



DEPARTMENT OF ADMINISTRATION

Enterprise Policy

DOIT-02-03-2013

DIVISION OF INFORMATION TECHNOLOGY

Domain Controller Standard

Date of Last Revision 03/17/2013

Bijay Kumar

(401) 574-9220

bijay.kumar@doit.ri.gov

1. Purpose

- a. To define an effective, scalable, secure and manageable Active Directory™ Domain Controller design and to facilitate one standardized infrastructure for the State's Active Directory. The Division of Information Technology (DoIT) shall govern the implementation and operation of Microsoft's Active Directory™ Domain Controller design on the State's enterprise network.

2. Definitions

- a. **Domain Controller** - On Windows Server Systems, a domain controller (DC) is a server that responds to security authentication requests (logging in, checking permissions, etc.) within the Windows Server domain. Windows 2000 and later introduced Active Directory ("AD"), which largely eliminated the concept of primary and backup domain controllers in favor of the multi-master replication technology available in Windows. However, there are still a number of roles that only one domain controller can perform, called the "Flexible Single Master Operation" roles (some of these roles must be filled by one DC per domain, while others only require one DC per AD forest). If the server performing one of these roles is lost the domain can still function, and if the server will not be available again an administrator can designate an alternate DC to assume the role (a process known as "seizing" the role).
- b. **Physical Location** – A location is a facility used to house computer systems and associated components. It generally includes environmental controls (air conditioning, fire suppression, etc.), backup power supplies, data communications connections and physical security.
- c. **Domain Name Service** - Domain Name Service (DNS) is a hierarchical distributed database used for name/address translation and client server rendezvous. Domain Name Service is the namespace used on the Internet to translate computer and service names into TCP/IP addresses. Active Directory™ uses DNS as its location service which enables clients to find domain controllers using DNS queries.
- d. **Firewalls** - A firewall is a system that secures a network, shielding it from access by unauthorized users. Firewalls can be implemented in software, hardware or a combination of both. In addition to preventing unrestricted access into a network, a firewall can also restrict data from flowing out of a network.
- e. **Site** - A site is defined as one or more well connected TCP/IP subnets.

3. Scope

- a. This standard applies to any Agency's implementation of Active Directory™. This standard covers implementation of any Active Directory™ Domain Controller established on the State's enterprise network within a production environment.

4. Standard

- a. Department, agencies, boards and commissions, and other entities participating in the State's Active Directory™ shall comply with all Active Directory™ Domain Controller prescribed standards, processes, and specifications defined by the Division of Information Technology. DoIT will publish specific procedures and processes that Agencies will follow to implement Active Directory™.

b. Control

- (i.) All new Domain Controller Deployment requests start with existing Change Management approval process. All requests shall be reviewed by AD committee for determination of need and/or proper placement based on an analysis of available bandwidth, number of users, and Microsoft Best Practices.

c. Physical/Configuration

- (i.) Domain controllers shall be built, configured and introduced to AD as specified in the Domain Controller Configuration Procedure and follow the General Environment and Configuration Standards.

- 1. Addition to the above standards, there must be a minimum of 2 Domain Controllers deployed per Domain.

d. Applications

- (i.) All Domain Controllers shall be configured to conform to the state's DNS model and structure.
- (ii.) The only acceptable applications that can run on a Domain Controller are DNS, DHCP, or WINS. Any other application will require approval through the Change Management process.
- (iii.) The use of Domain controllers as a general workstation is prohibited. Users should not be using a domain controller to surf the Web or perform any other activities that could allow the introduction of malicious code except for Maintenance Activities.

e. Antivirus

- (i.) Antivirus software must be installed on all domain controllers in the enterprise. Antivirus software must be configured to monitor all files and directories within domain controller.
- (ii.) Please refer to the Domain Controller Antivirus Procedures for information.

5. Exceptions

- (i.) Requests for variance and exceptions to this standard must be submitted through the DoIT change management process.

6. Signatures

Assistant Director of Planning, Policy & Technology

Date

Director of Operations

Date

Chief Information Officer

Date

Director, Department of Administration

Date