ADMT Migration: Complete Implementation Guide

Enterprise Active Directory Migration with Microsoft 365 Integration

---

Document Information

- **Version:** 1.0
- **Date:** Current
- **Classification:** Internal Use
- **Scope:** Enterprise Active Directory Migration
- **Duration:** 4-8 Months

Table of Contents

Executive Summary

Purpose and Scope

This document provides a comprehensive implementation guide for enterprise Active Directory migration using Microsoft's Active Directory Migration Toolkit (ADMT) with integrated Microsoft 365 services. The

migration strategy focuses on minimizing business disruption while ensuring complete functionality of identity-dependent services including Exchange Online, SharePoint Online, and hybrid cloud services.

Migration Approach

The recommended approach utilizes cross-forest migration methodology, which provides:

- **Risk Isolation:** Source and target domains remain separate during migration
- **Rollback Capability:** Complete rollback possible throughout most of the process
- **Phased Execution:** Wave-based migration reduces impact scope
- **Service Continuity:** Critical services remain operational during migration

Key Success Factors

1. **Comprehensive Discovery:** Understanding all dependencies before migration begins
2. **Thorough Testing:** Pilot migration validates processes and identifies issues
3. **Clear Communication:** Stakeholder engagement and user preparation
4. **Expert Team:** Skilled professionals with migration experience
5. **Proper Tooling:** ADMT, Azure AD Connect, and supporting tools configured correctly

---

Phase 0: Foundation & Governance

Duration: Weeks 1-2
Critical Path: Yes
Stakeholders: Executive sponsors, project team, IT leadership

Overview

The foundation phase establishes project governance, team structure, and communication frameworks that determine migration success. This phase is often underestimated but represents the most critical success factor for enterprise migrations.

1. Project Organization

1.1 Executive Sponsorship

Objective: Secure visible, committed leadership support with decision-making authority.

Activities:

- Identify C-level executive sponsor with authority to remove organizational roadblocks

- Establish executive steering committee with representatives from IT, business units, and security
- Define escalation paths for technical and business decisions
- Secure budget approval for tools, resources, and potential service interruptions

Deliverables:

- Signed project charter with executive sponsor commitment
- Steering committee charter with meeting schedules and decision authorities
- Budget approval documentation
- Risk tolerance and business continuity requirements

1.2 Core Team Assembly

Objective: Assemble skilled team with clear roles and responsibilities.

Team Structure:

- **Project Manager:** Enterprise migration experience, PMP certification preferred
- **Active Directory Lead:** Deep AD knowledge, ADMT experience, schema expertise
- **Server Infrastructure Lead:** Windows Server expertise, virtualization, backup/recovery
- **Application Lead:** Application inventory, dependency mapping, vendor relationships
- **Network Lead:** DNS, DHCP, firewall configuration, network segmentation
- **Security Lead:** Identity security, compliance requirements, audit coordination
- **Desktop Lead:** Workstation management, user profile migration, software compatibility
- **Microsoft 365 Lead:** Azure AD Connect, Exchange Online, SharePoint Online expertise

Responsibilities Definition:

- Document specific roles and decision-making authority for each team member
- Establish communication protocols and escalation procedures
- Define work streams and interdependencies between teams
- Create RACI matrix for major project activities

2. Communication Strategy

2.1 Stakeholder Communication Plan

Executive Level:

- **Frequency:** Weekly steering committee meetings

- **Format:** Executive dashboard with RAG status indicators
- **Content:** High-level progress, risks, decisions needed, budget status
- **Escalation:** Critical issues requiring executive intervention

IT Department:

- **Frequency:** Daily stand-up meetings during active phases
- **Format:** Technical deep-dive sessions, shared documentation platform
- **Content:** Technical progress, blockers, resource needs, detailed scheduling
- **Collaboration:** Shared project workspace with real-time updates

Business Users:

- **Frequency:** Bi-weekly departmental briefings
- **Format:** Department-specific impact presentations
- **Content:** Migration schedule, expected changes, training requirements
- **Support:** FAQ development and distribution, training material preparation

2.2 Change Management Framework

User Preparation:

- Develop user impact assessment by department
- Create training materials for post-migration environment
- Establish user advocate program with department representatives
- Plan communication timeline with clear milestones and expectations

Support Team Preparation:

- Train help desk staff on migration timeline and expected issues
- Develop escalation procedures for migration-related problems
- Create knowledge base articles for common post-migration scenarios
- Establish dedicated support channels during migration windows

3. Risk Assessment and Mitigation

3.1 Risk Identification Matrix

High-Risk Areas:

- **Application Compatibility:** Legacy applications with hardcoded domain dependencies
- **Data Loss or Corruption:** Inadequate backup or replication failures
- **Extended Downtime:** Migration activities taking longer than planned
- **Authentication Failures:** Trust relationships or certificate issues
- **Microsoft 365 Integration:** Azure AD Connect sync issues or mailbox access problems

Medium-Risk Areas:

- **Network Connectivity:** Firewall or DNS configuration issues
- **User Resistance:** Inadequate training or change management
- **Performance Degradation:** Resource constraints during migration
- **Group Policy Issues:** Policy application failures in new domain
- **File Share Access:** Permission mapping problems

Risk Mitigation Strategies:

- Comprehensive testing in isolated lab environment
- Multiple backup strategies and validated restore procedures
- Detailed rollback plans for each migration phase
- 24/7 support coverage during critical migration windows
- Vendor engagement for legacy application support

3.2 Business Continuity Planning

Service Level Agreements:

- Define acceptable downtime windows for each service type
- Establish recovery time objectives (RTO) and recovery point objectives (RPO)
- Document critical vs. non-critical services and their dependencies
- Plan alternative access methods during migration windows

Rollback Procedures:

- Document complete rollback procedures for each migration phase
- Test rollback procedures in lab environment
- Identify point-of-no-return decisions and required approvals
- Maintain source environment in operational state until final validation

---

Phase 1: Discovery & Analysis

Duration: Weeks 3-8
Critical Path: Yes
Stakeholders: Technical teams, application owners, business users

Overview

The discovery phase creates a comprehensive understanding of the current environment, dependencies, and requirements. This phase determines the complexity and approach for all subsequent migration activities.

1. Active Directory Comprehensive Inventory

1.1 Forest and Domain Analysis

Objective: Understand the current AD structure, health, and configuration.

Forest-Level Discovery:

- Document forest functional level and schema version
- Identify all domains within the forest and their trust relationships
- Map FSMO role holders and their current health status
- Analyze sites and services topology for replication efficiency
- Document any schema extensions and their impact on migration

Domain-Level Discovery:

- Record domain functional levels and upgrade requirements
- Document domain controllers, their roles, and hardware specifications
- Analyze DNS integration and zone configurations
- Identify all organizational units and their delegation structure
- Map Group Policy objects and their application scope

Health Assessment Activities:

- Run comprehensive replication health checks using repadmin tools
- Perform DNS health validation across all domain controllers
- Analyze event logs for recurring errors or warnings
- Validate time synchronization across all domain controllers

- Check SYSVOL and NETLOGON share integrity

1.2 Object Inventory and Analysis

User Account Analysis:

- Total user count and breakdown by organizational unit
- Enabled vs. disabled accounts with last logon date analysis
- Service accounts identification and their associated services
- Privileged accounts and their administrative roles
- Password policy compliance and account lockout patterns
- User attributes population (email, phone, department, manager)

Computer Account Analysis:

- Total computer count by operating system version
- Server vs. workstation categorization
- Last logon date analysis to identify stale objects
- Computer account permissions and delegation
- Service Principal Names (SPNs) registered to computer accounts

Group Analysis:

- Security groups vs. distribution groups
- Group scope analysis (domain local, global, universal)
- Nested group relationships and circular dependencies
- Large groups that may impact migration performance
- Empty groups and cleanup opportunities
- Groups with external forest members (if applicable)

Organizational Unit Structure:

- Current OU hierarchy and naming conventions
- OU delegation and permissions structure
- Group Policy linking and inheritance patterns
- Opportunities for OU structure optimization

1.3 Security and Compliance Assessment

Privilege Analysis:

- Document all administrative groups and their members
- Identify service accounts with excessive privileges
- Analyze delegation of control assignments
- Review fine-grained password policies
- Document any custom security descriptors

Compliance Requirements:

- Identify regulatory requirements affecting migration (GDPR, HIPAA, SOX)
- Document audit requirements and retention policies
- Analyze encryption requirements for data in transit and at rest
- Review access control requirements and segregation of duties

2. Application and Service Dependency Mapping

2.1 Critical Service Dependencies

Microsoft Exchange Server (if applicable):

- Exchange server versions and roles (Mailbox, CAS, Hub Transport)
- Exchange organization configuration and routing groups
- Distribution groups and mail-enabled security groups
- Accepted domains and email address policies
- Hybrid configuration status with Exchange Online
- Public folder configuration and migration requirements

SharePoint Server (On-Premises):

