



# **ACTIVE DIRECTORY SECURITY CHECKLIST**

Version 1, Release 1.5

27 July 2007

**Developed by DISA for the DoD**

**UNCLASSIFIED**

## **Trademark Information**

Active Directory, Microsoft, Windows, Windows NT, and Windows server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

## TABLE OF CONTENTS

	<b>Page</b>
SUMMARY OF CHANGES .....	v
1. INTRODUCTION .....	1-1
1.1 Background.....	1-1
1.2 Organization of the Checklist .....	1-1
1.3 Supported Versions.....	1-2
1.4 Review Methodology.....	1-3
1.5 Referenced Documents .....	1-3
2. REVIEW RESULTS REPORT .....	2-1
2.1 Cover Sheet.....	2-1
2.2 Reviewer Summary.....	2-2
2.3 Site Information .....	2-2
2.4 Asset Information.....	2-3
2.4.1 Domain Controller (DC) Information.....	2-3
2.4.2 Domain Asset Information.....	2-4
2.4.3 Forest Asset Information.....	2-4
2.4.4 Synch\Maint Application Information.....	2-5
2.4.5 ADAM Instance Information.....	2-5
2.5 Interview Finding Details - AD Domain Controller .....	2-7
2.6 Interview Finding Details - AD Domain .....	2-8
2.7 Interview Finding Details - AD Forest .....	2-9
2.8 Interview Finding Details - Synch\Maint App.....	2-10
2.9 Manual Finding Details - AD Domain Controller .....	2-15
2.10 Manual Finding Details - AD Domain.....	2-17
2.11 Manual Finding Details - AD Forest .....	2-20
2.12 Manual Finding Details - Synch\Maint App.....	2-21
2.13 Manual Finding Details - ADAM Instance.....	2-24
2.14 Finding Summary: .....	2-25
3. SYSTEM ADMINISTRATOR / INFORMATION ASSURANCE OFFICER INTERVIEW QUESTIONS .....	3-1
3.1 Review Process Information.....	3-1
3.2 Active Directory Domain Controller .....	3-2
3.3 Active Directory Domain.....	3-6
3.4 Active Directory Forest.....	3-11
3.5 Directory Service Synchronization \ Maintenance Application .....	3-12
3.6 Active Directory Application Mode Instance .....	3-32
4. AUTOMATED CHECK PROCEDURES.....	4-1
5. MANUAL CHECK PROCEDURES .....	5-1
5.1 Review Process Information.....	5-1
5.2 Active Directory Domain Controller .....	5-3
5.2.1 Data \ Program Access Control.....	5-3
5.2.2 Time Synchronization Control.....	5-6
5.2.3 Domain Controller Characteristics .....	5-8
5.2.4 AD Object Access Permissions and Auditing .....	5-10

5.3	Active Directory Domain.....	5-16
5.3.1	Trust Relationships .....	5-16
5.3.2	Privileged Group Membership.....	5-22
5.3.3	Other Domain Characteristics.....	5-25
5.4	Active Directory Forest.....	5-30
5.5	Directory Service Synchronization \ Maintenance Application .....	5-32
5.6	Active Directory Application Mode Instance .....	5-44
APPENDIX A: OBJECT PERMISSIONS AND AUDIT SETTINGS .....		A-1
A.1	File and Directory Permissions.....	A-1
A.1.1	AD Data Permissions.....	A-1
A.1.2	Windows Support Tools Permissions .....	A-2
A.1.3	Synchronization\Maintenance Software Permissions.....	A-2
A.1.4	Synchronization\Maintenance Data Permissions.....	A-3
A.1.5	Synchronization\Maintenance Audit Data Permissions.....	A-3
A.2	Registry Key Permissions .....	A-3
A.3	AD Object Permissions.....	A-3
A.4	AD Object Audit Settings .....	A-4
APPENDIX B: DOCUMENTATION.....		B-1
B.1	Pre-Trip Information Gathering.....	B-1
B.1.1	Pre-Trip Interview Questions.....	B-1
B.1.2	Pre-Trip Documentation .....	B-2
B.2	AD Documentation Examples .....	B-3
B.2.1	Trust Relationship Documentation .....	B-3
B.2.1.1	Example Trust Relationship Documentation - Child Domain.....	B-3
B.2.1.2	Example Trust Relationship Documentation - Forest Root Domain .....	B-4
APPENDIX C: VMS PROCESS GUIDANCE .....		C-1
C.1	AD Implementation Data - AD Domain Controller, AD Domain, AD Forest.....	C-1
C.1.1	AD Domain Controller Asset Data.....	C-2
C.1.2	AD Domain Asset Data .....	C-2
C.1.3	AD Forest Asset Data .....	C-3
C.2	Synchronization\Maintenance Application Asset Data .....	C-4
C.3	ADAM Instance Asset Data.....	C-5
APPENDIX D: DIRECTORY INFORMATION GATHERING.....		D-1
D.1	Active Directory.....	D-1
D.1.1	Identifying Domain Controllers.....	D-1
D.1.2	Determining “Immediate” Domain Structure .....	D-2
D.1.3	Identifying Holders of FSMO Roles.....	D-4

## SUMMARY OF CHANGES

### **Version 1 R1.5 – 27 July 2007**

- General - Updated version to V1R1.5 and date to 27 July 2007.
- Appendix A - A.3 – Added ENTERPRISE DOMAIN CONTROLLERS with Read access allowed for Group Policy Objects. Also added text to the note to clarify that 1) authenticated users\groups may be assigned permissions and 2) unauthenticated users (Anonymous Logon \ Guest) may not be assigned permissions without justification documented with the IAO.

### **Version 1 R1.4 – 25 May 2007**

- General - Updated version to V1R1.4 and date to 25 May 2007.
- Section 5 - DS00.0150 – Re-sequenced Check procedures to put Windows 2000 Server Procedures first.
- DS10.0295 – Re-sequenced Check procedures to put Windows 2000 Server Procedures first.

### **Version 1 R1.3 – 24 November 2006**

- General - Updated version to V1R1.3 and date to 24 November 2006.
- Added one Cat III check: DS10.9100.
- Section 2 - 2.5 - Added one row for new check DS10.9100.
- 2.9 \ 2.10 - Moved rows from 2.10 to 2.9 and updated section references to reflect reassignment of three checks.
- 2.14 - Updated Possible values to reflect one new check and reassignment of three checks.
- Section 3 - DS00.0160 - Changed V-Key from V0008301 to V0002369.
- DS10.9100 - Added this new Active Directory Domain Controller (3.2) check to verify that the hosting AD domain and forest are being or have been reviewed.
- Section 5 - 5.2 - Corrected subsection numbering.
- 5.2 \ 5.3 - Moved section 5.3.1 (including three checks: DS00.0130, DS00.0140, and DS10.0210) to 5.2.4 and renumbered remaining subsections in 5.3.
- DS00.0130 - Reassigned from Active Directory Domain (5.3) check to Active Directory Domain Controller (5.2) check.
- Changed V-Key from V0008528 to V0002370.
- DS00.0140 - Reassigned from Active Directory Domain (5.3) check to Active Directory Domain Controller (5.2) check.
- Changed V-Key from V0008529 to V0004243.
- DS10.0210 - Reassigned from Active Directory Domain (5.3) check to Active Directory Domain Controller (5.2) check.
- Changed V-Key from V0011758 to V0012780.

### **Version 1 R1.2 – 22 September 2006**

- General - Updated version to V1R1.2 and date to 22 September 2006.
- Section 1
  - 1.2 - Updated description of Appendix B.
  - 1.4 - Renamed section to “Review Methodology” and added paragraph to reference new “Pre-Trip Information Gathering” section.
- Section 2
  - 2.4 - Revised section to map appropriately to the specific review items.
- Section 3
  - 3.1 – Added paragraph to note the value of gathering information in advance and reference new “Pre-Trip Information Gathering” section. Added paragraph to reference FSMO information gathering procedures in Appendix D.
  - DS10.0260 - Updated text to clarify that list is required only if privileged accounts exist.
    - Updated (VMS Fixes) text to add example justification statement.
  - DS10.0350 - Added text to note that pre-requisite check (DS10.0100) is a manual check in section 5.
  - DS05.0170 - Added text to note that pre-requisite check (DS05.0160) is a manual check in section 5.
- Section 5
  - 5.1 - Added paragraph to note the value of gathering information in advance and reference new “Pre-Trip Information Gathering” section. Added paragraph to reference FSMO information gathering procedures in Appendix D.
  - DS00.0120 - Corrected STIG reference to 2.3.3.3.
  - DS10.0140 - Added “ADAM\_instance” as an additional example.
    - Added note that MS Windows-based DNS is an acceptable application.
  - DS10.0170 - Added text to clarify that the objective is to verify that a \*current\* need for each trust exists.
  - DS10.0180 - Added text to clarify that check applies only to trusts between DoD organizations.
  - DS10.0240 - Updated (VMS Fixes) text to add example justification statement.
  - DS10.0250 - Added text to show the format of an account from an outside domain.
  - DS10.0295 - Updated header text to indicate that check applies only to the forest root PDC Emulator DC.
- Appendix A
  - A.1.1 - Added explanation of accounts marked with an asterisk.
- Appendix B
  - Renamed to “Documentation”.
  - Inserted section B.1, “Pre-Trip Information Gathering”.
  - B.2.1.1 - Corrected the “N\A” value to “No” in the Transitive column for the Realm trust example.

## 1. INTRODUCTION

### 1.1 Background

This *Active Directory Security Checklist* provides the procedures for conducting a Security Readiness Review (SRR) to determine compliance with the requirements in the *Active Directory Security Technical Implementation Guide (STIG)*. This Checklist document must be used together with the corresponding version of the STIG document.

As in the related STIG, this Checklist addresses three review subjects:

- Active Directory Implementation - This subject covers checks for AD Domain Controllers, AD Domains, and the AD Forest that make up an implementation of Active Directory.
- Synchronization\Maintenance Application - This subject covers checks for an individual installation of an application used to perform synchronization or maintenance on one or more Active Directory implementations.
- ADAM - This subject covers checks for an individual installation of ADAM as a directory service.

The procedures in this document are part of the effort to ensure that the security configuration guidelines required by Department of Defense (DoD) Directive 8500.1, *Information Assurance*, and other relevant guidance are properly implemented.

In order to minimize repetition, certain procedures in this document reference information in the *Windows 2000 Security Checklist* and the *Windows Server 2003 Security Checklist*. Therefore, familiarity with those documents is considered a prerequisite to this checklist.

NOTE: Security patches required by the DoD Information Assurance Vulnerability Management (IAVM) process are reviewed during a Windows operating system security review. Because the IAVM-mandated patches applicable to AD are reviewed there, they are not listed in this document.

### 1.2 Organization of the Checklist

The *Active Directory Security Checklist* is composed of the following major sections and appendices. The organization is:

Section 1	<u>Introduction</u> This section contains summary information about the sections and appendix that comprise the <i>Active Directory Security Checklist</i> . The software version applicability, methods for reviews, and referenced documents are listed.
-----------	---

Section 2	<u>Review Results Report</u> This section is a template that allows a reviewer to manually document details about the object of the review and the vulnerabilities found during the review process. Information about the items listed is obtained through the procedures documented in Sections 3 and 5.
Section 3	<u>System Administrator /Information Assurance Officer Interview Questions</u> This section documents the questions that a reviewer discusses with the System Administrator (SA) or Information Assurance Officer (IAO) during the review process. The items reviewed correspond to a subset of those listed in Section 2.
Section 4	<u>Automated Check Procedures</u> This section is reserved for the procedures to be developed at a later time to perform a review using automated procedures.
Section 5	<u>Manual Check Procedures</u> This section documents the procedures to be used to perform a review manually. The items reviewed correspond to a subset of those listed in Section 2.
Appendix A	<u>Object Permissions and Audit Settings</u> This appendix documents any required Access Control Lists (ACLs) and audit settings for file, registry, and AD objects. The tables in this appendix are referenced in Section 5.
Appendix B	<u>Documentation</u> This appendix consists of two parts. The first part provides guidance on gathering information before the review trip. The second part provides examples of documentation used to satisfy some requirements. The examples in this appendix are referenced in Section 5.
Appendix C	<u>VMS Process Guidance</u> This appendix provides guidance for entering and accessing the asset information in VMS for the items covered by the Checklist.
Appendix D	<u>Directory Information Gathering</u> This appendix describes tools and methods that could be used to gather directory information.

### 1.3 Supported Versions

This document describes processes to review an AD environment composed of Windows 2000 Server or Windows Server 2003 domain controllers.

## 1.4 Review Methodology

This document provides manual procedures to perform a successful SRR. At a future date, procedures for using automation tools will be added to this document.

To accomplish a successful review, it is necessary to understand how the AD architecture is implemented in the environment and to examine several pieces of documentation. If this information can be gathered in advance of a review, the process is more efficient for the person performing the review and the site being reviewed. Appendix B Section B.1, Pre-Trip Information Gathering, provides a list of interview questions that can help target the review and a list of documentation that provides answers to several of the checks that are performed.

## 1.5 Referenced Documents

The following documents are referenced:

<b>Date</b>	<b>Description</b>
22 December 2005	<i>Active Directory Security Technical Implementation Guide, Version 1.1</i>
24 October 2002	<i>DoD Directive 8500.1, Information Assurance (IA)</i>
13 August 2004	<i>DoD Instruction 8551.1, Ports, Protocols, and Services Management (PPSM)</i>
16 December 2005	<i>Network Infrastructure Security Technical Implementation Guide, Version 6.4</i>
27 January 2006	<i>Strategic Command Directive SD 527-1, Department of Defense (DoD) Information Operations Condition (INFOCON) System Procedures</i>
29 August 2005	<i>Windows 2003/XP/2000 Addendum, Version 5.1</i>
Current	<i>Windows 2000 Security Checklist, Version 5.x.x</i>
Current	<i>Windows Server 2003 Security Checklist, Version 5.x.x</i>

This page is intentionally left blank.

## 2. REVIEW RESULTS REPORT

This section of the Checklist provides a template for manually recording review results.

