing activities have been time-boxed to four days. Testing processes extending beyond this timeframe are considered out of scope for this project. |
| Cloud Services Planning | Planning for cloud services such as Microsoft Azure Networking, Azure Storage, or Azure Active Directory. |
| Data migration | Data migration activities, including the migration of Active Directory objects into this new environment, are not in scope for this project. |
| Hardware | Microsoft will not provide hardware for this project. |
| Integration with third- party software | Microsoft will not be responsible for integration with third-party software. |
| Directory Migration or Consolidation | Migration, consolidation, or rationalization of AD DS objects, including users, groups, workstations, servers, applications, logon scripts, or group policies. |
| Organizational change management | Designing—or redesigning—the Customer’s functional organization is not included. |
| Process reengineering | Designing functional business components of the solution is not included. |
| Product bugs and upgrades | Product upgrades, bugs, and design change requests for Microsoft products are not in scope for this project. |
| Product licenses and subscriptions | Product licenses (Microsoft or non-Microsoft) and cloud service subscriptions are not included. |
| Role Definition | Custom definition of roles and the creation of new accounts or roles (such as groups) are out of scope for this project. |
| Source code review | The Customer will not provide Microsoft with access to non-Microsoft source code or source code information. For any non-Microsoft code, Microsoft Services will be limited to the analysis of binary data, such as a process dump or network monitor trace. |
| System integration | System integration and interfaces are not in scope for this project. |

# Project approach and timeline

## Approach

Microsoft follows a structured approach for the deployment of AD DS environments. This approach is as follows:

* + - **Assess:** during the Assess phase, Microsoft works with you to begin the project and complete design and planning workshops. The result is an updated AD DS design which will be built and deployed into your production environment during the Enable phase.
    - **Enable:** during the Enable phase, Microsoft works with you to prepare, deploy and validate the new AD DS environment into your production network environment.

This section will provide additional detail regarding key activities, work products (Microsoft and ), and assumptions for each phase of this project.

### Assess Phase

The Assess phase begins with the project initiation (kickoff) and ends with the completion of an AD DS design, which will be configured and deployed in the Enable phase. Microsoft will support the customer in the following areas marked as “Microsoft activities”:

|  |  |
| --- | --- |
| **Category** | **Description** |
| **Microsoft activities** The activities to be performed by Microsoft | * Conduct Kick-off and Scope Validation meeting * Conduct AD DS Design Workshops * Supports Solution Design Document and Review with * Supports Draft Test Plan Document and Review with |
| **Customer activities** The activities to be performed by | * Work with Microsoft to identify the Project team members * Participate in Kick-off and Scope Validation meeting * Participate in Design Workshops * Facilitate any necessary communication or information in preparation for requests that might result from discussions during the design workshops and information gathering exercises * Make decisions when architectural options are presented * Participate in the review and approval process of the Solution Design Document. * Participate in the review and approval process of the Test Plan Document |
| **Key assumptions** | * SMEs will be available for Design Workshops. * All required personnel will attend design workshops to determine specific configuration elements for the AD DS |

|  |  |
| --- | --- |
| **Category** | **Description** |
|  | deployment. Decisions will be made during the workshops so that the final design can be completed.   * has a complete listing of all IP subnets that will participate within this new AD DS environment. * will provide an Internet-resolvable DNS namespace that is a subzone of their current DNS namespace to serve as the AD DS DNS namespace. * Physical hardware or virtual machines are available on the production network of and have been built per the specifications that are outlined in the design document for this project. |

#### Workshops

|  |  |  |  |
| --- | --- | --- | --- |
| **Workshop** | **Topics Covered** | **Maximum Hours per Session** | **Maximum Number of Sessions** |
| Kick-off and Scope Validation Workshop | * Initiate the project * Validate scope * Assign appropriate project team members | 4 | 1 |
| Forest/Domain Name and DNS Design Workshop | * Forest Name * Domain Name * DNS Namespace | 2 | 1 |
| Site Design and Domain Controller Physical/Logical HW Design Workshop | * Site Design * Domain Controller Design * DC Naming | 2 | 1 |
| GPO Design Workshop | * Solution Group Policy * Account Policy Settings | 2 | 1 |
| Administrative Model Workshop | * Solution Administrative Model * Delegations * Role Members | 2 | 1 |