- SharePoint farm configuration and service applications
- Service account inventory and their permissions
- Web application authentication methods (NTLM, Kerberos, SAML)
- User profile service synchronization configuration
- Search service application and crawl account configuration
- Database server dependencies and authentication methods

System Center Configuration Manager (SCCM/MECM):

- Site hierarchy and site system roles
- Client push installation account and permissions
- Discovery methods and Active Directory integration
- Boundary groups and content distribution points
- Software update points and WSUS integration
- Operating system deployment accounts and task sequences

Distributed File System (DFS):

- DFS namespace configuration and root servers
- Folder targets and their hosting servers
- DFS replication groups and member servers
- Replication schedules and bandwidth throttling
- File share permissions and NTFS security
- Backup and recovery procedures for DFS data

2.2 Legacy Application Discovery

Application Inventory Process:

- Catalog all applications with Active Directory dependencies
- Identify authentication methods used by each application
- Document service accounts and their associated applications
- Map application-to-server relationships and dependencies
- Identify hardcoded server names or IP addresses in configurations

Authentication Method Analysis:

- **Integrated Windows Authentication:** Applications using NTLM or Kerberos
- **LDAP Bind:** Applications performing direct LDAP queries
- **Service Principal Names:** Applications requiring Kerberos delegation
- **Machine Authentication:** Applications using computer accounts for authentication

Critical Discovery Questions:

- Does the application support domain name changes?
- Are server names hardcoded in configuration files?

- What service accounts does the application use?
- How does the application handle domain controller failover?
- Are there any custom schema extensions required?
- What is the vendor's migration support policy?

2.3 File and Print Services

File Server Analysis:

- Inventory all file servers and their shares
- Document share permissions and NTFS security
- Identify shares with large user bases or complex permissions
- Analyze file server clustering and high availability configurations
- Map home directory and profile share configurations

Print Server Dependencies:

- Print server configurations and driver repositories
- Printer security and user access controls
- Print queue permissions and delegation
- Network printer configurations and authentication requirements

3. Microsoft 365 Environment Analysis

3.1 Current Hybrid Configuration

Azure AD Connect Assessment:

- Current Azure AD Connect version and configuration
- Synchronization scope and filtering rules
- Password hash synchronization vs. federation configuration
- Custom attribute mappings and transformations
- Synchronization error analysis and resolution procedures

Exchange Online Hybrid:

- Hybrid configuration status and mail flow
- On-premises vs. cloud mailbox distribution
- Accepted domains and SMTP routing configuration

- Migration endpoint configurations and certificates
- Free/busy information sharing and calendar integration

SharePoint Online Integration:

- Hybrid SharePoint configuration and service connections
- User profile synchronization with SharePoint Online
- Hybrid search configuration and content sources
- Business Connectivity Services configuration

3.2 Identity and Access Management

Current Identity State:

- User Principal Name (UPN) vs. SMTP address alignment
- ImmutableID configuration and soft matching setup
- Proxy addresses and alias configurations
- License assignment strategies and automation

Authentication and Authorization:

- Conditional access policies and their scope
- Multi-factor authentication configuration
- Privileged Identity Management usage
- Application registrations and service principal dependencies

3.3 Microsoft 365 Service Dependencies

Exchange Online Analysis:

- Mailbox size distribution and migration complexity estimates
- Shared mailboxes and resource mailbox configurations
- Distribution groups and mail-enabled security groups
- Mail flow rules and data loss prevention policies
- Retention policies and compliance configurations

SharePoint Online and OneDrive:

- Site collection inventory and external sharing configurations
- User profile service dependencies

- Custom solutions and third-party integrations
- Information governance and compliance policies

Teams and Collaboration Services:

- Teams dependency on Active Directory groups
- Guest user access and external collaboration requirements
- Compliance and retention policies for Teams data

Phase 2: Strategy & Design

Duration: Weeks 9-12
Critical Path: Yes
Stakeholders: Architecture team, business stakeholders, security team

Overview

The strategy and design phase transforms discovery findings into a concrete migration plan with detailed target environment specifications and risk mitigation strategies.

1. Migration Strategy Selection

1.1 Migration Approach Evaluation

Cross-Forest Migration (Recommended):

- **Use Cases:** Company mergers, major restructuring, clean slate requirements
- **Advantages:** Risk isolation, complete rollback capability, parallel operation
- **Disadvantages:** Higher complexity, additional hardware requirements, longer timeline
- **Tools Required:** ADMT, PES, trust relationships, conditional forwarders

In-Place Domain Upgrade:

- **Use Cases:** Simple modernization, stable environment, minimal restructuring
- **Advantages:** Simpler process, existing hardware utilization, shorter timeline
- **Disadvantages:** Limited rollback options, higher risk, less flexibility
- **Requirements:** Modern hardware, healthy AD environment, compatibility verification

Green-Field Deployment:

- **Use Cases:** Complete redesign, poor current structure, new organization requirements

- **Advantages:** Modern architecture, optimized design, clean configuration
- **Disadvantages:** Highest effort, extensive reconfiguration, longest timeline
- **Considerations:** User data migration, application reconfiguration, extensive testing

1.2 Decision Matrix Framework

Evaluation Criteria:

- Current environment health and stability
- Business timeline and downtime tolerance
- Available resources and expertise
- Compliance and security requirements
- Future scalability and growth plans
- Budget constraints and hardware availability

Risk vs. Benefit Analysis:

- Document pros and cons for each approach
- Quantify risk levels and mitigation strategies
- Estimate timeline and resource requirements
- Calculate total cost of ownership
- Assess business impact and user disruption

2. Target Environment Architecture

2.1 Domain and Forest Design

Naming Strategy:

- **Forest Root Domain:** corp.company.com
- **NetBIOS Name:** CORP (short, meaningful, avoid conflicts)
- **Alternative Considerations:** region.company.com for global organizations
- **DNS Integration:** Ensure compatibility with existing DNS infrastructure

Forest Functional Level Planning:

- Target functional level based on oldest domain controller OS
- Schema update requirements and timing
- Feature enablement roadmap post-migration

- Compatibility requirements for legacy applications

2.2 Organizational Unit Structure Design

Design Principles:

- Administrative delegation requirements
- Group Policy application efficiency
- Object management and maintenance
- Future growth and organizational changes
- Separation of users, computers, and administrative objects

Recommended Structure:

```
DC=corp,DC=company,DC=com
├── OU=Administration
│   ├── OU=Service Accounts
│   │   ├── OU=SQL Service Accounts
│   │   ├── OU=SharePoint Service Accounts
│   │   └── OU=Exchange Service Accounts
│   ├── OU=Administrative Users
│   │   ├── OU=Domain Admins
│   │   ├── OU=Server Admins
│   │   └── OU=Help Desk
│   └── OU=Delegated Management Groups
├── OU=Resources
│   ├── OU=Servers
│   │   ├── OU=Domain Controllers
│   │   ├── OU=File Servers
│   │   ├── OU=Application Servers
│   │   ├── OU=Database Servers
│   │   └── OU=Infrastructure Servers
│   ├── OU=Workstations
│   │   ├── OU=Desktops
│   │   ├── OU=Laptops
│   │   ├── OU=Virtual Desktops
│   │   └── OU=Kiosks
│   └── OU=Shared Resources
│       ├── OU=Printers
│       └── OU=Shared Mailboxes
├── OU=Security
│   ├── OU=Security Groups
│   │   ├── OU=File Share Groups
│   │   ├── OU=Application Groups
│   │   └── OU=Administrative Groups
│   ├── OU=Distribution Lists
│   └── OU=Mail-Enabled Security Groups
└── OU=Users
    ├── OU=Standard Users
    │   ├── OU=Finance Department
    │   ├── OU=Human Resources
    │   ├── OU=Information Technology
    │   └── OU=[Other Departments]
    ├── OU=Privileged Users
    │   ├── OU=Service Account Users
    │   └── OU=Administrative Users
```

```
└── OU=Migration
    └── OU=Staging (temporary migration OU)
```

2.3 Security Group Strategy

Group Naming Convention:

- **Format:** [Type]*[Resource]*[Permission Level]
- **Examples:**
  - SG_FileShare_Finance_ReadWrite
  - SG_App_SharePoint_Users
  - SG_Resource_Printers_ColorPrinting

Group Scope Strategy:

- **Domain Local Groups:** Resource permissions (file shares, applications)
- **Global Groups:** User collections by department or role
- **Universal Groups:** Cross-domain access (if multi-domain forest)

Permission Model:

- Implement AGDLP (Account, Global, Domain Local, Permission) model
- Minimize direct user permissions to resources
- Use role-based access control principles
- Plan for delegation and administrative separation

3. Migration Wave Planning

3.1 Wave Definition Strategy

Wave 1: Foundation and IT Infrastructure (Week 18)

- **Scope:** IT department users, infrastructure servers, core service accounts
- **Rationale:** IT team can validate processes and provide immediate feedback
- **Objects:** 50-100 users, 10-20 servers, critical security groups
- **Success Criteria:** All IT systems functional, help desk operational

