

State of Wisconsin
Active Directory (AD)
Service Offering Definition (SOD)



Document Revision History

Date	Version	Creator	Notes
January 22, 2009	1.0	Troy Olson	Initial Draft
February 4, 2009	1.5	Trina Zanow	Updates to the document to include standard template information
March 18, 2009	1.6	Trina Zanow	Updates to the document to include comments from initial review of SOD Team
March 20, 2009	1.7	Kevin Acker	Update document
March 25, 2009	1.8	Kevin Acker and Trina Zanow	Update document based upon feedback received during SOD review
April 17, 2009	1.8	Dan Proud	Formatting edits

Table of Contents

Introduction	4
What Is Included	5
What Is Not Included.....	5
Benefits.....	6
Service Description	6
Service Period	6
Roles and Responsibilities	6
Business Continuity.....	6
Performance Metrics (Monitoring/Alerting/Reporting)	7
How Services Are Charged	7

Introduction

This service consists of a distributed directory service for secure centralized management of an entire network, which might span a building, a city, or multiple locations throughout the State of Wisconsin. This includes the Lightweight Directory Access Protocol (LDAP) directory database, server hardware and infrastructure, and internal Domain Name Service (DNS).

DET maintains all aspects of Active Directory (AD) services infrastructure and domain controllers. Delegation of management of directory objects such as user accounts, security groups, and computer accounts is provided to the customer.

There are three options within the service for AD implementation. Which options each agency uses will be determined through discussions with DET, as some business requirements do not lend themselves to certain options.

Agencies that have elected only the Agency-Managed Virtual System (AMVS) or Agency-Managed Physical System (AMPS) services provided by DET are responsible for managing their Active Directory environment. These agencies either currently own or will need to purchase the necessary software licenses to provide this service to their agency. DET will provide consulting support to agencies managing their own Active Directory environment but will not engage in standard support work associated with managing the agency's AD environment.

Option 1: DET Managed Agency Using Shared Agency Shared Infrastructure (SASI) Domain

When Applicable: This option is selected when the agencies needs are addressed when only management of directory objects is needed and the policy standards follow the standards set within the shared infrastructure. The AD infrastructure and domain controller servers must be managed by DET.

In a shared infrastructure environment the AD service offering by DET is as follows:

- DET provides: Redundant domain controllers, forest and domain-level policy maintenance, patching, backup, monitoring, and capacity management.
- Consolidated agency needs to request/maintain Citrix access through the DET Citrix service for the management tool, create/maintain their AD objects, and network connectivity.

Option 2: DET Managed Agency Using Child Domain

When Applicable: This option is selected when the agency's policy requirements are not met by shared infrastructure or the agency has a distributed environment that would require additional considerations for DS replication. The AD infrastructure and domain controller servers must be managed by DET.

In a consolidated child environment the AD service offering by DET is as follows:

- DET provides: Redundant domain controllers, forest and domain-level policy maintenance, patching, backup, monitoring, and capacity management.
- Consolidated agency needs to request/maintain Citrix access through the DET Citrix service for the management tool, create/maintain their AD objects, and network connectivity. In addition, the agency needs to request policy creation or policy maintenance through the DET service request process.

Option 3: DET Managed Agency Using a Separate Forest

When Applicable: Currently there are two agencies that had an AD implementation prior to consolidation efforts beginning and those AD environments remained as a separate forest during the consolidation process. This option has been sunset and is not available to new subscribers.

What Is Included

- Directory Services—Software system that provides storage, organization, and authentication processing, using an LDAP directory database
- Distributed File Services—Hierarchical view of multiple file servers and shares on the network
- Hardware and OS support—Domain Controller support as defined by the Server/OS SOD
- AD Domain Name Service—Internal host name to IP resolution
- Windows Internet Name Service (WINS)—Another form of Internal hostname to IP resolution and will be enabled only for those legacy applications requiring its use; the standard is to use the AD Domain Name Service
- Secure Kerberos trust connections with the state enterprise forest
- Delegation of management, to the agency, of standard user accounts, computer accounts and security groups, and OU level group policies, as defined by the [AD Roles and Responsibilities](#)
- LDAP search referrals through the state enterprise forest (global catalog)
- Backup and recovery of the servers OS, AD objects, application and data through DET standard backup/recovery software
- Maintenance and installation of infrastructure components depending on the configuration selected; this includes the operating system, software patches, product upgrades, and security fixes
- Monitoring of the servers Up/Down status and specific system services and events
- Systems performance monitoring performed by the current monitoring tool
- Planning and design options, system setup, and other customer-specific requirements based on the configuration chosen

What Is Not Included

- Citrix licenses for customers who need direct access to Active Directory management tools
- Management or support of AD servers that are owned, operated, and maintained by customer agency staff
- Batch job development or troubleshooting
- Customer product use training
- Adding agency-managed domain servers into the DET-managed domain

Benefits

- Directory Services are used to authenticate and authorize access to resources
- A hierarchical structure facilitates delegation of responsibility and efficient management/maintenance of the objects contained in the directory
- Sharing of infrastructure and software, which can lead to reduction in hardware, software, and support costs
- Shared infrastructure simplifies the sharing of resources across agencies

Service Description

The Active Directory service offering provides an agency with full control over the objects and attributes associated with that agency. Agency staff can add, modify, and delete objects in their container, with clear boundaries between each agency.

Option 1 allows the agency full control of its objects, but requires that it share higher-level policies with other agencies using option 1. It also requires that the agency have networking infrastructure sufficient to support the replication requirements of directory services.

Option 2 allows the agency full control of its objects but it also allows unique higher-level policies for the agency. It is also preferred when networking infrastructure is insufficient to support the replication requirements of option 1. For the remote site DCs, we follow the DET Server Management and Lifecycle Policy for the replacement of servers. If we lose a DC, we remove it from AD and the site is redirected to Madison. After the equipment has been replaced and brought back online, it is then promoted back to DC status.

Service Period

July 1 through June 30 reviewed and renewed annually.

Roles and Responsibilities

Roles and Responsibilities for the Active Directory service can be found [here](#).

Roles and Responsibilities for DOC's specific implementation can be found [here](#). This option has been sunset and is not available for new subscribers.

Business Continuity

Business Continuity considerations are covered by the AD servers running on multiple servers, with automatic data replication, at multiple physical locations. Any individual server can fail without impacting the overall service provided.

Performance Metrics (Monitoring/Alerting/Reporting)

Monitoring: The AD servers are monitored by DET's Enterprise Monitoring product for items such as server disk space, CPU, and memory usage. There is also monitoring for the Up/Down status and selected services/processes on these servers.

Alerting: For problems with the AD system or servers, the DET Enterprise Monitoring product sends alerts when a monitored event's condition or threshold is met. This alert is in the form of an e-mail and/or automated incident ticket that is generated and assigned to DET technical staff.

For further information on Monitoring, please see the Distributed Systems Monitoring SOD.

How Services Are Charged

This service is a component of the Infrastructure and Operations fee each agency pays today.

An agency that has elected only the Agency-Managed Virtual System (AMVS) or Agency-Managed Physical System (AMPS) services needs to utilize the DET Consulting Service if it requires assistance within its Active Directory environment. The consulting rate is applied if an agency requests DET services for planning, designing, implementing, and troubleshooting any portion of its agency AD environment.