**Documents**

|  |  |
| --- | --- |
| **Name** | **Description** |
| Solution Design Document | Word document detailing the AD DS design, including any specific configuration details as determined during the design workshops |

|  |  |
| --- | --- |
| **Name** | **Description** |
| Draft Test Plan Document | Word document detailing the test cases which will satisfy the validation of the deployed environment |
| Communications Plan | Plan for communicating with stakeholder groups during the project |
| Project Plan | Schedule for domain controller build and testing activities |

### Enable Phase

During the Enable phase, the AD DS design is installed onto a production network and validated (tested) to make sure that the design meets the specifications in the solution design document. After it is validated, the AD DS deployment is deemed production-ready, and an engagement closeout meeting completes the project. Microsoft will support the customer in the following areas marked as “Microsoft activities”:

|  |  |
| --- | --- |
| **Category** | **Description** |
| **Microsoft activities** The activities to be performed by Microsoft | * Validate environmental prerequisites * Validate software hash against ’ media * Prepare and update hydration scripts for environment * Supports the implementation guide document and review with * Deploy AD DS domain controllers * Complete System Testing * Remediate or mitigate P1 defects within System Testing timebox. * Review and update Test Plan document with testing results and feedback. * Cooperate final test plan document and review with |
| **Customer activities** The activities to be performed by the Customer | * Prepare all environment prerequisites including software, hardware, or virtual machines for the deployment of AD DS as illustrated in the solution design document * Provide appropriate personnel to assist in the system testing process * Provide appropriate personnel to assist in mitigating any P1 defects * Fix or mitigate all P2, P3, or P4 defects * Participate in the review and approval process of the test plan document * Attend and participate in the project closeout meeting |
| **Key assumptions** | * All required personnel will work with Microsoft during the system testing processes. * Physical hardware or virtual machines are available on the ’ production network and have been built per the   specifications that are outlined in the design document for this project. |

|  |  |
| --- | --- |
| **Category** | **Description** |
|  | * will provide change management approvals for the AD DS installations |

#### Documents

|  |  |
| --- | --- |
| **Name** | **Description** |
| Implementation Guide Document | A Word document that provides step-by-step instructions for installing Active Directory domain controllers |
| Final Test Plan Document | Expanding upon the draft version that was completed during the Assess phase, a Word document that includes all test cases and test results |

## Timeline

A propose timeline for this engagement, built on the phases described in the previous chapter, is presented below. All dates and durations are relative to the project start date and are estimates only.

Assess

1.5 Weeks

Enable

6.5 Weeks

During project planning of the project, a detailed project timeline will be developed.

# Project organization

has the overall responsibility for the project and the project management. Microsoft supports the project with services and technical consulting.

The Services are provided in cooperation and in a joint team of Microsoft and .

## Project roles and responsibilities

The key project roles and the responsibilities are as follows.

#### Customer

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Project sponsor | * Provide the estimated project commitment: part-time * Make key project decisions. * Serve as a point of escalation to support clearing project roadblocks. |
| Project manager | * Provide the estimated project commitment: full time * Serve as primary point of contact for the Microsoft team * Manage the overall project. * Cooperate the project on schedule. * Take responsibility for customer resource allocation, risk management, and project priorities. * Communicate with executive stakeholders. |
| Technical team lead | * Provide the estimated project commitment: full time * Serve as primary technical point of contact. * Take ownership of technical architecture and code outcome. |
| Lead business analyst | * Provide the estimated project commitment: half time * Serve as primary functional point of contact for the team that is responsible for functional business analysis. |

**Microsoft**

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Microsoft architect | * Provide guidance based on Microsoft-recommended practices. * Identify and manage technical risks. * Quality review of outcome. |
| Microsoft consultant | * Provide technical design leadership. * Cooperate workshops and sessions. * Responsible for development and technical outcome. |