Wave 2: Early Adopter Department (Week 19-20)

- **Scope:** Friendly business department with strong change management

- **Rationale:** Business validation of migration process with supportive users
- **Objects:** 100-200 users, department-specific applications and servers
- **Success Criteria:** Business processes functional, user satisfaction positive

Wave 3-4: Core Business Operations (Weeks 21-24)

- **Scope:** Major business departments and critical applications
- **Rationale:** Main migration effort with proven processes
- **Objects:** 500-1000 users per wave, production servers and applications
- **Success Criteria:** All business operations normal, performance maintained

Wave 5: Final Cleanup and Validation (Week 25-26)

- **Scope:** Remaining users, legacy systems, orphaned objects
- **Rationale:** Complete migration and address edge cases
- **Objects:** Remaining users and computers, final validation
- **Success Criteria:** 100% migration completion, all systems validated

3.2 Dependencies and Prerequisites

Inter-Wave Dependencies:

- Security groups must be migrated before their members
- Service accounts must be migrated before the servers that use them
- File servers must be migrated before updating client computer mappings
- Application servers must be migrated before dependent workstations

Technical Prerequisites per Wave:

- Trust relationships validated and functional
- DNS conditional forwarders configured and tested
- Network connectivity verified for all migration components
- Backup and rollback procedures tested and validated

4. Microsoft 365 Integration Strategy

4.1 Identity Synchronization Planning

Azure AD Connect Configuration:

- **Installation Location:** Target domain member server with high availability
- **Synchronization Scope:** Filtered sync during migration, full sync post-migration
- **Matching Strategy:** Soft matching based on SMTP addresses and ImmutableID
- **Attribute Mapping:** Custom attributes for migration tracking and validation

Identity Matching Approach:

- Pre-populate target domain users with matching SMTP proxy addresses
- Maintain ImmutableID consistency through migration process
- Plan for conflicting object resolution procedures
- Document identity resolution for edge cases

4.2 Exchange Online Migration Integration

Mailbox Migration Strategy:

- **Timing:** Post user object synchronization and validation
- **Batch Sizing:** 50-100 mailboxes per batch to manage performance
- **Migration Endpoint:** Configure hybrid connectors with proper certificates
- **Validation Process:** Mail flow testing and client connectivity verification

Mail-Enabled Object Handling:

- Distribution groups migration and mail-enablement in target domain
- Shared mailbox access permission migration
- Resource mailbox calendar permissions and booking policies
- Mail contact and public folder mail-enablement

4.3 SharePoint Online Integration

User Profile Synchronization:

- Allow 24-48 hours for user profile synchronization post-migration
- Plan for manual profile import if automatic sync fails
- Validate manager hierarchy and organizational chart data
- Test SharePoint site access and permissions post-migration

SharePoint Hybrid Configuration:

- Maintain hybrid search configuration during migration

- Update service application proxy connections
- Validate Business Connectivity Services connections
- Test hybrid site features and authentication

Phase 3: Pre-Migration Preparation

Duration: Weeks 13-16
Critical Path: Yes
Stakeholders: Infrastructure team, application teams, security team

Overview

The preparation phase builds and configures the target environment, installs migration tools, and remediates application dependencies to ensure successful migration execution.

1. Target Domain Infrastructure Build

1.1 Domain Controller Deployment

Hardware and Virtualization Requirements:

- **Server Specifications:** Windows Server 2022, minimum 8GB RAM, 4 CPU cores
- **Storage:** SSD storage for SYSVOL and database, separate log drives
- **Network:** Multiple network adapters for redundancy, 1GB minimum
- **Virtualization:** Follow vendor best practices for virtual domain controllers

Domain Controller Configuration:

- Install Active Directory Domain Services role
- Promote to domain controller with DNS server role
- Configure sites and services for proper replication topology
- Implement time synchronization with reliable time sources
- Configure monitoring and alerting for domain controller health

Replication and Backup Configuration:

- Establish replication schedules and bandwidth throttling
- Configure System State backup schedules and retention
- Test domain controller promotion and demotion procedures

- Validate FSMO role placement and seizure procedures
- Document disaster recovery procedures for domain controllers

1.2 DNS Infrastructure Configuration

DNS Zone Configuration:

- Create forward and reverse lookup zones for target domain
- Configure zone transfer settings and security
- Implement DNS scavenging and aging policies
- Configure DNS logging and monitoring

Conditional Forwarder Setup:

```
Target Domain → Source Domain
corp.company.com → olddomain.com (conditional forwarder)

Source Domain → Target Domain
olddomain.com → corp.company.com (conditional forwarder)
```

DNS Security Considerations:

- Implement DNS cache locking to prevent poisoning
- Configure DNS over HTTPS (DoH) if organizational policy permits
- Review and update DNS security policies
- Test DNS resolution from all network segments

1.3 Trust Relationship Establishment

Trust Configuration Process:

1. **Preparation:** Verify network connectivity and name resolution
2. **Creation:** Establish two-way forest trust between domains
3. **Validation:** Test trust relationship functionality
4. **Security:** Configure selective authentication if required
5. **Monitoring:** Implement trust relationship health monitoring

Trust Security Configuration:

- Configure SID filtering based on security requirements

- Implement selective authentication for enhanced security
- Document trust authentication flow and troubleshooting
- Plan trust relationship maintenance and monitoring

Trust Validation Procedures:

- Test cross-domain authentication using nltest commands
- Validate Global Catalog connectivity across forests
- Verify Kerberos ticket-granting functionality
- Test resource access across trust boundaries

2. ADMT and PES Installation

2.1 SQL Server Preparation

SQL Server Installation:

- Install SQL Server 2019 or later (Express edition acceptable)
- Configure SQL Server for ADMT database requirements
- Implement backup strategy for ADMT database
- Configure SQL Server security and access permissions

Database Configuration:

- Create ADMT database with appropriate sizing
- Configure database maintenance plans and backup schedules
- Implement monitoring for database performance and growth
- Document database restoration procedures

2.2 ADMT Installation and Configuration

Installation Prerequisites:

- Target domain member server (not domain controller)
- Local administrator rights and domain administrator permissions
- SQL Server connectivity and database creation permissions
- Network connectivity to source domain controllers

ADMT Configuration Steps:

1. **Installation:** Run ADMT setup with custom database configuration
2. **Database Setup:** Configure ADMT database connection and permissions
3. **Logging:** Configure comprehensive logging for troubleshooting
4. **Testing:** Validate ADMT functionality with test object migration
5. **Security:** Secure ADMT server and database access

ADMT Agent Deployment:

- Deploy ADMT agents to source domain computers for computer migration
- Configure agent communication security and certificates
- Test agent connectivity and command execution
- Plan agent removal post-migration

2.3 Password Export Server (PES) Installation

PES Installation on Source Domain:

- Install PES on source domain controller or dedicated member server
- Generate and secure encryption keys for password migration
- Configure PES service account with appropriate permissions
- Test PES connectivity and password export functionality

Encryption Key Management:

```
admt key /option:create /sourcedomain:olddomain.com
/keyfile:C:\PES\migration.key /keypassword:ComplexPassword123!
```

PES Security Configuration:

- Secure encryption key files with appropriate file system permissions
- Configure PES service account with minimum required privileges
- Implement PES service monitoring and alerting
- Plan encryption key rotation and management procedures

Network Security for PES:

- Configure firewall rules for PES communication (port 1478)
- Implement network segmentation for migration traffic

- Configure RPC endpoint mapping for proper communication
- Test PES connectivity from ADMT server

3. Application Dependency Remediation

3.1 SharePoint Server Preparation

Service Account Planning:

- Document all SharePoint service accounts and their permissions
- Create equivalent service accounts in target domain
- Plan service account transition during server migration
- Update service account passwords and security policies

SharePoint Configuration Backup:

- Export SharePoint configuration database settings
- Backup service application configurations
- Document web application authentication settings
- Export search service application configuration

Post-Migration SharePoint Tasks:

- Plan for search service application rebuilding
- Prepare for user profile service re-synchronization
- Update authentication provider configurations
- Test SharePoint functionality post-migration

3.2 SCCM/MECM Preparation

Account and Configuration Management:

- Create SCCM service accounts in target domain
- Update client push installation account configuration
- Plan boundary group updates for new domain structure
- Document discovery method configurations

Client Migration Strategy:

- Plan SCCM client re-assignment to new management points

- Prepare client configuration scripts for domain change
- Test client communication with new domain controllers
- Plan software deployment and policy application validation

Site System Preparation:

- Document site system roles and their dependencies
- Plan site system server migration order
- Prepare certificate renewal for site system communications
- Test inter-site communication and replication

3.3 DFS Namespace and Replication

DFS Namespace Preparation:

- Document namespace server configurations and folder targets
- Plan namespace server migration and target updates
- Prepare namespace client referral updates
- Test namespace accessibility and failover procedures