### 2.1 Cover Sheet

#### UNCLASSIFIED Until Filled In

*CIRCLE ONE:*      **FOR OFFICIAL USE ONLY** (mark each page)

**CONFIDENTIAL and SECRET** (mark each page and each finding)

#### **Classification of Checklist report is based on classification of system reviewed:**

Unclassified System = FOUO Checklist

Confidential System = CONFIDENTIAL Checklist

Secret System = SECRET Checklist

Top Secret System = SECRET Checklist

## 2.2 Reviewer Summary

Reviewer: \_\_\_\_\_ Date: \_\_\_\_\_  
System: \_\_\_\_\_

<b><u>Finding Totals:</u></b>	<b><u>Comments:</u></b>
Category I: _____	_____
Category II: _____	_____
Category III: _____	_____
Category IV: _____	_____
<b>Total:</b> _____	

## 2.3 Site Information

Site: \_\_\_\_\_

### System Administrator Information:

Name: \_\_\_\_\_  
E-mail Address: \_\_\_\_\_  
Phone: (Commercial) \_\_\_\_\_ DSN: \_\_\_\_\_

### IAO Information:

Name: \_\_\_\_\_  
E-mail Address: \_\_\_\_\_  
Phone: (Commercial) \_\_\_\_\_ DSN: \_\_\_\_\_

## 2.4 Asset Information

### 2.4.1 Domain Controller (DC) Information

AD Domain Controller Host Asset Name: \_\_\_\_\_

Registered in VMS      VMS Asset ID: \_\_\_\_\_ (IP Address)

Asset Description: \_\_\_\_\_

#### DC Hardware

Make \ Model: \_\_\_\_\_

Barcode \ Serial No. \_\_\_\_\_

Location (building\room): \_\_\_\_\_

**DC Operating System:**  Windows 2000 Server (any edition)

Windows Server 2003 (any edition)

Other \_\_\_\_\_

**FSMO Role(s):**       Domain Naming       Schema

PDC Emulator       RID       Infrastructure

**AD Forest Root Domain DC:**       YES       NO

#### Asset Classification \ MAC \ Confidentiality Levels

Classification:       UNCLASSIFIED       SECRET

CONFIDENTIAL       TOP SECRET

Mission Assurance Category:       MAC I       MAC II       MAC III

Confidentiality:       CLASSIFIED       SENSITIVE       PUBLIC

**Other Notes:** \_\_\_\_\_  
\_\_\_\_\_

### 2.4.2 Domain Asset Information

AD Domain Asset Name: AD-Domain(\_\_\_\_\_)

Registered in VMS

Asset Description: \_\_\_\_\_

AD Forest Root Domain:  YES  NO

#### Asset Classification \ MAC \ Confidentiality Levels

[Projected from the highest level of any DC in the AD domain]

Classification:  UNCLASSIFIED  SECRET  
 CONFIDENTIAL  TOP SECRET

Mission Assurance Category:  MAC I  MAC II  MAC III

Confidentiality:  CLASSIFIED  SENSITIVE  PUBLIC

Enclave: \_\_\_\_\_

Other Notes: \_\_\_\_\_

\_\_\_\_\_

### 2.4.3 Forest Asset Information

AD Forest Asset Name: AD-Forest(\_\_\_\_\_)

Registered in VMS

Asset Description: \_\_\_\_\_

#### Asset Classification \ MAC \ Confidentiality Levels

[Projected from the highest level of any AD domain in the AD forest]

Classification:  UNCLASSIFIED  SECRET  
 CONFIDENTIAL  TOP SECRET

Mission Assurance Category:  MAC I  MAC II  MAC III

Confidentiality:  CLASSIFIED  SENSITIVE  PUBLIC

Enclave: \_\_\_\_\_

Other Notes: \_\_\_\_\_

\_\_\_\_\_

### 2.4.4 Synch\Maint Application Information

Application Host Asset Name: \_\_\_\_\_

Registered in VMS      VMS Asset ID: \_\_\_\_\_ (IP Address)

Asset Description: \_\_\_\_\_

- Application:**
- CPS Systems SimpleSync
  - Microsoft Identity Integration Server (MIIS)
  - Identity Integration Feature Pack (IIFP)
  - Other \_\_\_\_\_

#### Asset Classification \ MAC \ Confidentiality Levels

Classification:       UNCLASSIFIED       SECRET  
                          CONFIDENTIAL       TOP SECRET

Mission Assurance Category:       MAC I       MAC II       MAC III

Confidentiality:       CLASSIFIED       SENSITIVE       PUBLIC

**Other Notes:** \_\_\_\_\_  
\_\_\_\_\_

### 2.4.5 ADAM Instance Information

ADAM Host Asset Name: \_\_\_\_\_

Registered in VMS      VMS Asset ID: \_\_\_\_\_ (IP Address)

Asset Description: \_\_\_\_\_

#### Asset Classification \ MAC \ Confidentiality Levels

Classification:       UNCLASSIFIED       SECRET  
                          CONFIDENTIAL       TOP SECRET

Mission Assurance Category:       MAC I       MAC II       MAC III

Confidentiality:       CLASSIFIED       SENSITIVE       PUBLIC

**Other Notes:** \_\_\_\_\_  
\_\_\_\_\_

This page is intentionally left blank.

## 2.5 Interview Finding Details - AD Domain Controller

Procedure Section Headings		Finding Information			Vulnerability Information	
Man.	Script	Sev	Status	Comments	STIG ID	Short Name
3.2		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS00.0160	Directory Data Backup
3.2		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10.0150	DSRM Password Complexity
3.2		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10.0151	DSRM Password Change Policy
3.2		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10.0320	DSRM Password Physical Protection
3.2		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10.0310	Physical Access - Root FSMO Domain Controllers

Procedure Section Headings		Finding Information			Vulnerability Information	
Man.	Script	Sev	Status	Comments	STIG ID	Short Name
3.2		III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .9100	Review of Hosting Domain and Forest

### 2.6 Interview Finding Details - AD Domain

Procedure Section Headings		Finding Information			Vulnerability Information	
Man.	Script	Sev	Status	Comments	STIG ID	Short Name
3.3		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0260	AD Object Ownership Delegation
3.3		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0110	AD Inter-Enclave VPN Usage
3.3		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0300	IDS Visibility of AD VPN Data Transport

Procedure Section Headings			Finding Information			Vulnerability Information	
Man.		Script	Sev	Status	Comments	STIG ID	Short Name
3.3			III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0330	AD Architecture Disaster Recovery Documentation
3.3			III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0350	Trust Relationship INFOCON Procedures

**2.7 Interview Finding Details - AD Forest**

Procedure Section Headings			Finding Information			Vulnerability Information	
Man.		Script	Sev	Status	Comments	STIG ID	Short Name
3.4			III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS00 .0100	Schema Change Configuration Management

## 2.8 Interview Finding Details - Synch\Maint App

Procedure Section Headings		Finding Information			Vulnerability Information	
Man.	Script	Sev	Status	Comments	STIG ID	Short Name
3.5		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0130	Synch\Maint Inter-Enclave LDAP\HTTP Usage
3.5		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0140	Synch\Maint Inter-Enclave LDAPS\HTTPS Usage
3.5		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0170	Synch\Maint Software Migration Planning
3.5		III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0180	Synch\Maint Software Baseline Inventory
3.5		I	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0210	Synch\Maint Password Protection

Procedure Section Headings		Finding Information			Vulnerability Information	
Man.	Script	Sev	Status	Comments	STIG ID	Short Name
3.5		III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0270	Synch\Maint Audit Data Backup
3.5		III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0280	Synch\Maint Audit Data Retention
3.5		III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0320	Synch\Maint Local Code Configuration Management
3.5		III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0440	Synch\Maint Local Code Backup
3.5		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0330	Synch\Maint Data Transport Encryption

Procedure Section Headings		Finding Information			Vulnerability Information	
Man.	Script	Sev	Status	Comments	STIG ID	Short Name
3.5		III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0360	Synch\Maint Data Transport Signing
3.5		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0340	Synch\Maint Aggregate Transport Encryption
3.5		III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0350	Synch\Maint Certificate Validity Checking
3.5		III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0370	Synch\Maint Mutual Authentication
3.5		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0380	Synch\Maint Privileged Remote Access Control

Procedure Section Headings		Finding Information			Vulnerability Information	
Man.	Script	Sev	Status	Comments	STIG ID	Short Name
3.5		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0390	Synch\Maint Remote Access Session Logs
3.5		III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0400	Synch\Maint Non-privileged Remote Access Control
3.5		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0410	Synch\Maint Remote Access Encryption
3.5		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0420	Synch\Maint Server Physical Access
3.5		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0430	Synch\Maint Data Backup

Procedure Section Headings		Finding Information			Vulnerability Information	
Man.	Script	Sev	Status	Comments	STIG ID	Short Name
3.5		III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05.0450	Synch\Maint Disaster Recovery Documentation
3.5		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05.0460	Synch\Maint Security Patch Implementation

## 2.9 Manual Finding Details - AD Domain Controller

Procedure Section Headings			Finding Information			Vulnerability Information	
Man.		Script	Sev	Status	Comments	STIG ID	Short Name
5.2.1			I	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS00 .0120	Directory Data File Access Permissions
5.2.1			II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0130	AD Data File Locations
5.2.1			II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0120	Support Tools Access Permissions
5.2.2			II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS00 .0150	Time Synchronization
5.2.2			III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS00 .0151	Time Synchronization Source Logging

Procedure Section Headings		Finding Information			Vulnerability Information	
Man.	Script	Sev	Status	Comments	STIG ID	Short Name
5.2.3		III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0140	Domain Controller Dedication
5.2.3		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0290	Windows Services Startup
5.2.4		I	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS00 .0130	Directory Data Object Access Control
5.2.4		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS00 .0140	Directory Data Object Auditing
5.2.4		I	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0210	Synchronize Directory Service Data Right

### 2.10 Manual Finding Details - AD Domain

Procedure Section Headings		Finding Information			Vulnerability Information	
Man.	Script	Sev	Status	Comments	STIG ID	Short Name
5.3.1		III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0100	Trust Relationship Documentation
5.3.1		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0170	Trust Relationship Need
5.3.1		I	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0180	Trust Relationship Inter-Classification Levels
5.3.1		I	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0181	Trust Relationship Inter-Organization
5.3.1		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0190	SID Filtering Trust Option

Procedure Section Headings		Finding Information			Vulnerability Information	
Man.	Script	Sev	Status	Comments	STIG ID	Short Name
5.3.1		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0200	Selective Authentication Trust Option
5.3.2		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0220	Pre-Windows 2000 Compatible Access Membership
5.3.2		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0240	Privileged Group Membership - Intra-Forest
5.3.2		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0250	Privileged Group Membership - Inter-Forest
5.3.3		III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS00 .0110	Directory E-mail Attributes

Procedure Section Headings		Finding Information			Vulnerability Information	
Man.	Script	Sev	Status	Comments	STIG ID	Short Name
5.3.3		III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10.0160	Domain Functional Level
5.3.3		IV	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10.0270	Domain Object Ownership Quota
5.3.3		III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10.0280	Site Link Replication Properties
5.3.3		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10.0340	Domain Controller Availability

### 2.11 Manual Finding Details - AD Forest

Procedure Section Headings			Finding Information			Vulnerability Information	
Man.		Script	Sev	Status	Comments	STIG ID	Short Name
5.4			II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0230	dsHeuristics Option
5.4			II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS10 .0295	Time Synchronization - Forest Authoritative Source

**2.12 Manual Finding Details - Synch\Maint App**

Procedure Section Headings		Finding Information			Vulnerability Information	
Man.	Script	Sev	Status	Comments	STIG ID	Short Name
5.5		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0120	Synch\Maint Cryptographic Use
5.5		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0220	Synch\Maint PKI Certificate Source
5.5		I	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0160	Synch\Maint Non- Supported Release
5.5		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0190	Synch\Maint Public Domain Software
5.5		III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0200	Synch\Maint Code \ Data File Locations

Procedure Section Headings		Finding Information			Vulnerability Information	
Man.	Script	Sev	Status	Comments	STIG ID	Short Name
5.5		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0150	Synch\Maint Software File Access Permissions
5.5		I	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0230	Synch\Maint Data File Access Permissions
5.5		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0240	Synch\Maint Aggregate Data File Encryption
5.5		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0250	Synch\Maint Program Auditing
5.5		III	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0260	Synch\Maint Audit Data Tools

Procedure Section Headings		Finding Information			Vulnerability Information	
Man.	Script	Sev	Status	Comments	STIG ID	Short Name
5.5		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0290	Synch\Maint Audit Data Access Permissions
5.5		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0300	Synch\Maint Application Account Membership
5.5		II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS05 .0310	Synch\Maint Application Account Dedication

**2.13 Manual Finding Details - ADAM Instance**

Procedure Section Headings			Finding Information			Vulnerability Information	
Man.		Script	Sev	Status	Comments	STIG ID	Short Name
5.6			I	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS15 .0100	ADAM Host OS
5.6			II	<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed		DS15 .0110	ADAM Service Account

**2.14 Finding Summary:**

**AD Domain Controller**

Severity	Possible	Actual
Cat I	3	
Cat II	10	
Cat III	3	
Cat IV	0	-
<b>Total</b>	16	

**AD Domain**

Severity	Possible	Actual
Cat I	2	
Cat II	10	
Cat III	6	
Cat IV	1	
<b>Total</b>	19	

**AD Forest**

Severity	Possible	Actual
Cat I	0	-
Cat II	2	
Cat III	1	
Cat IV	0	-
<b>Total</b>	3	

**Synch\Maint App**

Severity	Possible	Actual
Cat I	3	
Cat II	19	
Cat III	13	
Cat IV	0	-
<b>Total</b>	35	

**ADAM Instance**

Severity	Possible	Actual
Cat I	1	
Cat II	1	
Cat III	0	-
Cat IV	0	-
<b>Total</b>	2	

This page intentionally blank.

### **3. SYSTEM ADMINISTRATOR / INFORMATION ASSURANCE OFFICER INTERVIEW QUESTIONS**

This section of the Checklist provides questions that must be asked of the System Administrator (SA) or the Information Assurance Officer (IAO) in an interview during the review. The responses to these questions may be recorded on a copy of the Review Results Report in Section 2.

#### **3.1 Review Process Information**

The text in this section identifies a single individual, by role, to respond to the interview questions. In most cases this is the IAM or IAO. However, it is understood that in many cases the information will come from an SA or application SA.

The following items should be available to accelerate the interview process:

- Locations of AD forest root FSMO domain controllers  
[This includes the Windows server(s) holding the Domain Naming Master, Schema Master, PDC Emulator, RID Master, and Infrastructure Master FSMO roles.]
- Locations of AD domain controllers and AD sites, relative to the local Enclave network boundaries
- Lists of accounts assigned to AD privileged groups (Domain Admins, Enterprise Admins, Schema Admins, Group Policy Creator Owners, and Incoming Forest Trust Builders)
- List of accounts with the right to create AD objects (e.g., accounts, printers), but that are not members of the built-in AD privileged groups.
- Backup and continuity of operations or disaster recovery documents related to the Windows domain controllers
- Information about specific directory synchronization and maintenance applications that are implemented. This includes products such as CPS Systems SimpleSync, Microsoft Identity Integration Server (MIIS), and Microsoft Identity Integration Feature Pack (IIFP).

Please note that it would be significantly more efficient to gather this information prior to the start of a review. Appendix B Section B.1, Pre-Trip Information Gathering, provides lists of interview questions and documentation items that should be used in advance to assemble the required information.

Please reference Appendix D, Directory Information Gathering, for tools and procedures that can be used to gather some of the information required for a review. In particular, Section D.1.3, Identifying Holders of FSMO Roles, can be used to gather the current FSMO information for the AD environment.