DFS Replication Group Management:

- Document replication group memberships and schedules
- Plan member server removal and re-addition procedures
- Prepare replication health monitoring and validation
- Test replication conflict resolution and convergence

DFS Migration Process:

1. **Pre-Migration:** Document all DFS configurations and dependencies
2. **Namespace Migration:** Migrate namespace servers and update targets
3. **Replication Migration:** Remove and re-add servers to replication groups
4. **Validation:** Test DFS functionality and replication health
5. **Cleanup:** Remove old namespace servers and clean up configurations

3.4 Legacy Application Remediation

Application Assessment and Planning:

- Engage application vendors for migration support and compatibility

- Test applications in lab environment with new domain structure
- Plan configuration updates for hardcoded domain references
- Prepare application-specific migration procedures

Service Account Management:

- Create application service accounts in target domain
- Update application configurations with new service account details
- Test application authentication with new service accounts
- Plan service account credential updates during migration

Authentication Configuration Updates:

- Update LDAP connection strings and authentication settings
- Reconfigure integrated Windows authentication settings
- Update Service Principal Name (SPN) registrations
- Test application authentication flows with new domain

4. Microsoft 365 Environment Preparation

4.1 Azure AD Connect Preparation

Installation and Configuration:

- Install Azure AD Connect on target domain member server
- Configure staging mode to prevent accidental synchronization
- Set up custom attribute mappings for migration tracking
- Test synchronization connectivity and authentication

Synchronization Scope Configuration:

- Configure organizational unit filtering for staged synchronization
- Set up attribute filtering to exclude unnecessary attributes
- Configure group filtering for security and distribution groups
- Plan synchronization schedule and monitoring

Identity Matching Preparation:

- Export current ImmutableID mappings from source environment
- Prepare soft matching configuration based on SMTP addresses

- Plan identity conflict resolution procedures
- Test identity matching with pilot users

4.2 Exchange Online Migration Preparation

Migration Endpoint Configuration:

- Configure Exchange hybrid connectors for migration
- Update certificate configurations for secure communication
- Test migration endpoint connectivity and authentication
- Prepare migration batch CSV files for each wave

Mail-Enabled Object Preparation:

- Document current mail-enabled objects and their configurations
- Plan mail-enablement in target domain post-migration
- Prepare proxy address updates and SMTP routing changes
- Test mail flow between on-premises and Exchange Online

Migration Batch Planning:

- Plan migration batch sizes based on performance requirements
- Prepare user communication for mailbox migration schedules
- Configure migration endpoint throttling and performance settings
- Test migration procedures with pilot mailboxes

4.3 SharePoint Online Integration Preparation

User Profile Service Configuration:

- Document current user profile synchronization settings
- Plan user profile import procedures post-migration
- Prepare manager hierarchy and organizational data updates
- Test user profile synchronization with pilot users

Site Collection and Permissions:

- Document SharePoint Online site permissions and access
- Plan permission validation procedures post-migration
- Prepare site collection administrator updates

- Test SharePoint site access with migrated user accounts

Phase 4: Pilot Migration

Duration: Week 17
Critical Path: Yes
Stakeholders: IT team, pilot users, support team

Overview

The pilot migration validates the entire migration process with a small, controlled group of users and systems. This phase identifies issues, refines procedures, and builds confidence before production migration.

1. Pilot Group Selection and Preparation

1.1 Pilot Participant Criteria

User Selection Criteria:

- **IT Department Volunteers:** Technical understanding of migration process
- **Change Champions:** Users enthusiastic about technology changes
- **Diverse Application Usage:** Users representing different application portfolios
- **Geographic Distribution:** Users from different office locations if applicable
- **Risk Tolerance:** Users who can work around temporary issues

Pilot Group Composition:

- **IT Users (5-10):** System administrators, help desk staff, infrastructure team
- **Business Users (5-10):** Power users from friendly departments
- **Executive Sponsor:** Single executive for decision-making authority
- **Application Representatives:** Users for each critical application being tested

Computer Selection Criteria:

- **Operating System Diversity:** Windows 10, Windows 11, different build versions
- **Hardware Variety:** Desktop, laptop, and tablet configurations
- **Application Diversity:** Different software installations and configurations
- **Network Locations:** Users from different network segments or sites

1.2 Pilot Preparation Activities

Pre-Migration Communication:

- Conduct pilot user briefing sessions with detailed timeline
- Provide migration overview and expected changes
- Establish communication channels for issue reporting
- Set expectations for potential disruptions and workarounds

Backup and Recovery Preparation:

- Complete full system backups for all pilot servers
- Export pilot user profiles and application settings
- Document current application configurations and customizations
- Prepare rapid rollback procedures if critical issues arise

Support Team Readiness:

- Brief help desk team on pilot migration timeline and expected issues
- Prepare escalation procedures for pilot-specific problems
- Establish dedicated support channels for pilot participants
- Create rapid response team for critical pilot issues

2. Pilot Migration Execution Process

2.1 Pre-Migration Validation (Day -1)

Infrastructure Readiness Check:

- Verify trust relationship health and connectivity
- Test ADMT and PES functionality with sample objects
- Validate Azure AD Connect staging mode configuration
- Confirm backup completion for all pilot systems

Network and Security Validation:

- Test DNS resolution between source and target domains
- Verify firewall rules and network connectivity
- Validate certificate configurations for secure communications
- Test time synchronization across all domain controllers

Application and Service Health:

- Verify critical application functionality in source environment
- Test service account authentication and permissions
- Validate SharePoint, Exchange, and other service dependencies
- Confirm SCCM client communication and policy application

2.2 Security Group Migration (Hours 1-2)

Group Migration Process:

1. **Inventory:** Export security groups for pilot users and resources
2. **Validation:** Verify group dependencies and nesting relationships
3. **Migration:** Use ADMT to migrate security groups with SID history
4. **Verification:** Confirm group creation and membership in target domain
5. **Testing:** Validate group-based resource access functionality

Group Migration Command Example:

```
admt group migrate /sd:olddomain.com /td:corp.company.com
/sa:CORP\svc_admt /sp:Password123!
/to:"OU=Security Groups,DC=corp,DC=company,DC=com"
/c /mss:yes /ll:"C:\MigLogs\Pilot_Groups.log"
```

Post-Group Migration Validation:

- Verify all groups created successfully in target domain
- Test group membership queries from target domain computers
- Validate nested group relationships and inheritance
- Test file share access using migrated security groups

2.3 User Account Migration (Hours 2-4)

User Migration Preparation:

- Verify user account status and password policies
- Confirm Exchange attributes and proxy addresses
- Validate user profile paths and home directory locations
- Check for user account dependencies and service accounts

User Migration Process:

1. **Pre-Migration:** Export user account details and validate dependencies
2. **Migration:** Use ADMT with password migration and SID history preservation
3. **Attribute Update:** Verify Exchange and custom attribute preservation
4. **Profile Migration:** Update user profile paths and home directories
5. **Testing:** Validate user authentication and application access

User Migration Command Example:

```
admt user migrate /sd:olddomain.com /td:corp.company.com
/sa:CORP\svc_admt /sp:Password123!
/to:"OU=Migration,OU=Users,DC=corp,DC=company,DC=com"
/umt:Password /c /mss:yes /spp:yes
/ll:"C:\MigLogs\Pilot_Users.log"
```

Post-User Migration Validation:

- Test user authentication with existing passwords
- Verify group memberships including SID history
- Validate Exchange attributes and mail enablement
- Test user profile loading and application settings

2.4 Computer Migration (Hours 4-8)

Computer Migration Preparation:

- Document computer-specific configurations and applications
- Prepare for computer reboot and domain rejoin process
- Coordinate with users for computer availability windows
- Plan for application reconfiguration post-migration

Computer Migration Process:

1. **Pre-Migration:** Export computer account details and security settings
2. **Service Shutdown:** Stop critical services and prepare for migration
3. **ADMT Migration:** Migrate computer objects with security translation
4. **Domain Rejoin:** Reboot computers to join target domain

5. **Service Restart:** Restart services and validate functionality

Computer Migration Command Example:

```
admt computer migrate /sd:olddomain.com /td:corp.company.com
/sa:CORP\svc_admt /sp:Password123!
/to:"OU=Workstations,DC=corp,DC=company,DC=com"
/c /st:Yes /ll:"C:\MigLogs\Pilot_Computers.log"
```

Post-Computer Migration Tasks:

- Validate computer domain membership and authentication
- Test network resource access and mapped drive connectivity
- Verify application functionality and configuration preservation
- Update SCCM client configuration for new domain

3. Pilot Validation and Testing

3.1 Authentication and Access Validation

User Authentication Testing:

- Test user logon with existing credentials
- Verify single sign-on functionality with applications
- Test password change functionality
- Validate account lockout and unlock procedures

Resource Access Validation:

- Test file share access with both new and old permissions
- Verify printer access and driver installation
- Test application authentication and authorization
- Validate network resource connectivity

Group Membership Verification:

- Confirm user group memberships including SID history
- Test group-based access control functionality
- Verify nested group relationships and inheritance
- Validate administrative group memberships and permissions

3.2 Application Functionality Testing

Critical Application Testing:

- Test core business applications for functionality
- Verify application authentication and database connectivity
- Test application-specific integrations and interfaces
- Validate custom application configurations and settings

Office 365 Integration Testing:

- Test Outlook connectivity and mail synchronization
- Verify SharePoint site access and permissions
- Test OneDrive synchronization and file access
- Validate Teams functionality and collaboration features

Network Service Testing:

- Test DNS resolution and network connectivity
- Verify DHCP lease renewal and network configuration
- Test VPN connectivity and remote access
- Validate network printer access and functionality

3.3 Microsoft 365 Pilot Integration

Azure AD Connect Synchronization:

- Enable synchronization for pilot users only
- Monitor sync cycle completion and error reporting
- Verify user object matching and attribute synchronization
- Test password hash synchronization functionality

Exchange Online Validation:

- Test Exchange Online mailbox access via Outlook
- Verify Outlook Web App (OWA) functionality
- Test mobile device synchronization and access
- Validate calendar and contacts synchronization

SharePoint Online Testing:

- Test SharePoint site access and navigation
- Verify user profile information and updates
- Test document library access and synchronization
- Validate OneDrive for Business functionality

4. Pilot Results Analysis and Process Refinement

4.1 Issue Documentation and Resolution

Issue Classification:

- **Critical Issues:** Complete functionality loss requiring immediate attention
- **High Issues:** Significant functionality impact with workarounds available
- **Medium Issues:** Minor functionality impact with acceptable workarounds
- **Low Issues:** Cosmetic or minor inconvenience issues

Issue Resolution Process:

- Document all issues with detailed symptoms and impact
- Assign severity levels and resolution priorities
- Implement fixes and validate resolution effectiveness
- Update migration procedures based on lessons learned

Common Pilot Issues and Resolutions:

- **Trust Authentication:** Network connectivity and DNS resolution problems
- **Application Compatibility:** Configuration updates and service account changes
- **Group Policy:** Policy application timing and inheritance issues
- **User Profiles:** Profile loading and application settings preservation

4.2 Process Refinement and Documentation

Migration Procedure Updates:

- Refine migration scripts based on pilot experience
- Update timing estimates for production migration activities
- Improve error handling and validation procedures
- Document troubleshooting steps for common issues

Performance Optimization:

- Analyze migration performance and identify bottlenecks
- Optimize batch sizes and parallel processing options
- Improve network utilization and bandwidth management
- Enhance monitoring and progress reporting capabilities

Training and Communication Updates:

- Update user communication materials based on pilot feedback
- Refine help desk training and support procedures
- Improve migration timeline communication and expectations
- Enhance rollback procedures and decision criteria

4.3 Go/No-Go Decision Criteria

Success Criteria for Production Migration:

- All critical applications functional with minimal issues
- User authentication and resource access working correctly
- Microsoft 365 integration completed without major problems
- Support team confident in procedures and troubleshooting
- Business stakeholders comfortable with migration quality

No-Go Criteria:

- Critical applications non-functional or requiring extensive workarounds
- Significant data loss or corruption issues
- Authentication or security vulnerabilities discovered
- Support team lacking confidence in procedures
- Business stakeholders expressing serious concerns

Phase 5: Production Migration

Duration: Weeks 18-26+
Critical Path: Yes
Stakeholders: All users, business operations, support teams

Overview

Production migration executes the validated migration process across all users and systems in planned waves. This phase requires precise coordination, continuous monitoring, and rapid issue resolution to minimize business impact.

1. Wave-Based Migration Strategy

1.1 Migration Wave Planning and Coordination

Wave 1: IT Infrastructure and Foundation (Week 18)

- **Scope:** IT department users, core infrastructure servers, essential service accounts
- **Business Impact:** Minimal - IT team can adapt and provide feedback
- **Objects:** 50-100 users, 10-20 servers, critical security groups and service accounts
- **Duration:** Weekend (48-hour window)
- **Success Criteria:** IT infrastructure operational, help desk functional, no critical system failures

Wave 2: Early Adopter Business Department (Weeks 19-20)

- **Scope:** Friendly business department with strong change management capability
- **Business Impact:** Low - selected for adaptability and change tolerance
- **Objects:** 100-200 users, department-specific servers and applications
- **Duration:** Extended weekend (72-hour window)
- **Success Criteria:** Department operations normal, user satisfaction positive, applications functional

Wave 3-4: Core Business Operations (Weeks 21-24)

- **Scope:** Major business departments, critical production systems
- **Business Impact:** Medium to High - requires careful coordination and support
- **Objects:** 500-1000 users per wave, production servers, business-critical applications
- **Duration:** Staggered weekends (48-hour windows each)
- **Success Criteria:** Business operations maintained, performance acceptable, minimal disruption

Wave 5: Final Migration and Cleanup (Weeks 25-26)

- **Scope:** Remaining users, legacy systems, edge cases
- **Business Impact:** Low - final completion activities
- **Objects:** All remaining objects, cleanup of orphaned items

- **Duration:** Standard weekend (48-hour window)
- **Success Criteria:** 100% migration completion, all systems validated

1.2 Pre-Wave Communication and Preparation

Communication Timeline:

- **T-14 Days:** Executive announcement of migration schedule
- **T-7 Days:** Detailed user notification with specific timeline
- **T-3 Days:** Final reminder with preparation checklist
- **T-1 Day:** "Migration Eve" communication with final instructions
- **T-Day:** Migration commencement notification

User Preparation Requirements:

- Save all work and close applications before migration window
- Ensure laptops are connected to corporate network during migration
- Backup critical local data not stored on network shares
- Prepare for potential password reset if migration issues occur
- Identify key contacts for support during migration window

IT Team Preparation:

- Validate all prerequisite checks and system health
- Confirm backup completion for all systems in migration scope
- Brief support teams on wave-specific issues and procedures
- Prepare rollback procedures and decision criteria
- Establish communication channels and escalation procedures

2. Detailed Migration Execution Process

2.1 Migration Day Schedule and Activities

Friday Evening Preparation (17:00-18:00):

- Final go/no-go decision based on environment health
- Activate migration support team and establish communication channels
- Send final user notification confirming migration commencement
- Complete final system health checks and validation

- Begin migration log monitoring and documentation

Phase 1: Security Group Migration (18:00-20:00):

- Export and validate security groups for migration wave
- Execute ADMT group migration with SID history preservation
- Verify group creation and membership in target domain
- Test sample group-based resource access
- Update documentation with group migration results

Phase 2: Service Account Migration (20:00-21:00):

- Migrate service accounts used by servers in current wave
- Update service configurations with new domain credentials
- Test service account authentication and functionality
- Validate service dependencies and interconnections
- Restart services as required for new domain authentication

Phase 3: User Account Migration (21:00-24:00):

- Execute user account migration in batches of 50-100 accounts
- Monitor password migration success and SID history preservation
- Validate Exchange attribute preservation and mail enablement
- Test sample user authentication and resource access
- Update user profile paths and home directory references

Phase 4: Computer Migration (24:00-04:00):

- Migrate computer objects and initiate domain rejoin process
- Coordinate computer reboots with users or automation
- Validate computer domain membership and authentication
- Update SCCM client configurations and site assignments
- Test application functionality and network connectivity

Phase 5: Validation and Testing (04:00-08:00):

- Execute comprehensive validation scripts and procedures
- Test critical applications and business processes

- Validate Microsoft 365 integration and synchronization
- Resolve high-priority issues and document workarounds
- Prepare status report for business leadership

2.2 Microsoft 365 Integration During Migration

Azure AD Connect Synchronization Management:

- Monitor Azure AD Connect sync cycles during migration
- Force delta synchronization after user migration completion
- Validate object matching and resolve synchronization conflicts
- Update organizational unit filtering for newly migrated objects
- Monitor sync error reports and resolve issues immediately

Exchange Online Mailbox Migration Process:

1. **Pre-Migration:** Validate user synchronization to Azure AD
2. **Batch Creation:** Create migration batches for Exchange Online mailboxes
3. **Migration Start:** Initiate mailbox migration for synchronized users
4. **Monitoring:** Track migration progress and resolve errors
5. **Completion:** Complete migration batches and validate mail flow

Exchange Online Migration Commands:

```
# Create migration batch
New-MigrationBatch -Name "Wave1_Migration" -SourceEndpoint "HybridMigration"
-TargetDeliveryDomain "company.com"
-CSVData ([System.IO.File]::ReadAllBytes("C:\Migration\Wave1_Users.csv"))
-AutoStart

# Monitor migration progress
Get-MigrationBatch -Identity "Wave1_Migration" |
Select-Object Identity, Status, TotalCount, SyncedCount, FinalizedCount

# Complete migration batch
Complete-MigrationBatch -Identity "Wave1_Migration"
```