### 3.2 Active Directory Domain Controller

**Notes:** The checks in this section apply to assets with a Windows server OS and the Domain Controller role and are performed for **all domain controllers selected for review** in an AD domain. [This may be a sample of one or more domain controllers.]

#### DS00.0160 Directory Data Backup

<b>STIG ID \ V-Key</b>	<b>DS00.0160 \ V0002369</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Directory Data Backup
<b>IA Controls</b>	CODB-1, CODB-2, CODB-3
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.6

**Long Name:** Directory data is not backed up on a daily or weekly basis.

**Checks:**

- Interview the IAO.
- Obtain a copy of the site's SOP for backups.
- Check the SOP for the frequency at which directory data is backed up. Alternatively, physically verify that backups are being taken.  
- For AD domain controllers, this must be a System State data backup.
- If the directory data for a MAC III system is not backed up at least weekly, then this is a Finding.
- If the directory data for a MAC I or II system is not backed up at least daily, then this is a Finding.

This check replaces the functions of Windows Checklist item 1.023 that was removed from the Windows Checklists.

---

DS10.0150 DSRM Password Complexity

<b>STIG ID \ V-Key</b>	<b>DS10.0150 \ V0008303</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	DSRM Password Complexity
<b>IA Controls</b>	IAIA-1, IAIA-2
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CS
<b>References</b>	AD STIG 2.3.2

**Long Name:** The DSRM password does not meet complexity standards.

**Checks:**

- Interview the IAO.
- Obtain a copy of the site's policy that addresses password complexity.
- Check that the policy addresses the password complexity standards (length, upper/lower case, special characters) for the AD DSRM password.  
Note that there is no known method to check password complexity online while the server is active as a domain controller.
- If the policy does not address the complexity standards for the DSRM password, then this is a Finding.

---

DS10.0151 DSRM Password Change Policy

<b>STIG ID \ V-Key</b>	<b>DS10.0151 \ V0008310</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	DSRM Password Change Policy
<b>IA Controls</b>	IAIA-1, IAIA-2
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CS
<b>References</b>	AD STIG 2.3.2

**Long Name:** There is no policy to ensure that the DSRM password is changed often enough.

**Checks:**

- Interview the IAM.
- Obtain a copy of the site's policy that addresses password change frequency.
- Check that the policy addresses the requirement for the AD DSRM password to be changed at least yearly. Alternatively review logs or other evidence that indicates that the password has been changed within the last year.  
Note that there is no known method to check password age online while the server is active as a domain controller.
- If there is no policy for changing the DSRM password at least yearly or no indication that it has been changed within the last year, then this is a Finding.

---

DS10.0320 DSRM Password Physical Protection

<b>STIG ID \ V-Key</b>	<b>DS10.0320 \ V0008311</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	DSRM Password Physical Protection
<b>IA Controls</b>	COBR-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.6

**Long Name:** The offline copy of the DSRM password is not subject to adequate physical protections.

**Checks:**

- Interview the IAO.
- Check the location to verify that a copy of the DSRM password is stored in a locked, fire-rated container or is subject to other appropriate physical protections from loss.
- If there is no copy of the DSRM password or it is not adequately physically protected, then this is a Finding.

---

DS10.0310 Physical Access - Root FSMO Domain Controllers

<b>STIG ID \ V-Key</b>	<b>DS10.0310 \ V0008313</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Physical Access - Root FSMO Domain Controllers
<b>IA Controls</b>	PECF-1, PECF-2
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CS
<b>References</b>	AD STIG 2.3.5

**Long Name:** Physical access to the AD forest root FSMO domain controllers is not restricted to specifically authorized personnel.

**Checks:**

- Interview the IAO.
- Verify that physical access to the forest root FSMO domain controllers is restricted to specifically authorized personnel.
  - This includes the Windows server(s) holding the Domain Naming Master, Schema Master, PDC Emulator, RID Master, and Infrastructure Master FSMO roles.
- If physical access to any server holding a FSMO role for the forest root domain is not restricted, then this is a Finding.

DS10.9100 Review of Hosting Domain and Forest

<b>STIG ID \ V-Key</b>	<b>DS10.9100 \ V0012778</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Review of Hosting Domain and Forest
<b>IA Controls</b>	ECSC-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3

**Long Name:** The AD domain and forest in which the domain controller resides have not been reviewed for vulnerabilities.

**Checks:**

- Interview the IAO.
- Verify that the AD domain \*and\* forest in which the domain controller resides have been reviewed for compliance with the requirements in the AD STIG.
  - The reviews must be conducted at the same time or no more than 1 year prior to the review of the domain controller.
  - VMS asset information, dated reports, or other documentation can be used to provide verification.
- If it not possible to verify that the AD domain and forest have been reviewed, then this is a Finding.

### 3.3 Active Directory Domain

**Notes:** The checks in this section apply to Active Directory Domain assets and are performed **only once per AD domain**, on any one domain controller.

#### DS10.0260 AD Object Ownership Delegation

<b>STIG ID \ V-Key</b>	<b>DS10.0260 \ V0008521</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	AD Object Ownership Delegation
<b>IA Controls</b>	ECLP-1, ECPA-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.6

**Long Name:** The number of accounts is excessive or documentation does not exist for the accounts that have been delegated AD object ownership or update permissions and are \*not\* members of Windows built-in administrative groups.

**Checks:**

- Interview the IAM.
- Obtain the list of accounts that have been delegated AD object ownership or update permissions and that are \*not\* members of Windows built-in administrative groups.  
[This includes accounts for help desk or support personnel who are not Administrators, but have authority in AD to maintain user accounts or printers.]
- If accounts with delegated authority are defined and there is no list, then this is a Finding.
- Count the number of accounts on the list.
- If the number of accounts with delegated authority is greater than ten (10), review the site documentation that justifies this number.  
- The object is to validate that the IAM explicitly acknowledges the need to have a high number of privileged users.
- If the number of accounts with delegated authority is greater than ten (10) and there is no statement in the documentation that justifies the number, then this is a Finding.

DS10.0110 AD Inter-Enclave VPN Usage

<b>STIG ID \ V-Key</b>	<b>DS10.0110 \ V0008522</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	AD Inter-Enclave VPN Usage
<b>IA Controls</b>	DCPP-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.1.3 DODI 8551.1

**Long Name:** An AD implementation (domains or forest) that spans enclave boundaries does not use a VPN to protect AD network traffic.

**Checks:**

- Interview the IAM.
- With the assistance of the SA, NSO, or network reviewer as required, review the site network diagram(s) to determine if domain controllers for the AD forest are located in multiple enclaves.  
- The object is to determine if AD network traffic is traversing enclave network boundaries.
- If domain controllers are \*not\* located in multiple enclaves, then this check is Not Applicable.
- If domain controllers are located in multiple enclaves, verify that a VPN is used to transport the AD network traffic (replication, user logon, AD queries, etc.). [Retain this location and VPN information for use in a subsequent check.]
- If a VPN solution is not used to transport AD network traffic across enclave boundaries, then this is a Finding.

Note: This check and the associated requirement are based on DoD ports and protocols restrictions stated in DoD Instruction 8551.1 and linked documents.

DS10.0300 IDS Visibility of AD VPN Data Transport

<b>STIG ID \ V-Key</b>	<b>DS10.0300 \ V0008523</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	IDS Visibility of AD VPN Data Transport
<b>IA Controls</b>	EBVC-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.4

**Long Name:** The VPN used to protect AD network traffic does not support visibility by an IDS.

**Checks:**

- Interview the IAO.
- If the response to check DS10.0110 indicates that domain controllers are *\*not\** located in multiple enclaves, then this check is Not Applicable.
- If the response to check DS10.0110 indicates that domain controllers *\*are\** located in multiple enclaves and a VPN is *\*not\** used, then this check is Not Applicable.
- If the response to check DS10.0110 indicates that domain controllers *\*are\** located in multiple enclaves and a VPN *\*is\** used, review the site network diagram(s) with the SA, NSO, or network reviewer as required to determine if the AD network traffic is visible to a network or host IDS.
- If the AD network traffic is not visible to a network or host IDS, then this is a Finding.

DS10.0330 AD Architecture Disaster Recovery Documentation

<b>STIG ID \ V-Key</b>	<b>DS10.0330 \ V0008525</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	AD Architecture Disaster Recovery Documentation
<b>IA Controls</b>	CODP-1, CODP-2, CODP-3, COEF-1, COEF-2
<b>MAC /Conf</b>	1-CSP, 2-CSP
<b>References</b>	AD STIG 2.3.6

**Long Name:** Disaster recovery plans do not include sufficient AD architecture information such as forest, tree, and domain structure.

**Checks:**

- Interview the IAO.
- Determine the MAC level information for the AD Domain asset.  
- This is available in VMS by using **Asset Finding Maint.** and navigating to the asset or by running an **Asset Information (AS01)** report for the location.
- If the MAC level of the AD Domain is III, this check is Not Applicable.
- Obtain a copy of the site's disaster recovery planning documents.
- Check the disaster recovery plans for documentation on the AD forest, tree, and domain structure.  
[A chart showing forest hierarchy and domain names is the minimum suggested.]
- If the disaster recovery plans that cover a MAC I or II level AD Domain do not include AD structure information, then this is a Finding.

DS10.0350 Trust Relationship INFOCON Procedures

<b>STIG ID \ V-Key</b>	<b>DS10.0350 \ V0008526</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Trust Relationship INFOCON Procedures
<b>IA Controls</b>	VIIR-1, VIIR-2
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.7 Strategic Command Directive (SD) 527-1

**Long Name:** AD trust relationships have not been evaluated with respect to possible INFOCON procedures.

**Checks:**

- Interview the IAO.
- Refer to the list of actual trusts obtained in check DS10.0100.  
\*Note\* - Check DS10.0100 (V0008530) is a manual check located in Section 5, Manual Check Procedures.
- If there are no external, forest, or realm AD trust relationships, this check is Not Applicable.
- Obtain a copy of the site's supplemental INFOCON procedures as required by Strategic Command Directive (SD) 527-1.
- Verify that it has been determined by the IAM whether INFOCON response actions are to include procedures to disable external, forest, or realm AD trust relationships.  
- The object is to determine if the need has been explicitly evaluated.
- If it has been determined that actions to disable AD trust relationships \*are not\* required, then this check is Not Applicable.
- If it has been determined that actions to disable AD trust relationships \*are\* required, verify that the policy to implement these actions has been documented.
- If actions to disable AD trust relationships \*are\* required and no policy has been documented, then this is a Finding.

### 3.4 Active Directory Forest

**Notes:** The checks in this section apply to Active Directory Forest assets and are performed on **only once per AD forest.**

#### DS00.0100 Schema Change Configuration Management

<b>STIG ID \ V-Key</b>	<b>DS00.0100 \ V0008527</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Schema Change Configuration Management
<b>IA Controls</b>	DCPR-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.1.2

**Long Name:** There is no policy to ensure that changes to the directory schema are subject to a configuration management process.

**Checks:**

- Interview the IAM.
- Obtain a copy of the site's configuration management procedures documentation.
- Verify that there is a local policy that requires changes to the directory schema to be processed through a configuration management process.  
- For AD this refers to changes to the AD schema.
- If there is no policy that requires changes to the directory schema to be processed through a configuration management process, then this is a Finding.

### 3.5 Directory Service Synchronization \ Maintenance Application

The checks in this section apply to Synch\Maint App assets and are performed **once for each system** on which a directory synchronization or maintenance product is installed. Note that this may not be a Windows server because some software is capable of executing on workstation operating systems.

These products include CPS Systems SimpleSync, Microsoft Identity Integration Server (MIIS), and Microsoft Identity Integration Feature Pack (IIFP).

Please note the following terminology used in this section:

- The term Application SA is used to indicate the person responsible for the maintenance of the synchronization or maintenance application.
- The phrase “routine, scheduled operations” is intended to indicate that the requirement applies where synchronization or maintenance applications are used regularly and in a production environment. Requirements with this text would not apply where the application is used only occasionally or for research or testing purposes.
- The phrase “security principal” refers to a Windows account that has access to data and other resources. This is contrasted with a contact object that represents an e-mail address.

#### DS05.0100 Synch\Maint Product Validation

<b>STIG ID \ V-Key</b>	<b>DS05.0100</b>
<b>Severity</b>	
<b>Short Name</b>	Synch\Maint Product Validation
<b>IA Controls</b>	DCAS-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.1.1

Note: At this time no commercial synchronization \ maintenance applications been evaluated or validated by the NIAP so this check is not active.

---

#### DS05.0110 Synch\Maint Product Robustness

<b>STIG ID \ V-Key</b>	<b>DS05.0110</b>
<b>Severity</b>	
<b>Short Name</b>	Synch\Maint Product Robustness
<b>IA Controls</b>	DCSR-1, DCSR-2, DCSR-3
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.1.1

Note: At this time no commercial synchronization \ maintenance applications been evaluated or validated by the NIAP so this check is not active.

---

DS05.0130 Synch\Maint Inter-Enclave LDAP\HTTP Usage

<b>STIG ID \ V-Key</b>	<b>DS05.0130 \ V0011760</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Synch\Maint Inter-Enclave LDAP\HTTP Usage
<b>IA Controls</b>	DCPP-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.1.3 DODI 8551.1

**Long Name:** A synch\maint implementation that spans enclave boundaries and uses LDAP or HTTP protocol does not use a VPN to protect the network traffic.

**Checks:**

- Interview the Application SA.
- With the assistance of the SA, NSO, or network reviewer as required, review the application documentation and the site network diagram(s) to determine if the synch\maint implementation transfers directory data across enclave boundaries and uses the LDAP or HTTP protocol.  
- The object is to determine if application traffic is traversing enclave network boundaries and if LDAP or HTTP is used.  
[Retain this information for use in a subsequent check.]
- If the synch\maint implementation does \*not\* transfer data across enclave boundaries or does \*not\* use LDAP or HTTP, then this check is Not Applicable.
- If the synch\maint implementation transfers data using LDAP or HTTP, review the site network diagram(s) with the assistance of the SA, NSO, or network reviewer as required, to determine if a VPN is used to transport the directory data network traffic.
- If a VPN solution is not used to transport directory data network traffic across enclave boundaries, then this is a Finding.

Note: This check and the associated requirement are based on DoD ports and protocols restrictions stated in DoD Instruction 8551.1 and linked documents.

DS05.0140 Synch\Maint Inter-Enclave LDAPS\HTTPS Usage

<b>STIG ID \ V-Key</b>	<b>DS05.0140 \ V0011761</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Synch\Maint Inter-Enclave LDAPS\HTTPS Usage
<b>IA Controls</b>	DCPP-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.1.3 DODI 8551.1

**Long Name:** A synch\maint implementation that spans enclave boundaries and uses LDAPS or HTTPS protocol does not use a DODI 8551.1-compliant solution to protect the network traffic.