SharePoint Online User Profile Synchronization:

- Allow 24-48 hours for automatic user profile synchronization

- Monitor user profile service health and synchronization status
- Validate manager hierarchy and organizational chart updates
- Test SharePoint site access and permissions for migrated users
- Force user profile import if automatic synchronization fails

2.3 Application-Specific Migration Procedures

SharePoint Server Migration Process:

1. **Pre-Migration:** Document service application configurations and dependencies
2. **Service Account Update:** Update SharePoint service accounts to target domain
3. **IIS Configuration:** Update application pool identities and authentication settings
4. **Service Restart:** Restart SharePoint services with new domain authentication
5. **Search Rebuild:** Initiate full search crawl with new service account
6. **Validation:** Test SharePoint functionality and user access

SCCM Client Migration Process:

1. **Management Point Assignment:** Update client management point assignments
2. **Site Boundary Updates:** Configure new site boundaries for target domain
3. **Client Configuration:** Update client registry settings for new domain
4. **Policy Refresh:** Force client policy refresh and validation
5. **Inventory Update:** Initiate hardware and software inventory updates
6. **Application Deployment:** Test software deployment and policy application

DFS Migration Process:

1. **Namespace Server Migration:** Migrate DFS namespace servers to target domain
2. **Replication Group Updates:** Remove and re-add servers to DFS replication groups
3. **Client Referral Updates:** Update client referrals to new domain namespace servers
4. **Replication Validation:** Verify DFS replication health and convergence
5. **Access Testing:** Test file share access through DFS namespace

3. Migration Monitoring and Issue Resolution

3.1 Real-Time Monitoring and Alerting

Automated Monitoring Systems:

- ADMT migration progress and error monitoring
- Azure AD Connect synchronization health and error tracking
- Domain controller replication health and performance
- Critical application availability and response time monitoring
- Network connectivity and bandwidth utilization tracking

Key Performance Indicators (KPIs):

- Migration object success rate (target: >95%)
- User authentication success rate (target: >98%)
- Application availability during migration (target: >90%)
- Support ticket volume and resolution time
- Azure AD Connect sync cycle completion time

Alerting Thresholds:

- Migration failure rate exceeding 5% triggers immediate investigation
- Authentication failure rate exceeding 2% requires escalation
- Critical application downtime exceeding 30 minutes triggers rollback consideration
- Azure AD Connect sync errors require immediate resolution
- Domain controller replication failures trigger emergency procedures

3.2 Issue Classification and Resolution Process

Issue Severity Classification:

- **Severity 1 (Critical):** Complete service failure affecting business operations
- **Severity 2 (High):** Significant functionality impact with limited workarounds
- **Severity 3 (Medium):** Moderate impact with acceptable workarounds available
- **Severity 4 (Low):** Minor inconvenience or cosmetic issues

Issue Resolution Workflow:

1. **Detection:** Automated monitoring or user report identifies issue
2. **Classification:** Assign severity level and impact assessment
3. **Assignment:** Route to appropriate technical team based on issue type
4. **Investigation:** Diagnose root cause and determine resolution approach

5. **Resolution:** Implement fix and validate resolution effectiveness
6. **Documentation:** Update issue tracking and knowledge base

Escalation Procedures:

- Severity 1 issues require immediate escalation to migration team lead
- Unresolved Severity 2 issues escalate after 1 hour
- Multiple related issues may indicate systemic problem requiring escalation
- Business impact exceeding acceptable thresholds triggers executive notification
- Rollback consideration required for multiple critical failures

3.3 Communication During Migration Execution

Status Communication Schedule:

- **Hourly Updates:** Internal migration team status and progress reports
- **4-Hour Updates:** IT leadership briefing on migration progress and issues
- **8-Hour Updates:** Business leadership dashboard with high-level status
- **Issue Notifications:** Immediate communication for critical issues
- **Completion Report:** Final migration status and next steps

User Communication Strategy:

- **Migration Start:** Confirmation that migration has begun as scheduled
- **Progress Updates:** Periodic updates on migration progress and timeline
- **Issue Notifications:** Communication of known issues and workarounds
- **Completion Notice:** Notification when migration is complete and validated
- **Support Information:** Clear instructions for reporting issues and getting help

Communication Channels:

- Email notifications to all users in current migration wave
- Intranet/portal updates with current status and known issues
- Dedicated migration hotline for urgent user issues
- Instant messaging for real-time team coordination
- Video conferences for executive briefings and decision-making

4. Post-Wave Validation and Cleanup

4.1 Comprehensive Validation Procedures

Authentication and Access Validation:

- Test user authentication across all domain controllers
- Verify group membership and SID history preservation
- Validate file share access with both new and legacy permissions
- Test application authentication and single sign-on functionality
- Confirm administrative access and delegation of control

Application Functionality Testing:

- Execute automated application health checks
- Test critical business processes and workflows
- Verify database connectivity and application integrations
- Validate custom application configurations and settings
- Test application performance and response times

Microsoft 365 Service Validation:

- Verify Exchange Online mailbox access and mail flow
- Test SharePoint Online site access and permissions
- Validate OneDrive synchronization and file access
- Test Teams functionality and collaboration features
- Confirm mobile device access to Microsoft 365 services

4.2 Performance and Health Monitoring

System Performance Metrics:

- Domain controller CPU, memory, and disk utilization
- Network bandwidth utilization and latency measurements
- Application response times and availability metrics
- User logon times and authentication performance
- File server access times and throughput measurements

Health Check Procedures:

- Execute comprehensive Active Directory health checks
- Validate replication health across all domain controllers
- Test DNS resolution and zone transfer functionality
- Verify time synchronization across all systems
- Check event logs for errors and warnings

User Experience Monitoring:

- Survey user satisfaction and functionality feedback
- Track help desk ticket volume and resolution times
- Monitor user productivity metrics and business process completion
- Identify common user issues and improvement opportunities
- Validate training effectiveness and user adoption

4.3 Wave Cleanup and Preparation for Next Wave

Migration Cleanup Tasks:

- Archive migration logs and documentation for historical reference
- Clean up temporary migration accounts and permissions
- Remove ADMT agents from migrated computers
- Update migration status tracking and reporting systems
- Prepare lessons learned documentation for next wave

Next Wave Preparation:

- Update migration procedures based on current wave experience
- Refine timing estimates and resource allocation
- Prepare communication materials for next wave participants
- Schedule infrastructure maintenance and optimization tasks
- Review and update rollback procedures and criteria

Continuous Improvement Process:

- Analyze migration metrics and identify improvement opportunities
- Update automation scripts and validation procedures
- Enhance monitoring and alerting capabilities

- Refine issue resolution processes and escalation procedures
- Improve user communication and support procedures

Phase 6: Post-Migration & Cleanup

Duration: Weeks 27-30+
Critical Path: Medium
Stakeholders: All users, IT operations, business stakeholders

Overview

The post-migration phase ensures long-term stability, removes temporary migration artifacts, and transitions to normal operations. This phase includes extensive validation, SID history cleanup, and source domain decommissioning.

1. 30-Day Validation and Stabilization Period

1.1 Continuous Monitoring and Health Assessment

Daily Health Monitoring:

- Active Directory replication health across all domain controllers
- Azure AD Connect synchronization cycles and error monitoring
- Exchange Online mail flow and mailbox access validation
- Critical application availability and performance monitoring
- User authentication success rates and support ticket trends

Weekly Comprehensive Validation:

- Execute full migration validation scripts across all migrated objects
- Test critical business processes and workflow functionality
- Validate backup and recovery procedures for new domain environment
- Review security audit logs and compliance reporting
- Assess user satisfaction and productivity metrics

Performance Baseline Establishment:

- Establish performance baselines for new domain environment
- Compare pre-migration and post-migration performance metrics

- Identify and address performance degradation issues
- Optimize domain controller placement and configuration
- Fine-tune network and application configurations

1.2 Issue Tracking and Resolution

Post-Migration Issue Classification:

- **Migration-Related Issues:** Problems directly caused by migration process
- **Environmental Issues:** Problems with new domain environment configuration
- **User Adaptation Issues:** Problems related to user adjustment and training
- **Integration Issues:** Problems with application or service integration
- **Performance Issues:** Problems with system or application performance

Issue Resolution Process:

1. **Issue Identification:** Through monitoring, user reports, or proactive checking
2. **Impact Assessment:** Determine business impact and urgency of resolution
3. **Root Cause Analysis:** Investigate underlying cause and contributing factors
4. **Resolution Planning:** Develop resolution approach and timeline
5. **Implementation:** Execute resolution and validate effectiveness
6. **Documentation:** Update knowledge base and lessons learned

Common Post-Migration Issues and Solutions:

Issue Type	Common Problems	Typical Solutions
Authentication	Sporadic login failures	Update cached credentials, clear Kerberos tickets
File Access	Mapped drives disconnecting	Update drive mapping scripts, refresh group memberships
Email	Outlook profile issues	Recreate Outlook profiles, update autodiscover settings
Applications	Service account failures	Update service account configurations, restart services
Performance	Slow logon times	Optimize Group Policy processing, update DNS configurations

1.3 User Support and Training

Enhanced Support Coverage:

- Extend help desk hours during initial post-migration period
- Provide specialized migration support team for complex issues

- Create user self-service portal with migration-specific resources
- Establish rapid escalation procedures for critical user issues
- Monitor user satisfaction and adjust support coverage accordingly

Additional Training and Communication:

- Conduct post-migration training sessions for complex applications
- Provide updated user guides and documentation for new environment
- Create video tutorials for common post-migration tasks
- Establish user feedback channels for continuous improvement
- Recognize and address user concerns proactively

2. SID History Cleanup and Security Optimization

2.1 SID History Validation and Cleanup Preparation

Pre-Cleanup Validation Process:

1. **Access Verification:** Confirm all users can access required resources using new domain permissions
2. **Application Testing:** Validate all applications function correctly without SID history dependencies
3. **Permission Auditing:** Verify all file shares and applications use new domain security groups
4. **Business Process Testing:** Confirm all critical business processes function normally
5. **Stakeholder Approval:** Obtain business approval for SID history removal

SID History Dependency Assessment:

- Audit all file share permissions for references to old domain SIDs
- Review application configurations for hardcoded security references
- Check SQL Server logins and database permissions for old domain references
- Validate Exchange permissions and distribution group memberships
- Verify SharePoint permissions and user profile configurations

Cleanup Risk Assessment:

- Identify systems or applications that may still depend on SID history
- Plan for rapid SID history restoration if critical issues arise
- Prepare rollback procedures for SID history cleanup process
- Establish monitoring for access failures post-cleanup

- Create emergency response procedures for critical access issues

2.2 SID History Removal Process

Staged SID History Cleanup:

1. **Test Environment Cleanup:** Remove SID history in test environment and validate functionality
2. **Pilot Group Cleanup:** Remove SID history for small pilot group and monitor for issues
3. **Department-by-Department:** Remove SID history by department with validation between each
4. **Service Accounts:** Remove SID history from service accounts after application validation
5. **Administrative Accounts:** Remove SID history from administrative accounts last

SID History Removal Commands:

```
powershell

# Remove SID history from user accounts
Get-ADUser -Filter * -Properties SidHistory |
Where-Object {$_.SidHistory} |
ForEach-Object {
    Write-Host "Removing SID History for $($_.SamAccountName)" -ForegroundColor Yellow
    Set-ADUser -Identity $_.SamAccountName -Clear sidHistory
    Write-Host "SID History removed for $($_.SamAccountName)" -ForegroundColor Green
}

# Remove SID history from security groups
Get-ADGroup -Filter * -Properties SidHistory |
Where-Object {$_.SidHistory} |
ForEach-Object {
    Write-Host "Removing SID History for group $($_.Name)" -ForegroundColor Yellow
    Set-ADGroup -Identity $_.Name -Clear sidHistory
    Write-Host "SID History removed for group $($_.Name)" -ForegroundColor Green
}
```

Post-Cleanup Validation:

- Test critical application functionality immediately after cleanup
- Verify user access to file shares and network resources
- Validate email access and distribution group functionality
- Check database access and application authentication
- Monitor support tickets for access-related issues

2.3 Security Hardening and Optimization

Active Directory Security Optimization:

- Review and update administrative group memberships
- Implement least privilege access principles
- Configure advanced audit policies for enhanced monitoring
- Enable Privileged Access Management (PAM) features
- Implement Just-In-Time (JIT) administrative access

Password and Authentication Security:

- Implement fine-grained password policies for different user types
- Enable Azure AD Password Protection for on-premises accounts
- Configure account lockout policies and monitoring
- Implement multi-factor authentication for privileged accounts
- Review and update service account password policies

Group Policy Security Baseline:

- Implement Microsoft Security Compliance Toolkit baselines
- Configure Windows Defender and endpoint protection policies
- Implement application control and device guard policies
- Configure network security and firewall policies
- Enable security auditing and logging policies

3. Microsoft 365 Integration Finalization

3.1 Azure AD Connect Optimization

Synchronization Optimization:

- Remove staging mode and enable full synchronization
- Optimize synchronization schedules for business requirements
- Configure delta synchronization for optimal performance
- Implement custom attribute mappings for business requirements
- Enable password writeback if required for self-service scenarios

Synchronization Monitoring and Alerting:

- Configure Azure AD Connect Health monitoring
- Set up synchronization error alerting and resolution procedures
- Implement custom monitoring for business-critical attributes
- Configure backup and disaster recovery for Azure AD Connect server
- Document troubleshooting procedures for common sync issues

Identity Governance and Compliance:

- Implement Azure AD Identity Governance features
- Configure access reviews for privileged access
- Implement entitlement management for resource access
- Configure conditional access policies for security
- Enable audit logging and compliance reporting

3.2 Exchange Online Finalization

Mail Flow Optimization:

- Update MX records to point directly to Exchange Online (if fully cloud)
- Configure mail flow rules and transport rules
- Implement data loss prevention (DLP) policies
- Configure retention policies and compliance features
- Optimize mailbox size and storage configurations

Exchange Hybrid Cleanup (if applicable):

- Remove on-premises Exchange servers if no longer needed
- Clean up hybrid configuration objects and settings
- Update mail routing and accepted domain configurations
- Archive or migrate public folders to Exchange Online
- Document remaining hybrid dependencies and maintenance procedures

3.3 SharePoint Online Integration Validation

SharePoint Online Optimization:

- Validate user profile synchronization and organizational data
- Configure SharePoint Online governance policies

- Implement information protection and compliance features
- Optimize SharePoint Online performance and configuration
- Configure external sharing and guest access policies

OneDrive for Business Validation:

- Verify OneDrive access and synchronization for all users
- Configure OneDrive policies and storage quotas
- Implement OneDrive backup and version history features
- Validate mobile device access and synchronization
- Configure OneDrive sharing and collaboration policies

4. Source Domain Decommissioning

4.1 Pre-Decommissioning Validation

Final Environment Validation:

- Confirm all objects successfully migrated to target domain
- Verify all applications function correctly in new environment
- Validate all data access works through new domain authentication
- Confirm all service dependencies updated to new domain
- Obtain final business sign-off for source domain decommissioning

Dependency Verification Process:

1. **Application Scanning:** Scan all applications for references to source domain
2. **Service Account Audit:** Verify all service accounts updated to target domain
3. **File Share Scanning:** Check all file shares for source domain security references
4. **Database Validation:** Verify all database logins updated to target domain
5. **Network Service Validation:** Confirm all network services use target domain authentication

Final Backup and Archive:

- Complete final backup of source domain Active Directory database
- Export all Group Policy objects and configurations for reference
- Archive all migration logs and documentation
- Backup certificate authority configurations and certificates

- Create complete documentation of source domain configuration

4.2 Trust Relationship Removal

Trust Removal Preparation:

- Verify no applications or services depend on cross-domain authentication
- Update any remaining service accounts or application configurations
- Test all functionality without trust relationship in isolated environment
- Prepare rollback procedures in case trust removal causes issues
- Schedule trust removal during low-impact time window

Trust Removal Process:

```
powershell

# Remove trust from source domain perspective
Remove-ADTrust -Identity "corp.company.com" -Server "olddomain.com" -Confirm:$false

# Remove trust from target domain perspective
Remove-ADTrust -Identity "olddomain.com" -Server "corp.company.com" -Confirm:$false

# Verify trust removal
Get-ADTrust -Filter * -Server "corp.company.com"
Get-ADTrust -Filter * -Server "olddomain.com"
```

Post-Trust Removal Validation:

- Test critical applications and services functionality
- Verify user authentication and resource access
- Check for any remaining cross-domain dependencies
- Monitor event logs for authentication errors
- Validate backup and recovery procedures work without trust

4.3 Domain Controller Decommissioning

Graceful Domain Controller Demotion:

1. **FSMO Role Transfer:** Transfer any remaining FSMO roles to other domain controllers
2. **Replication Verification:** Ensure all changes replicated to remaining domain controllers
3. **Service Shutdown:** Stop Active Directory Domain Services on domain controller

4. **Metadata Cleanup:** Clean up domain controller metadata from Active Directory
5. **DNS Cleanup:** Remove domain controller references from DNS zones

Domain Controller Demotion Process:

```powershell
# Transfer FSMO roles before demotion (if applicable)
Move-ADDirectoryServerOperationMasterRole -Identity "NewDC.corp.company.com" -OperationMasterRole RIDMaste

# Demote domain controller
Uninstall-ADDSDomainController -DemoteOperationMasterRole -LastDomainControllerInDomain -RemoveApplication

# Clean up DNS references
Remove-DnsServerResourceRecord -Name "OldDC" -RecordType "A" -ZoneName "olddomain.com"
```