**Checks:**

- Interview the Application SA.
- If the response to check DS05.0130 indicates that directory data *\*is\** transferred across enclave boundaries, review the application documentation to determine if the synch\maint implementation uses the LDAPS or HTTPS protocol.
- If directory data is *\*not\** transferred across enclave boundaries or does *\*not\** use LDAPS or HTTPS, then this check is Not Applicable.
- If the synch\maint implementation transfers data using LDAPS or HTTPS, review the site network diagram(s) with the assistance of the SA, NSO, or network reviewer as required, to determine if a DODI 855.1-compliant network configuration is in use.
  - This generally means that the traffic must flow through a DMZ to comply with the PPSM requirements for LDAPS and HTTPS.
- If the LDAPS or HTTPS traffic does not flow through a compliant network configuration, then this is a Finding.

DS05.0170 Synch\Maint Software Migration Planning

<b>STIG ID \ V-Key</b>	<b>DS05.0170 \ V0011762</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Synch\Maint Software Migration Planning
<b>IA Controls</b>	DCSL-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.1.4

**Long Name:** A migration plan has not been developed to remove or upgrade a synch\maint product for which vendor support is soon being or already has been dropped.

**Checks:**

- Interview the Application SA.
- Refer to the result of check DS05.0160 to determine if the installed synch\maint product is no longer supported or will soon be (three months) unsupported.  
\*Note\* - Check DS05.0160 (V0011784) is a manual check located in Section 5, Manual Check Procedures.
- If an installed synch\maint product is no longer supported or will soon be unsupported, examine the site's plan for removing or upgrading the product.
- If there is no plan to remove or upgrade the unsupported product, then this is a Finding.

DS05.0180 Synch\Maint Software Baseline Inventory

<b>STIG ID \ V-Key</b>	<b>DS05.0180 \ V0011763</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Synch\Maint Software Baseline Inventory
<b>IA Controls</b>	DCSW-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.1.4

**Long Name:** A synch\maint product used in routine, scheduled operations is not documented in the CCB and C&A software inventory or the inventory backup copy is not subject to adequate physical protections.

**Checks:**

- Interview the Application SA.
- Verify whether the synch\maint product is used in routine, scheduled operations.
- If the product is not used in routine, scheduled operations, then this check is Not Applicable.
- Review the following local documentation to determine if the synch\maint product is listed:
  - a) baseline software inventory of the CCB
  - b) applicable C&A documents
  - c) software inventory backup copy stored in a fire-rated container or subject to other appropriate physical protections from loss.
- If the synch\maint product is \*not\* documented in the required locations, then this is a Finding.

DS05.0210 Synch\Maint Password Protection

<b>STIG ID \ V-Key</b>	<b>DS05.0210 \ V0011764</b>
<b>Severity</b>	Cat I
<b>Short Name</b>	Synch\Maint Password Protection
<b>IA Controls</b>	IAIA-1, IAIA-2
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CS
<b>References</b>	AD STIG 2.3.2

**Long Name:** A password used in the execution of a synch\maint implementation is embedded in a script or stored in an unencrypted file.

**Checks:**

- Interview the Application SA.
- Verify whether the execution of the synch\maint implementation uses a script in which a password is embedded or uses any unencrypted file that contains a password.
  - Verification can involve review of the operating documentation or observation of the execution of a synch\maint cycle.
- If execution of the synch\maint implementation uses a script in which a password is embedded or uses any unencrypted file that contains a password, then this is a Finding.

DS05.0270 Synch\Maint Audit Data Backup

<b>STIG ID \ V-Key</b>	<b>DS05.0270 \ V0011765</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Synch\Maint Audit Data Backup
<b>IA Controls</b>	ECTB-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-C
<b>References</b>	AD STIG 2.3.3.5

**Long Name:** Audit data from a synch\maint implementation is not backed up at least weekly on external media or on a system other than where the implementation executes.

**Checks:**

Note: This check is Not Applicable if the audit data is collected in a Windows Event Log. [Windows Event Log backup is reviewed in the Windows Checklist.]

- Interview the Application SA.
- Obtain a copy of the site's policy that addresses (audit) data backup.
- Check that the policy addresses the requirement for the audit data from a synch\maint implementation to be:
  - Backed up at least weekly
  - Backed up on external media or to a system other than the one on which the implementation runs.Alternatively review logs or other evidence that indicates audit data backup frequency and output destination.
- If the audit data is not backed up at least weekly or is not backed up to a detached location, then this is a Finding.

DS05.0280 Synch\Maint Audit Data Retention

<b>STIG ID \ V-Key</b>	<b>DS05.0280 \ V0011766</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Synch\Maint Audit Data Retention
<b>IA Controls</b>	ECRR-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.5

**Long Name:** Audit data from a synch\maint implementation is not retained for at least one year.

**Checks:**

Note: This check is Not Applicable if the audit data is collected in a Windows Event Log. [Windows audit retention is reviewed in the Windows Checklist.]

- Interview the Application SA.
- Obtain a copy of the site's policy that addresses audit data retention.
- Check that the policy addresses the retention requirement for the audit data from a synch\maint implementation.  
Alternatively review logs or other evidence that indicates audit data retention.
- If the audit data is not retained for at least one year, then this is a Finding.

DS05.0320 Synch\Maint Local Code Configuration Management

<b>STIG ID \ V-Key</b>	<b>DS05.0320 \ V0011767</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Synch\Maint Local Code Configuration Management
<b>IA Controls</b>	ECSD-1, ECSD-2
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.7

**Long Name:** There is no policy to ensure that code that is not vendor-provided and is used in a synch\maint implementation that updates security principal accounts is subject to a configuration management process.

**Checks:**

- Interview the Application SA.
- Determine if a synch\maint implementation that updates security principal accounts includes code not provided by the vendor.  
- For MIIS\IIFP, this refers to Management Agents (MAs) not provided from Microsoft.  
[Retain this code information for use in a subsequent check.]
- If the synch\maint implementation does *\*not\** use non-vendor code, then this check is Not Applicable.
- If the synch\maint implementation *\*does\** use non-vendor code, obtain a copy of the site's configuration management procedures documentation.
- Verify that there is a local policy that requires implementation and changes to the code to be processed through a configuration management process.
- If there is no policy that requires code implementation and changes to be processed through a configuration management process, then this is a Finding.

DS05.0440 Synch\Maint Local Code Backup

<b>STIG ID \ V-Key</b>	<b>DS05.0440 \ V0011768</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Synch\Maint Local Code Backup
<b>IA Controls</b>	COSW-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.6

**Long Name:** Code used in a synch\maint implementation that is not vendor-provided is not backed up periodically.

**Checks:**

- Interview the Application SA.
- If the information obtained in check DS05.0320 indicates the synch\maint implementation does *\*not\** use non-vendor code, then this check is Not Applicable.
- If the synch\maint implementation *\*does\** use non-vendor code, obtain a copy of the site's policy that addresses backup for the application.
- Check that the policy addresses the requirement for the code to be backed up at least semi-annually.  
Alternatively review logs or other evidence that indicates the code is backed up.
- If the non-vendor code is not backed up at least semi-annually, then this is a Finding.

DS05.0330 Synch\Maint Data Transport Encryption

<b>STIG ID \ V-Key</b>	<b>DS05.0330 \ V0011769</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Synch\Maint Data Transport Encryption
<b>IA Controls</b>	ECCT-1, ECCT-2, ECNK-1, ECNK-2
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CS
<b>References</b>	AD STIG 2.3.3.8

**Long Name:** A synch\maint implementation that transfers data over wireless or non-DoD networks does not use FIPS 140-2-validated encryption to protect the network traffic.

**Checks:**

- Interview the Application SA.
- With the assistance of the SA, NSO, or network reviewer as required, review the site network diagram(s) and application documentation to determine if the synch\maint implementation transfers data over wireless or non-DoD networks.
- If data is *\*not\** transferred over wireless or non-DoD networks, then this check is Not Applicable.
- If data *\*is\** transferred over wireless or non-DoD networks, review the site network diagram(s) and application documentation to determine if FIPS 140-2-validated encryption is used to protect the network traffic.
  - This includes encryption of the data on the host before transmission, the use of LDAPS or HTTPS protocol, or the use of network components (such as a VPN) to perform encryption.
- If data *\*is\** transferred over wireless or non-DoD networks and acceptable encryption is not used, then this is a Finding.

DS05.0360 Synch\Maint Data Transport Signing

<b>STIG ID \ V-Key</b>	<b>DS05.0360 \ V0011770</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Synch\Maint Data Transport Signing
<b>IA Controls</b>	ECTM-1. ECTM-2
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.8

**Long Name:** A synch\maint implementation does not use data signing or other methods to ensure the integrity of directory data network traffic.

**Checks:**

- Interview the Application SA.
- Review the application documentation or configuration settings to determine if the synch\maint implementation signs the data or uses other integrity checks on data transferred over any network.
  - The use of encryption is an acceptable method of addressing data integrity. If the LDAPS or HTTPS protocol or a VPN is used for transmission, this meets the requirement.
- If the synch\maint implementation does not use data signing or other methods to ensure the integrity of transmitted data, then this is a Finding.

DS05.0340 Synch\Maint Aggregate Transport Encryption

<b>STIG ID \ V-Key</b>	<b>DS05.0340 \ V0011771</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Synch\Maint Aggregate Transport Encryption
<b>IA Controls</b>	ECCT-1, ECCT-2, ECNK-1, ECNK-2
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CS
<b>References</b>	AD STIG 2.3.3.8

**Long Name:** A synch\maint implementation that transfers a substantial aggregate of the directory data for an entire geographic command does not use FIPS 140-2-validated encryption to protect the network traffic.

**Checks:**

- Interview the Application SA.
- Determine if data transmitted by the synch\maint implementation contains directory information for an *\*entire\** geographic command such as DISA CONUS, DISA EUROPE, or DISA PACIFIC or for *\*all\** members of a Service or other Component.
  - An examination of the application documentation or directory query strings can be used to establish this.
- If the data transmitted by the synch\maint implementation does *\*not\** contain substantial aggregates, then this check is Not Applicable.
- If the data transmitted by the synch\maint implementation *\*does\** contain a substantial aggregate, review the application documentation and site network diagram(s) to determine if FIPS 140-2-validated encryption is used to protect the network traffic.
  - This includes encryption of the data on the host before transmission, the use of LDAPS or HTTPS protocol, or the use of network components (such as a VPN) to perform encryption.
- If the data transmitted by the synch\maint implementation contains a substantial aggregate and it is not encrypted, then this is a Finding.

DS05.0350 Synch\Maint Certificate Validity Checking

<b>STIG ID \ V-Key</b>	<b>DS05.0350 \ V0011772</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Synch\Maint Certificate Validity Checking
<b>IA Controls</b>	IAAC-1
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CS
<b>References</b>	AD STIG 2.3.3.8

**Long Name:** A synch\maint product that utilizes PKI certificates does not perform certificate validation that includes CRL or OCSP checking.

**Checks:**

- Interview the Application SA.
- Review the application documentation or configuration settings to determine if the synch\maint implementation utilizes PKI certificates.
- If PKI certificates are *\*not\** used, then this check is Not Applicable.
- If PKI certificates *\*are\** used, review the application documentation or configuration settings to determine if the product performs certificate validation that includes CRL or OCSP checking.
  - Note that certificates could be used in multiple parts of the implementation such as client authentication of the server *\*and\** server authentication of the client. All uses should be examined.
- If the synch\maint implementation utilizes PKI certificates and the product does not perform certificate validation that includes CRL or OCSP checking, then this is a Finding.

Note: At this time it is understood that SimpleSync, MIIS, and IIFP do *\*not\** perform CRL or OCSP checking.

DS05.0370 Synch\Maint Mutual Authentication

<b>STIG ID \ V-Key</b>	<b>DS05.0370 \ V0011773</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Synch\Maint Mutual Authentication
<b>IA Controls</b>	ECTM-1. ECTM-2
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.8

**Long Name:** A synch\maint implementation does not perform authentication of the synch\maint client and target directory server (mutual authentication).

**Checks:**

- Interview the Application SA.
- Review the application documentation or configuration settings to determine if the synch\maint implementation performs authentication of the synch\maint client \*and\* the target directory server.
  - For client authentication this could include the use of an ID\password for the client to access the server.
  - For the server authentication this could include the use of LDAPS or HTTPS in which the client validates the server's PKI certificate.
- If the synch\maint implementation does not perform mutual authentication, then this is a Finding.

DS05.0380 Synch\Maint Privileged Remote Access Control

<b>STIG ID \ V-Key</b>	<b>DS05.0380 \ V0011774</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Synch\Maint Privileged Remote Access Control
<b>IA Controls</b>	EBRP-1
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CS
<b>References</b>	AD STIG 2.3.4

**Long Name:** Privileged remote access to a synch\maint implementation is not implemented through a managed access control point and with increased session security mechanisms.

**Checks:**

- Interview the Application SA.
- With the assistance of the SA, NSO, or network reviewer as required, review the site network diagram(s) and application documentation to determine if the synch\maint implementation supports and utilizes \*privileged\* remote access.  
- For example, determine if the application SA located in one enclave can access the server hosting the synch\maint implementation in another enclave.  
[Retain this remote access information for use in a subsequent check.]
- If the synch\maint implementation does \*not\* support privileged remote access, then this check is Not Applicable.
- If the synch\maint implementation \*does\* support and utilize privileged remote access, review the site network diagram(s) with the assistance of the SA, NSO, or network reviewer as required, to determine if a managed access control point with increased session security mechanisms (such as two-factor authentication) is used.  
- A remote access server (RAS) located in a DMZ is an example of a compliant solution. Additional information for remote access solutions is located in the Network Infrastructure STIG.
- If the synch\maint implementation supports and utilizes privileged remote access and the appropriate access controls are not used, then this is a Finding.

DS05.0390 Synch\Maint Remote Access Session Logs

<b>STIG ID \ V-Key</b>	<b>DS05.0390 \ V0011775</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Synch\Maint Remote Access Session Logs
<b>IA Controls</b>	EBRP-1
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CS
<b>References</b>	AD STIG 2.3.4

**Long Name:** Sessions for privileged remote access to a synch\maint implementation are not logged or the logs are not reviewed at least weekly.

**Checks:**

- Interview the Application SA.
- If the information obtained in check DS05.0380 indicates the synch\maint implementation does \*not\* support and utilize privileged remote access, then this check is Not Applicable.
- Obtain a copy of the site's policy that addresses privileged remote access.
- Check that the policy addresses the requirements to capture session logs and to review them at least weekly.  
Alternatively review the logs or other evidence that indicates session capture and review.
- If session logs are not captured or the logs are not reviewed at least weekly, then this is a Finding.

DS05.0400 Synch\Maint Non-privileged Remote Access Control

<b>STIG ID \ V-Key</b>	<b>DS05.0400 \ V0011776</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Synch\Maint Non-privileged Remote Access Control
<b>IA Controls</b>	EBRU-1
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CS
<b>References</b>	AD STIG 2.3.4

**Long Name:** Non-privileged remote access to a synch\maint implementation is not implemented through a managed access control point.

**Checks:**

- Interview the Application SA.
- With the assistance of the SA, NSO, or network reviewer as required, review the site network diagram(s) and application documentation to determine if the synch\maint implementation supports and utilizes \*non-privileged\* remote access.
  - For example, determine if a user located in one enclave can access the server hosting the synch\maint implementation in another enclave.  
[Retain this remote access information for use in a subsequent check.]
- If the synch\maint implementation does \*not\* support and utilize non-privileged remote access, then this check is Not Applicable.
- If the synch\maint implementation \*does\* support and utilize non-privileged remote access, review the site network diagram(s) with the assistance of the SA, NSO, or network reviewer as required, to determine if a managed access control point is used.
  - A remote access server (RAS) located in a DMZ is an example of a compliant solution. Additional information for remote access solutions is located in the Network Infrastructure STIG.
- If the synch\maint implementation supports and utilizes non-privileged remote access and a managed access control point is not used, then this is a Finding.

DS05.0410 Synch\Maint Remote Access Encryption

<b>STIG ID \ V-Key</b>	<b>DS05.0410 \ V0011777</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Synch\Maint Remote Access Encryption
<b>IA Controls</b>	EBRU-1
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CS
<b>References</b>	AD STIG 2.3.4

**Long Name:** Remote access to a synch\maint implementation is not encrypted.

**Checks:**

- Interview the Application SA.
- If the information obtained in checks DS05.0380 and DS05.0400 indicate the synch\maint implementation does *\*not\** support and utilize privileged or non-privileged remote access, then this check is Not Applicable.
- If the synch\maint implementation *\*does\** support and utilize remote access, review the application documentation and site network diagram(s) to determine if FIPS 140-2-validated encryption is used to protect the network traffic.
  - This includes encryption of the data on the host before transmission, the use of LDAPS or HTTPS protocol, or the use of network components (such as a VPN) to perform encryption.
- If the synch\maint implementation supports and utilizes remote access and FIPS 140-2-validated encryption is not used, then this is a Finding.

Note: The use of properly configured (as validated through the Windows Checklist) Windows Terminal Services meets this requirement.

DS05.0420 Synch\Maint Server Physical Access

<b>STIG ID \ V-Key</b>	<b>DS05.0420 \ V0011778</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Synch\Maint Server Physical Access
<b>IA Controls</b>	PECF-1, PECF-2
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CS
<b>References</b>	AD STIG 2.3.5

**Long Name:** Physical access to a host used in routine, scheduled synch\maint operations is not restricted to authorized personnel.

**Checks:**

- Interview the Application SA.
- Verify that physical access to hosts used in routine, scheduled synch\maint operations is restricted to authorized personnel.
  - This includes the Windows host(s) holding any synch\maint databases and synch\maint application executables.
- If physical access to a host used in routine, scheduled synch\maint operations is not restricted, then this is a Finding.

---

DS05.0430 Synch\Maint Data Backup

<b>STIG ID \ V-Key</b>	<b>DS05.0430 \ V0011779</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Synch\Maint Data Backup
<b>IA Controls</b>	CODB-1, CODB-2, CODB-3
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.6

**Long Name:** Production data from routine, scheduled synch\maint operations is not backed up periodically.

**Checks:**

- Interview the Application SA.
- Obtain a copy of the site's SOP for backups.
- Check the SOP for the frequency at which data used in routine, scheduled synch\maint operations is backed up.
  - Alternatively, physically verify that backups are being taken.
- If the synch\maint data for a MAC III system is not backed up weekly or at least after each execution, then this is a Finding.
- If the synch\maint data for a MAC I or II system is not backed up daily or at least after each execution, then this is a Finding.

DS05.0450 Synch\Maint Disaster Recovery Documentation

<b>STIG ID \ V-Key</b>	<b>DS05.0450 \ V0011780</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Synch\Maint Disaster Recovery Documentation
<b>IA Controls</b>	COEF-2
<b>MAC /Conf</b>	1-CSP, 2-CSP
<b>References</b>	AD STIG 2.3.6

**Long Name:** Disaster recovery plans do not include identification of products used in routine, scheduled synch\maint operations.

**Checks:**

- Interview the Application SA.
- Obtain a copy of the site's disaster recovery planning documents.
- Verify that the disaster recovery plans include documentation of the products used in routine, scheduled synch\maint operations.
- If the disaster recovery plans do not include documentation of the products, then this is a Finding.

---

DS05.0460 Synch\Maint Security Patch Implementation

<b>STIG ID \ V-Key</b>	<b>DS05.0460 \ V0011781</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Synch\Maint Security Patch Implementation
<b>IA Controls</b>	VIVM-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.7

**Long Name:** Security related patches for synch\maint products are not applied or the application status is not documented.

**Checks:**

- Interview the Application SA.
- Obtain a copy of the site's policy that addresses security patch implementation.
- Verify that the local policy requires all vendor-provided security patches to be applied and the status to be documented for synch\maint products.
- If there is no policy that requires all the vendor-provided security patches to be applied and the status to be documented, then this is a Finding.

---

### 3.6 Active Directory Application Mode Instance

This section is reserved for future interview checks for ADAM instances.

#### **4. AUTOMATED CHECK PROCEDURES**

This section of the Checklist is reserved for the procedures to be used to conduct a review for the *Active Directory STIG* requirements using automated tools.

At this time there are no automated tools to perform a review. The manual procedures described in Section 5 must be used.

This page is intentionally left blank.

## 5. MANUAL CHECK PROCEDURES

This section of the Checklist describes the procedures to be used to conduct a manual review for the *Active Directory STIG* requirements. The results from the procedures in this section can be recorded on a copy of the Review Results Report in Section 2.

### 5.1 Review Process Information

All of the AD domain and forest checks in this document are performed on a Windows domain controller **using a Windows account that is a member of the Domain Admins security group**. While it is possible to perform these checks remotely, the documented procedures assume that the reviewer is using the console of the domain controller.

The checks for synchronization and maintenance products require the input and assistance of the administrator of the application. A Windows account with administrative privileges for the application is required.

It is assumed that the reviewer is familiar with the tools and procedures documented in the Windows Security Checklists. While the procedures in this document are generally explicit, basic procedures such as the process for checking file system ACLs are not documented.

The following tools are used during the review process and are available on all Windows domain controllers:

- Windows Explorer
- Microsoft Management Console (MMC) Snap-ins:
  - AD Users and Computers (dsa.msc)
  - AD Domains and Trusts (domain.msc)
  - AD Sites and Services (dssite.msc)
  - Services (services.msc)
- Registry Editor
- Command Prompt Invocation:
  - Shared resources (net share)
  - Directory Service Query (dsquery.exe) - Win2K3

The following tool is used during the review process and is only available if the Windows Support Tools have been installed:

- Command Prompt Invocation:
  - Support Tools Domain Manager (netdom.exe)

The following information should be available to accelerate the review process:

- AD trust relationship documentation  
[Appendix B provides examples.]
- Lists of accounts assigned to AD privileged groups (Domain Admins, Enterprise Admins, Schema Admins, Group Policy Creator Owners, and Incoming Forest Trust Builders)
- List of accounts with the right to create AD objects (e.g., accounts, printers), but that are not members of the built-in AD privileged groups

- Locations of AD domain controllers and AD sites, relative to the local Enclave network boundaries
- Location of the AD forest root PDC Emulator FSMO domain controller
- Presence of any Windows NT and Windows Server 2003 domain controllers operating in the AD domain.

Please note that it would be significantly more efficient to gather this information prior to the start of a review. Appendix B Section B.1, Pre-Trip Information Gathering, provides lists of interview questions and documentation items that should be used in advance to assemble the required information.

Please reference Appendix D, Directory Information Gathering, for tools and procedures that can be used to gather some of the information required for a review. In particular, Section D.1.3, Identifying Holders of FSMO Roles, can be used to gather the current FSMO information for the AD environment.

## 5.2 Active Directory Domain Controller

**Notes:** The checks in this section apply to assets with a Windows server OS and the Domain Controller role and are performed for **all domain controllers selected for review** in an AD domain. [This may be a sample of one or more domain controllers.]

### 5.2.1 Data \ Program Access Control

The checks in this section address access control for the AD data files and the Windows Support Tools that may update those files.

#### DS00.0120 Directory Data File Access Permissions

<b>STIG ID \ V-Key</b>	<b>DS00.0120 \ V0008316</b>
<b>Severity</b>	Cat I
<b>Short Name</b>	Directory Data File Access Permissions
<b>IA Controls</b>	ECAN-1, ECCD-1, ECCD-2
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CSP
<b>References</b>	AD STIG 2.3.3.3

**Long Name:** Directory service data files do not have proper access permissions (ACLs).

**Checks:**

- Use Registry Editor to navigate to the following:  
HKLM\System\CurrentControlSet\Services\NTDS\Parameters.
- Note the values for:
  - DSA Database file
  - Database log files path
  - DSA Working Directory.
- Using the noted locations, compare the ACLs of the AD database, log, and work files to the specifications in Checklist appendix A.1.1.
- If the actual permissions are not at least as restrictive as those in the appendix, then this is a Finding.
- Use Registry Editor to navigate to the following:  
HKLM\System\CurrentControlSet\Services\NtFrs\Parameters.
- Note the value for: Working Directory.
- Using the noted location, compare the ACL of the FRS directory to the specifications in Checklist appendix A.1.1.
- If the actual permissions are not at least as restrictive as those in the appendix, then this is a Finding.
- At a command line prompt enter “net share”.
- Note the location for the SYSVOL share.
- Using the noted location, compare the ACLs of the GPT directories (GPT parent and GPT Policies directories) to the specifications in Checklist appendix A.1.1.
- If the actual permissions are not at least as restrictive as those in the appendix, then this is a Finding.

DS10.0130 AD Data File Locations

<b>STIG ID \ V-Key</b>	<b>DS10.0130 \ V0008317</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	AD Data File Locations
<b>IA Controls</b>	DCSP-1
<b>MAC /Conf</b>	1-CSP, 2-CSP
<b>References</b>	AD STIG 2.3.1.5

**Long Name:** The AD data files are located on the same logical partition as directories and files owned by users.

**Checks:**

- Refer to the AD database, log, and work file information obtained in check DS00.0120. Note the logical drive (e.g., "C:") on which the files are located.
- At a command line prompt enter "net share".
- Record the logical drive(s) for any site-created shares. [Ignore all system (NETLOGON, SYSVOL, and administrative (ending in \$)) shares.]
- If any site-created shares are located on the same logical drive as the AD database, log, or work files, then this is a Finding.

### DS10.0120 Support Tools Access Permissions

<b>STIG ID \ V-Key</b>	<b>DS10.0120 \ V0008320</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Support Tools Access Permissions
<b>IA Controls</b>	DCSL-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.1.4

**Long Name:** Windows Support Tools program files do not have proper access permissions (ACLs).

**Checks:**

- Start Windows Explorer.
- Right-click the “My Computer” item and select “Search...”
  - Enter “Support\*” in the file name field.
  - Select “Local Hard Drives” in the “Look in:” field.
  - Click the Search button.
- Record the location for the “Support Tools” directory.  
Note: The SA may have installed the Support Tools in an alternate location. If the default directory is not found, ask the SA.
- If the directory is not found and the SA confirms that the Support Tools are not installed, then this check is Not Applicable.
- Using the recorded location, compare the ACL of the Support Tools directory to the specifications in Checklist appendix A.1.2.
- If the actual permissions are not at least as restrictive as those in the appendix, then this is a Finding.

## 5.2.2 Time Synchronization Control

The checks in this section address the need to ensure that the system clock on domain controllers is synchronized and that changes to the time source are logged.

### DS00.0150 Time Synchronization

<b>STIG ID \ V-Key</b>	<b>DS00.0150 \ V0008322</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Time Synchronization
<b>IA Controls</b>	ECTM-1, ECTM-2
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.8

**Long Name:** A time synchronization tool is not implemented on the directory server (domain controller).

**Checks:**

Note: This check is Not Applicable on the forest root domain controller that holds the PDC Emulator FSMO role. (See DS10.0295 for the equivalent for that system.)

The following procedures check the Windows Time service. This is the preferred time synchronization tool for Windows domain controllers.

A. Windows 2000 Server Procedures

- Use Registry Editor to navigate to the following:  
HKLM\System\CurrentControlSet\Services\W32Time\Parameters.
- If the value for “Type” is not “NT5DS” (preferred) or “NTP”, then this is a Finding.

B. Windows Server 2003 Procedures

- Use Registry Editor to navigate to the following:  
HKLM\System\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient.
- If the value for “Enabled” is not “1”, then this is a Finding.
- Use Registry Editor to navigate to the following:  
HKLM\System\CurrentControlSet\Services\W32Time\Parameters.
- If the value for “Type” is not “NT5DS” (preferred), “NTP” or “AllSync”, then this is a Finding.

Note: If these checks indicate a Finding because the NtpClient is not enabled, ask the SA to demonstrate that an alternate time synchronization tool is installed and enabled.

- If the Windows Time service is not enabled and no alternate tool is enabled, then this is a Finding.

### DS00.0151 Time Synchronization Source Logging

<b>STIG ID \ V-Key</b>	<b>DS00.0151 \ V0008324</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Time Synchronization Source Logging
<b>IA Controls</b>	ECTM-1, ECTM-2
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.8

**Long Name:** The time synchronization tool does not log changes to the time source.

**Checks:**

The following procedures check the Windows Time service. This is the preferred time synchronization tool for Windows domain controllers.

A. Windows 2000 Server Procedures

- Use Registry Editor to navigate to the following:  
HKLM\System\CurrentControlSet\Services\W32Time\Parameters.
- If the value for “WriteLog” is not “True” or the value for “Log” is not “0x00000064” or greater, then this is a Finding.
- If the “WriteLog” or “Log” entries are not found, then this is a Finding.

B. Windows Server 2003 Procedures

- Use Registry Editor to navigate to the following:  
HKLM\System\CurrentControlSet\Services\W32Time\Config.
- If the value for “EventLogFlags” is not “2”, then this is a Finding.

If the SA has demonstrated that an alternate time synchronization tool is being used, check to see if the tool can log time source changes. [Review the available configuration options and logs.] If the tool has that capability and it is not enabled, then this is a Finding.

### 5.2.3 Domain Controller Characteristics

The checks in this section address some miscellaneous characteristics that affect the operational integrity of each domain controller.

#### DS10.0140 Domain Controller Dedication

<b>STIG ID \ V-Key</b>	<b>DS10.0140 \ V0008326</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Domain Controller Dedication
<b>IA Controls</b>	DCSP-1
<b>MAC /Conf</b>	1-CSP, 2-CSP
<b>References</b>	AD STIG 2.3.1.5

**Long Name:** The domain controller is not dedicated to that function. It is hosting an application such as a database server, e-mail server, e-mail client, web server, or DHCP server.