Final Source Domain Cleanup:

- Power down remaining source domain controllers
- Remove source domain DNS zones and conditional forwarders
- Clean up network references to source domain
- Archive source domain documentation and configurations
- Update network documentation to reflect new domain structure

4.4 Migration Project Closure

Final Documentation and Knowledge Transfer:

- Complete final migration report with statistics and lessons learned
- Update IT documentation to reflect new domain structure
- Transfer knowledge to operations team for ongoing maintenance
- Archive all migration project documentation and artifacts
- Create standard operating procedures for new domain environment

Post-Migration Review and Lessons Learned:

- Conduct post-migration review with all project stakeholders
- Document lessons learned and best practices for future migrations
- Identify process improvements and tool recommendations

- Update migration methodology based on project experience
- Create case study and reference materials for future projects

Project Success Metrics:

- Migration completion percentage (target: 100%)
- User satisfaction scores (target: >85% satisfied)
- Application availability during migration (target: >95%)
- Migration timeline adherence (target: within 10% of plan)
- Budget adherence (target: within 10% of approved budget)

Risk Management

High-Impact Risks

Application Compatibility Risks

- **Risk:** Legacy applications fail to function with new domain
- **Impact:** Business process disruption, potential data loss
- **Mitigation:** Comprehensive application testing, vendor engagement, rollback procedures
- **Contingency:** Maintain source domain until application compatibility confirmed

Data Loss or Corruption Risks

- **Risk:** Migration process causes data loss or corruption
- **Impact:** Critical business data unavailable or damaged
- **Mitigation:** Multiple backup strategies, transaction logging, validation procedures
- **Contingency:** Restore from backup, rollback to source domain if necessary

Extended Downtime Risks

- **Risk:** Migration takes longer than planned, extending business disruption
- **Impact:** Lost productivity, customer impact, revenue loss
- **Mitigation:** Realistic timeline estimation, parallel processing, automated procedures
- **Contingency:** Rollback procedures, alternative access methods, business continuity plans

Medium-Impact Risks

Network Connectivity Risks

- **Risk:** Network issues prevent migration completion
- **Impact:** Migration delays, potential data inconsistency
- **Mitigation:** Redundant network paths, connectivity testing, network monitoring
- **Contingency:** Alternative network paths, point-to-point connections, timeline adjustment

User Resistance and Training Risks

- **Risk:** Users resist changes or lack adequate training
- **Impact:** Reduced productivity, increased support costs
- **Mitigation:** Change management program, comprehensive training, user advocates
- **Contingency:** Additional training sessions, enhanced support coverage, user incentives

Risk Monitoring and Response

Risk Assessment Process

- Weekly risk assessment meetings during active migration phases
- Continuous monitoring of risk indicators and early warning signs
- Regular communication with stakeholders about risk status
- Proactive risk mitigation implementation before issues occur

Risk Response Procedures

- Defined escalation procedures for each risk category
- Pre-approved response actions for common risk scenarios
- Executive decision-making authority for major risk events
- Communication plans for risk event notification and status updates

---

Success Metrics

Technical Success Metrics

Migration Completion Metrics

- **Object Migration Success Rate:** >99% of all objects migrated successfully
- **Authentication Success Rate:** >98% of user authentication attempts successful
- **Application Availability:** >95% uptime for critical applications during migration

- **Data Integrity:** 100% data integrity validation success

Performance Metrics

- **User Logon Time:** Within 10% of pre-migration performance
- **Application Response Time:** Within 15% of pre-migration performance
- **Network Performance:** No degradation in network throughput or latency
- **System Resource Utilization:** Within acceptable limits for all systems

Business Success Metrics

User Satisfaction Metrics

- **User Satisfaction Survey:** >85% of users satisfied with migration experience
- **Help Desk Ticket Volume:** Within 20% of normal volume within 30 days
- **User Productivity:** Return to pre-migration productivity levels within 14 days
- **Training Effectiveness:** >90% of users complete training successfully

Operational Metrics

- **Timeline Adherence:** Migration completed within 110% of planned timeline
- **Budget Adherence:** Total costs within 110% of approved budget
- **Business Continuity:** No critical business process interruptions
- **Compliance Maintenance:** All regulatory and compliance requirements met

Long-Term Success Metrics

Stability and Reliability

- **System Uptime:** >99.5% uptime for all critical systems post-migration
- **Incident Rate:** Reduction in IT incidents compared to pre-migration baseline
- **Mean Time to Resolution:** Improvement in incident resolution times
- **Change Success Rate:** >95% success rate for future changes and updates

Return on Investment

- **Administrative Efficiency:** Reduction in administrative overhead and complexity
- **Support Cost Reduction:** Decrease in ongoing support and maintenance costs
- **Scalability Improvement:** Enhanced ability to support business growth
- **Security Posture:** Improved security baseline and compliance posture

Appendices

Appendix A: Technical Prerequisites and Requirements

Hardware Requirements

- **Domain Controllers:** Windows Server 2022, 8GB RAM, 4 CPU cores, SSD storage
- **ADMT Server:** Windows Server 2019+, 16GB RAM, 8 CPU cores, high-speed network
- **Azure AD Connect Server:** Windows Server 2019+, 8GB RAM, 4 CPU cores, reliable connectivity
- **Backup Infrastructure:** Sufficient capacity for full environment backup

Software Requirements

- **Operating Systems:** Windows Server 2019/2022, Windows 10/11
- **Active Directory:** Forest/Domain Functional Level 2016 or higher
- **SQL Server:** SQL Server 2017 or later for ADMT database
- **PowerShell:** PowerShell 5.1 or PowerShell 7+ for automation scripts

Appendix B: Network Configuration Requirements

Required Network Ports

Service	Ports	Protocol	Direction	Purpose
DNS	53	TCP/UDP	Bidirectional	Name resolution
Kerberos	88	TCP/UDP	Bidirectional	Authentication
RPC Endpoint Mapper	135	TCP	Bidirectional	RPC communication
NetBIOS Session	139	TCP	Bidirectional	File sharing
LDAP	389	TCP	Bidirectional	Directory queries
SMB	445	TCP	Bidirectional	File sharing
LDAPS	636	TCP	Bidirectional	Secure directory
Global Catalog	3268	TCP	Bidirectional	GC queries
Global Catalog SSL	3269	TCP	Bidirectional	Secure GC queries
RPC Dynamic	1024-5000	TCP	Bidirectional	Dynamic RPC
PES	1478	TCP	Inbound	Password export

DNS Configuration

- Conditional forwarders between source and target domains
- Reverse lookup zones for all network segments
- DNS scavenging and aging policies
- DNS security and cache locking configurations

Appendix C: Security Considerations

Account Security

- Dedicated migration service accounts with minimal required privileges
- Secure password policies for all service accounts
- Regular password rotation and security monitoring
- Privileged access management for administrative accounts

Data Protection

- Encryption in transit for all migration data
- Secure storage of encryption keys and certificates
- Data loss prevention policies and monitoring
- Backup encryption and secure storage

Audit and Compliance

- Comprehensive audit logging for all migration activities
- Compliance validation for regulatory requirements
- Security baseline implementation and validation
- Regular security assessments and penetration testing

Appendix D: Automation Scripts and Tools

PowerShell Modules Required

- **ActiveDirectory:** For AD object management
- **GroupPolicy:** For GPO migration and management
- **DnsServer:** For DNS configuration
- **DFSN/DFSR:** For DFS management
- **ExchangeOnlineManagement:** For Exchange Online operations
- **Microsoft.Graph:** For Azure AD and Microsoft 365 operations

Custom Scripts and Functions

- Migration validation and health check scripts
- Automated backup and restore procedures
- User communication and notification systems
- Monitoring and alerting automation
- Rollback and recovery automation

Appendix E: Vendor Contact Information

Microsoft Support

- **Premier Support:** For escalated technical issues
- **FastTrack:** For Microsoft 365 migration assistance
- **Partner Support:** For partner-specific technical issues

Third-Party Vendors

- Application vendors for compatibility and support
- Network infrastructure vendors for configuration assistance
- Security solution vendors for integration support
- Backup and recovery solution vendors for validation

Appendix F: Project Templates and Checklists

Project Charter Template

- Executive sponsorship and approval
- Project scope and objectives
- Success criteria and metrics
- Risk tolerance and mitigation strategies
- Budget and resource allocation

Communication Plan Template

- Stakeholder identification and contact information
- Communication schedules and methods
- Escalation procedures and decision authority
- User training and change management plans

Validation Checklist Templates

- Pre-migration validation checklist
- Post-migration validation checklist
- Application functionality testing checklist
- Microsoft 365 integration validation checklist
- Security and compliance validation checklist

Document Version: 1.0
Last Updated: Current Date
Next Review Date: 6 months post-migration completion
Document Owner: Migration Project Manager
Approval Authority: Chief Information Officer