**Checks:**

- Start the Services console (“Start”, “Run...”, “services.msc”).
- Check to see if any application-related services have the “Started” status.  
\*Examples\* of some services that indicate the presence of applications are:
  - DHCP Server for DHCP server
  - IIS Admin Service for IIS web server
  - Microsoft Exchange System Attendant for Exchange
  - MSSQLServer for SQL Server
  - ADAM\_[instance] for ADAM directory service.
- If any application-related services have the “Started” status, then this is a Finding.

Note: The Microsoft Windows-based Domain Name System (DNS) server \*is\* an acceptable application because, when securely deployed, it is integrated into AD.

### DS10.0290 Windows Services Startup

<b>STIG ID \ V-Key</b>	<b>DS10.0290 \ V0008327</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Windows Services Startup
<b>IA Controls</b>	ECTM-1, ECTM-2
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.7

**Long Name:** Windows services that are critical for AD are not configured for automatic startup.

**Checks:**

- Start the Services console (“Start”, “Run...”, “services.msc”)
- Check the Startup Type field for the following:
  - Distributed File System
  - DNS Client
  - File Replication Service
  - Intersite Messaging
  - Kerberos Key Distribution Center
  - Windows Time
- If the Startup Type for any of these services is not Automatic, then this is a Finding.

Note: The Windows Time service is not required \*if\* another time synchronization tool is implemented.

## 5.2.4 AD Object Access Permissions and Auditing

The checks in this section address access control and auditing for selected AD objects in the AD database. Access permissions are examined for AD objects including Group Policy Objects and Organizational Units. Auditing is examined for AD objects including Group Policy Objects, Organizational Units, and several other AD domain partition objects.

### DS00.0130 Directory Data Object Access Control

<b>STIG ID \ V-Key</b>	<b>DS00.0130 \ V0002370</b>
<b>Severity</b>	Cat I
<b>Short Name</b>	Directory Data Object Access Control
<b>IA Controls</b>	ECAN-1, ECCD-1, ECCD-2, ECLP-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.4

**Long Name:** Directory service data objects do not have proper access permissions (ACLs). For AD this includes Group Policy Objects and Organizational Units (OUs).

#### Checks:

- A. Group Policy Object Procedures - Site Policies
- Start the Active Directory Sites and Services console (“Start”, “Run...”, “dssite.msc”).
  - Select and expand the Sites item in the left pane.  
For each AD site that is defined (building icon):
    - Right-click the AD site and select the Properties item.
    - On the site Properties window, select the Group Policy tab.
    - For \*each\* Group Policy Object Link:
      - Select the Group Policy Object Link item
      - Select the Properties button.
      - On the site Group Policy Properties window, select the Security tab.
      - Compare the ACL of the site Group Policy to the specifications for Group Policy Objects in Checklist appendix A.3.
  - If the actual permissions for any AD site object are not at least as restrictive as those in the appendix, then this is a Finding.

Note: An AD instance may have no AD site Group Policies defined.

- B. Group Policy Object Procedures - Default Domain & OU Policies
- Start the Active Directory Users and Computers console (“Start”, “Run...”, “dsa.msc”). Ensure that the Advanced Features item on the View menu is enabled.

- Select the left pane item that matches the name of the domain being reviewed.
  - Right-click the domain name and select the Properties item.
  - On the domain Properties window, select the Group Policy tab and then the Properties button.
  - On the Default Domain Policy Properties window, select the Security tab.
  - Compare the ACL of the Default Domain Group Policy to the specifications for Group Policy Objects in Checklist appendix A.3.
- If the actual permissions for the Default Domain Policy Group Policy object are not at least as restrictive as those in the appendix, then this is a Finding.
- Return to the initial console view.
- For each OU that is defined (folder in folder icon):
  - Right-click the OU and select the Properties item.
  - On the OU Properties window, select the Group Policy tab.
  - For \*each\* Group Policy Object Link:
    - Select the Group Policy Object Link item
    - Select the Properties button.
    - On the OU Group Policy Properties window, select the Security tab.
    - Compare the ACL of the OU Group Policy to the specifications for Group Policy Objects in Checklist appendix A.3.
- If the actual permissions for any OU Group Policy object are not at least as restrictive as those in the appendix, then this is a Finding.

Note: Each domain has at least one OU that has a Group Policy. This will be the Domain Controllers OU.

#### C. Organizational Unit Object Procedures

- Start the Active Directory Users and Computers console (“Start”, “Run...”, “dsa.msc”). Ensure that the Advanced Features item on the View menu is enabled.
- For each OU that is defined (folder in folder icon):
  - Right-click the OU and select the Properties item.
  - On the OU Properties window, select the Security tab.
  - Compare the ACL of the OU to the specifications for Organizational Unit Objects in Checklist appendix A.3.
- If the actual permissions for any OU object are not at least as restrictive as those in the appendix, then this is a Finding.

This check replaces the functions of Windows Checklist item 2.013 that was removed from the Windows Checklists.

DS00.0140 Directory Data Object Auditing

<b>STIG ID \ V-Key</b>	<b>DS00.0140 \ V0004243</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Directory Data Object Auditing
<b>IA Controls</b>	ECAR-1, ECAR-2, ECAR-3
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.5

**Long Name:** Directory service data objects do not have proper audit settings. For AD this includes Group Policy Objects and other AD domain partition objects.

**Checks:**

A. Group Policy Object Procedures - Site Policies

- Start the Active Directory Sites and Services console (“Start”, “Run...”, “dssite.msc”).
- Select and expand the Sites item in the left pane.  
For \*each\* AD site that is defined (building icon):
  - Right-click the site and select the Properties item.
  - On the site Properties window, select the Group Policy tab.
  - For \*each\* Group Policy Object Link:
    - Select the Group Policy Object Link item
    - Select the Properties button.
    - On the site Group Policy Properties window, select the Security tab.
    - Select the Advanced button and then the Auditing tab.
    - Compare the audit settings of the site Group Policy to the specifications for Group Policy Objects in Checklist appendix A.4.
- If the actual audit settings for any site Group Policy object are not at least as inclusive as those in the appendix, then this is a Finding.

B. Group Policy Object Procedures - Default Domain & OU Policies

- Start the Active Directory Users and Computers console (“Start”, “Run...”, “dsa.msc”).
- Select the left pane item that matches the name of the domain being reviewed.
  - Right-click the domain name and select the Properties item.
  - On the domain Properties window, select the Group Policy tab and then the Properties button.
  - On the Default Domain Policy Properties window, select the Security tab.
  - Select the Advanced button and then the Auditing tab.
  - Compare the audit settings of the Default Domain Group Policy to the specifications for Group Policy Objects in Checklist appendix A.4.
- If the actual audit settings for the Default Domain Policy Group Policy object are not at least as inclusive as those in the appendix, then this is a Finding.

- Return to the initial console view.
- For \*each\* AD OU that is defined (folder in folder icon):
  - Right-click the OU and select the Properties item.
  - On the OU Properties window, select the Group Policy tab.
  - For \*each\* Group Policy Object Link:
    - Select the Group Policy Object Link item
    - Select the Properties button.
    - On the OU Group Policy Properties window, select the Security tab.
    - Select the Advanced button and then the Auditing tab.
    - Compare the audit settings of the OU Group Policy to the specifications for Group Policy Objects in Checklist appendix A.4.
- If the actual audit settings for any OU Group Policy object are not at least as inclusive as those in the appendix, then this is a Finding.

Note: Each domain has at least one OU that has a Group Policy. This will be the Domain Controllers OU.

#### C. Domain Object Procedures

- Start the Active Directory Users and Computers console (“Start”, “Run...”, “dsa.msc”). Ensure that the Advanced Features item on the View menu is enabled.
- Select the left pane item that matches the name of the domain being reviewed.
  - Right-click the domain name and select the Properties item.
  - On the domain object Properties window, select the Security tab.
  - Select the Advanced button and then the Auditing tab.
  - Compare the audit settings of the domain object to the specifications for Domain Objects in Checklist appendix A.4.
- If the actual audit settings are not at least as inclusive as those in the appendix, then this is a Finding.

#### D. Infrastructure Object Procedures

- Start the Active Directory Users and Computers console (“Start”, “Run...”, “dsa.msc”). Ensure that the Advanced Features item on the View menu is enabled.
- Select the left pane item that matches the name of the domain being reviewed.
  - Right-click the Infrastructure object and select the Properties item.
  - On the Infrastructure object Properties window, select the Security tab.
  - Select the Advanced button and then the Auditing tab.
  - Compare the audit settings of the Infrastructure object to the specifications for Infrastructure Objects in Checklist appendix A.4.
- If the actual audit settings are not at least as inclusive as those in the appendix, then this is a Finding.

#### E. AdminSDHolder Object Procedures

- Start the Active Directory Users and Computers console (“Start”, “Run...”, “dsa.msc”). Ensure that the Advanced Features item on the View menu is enabled.
- Select and expand the left pane item that matches the name of the domain being reviewed.
  - Select the System object.
  - Right-click the AdminSDHolder object and select the Properties item.
  - On the AdminSDHolder object Properties window, select the Security tab.
  - Select the Advanced button and then the Auditing tab.
  - Compare the audit settings of the AdminSDHolder object to the specifications for AdminSDHolder Objects in Checklist appendix A.4.
- If the actual audit settings are not at least as inclusive as those in the appendix, then this is a Finding.

#### F. RID Manager\$ Object Procedures

- Start the Active Directory Users and Computers console (“Start”, “Run...”, “dsa.msc”). Ensure that the Advanced Features item on the View menu is enabled.
- Select and expand the left pane item that matches the name of the domain being reviewed.
  - Select the System object.
  - Right-click the RID Manager\$ object and select the Properties item.
  - On the RID Manager\$ object Properties window, select the Security tab.
  - Select the Advanced button and then the Auditing tab.
  - Compare the audit settings of the RID Manager\$ object to the specifications for RID Manager\$ Objects in Checklist appendix A.4.
- If the actual audit settings are not at least as inclusive as those in the appendix, then this is a Finding.

#### G. Domain Controllers OU Object Procedures

- Start the Active Directory Users and Computers console (“Start”, “Run...”, “dsa.msc”).
- Right-click the Domain Controllers OU and select the Properties item.
  - On the OU Properties window, select the Security tab.
  - Select the Advanced button and then the Auditing tab.
  - Compare the audit settings of the OU to the specifications for Domain Controllers OU Objects in Checklist appendix A.4.
- If the actual audit settings for the Domain Controllers OU object are not at least as inclusive as those in the appendix, then this is a Finding.

This check replaces the functions of Windows Checklist item 2.021 that was removed from the Windows Checklists.

---

### DS10.0210 Synchronize Directory Service Data Right

<b>STIG ID \ V-Key</b>	<b>DS10.0210 \ V0012780</b>
<b>Severity</b>	Cat I
<b>Short Name</b>	Synchronize Directory Service Data Right
<b>IA Controls</b>	ECAN-1, ECCD-1, ECCD-2, ECLP-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.4

**Long Name:** The Synchronize Directory Service Data user right has been assigned to an account.

**Checks:**

- Use the procedures in Section 5.4, “Using the Microsoft Management Console,” of the Windows Checklist to start the Security Configuration and Analysis tool.  
- Note: It is not necessary to use the customized template file for this check. Any file that causes the “Synchronize Directory Service Data Right” to display is sufficient.
- Select and expand the “Security Configuration and Analysis” item in the left pane.
- Select and expand the “Local Policies” item in the left pane.
- Select the “User Rights Assignment” item in the left pane.
- Scroll down to the “Synchronize Directory Service Data Right” item in the right pane.
- Note the values indicated in the Computer Setting column.
- If any accounts (including groups) are assigned the “Synchronize Directory Service Data Right”, then this is a Finding.

This check replaces one rights check from Windows Checklist item 4.010 that was updated in the Windows Checklists.

### 5.3 Active Directory Domain

**Notes:** The checks in this section apply to Active Directory Domain assets and are performed on **only one domain controller per AD domain.**

Some of these checks apply only to Windows Server 2003 and must be done on that platform.

These checks examine characteristics that apply to an entire Windows domain. Because AD data is replicated among its domain controllers, performing these checks on a single (up-to-date) domain controller is sufficient.

#### 5.3.1 Trust Relationships

The checks in this section address the AD trust relationships that are manually created by administrators. This includes external, forest, and realm trusts.

##### DS10.0100 Trust Relationship Documentation

<b>STIG ID \ V-Key</b>	<b>DS10.0100 \ V0008530</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Trust Relationship Documentation
<b>IA Controls</b>	DCID-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.1.2

**Long Name:** Appropriate documentation is not maintained for each external, forest, and realm AD trust relationship.

**Checks:**

- Start the Active Directory Domains and Trusts console (“Start”, “Run...”, “domain.msc”).
- Select the left pane item that matches the name of the domain being reviewed.
  - Right-click the domain name and select the Properties item.
  - On the domain object Properties window, select the Trusts tab.
  - For \*each\* outgoing and incoming external, forest, and realm trust, record the name of the other party (domain name), the trust type, transitivity, and the trust direction.
- [Retain this trust information for use in subsequent checks.]
- Compare the list of actual trusts with the local documentation maintained by the IAO. [See note below.] For each trust the documentation must contain type (external, forest, or realm), name of the other party, MAC and classification level of the other party, trust direction (incoming and/or outgoing), transitivity, status of the Selective Authentication option, and status of the SID filtering option.
- If an actual trust is not listed in the documentation or if any of the required items are not documented, then this is a Finding.

Note: Checklist Appendix B contains samples of trust relationship documentation. While these specific formats are not required, it is highly recommended that all of the information on these samples be represented in the documentation maintained by the IAO.

---

DS10.0170 Trust Relationship Need

<b>STIG ID \ V-Key</b>	<b>DS10.0170 \ V0008533</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Trust Relationship Need
<b>IA Controls</b>	ECAN-1, ECCD-1, ECCD-2
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CSP
<b>References</b>	AD STIG 2.3.3.2

**Long Name:** An external, forest, or realm AD trust relationship is defined where access requirements do not support the need.

**Checks:**

- Refer to the list of actual trusts obtained in check DS10.0100.
- For each of the actual trusts, review the local documentation maintained by the IAO to confirm that the trust supports a known access requirement.  
Note: The objective of this check is verification that there is a \*current\* need for the trust to exist.
- If it cannot be confirmed that each trust supports a known access requirement, then this is a Finding.

### DS10.0180 Trust Relationship Inter-Classification Levels

<b>STIG ID \ V-Key</b>	<b>DS10.0180 \ V0008534</b>
<b>Severity</b>	Cat I
<b>Short Name</b>	Trust Relationship Inter-Classification Levels
<b>IA Controls</b>	ECIC-1
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CS
<b>References</b>	AD STIG 2.3.3.2

**Long Name:** An external, forest, or realm AD trust relationship is defined between systems at different classification levels.

**Checks:**

- Refer to the list of actual trusts obtained in check DS10.0100 and the trust documentation maintained by the IAO. Disregard any trusts with non-DoD organizations as these trusts are examined in check DS10.0181.
- For each of the actual trusts between DoD organizations, compare the classification level (unclassified, confidential, secret, top secret) of the domain being reviewed with the classification level of the other trust party as noted in the IAO documentation.
- If the classification level of the domain being reviewed is different than the classification level of any of the entities for which a trust relationship is defined, then this is a Finding.

DS10.0181 Trust Relationship Inter-Organization

<b>STIG ID \ V-Key</b>	<b>DS10.0181 \ V0008536</b>
<b>Severity</b>	Cat I
<b>Short Name</b>	Trust Relationship Inter-Organization
<b>IA Controls</b>	ECIC-1
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CS
<b>References</b>	AD STIG 2.3.3.2 Network Infrastructure STIG 3.1

**Long Name:** An external, forest, or realm AD trust relationship is defined between a DoD system and a non-DoD system without explicit approval of the DAA and appropriate documentation of the external network connection(s).

**Checks:**

- Refer to the list of actual trusts obtained in check DS10.0100.
- For each of the actual trusts, determine if the other trust party is a non-DoD entity. For example, if the fully qualified domain name of the other party does not end in “.mil”, the other party is probably not a DoD entity.
- Review the local documentation approving the external network connection and documentation indicating explicit approval of the trust by the DAA.  
- The external network connection documentation is maintained by the IAO\NSO for compliance with the Network Infrastructure STIG.
- If any trust is defined with a non-DoD system and there is no documentation indicating approval of the external network connection \*and\* explicit DAA approval of the trust, then this is a Finding.

### DS10.0190 SID Filtering Trust Option

<b>STIG ID \ V-Key</b>	<b>DS10.0190 \ V0008538</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	SID Filtering Trust Option
<b>IA Controls</b>	ECAN-1, ECCD-1, ECCD-2
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CSP
<b>References</b>	AD STIG 2.3.3.2

**Long Name:** An outgoing external or forest trust is configured without SID filtering.

**Checks:**

Note: Currently this check can only be performed using a command line program (netdom.exe) that is installed with the Windows Support Tools. If they are not installed, this check will be Not Reviewed.

A. Windows 2000 Server Procedures

- Start the Active Directory Domains and Trusts console (“Start”, “Run...”, “domain.msc”).
- Select the left pane item that matches the name of the domain being reviewed.
  - Right-click the domain name and select the Properties item.
  - On the domain object Properties window, select the Trusts tab.
  - For \*each\* outgoing external trust:
    - At a command line prompt enter  
 “netdom trust *trusting-domain* /D:*trusted-domain* /filtersids”  
 where *trusting-domain* is the domain being reviewed  
 and *trusted-domain* is the other party to the trust.
- If the output of the netdom commands indicates that SID filtering is not enabled on every outgoing external trust, then this is a Finding.

B. Windows Server 2003 Procedures

- Start the Active Directory Domains and Trusts console (“Start”, “Run...”, “domain.msc”).
- Select the left pane item that matches the name of the domain being reviewed.
  - Right-click the domain name and select the Properties item.
  - On the domain object Properties window, select the Trusts tab.
  - For \*each\* outgoing external and forest trust:
    - At a command line prompt enter  
 “netdom trust *trusting-domain* /D:*trusted-domain* /quarantine”  
 where *trusting-domain* is the domain being reviewed  
 and *trusted-domain* is the other party to the trust.
- If the output of the netdom commands indicates that SID filtering is not enabled on every outgoing external or forest trust, then this is a Finding.

DS10.0200 Selective Authentication Trust Option [Windows Server 2003 DC required]

<b>STIG ID \ V-Key</b>	<b>DS10.0200 \ V0008540</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Selective Authentication Trust Option
<b>IA Controls</b>	ECAN-1, ECCD-1, ECCD-2
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CSP
<b>References</b>	AD STIG 2.3.3.2

**Long Name:** An outgoing forest trust is configured without Selective Authentication.

**Checks:**

Note: This check is performed only on a domain with domain controller(s) running Windows Server 2003. For domains with only Windows 2000 Server domain controllers, this check will be Not Applicable.

- Start the Active Directory Domains and Trusts console (“Start”, “Run...”, “domain.msc”).
- Select the left pane item that matches the name of the domain being reviewed.
  - Right-click the domain name and select the Properties item.
  - On the domain object Properties window, select the Trusts tab.
  - For \*each\* outgoing forest trust:
    - Right-click the trust item and select the Properties item
    - On the trust Properties window, select the Authentication tab.
    - Determine if the Selective Authentication option is selected.
- If the Selective Authentication option is not selected on every outgoing forest trust, then this is a Finding.

### 5.3.2 Privileged Group Membership

The checks in this section address membership in Windows security groups that have privileges with respect to AD data and administrative functions.

#### DS10.0220 Pre-Windows 2000 Compatible Access Membership

<b>STIG ID \ V-Key</b>	<b>DS10.0220 \ V0008547</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Pre-Windows 2000 Compatible Access Membership
<b>IA Controls</b>	ECAN-1, ECCD-1, ECCD-2
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CSP
<b>References</b>	AD STIG 2.3.3.4

**Long Name:** The Pre-Windows 2000 Compatible Access group includes the Everyone or Anonymous Logon groups.

**Checks:**

- Start the Active Directory Users and Computers console (“Start”, “Run...”, “dsa.msc”).
- Select and expand the left pane item that matches the name of the domain being reviewed.
  - Select the Builtin item
  - Double-click the Pre-Windows 2000 Compatible Access group and select the Members tab.
- If the Anonymous Logon group or Everyone group is a member of the Pre-Windows 2000 Compatible group, then this is a Finding.

DS10.0240 Privileged Group Membership - Intra-Forest

<b>STIG ID \ V-Key</b>	<b>DS10.0240 \ V0008548</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Privileged Group Membership - Intra-Forest
<b>IA Controls</b>	ECLP-1, ECPA-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.6

**Long Name:** The number of accounts is excessive or documentation does not exist for the accounts that are members of the Domain Admins, Enterprise Admins, Schema Admins, Group Policy Creator Owners, or Incoming Forest Trust Builders groups.

**Checks:**

- Start the Active Directory Users and Computers console (“Start”, “Run...”, “dsa.msc”).
- Select and expand the left pane item that matches the name of the domain being reviewed.
- Select the Builtin container
  - If the Incoming Forest Trust Builders group is defined:
    - Double-click on the group and select the Members tab
    - Count the number of accounts in the group
    - Compare the accounts in the group with the local documentation.
- Select the Users container
  - For each of the Domain Admins, Enterprise Admins, Schema Admins, and Group Policy Creator Owners groups:
    - Double-click on the group and select the Members tab
    - Count the number of accounts in the group
    - Compare the accounts in the group with the local documentation.
- If an account in a highly privileged AD security group is not listed in the local documentation, then this is a Finding.
- If the number of accounts defined in a highly privileged AD security group is greater than the number below, review the site documentation that justifies this number.
  - For the Enterprise Admins, Schema Admins, Group Policy Creator Owners, and Incoming Forest Trust Builders groups, the number of accounts should be between zero (0) and five (5).
  - The number of Domain Admins should be between one (1) and ten (10).
- If the number of accounts defined in a highly privileged AD security group is greater than the guidance above and there is no documentation that justifies the number, then this is a Finding.

Note: It is possible to move the highly privileged AD security groups out of the AD Users container. If the Domain Admins, Enterprise Admins, Schema Admins, or Group Policy Creator Owners groups are not in the AD Users container, ask the SA for the new location and use that location for this check.

DS10.0250 Privileged Group Membership - Inter-Forest

<b>STIG ID \ V-Key</b>	<b>DS10.0250 \ V0008549</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Privileged Group Membership - Inter-Forest
<b>IA Controls</b>	ECLP-1, ECPA-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.6

**Long Name:** Accounts from another AD forest are members of Windows built-in administrative groups and the other forest is not under the control of the same organization or subject to the same security policies.

**Checks:**

- Start the Active Directory Users and Computers console (“Start”, “Run...”, “dsa.msc”).
- Select and expand the left pane item that matches the name of the domain being reviewed.
- Select the Users container
  - For each of the Domain Admins, Enterprise Admins, Schema Admins, and Group Policy Creator Owners groups:
    - Double-click on the group and select the Members tab
    - Examine the defined accounts to see if they are from a domain that is not in the forest being reviewed.
- Select the Builtin container
  - If the Incoming Forest Trust Builders group is defined:
    - Double-click on the group and select the Members tab
    - Examine the defined accounts to see if they are from a domain that is not in the forest being reviewed.
- If any account in an administrative group is from a domain outside the forest being reviewed and that outside forest is not maintained by the same organization (e.g., enclave) or subject to the same security policies, then this is a Finding.

Note: An account that is from an outside domain appears in the format “outside-domain-NetBIOSname\account” or “account@outside-domain-fully-qualified-name”. Examples are “AOFN21\jsmith” or “jsmith@AOFN21.DISAMIL”. It may be necessary to use the AD Domains and Trusts (domain.msc) console to determine if the domain is from another AD forest.

Note: It is possible to move the highly privileged AD security groups out of the AD Users container. If the Domain Admins, Enterprise Admins, Schema Admins, or Group Policy Creator Owners groups are not in the AD User container, ask the SA for the new location and use that location for this check.

### 5.3.3 Other Domain Characteristics

The checks in this section address some domain-wide characteristics that affect the level of security within an AD domain.

#### DS00.0110 Directory E-mail Attributes

<b>STIG ID \ V-Key</b>	<b>DS00.0110 \ V0008550</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Directory E-mail Attributes
<b>IA Controls</b>	ECAD-1
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CS
<b>References</b>	AD STIG 2.3.3.1

**Long Name:** For a directory service used by e-mail components (server or client), the contractor abbreviation or country code (for foreign nationals) is not maintained for the e-mail address and display name attributes.

**Checks:**

Note: This check addresses domains in which e-mail attributes have been populated on Windows user account definitions. This typically applies to configurations in which MS Exchange 2000 or later is installed in the AD forest of the domain being reviewed. This also applies where directory synchronization software is used to populate these attributes in AD contact entries. This check is Not Applicable for other domains.

- Ask the SA to identify one or more Windows accounts or contacts that are assigned to a foreign national and one or more accounts or contacts that are assigned to a contractor.  
This information is captured on DoD Form 2875. It may be necessary to ask the IAM to provide sample accounts for this check.
- Start the Active Directory Users and Computers console (“Start”, “Run...”, “dsa.msc”).
- Select the Users container or the OU in which the accounts or contacts are defined.  
For *\*each\** of the entries identified:
  - Right-click the entry and select the Properties item
  - Select the General tab
  - Examine the Display name field and the E-mail field.
- If the Display name field and the E-mail field have values, but do not contain the abbreviation “ctr” for contractors and the appropriate country code for foreign nationals, then this is a Finding.

### DS10.0160 Domain Functional Level

<b>STIG ID \ V-Key</b>	<b>DS10.0160 \ V0008551</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Domain Functional Level
<b>IA Controls</b>	ECAN-1, ECCD-1, ECCD-2, ECLP-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.2

**Long Name:** An AD domain that has no Windows NT domain controllers is at a domain functional level that allows the addition of new Windows NT domain controllers.

**Checks:**

- Start the Active Directory Users and Computers console (“Start”, “Run...”, “dsa.msc”).
- Determine if any domain controller in the AD domain being reviewed is running Windows NT:
  - Select the left pane item that matches the name of the domain being reviewed.
  - Right-click the domain name and select the Find item.
  - In the Find dialog box, select Custom Search.
  - Select the Advanced tab.
  - In the Enter LDAP query box, enter the following \*without the quotes or spaces\*:  
“(&(objectCategory=computer)(operatingSystemVersion=4\*)  
(userAccountControl:1.2.840.113556.1.4.803:=8192))”
  - Click the Find Now button.[This procedure is documented in Microsoft KB article 322692.]
- If any domain controller in the AD domain being reviewed is running Windows NT, then this is a Not a Finding.
- Return to the initial console view.
- Determine the domain functional level:
  - Select the left pane item that matches the name of the domain being reviewed.
  - Right-click the domain name and select the Properties item.
  - On the General tab, note the value of “Domain functional level” (Windows Server 2003) or “Domain operation mode” (Windows 2000 Server).
- If the current domain functional level is “Windows 2000 mixed” or “Windows Server 2003 interim” and there are no Windows NT domain controllers in the AD domain, then this is a Finding.

DS10.0270 Domain Object Ownership Quota [Windows Server 2003 only]

<b>STIG ID \ V-Key</b>	<b>DS10.0270 \ V0008552</b>
<b>Severity</b>	Cat IV
<b>Short Name</b>	Domain Object Ownership Quota
<b>IA Controls</b>	ECLP-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.6

**Long Name:** An object ownership quota has not been assigned to accounts that have been delegated the right to create AD objects, but are not members of Windows built-in administrative groups.

**Checks:**

Note: This check is Not Applicable for domains that contain no Windows Server 2003 domain controllers.

This check must be performed on a Windows Server 2003 domain controller.

- Review the local documentation for the list of accounts \*not\* in Windows built-in administrative groups (such as Administrators) that have been delegated the ability to create users or groups. [The Delegation of Control Wizard is one method used to create such accounts.]
- At a command line prompt enter:  
    “dsquery quota domainroot”  
- If there is any output, at a command line prompt enter:  
    “dsquery quota domainroot | dsget quota -acct -qlimit”
- Note the quotas established for each of the users with delegated authority or the default for the domain partition.
- If users with delegated authority exist and there is no domain-wide or user-specific quota established, then this is a Finding.

### DS10.0280 Site Link Replication Properties

<b>STIG ID \ V-Key</b>	<b>DS10.0280 \ V0008553</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Site Link Replication Properties
<b>IA Controls</b>	ECAN-1, ECCD-1, ECCD-2
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CSP
<b>References</b>	AD STIG 2.3.3.7

**Long Name:** An AD site link is defined with schedule and replication interval properties that prevent daily AD replication.

**Checks:**

- Start the Active Directory Sites and Services console (“Start”, “Run...”, “dssite.msc”).
- Select and expand the Sites item in the left pane.
  - Select and expand the Inter-Site Transports item and the IP item in the left pane
  - For \*each\* site link that is defined:
    - Right-click the site link item and select the Properties item
    - Note the interval indicated in the “Replicate every” field
    - Select the Change Schedule button.
    - Using the values indicated for “Replication Available”, determine if the replication interval would allow daily replication to occur. [See note below.]
    - Select the Cancel button for the Schedule window.
    - Select the Cancel button for the Properties window.
- If the replication interval and replication available properties do not allow daily replication, then this is a Finding.

Note: An AD instance may have no AD site links defined.

Note: The following are ways in which site link properties would prevent daily AD replication:

- Setting the “Replicate every” value to a number greater than 1440 (the number of minutes in one day)
- Setting the Schedule value for all hours in a day to “Replication Not Available”.

### DS10.0340 Domain Controller Availability

<b>STIG ID \ V-Key</b>	<b>DS10.0340 \ V0008524</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Domain Controller Availability
<b>IA Controls</b>	COTR-1
<b>MAC /Conf</b>	1-CSP, 2-CSP
<b>References</b>	AD STIG 2.3.6

**Long Name:** Only one domain controller supports an AD domain.

**Checks:**

- Determine the MAC level information for the AD Domain asset.  
- This is available in VMS by using **Asset Finding Maint.** and navigating to the asset or by running an **Asset Information (AS01)** report for the location.
- If the MAC level of the AD Domain is III, this check is Not Applicable.
- Start the Active Directory Users and Computers console (“Start”, “Run...”, “dsa.msc”).
- Select and expand the left pane item that matches the name of the domain being reviewed.
- Select the Domain Controllers [OU] item in the left pane.
- Count the number of computers (objects) in the Domain Controllers OU.
- If there is only one domain controller for a MAC I or II level domain, then this is a Finding.

## 5.4 Active Directory Forest

**Notes:** The checks in this section apply to Active Directory Forest assets and are performed on **only one or two domain controllers per AD forest** according to forest configuration as follows:

- DS10.0230 applies only for Windows Server 2003 and must be done on that platform.
- DS10.0295 applies only to the domain controller that holds the authoritative time source for the forest. When the Windows Time service is used, that is the root domain controller that holds the PDC Emulator FSMO role.

The checks in this section address some forest-specific characteristics that affect the level of security within an AD forest.

### DS10.0230 dsHeuristics Option [Windows Server 2003 only]

<b>STIG ID \ V-Key</b>	<b>DS10.0230 \ V0008555</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	dsHeuristics Option
<b>IA Controls</b>	ECAN-1, ECCD-1, ECCD-2
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CSP
<b>References</b>	AD STIG 2.3.3.4

**Long Name:** The dsHeuristics option is not configured to prevent anonymous access to AD.  
**Checks:**

Note: This check is Not Applicable for domains that contain no Windows Server 2003 domain controllers.

This check must be performed on a Windows Server 2003 domain controller.

- At a command line prompt enter (on a single line):  
`dsquery * "cn=directory service,cn=windows nt,cn=services,  
cn=configuration,dc=forest-name" -attr *`  
where *forest-name* is the fully qualified LDAP name of the root of the domain being reviewed.
- If the dsHeuristics attribute is listed, note the assigned value.
- If the dsHeuristics attribute is defined and has a “2” in the seventh character, then this is a Finding.

Note: An example of the dsquery command for the vcfm.disaost.mil forest is:

```
dsquery * "cn=directory service,cn=windows nt,cn=services,  

cn=configuration,dc=vcfn,dc=disaost,dc=mil" -attr *
```

Note: Examples of values that would be a Finding are: “0000002”, “0010002”, “0000002000001”.

DS10.0295 Time Synchronization - Forest Authoritative Source  
[Forest Root Domain PDC Emulator DC only]

<b>STIG ID \ V-Key</b>	<b>DS10.0295 \ V0008557</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Time Synchronization - Forest Authoritative Source
<b>IA Controls</b>	ECTM-1, ECTM-2
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.8

**Long Name:** The domain controller holding the forest authoritative time source is not configured to use a DoD-authorized external time source.

**Checks:**

Note: This check is Not Applicable for Component locations that do not have the AD forest root domain on site.

This check must be performed on the domain controller in the \*forest root domain\* that holds the PDC Emulator FSMO role.

The following procedures check the Windows Time service. This is the preferred time synchronization tool for Windows domain controllers.

A. Windows 2000 Server Procedures

- Use Registry Editor to navigate to the following:  
HKLM\System\CurrentControlSet\Services\W32Time\Parameters.
- If the value for “Type” is not “NTP”, then this is a Finding.

B. Windows Server 2003 Procedures

- Use Registry Editor to navigate to the following:  
HKLM\System\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient.
- If the value for “Enabled” is not “1”, then this is a Finding.
- Use Registry Editor to navigate to the following:  
HKLM\System\CurrentControlSet\Services\W32Time\Parameters.
- If the value for “Type” is not “NTP”, then this is a Finding.

Note: If these checks indicate a Finding because the NtpClient is not enabled, ask the SA to demonstrate that an alternate time synchronization tool is installed and enabled.

- If the Windows Time service is not enabled and no alternate tool is enabled, then this is a Finding.

## 5.5 Directory Service Synchronization \ Maintenance Application

The checks in this section apply to Synch\Maint App assets and are performed on **each system** on which a directory synchronization or maintenance product is installed.

These products include CPS Systems SimpleSync, Microsoft Identity Integration Server (MIIS), and Microsoft Identity Integration Feature Pack (IIFP).

The checks in this section require input from the administrator of the synchronization or maintenance product. In the text this administrator is referred to as the “application SA”.

### DS05.0120 Synch\Maint Cryptographic Use

<b>STIG ID \ V-Key</b>	<b>DS05.0120 \ V0011782</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Synch\Maint Cryptographic Use
<b>IA Controls</b>	DCNR-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.1.2

**Long Name:** An encryption, signing, or other cryptographic algorithm used in a directory synchronization or maintenance application is not FIPS 140-2 validated.

**Checks:**

- With the assistance of the application SA, display the cryptographic (signing or encryption) configuration settings for the synchronization or maintenance application.
  - The use of SSL\TLS-based communication protocols such as LDAPS or HTTPS indicates that cryptographic algorithms are being used.
  - For applications using LDAPS or HTTPS this includes displaying the PKI certificate(s) being used.
- If the cryptographic use involves PKI certificates and those certificates are issued by the DoD PKI, then this is a Not a Finding.
- If the cryptographic use involves PKI certificates and those certificates are \*not\* issued by the DoD PKI, review the application documentation that indicates the cryptographic implementation has been validated to the FIPS 140-2 standard.
- If the cryptographic use involves other implementations (such as file encryption), review the application documentation that indicates the cryptographic implementations have been validated to the FIPS 140-2 standard.
- If there is no documentation that the cryptographic implementation has been validated to the FIPS 140-2 standard, then this is a Finding.

Note: Documentation for validated cryptographic implementations is available at the NIST web site (<http://csrc.nist.gov/cryptval/>).

DS05.0220 Synch\Maint PKI Certificate Source

<b>STIG ID \ V-Key</b>	<b>DS05.0220 \ V0011783</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Synch\Maint PKI Certificate Source
<b>IA Controls</b>	IAKM-1, IAKM-2, IATS-1, IATS-2
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.2

**Long Name:** PKI certificates used in a directory synchronization or maintenance application are not issued by the DoD PKI.

**Checks:**

- With the assistance of the application SA, display all PKI certificate(s) being used by the synchronization or maintenance application.
  - For applications accessing directory data through LDAPS, this would include the certificate installed on the directory server.
  - For MIIS\IIFP or SimpleSync accessing AD, this would include the domain controller certificate.
  - For applications accessing directory data through HTTPS, this would include the certificate installed on the web server that provides DSML access.
- If any PKI certificate being used in a synchronization or maintenance function is not issued by the DoD PKI and there is no written plan to implement DoD PKI certificates (per the note below), then this is a Finding.

Note: Prior to DoD PKI support for Windows domain controller certificates, some Components established alternate (Microsoft Windows-based) Certificate Authorities (CAs) to provide certificates. As of December 2005, Windows domain controller certificates are available from the DoD PKI. Per guidance in JTF-GNO Communications Tasking Order (CTO) 06-02, a plan to implement DoD PKI certificates must be established no later than 31 July 2006.

DS05.0160 Synch\Maint Non-Supported Release

<b>STIG ID \ V-Key</b>	<b>DS05.0160 \ V0011784</b>
<b>Severity</b>	Cat I
<b>Short Name</b>	Synch\Maint Non-Supported Release
<b>IA Controls</b>	DCSL-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.1.4

**Long Name:** A non-vendor supported directory synchronization or maintenance product is in use.

**Checks:**

- With the assistance of the application SA, display the version \ release information for the synchronization or maintenance product.
  - For Windows applications, this is typically done using the Help | About menu item.
- Compare the installed version \ release information with the vendor's current product documentation.
  - For SimpleSync v3, release 3.4.3.x is the oldest supported version.
  - For SimpleSync v3, support will be discontinued as of Oct 1, 2006.
  - For SimpleSync v4, release 4.1.1 is the oldest supported version.
  - For Microsoft Metadirectory Services (MMS), there are no versions that are currently supported.
  - For MIIS\IIFP, all currently available versions are supported.
- If a synchronization or maintenance product for which there is no vendor support is installed, then this is a Finding.

Note: The following web sites may be useful for determining product support status:

- Microsoft: <http://support.microsoft.com/gp/lifeselectindex>
- CPS Systems: <http://www.cps-systems.com/kb/>

DS05.0190 Synch\Maint Public Domain Software

<b>STIG ID \ V-Key</b>	<b>DS05.0190 \ V0011785</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Synch\Maint Public Domain Software
<b>IA Controls</b>	DCPD-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.1.4

**Long Name:** Public domain software is used to perform directory synchronization or maintenance operations.

**Checks:**

- Search for instances of known public domain software:
  - Start Windows Explorer.
  - Right-click the “My Computer” item and select “Search...”
  - For each of the following program names:
    - adfind.exe, admod.exe, shedit.exe, and shedit2k3.exe
  - Enter the program name in the file name field.
  - Select “Local Hard Drives” in the “Look in:” field.
  - Click the Search button.
- Ask the SA or application SA to confirm that no other public domain software is being used to perform synchronization or maintenance operations.
- If instances of public domain software are installed and this software has not been assessed for information assurance impacts and approved explicitly by the DAA, then this is a Finding.

Note: This check and the associated requirement are based on DoD policy on the use of software for which original source code is not available \*and\* there is limited or no warranty or support. In these circumstances, the inability to examine or review potential vulnerabilities represents an unknown and unacceptable risk.

DS05.0200 Synch\Maint Code \ Data File Locations

<b>STIG ID \ V-Key</b>	<b>DS05.0200 \ V0011786</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Synch\Maint Code \ Data File Locations
<b>IA Controls</b>	DCSP-1
<b>MAC /Conf</b>	1-CSP, 2-CSP
<b>References</b>	AD STIG 2.3.1.5

**Long Name:** The source code for a directory synchronization or maintenance application is located in the same directory as data that is input to or output from the application.

**Checks:**

- With the assistance of the application SA, determine the directories containing synchronization or maintenance program *\*source\** files and a list of the directories containing *\*data\** files read or written by the synchronization or maintenance application.  
[Retain this *\*data\** file location information for use in subsequent checks.]
- Compare the names of directories containing program source files with those containing input or output data.
- If synchronization or maintenance program source files are contained in the same directory as input or output data, then this is a Finding.

Note: This check *\*does\** apply to cases where COTS applications have been extended or modified by the addition of local programs. For example, locally written Management Agents (MAs) for MIIS are included in the scope of this check.

DS05.0150 Synch\Maint Software File Access Permissions

<b>STIG ID \ V-Key</b>	<b>DS05.0150 \ V0011787</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Synch\Maint Software File Access Permissions
<b>IA Controls</b>	DCSL-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.1.4

**Long Name:** Directory synchronization or maintenance program or configuration files do not have proper access permissions (ACLs).

**Checks:**

- With the assistance of the application SA, determine the directories containing synchronization or maintenance program \*executable\* and configuration files.
- Using the locations determined, compare the ACLs of the directories to the specifications in Checklist appendix A.1.3.
- If the actual permissions are not at least as restrictive as those in the appendix, then this is a Finding.

DS05.0230 Synch\Maint Data File Access Permissions

<b>STIG ID \ V-Key</b>	<b>DS05.0230 \ V0011788</b>
<b>Severity</b>	Cat I
<b>Short Name</b>	Synch\Maint Data File Access Permissions
<b>IA Controls</b>	ECAN-1, ECCD-1, ECCD-2
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CS
<b>References</b>	AD STIG 2.3.3.3

**Long Name:** Directory synchronization or maintenance data files do not have proper access permissions (ACLs).

**Severity Override Guidance:**

- The severity category for Findings resulting from this check must be determined based on the content of the file involved.
  - If any file includes identification or authentication data (e.g., accounts, passwords, or password hash data) that will be used by systems to determine access control, then the severity is category I.
  - If all files include other directory information such as names, titles, and e-mail addresses, then the severity is category II.
  - If the content of the files is unknown, then the severity is category I.

**Checks:**

- Refer to the list of the directories containing synchronization or maintenance \*data\* obtained in check DS05.0200.
- With the assistance of the application SA, determine the nature of the content of the data files:
  - Determine if any file includes identification or authentication data (e.g., accounts, passwords, or password hash data) that will be used by systems to determine access control.
- Using the locations determined, compare the ACLs of the directories to the specifications in Checklist appendix A.1.4.
- If the actual permissions are not at least as restrictive as those in the appendix, then this is a Finding.

DS05.0240 Synch\Maint Aggregate Data File Encryption

<b>STIG ID \ V-Key</b>	<b>DS05.0240 \ V0011789</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Synch\Maint Aggregate Data File Encryption
<b>IA Controls</b>	ECCR-1, ECCR-2
<b>MAC /Conf</b>	1-CS, 2-CS, 3-CS
<b>References</b>	AD STIG 2.3.3.3

**Long Name:** A directory synchronization or maintenance data file that contains a substantial aggregate of the directory data for an entire geographic command is not encrypted.

**Checks:**

- With the assistance of the application SA, determine the geographic scope of the data in the synchronization or maintenance data files in the directories obtained in check DS05.0200. Specifically, determine if the data contains directory information for an \*entire\* geographic command such as DISA CONUS, DISA EUROPE, or DISA PACIFIC or for \*all\* members of a Service or other Component.
- If the synchronization or maintenance data files do not contain substantial aggregates, then this check is Not Applicable.
- If any synchronization or maintenance data file does contain a substantial aggregate, determine with the assistance of the application SA if the file is encrypted.
  - The use of a text editor to attempt to view the encrypted file or a Windows directory display indicating the file has the encrypted attribute can be used.
- If any synchronization or maintenance data file containing a substantial aggregate is not encrypted, then this is a Finding.

Note: This check is used to determine only \*if\* file encryption is used. Check DS05.0120 would be applied to determine if the implemented encryption is FIPS 140-2 validated.

DS05.0250 Synch\Maint Program Auditing

<b>STIG ID \ V-Key</b>	<b>DS05.0250 \ V0011790</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Synch\Maint Program Auditing
<b>IA Controls</b>	ECAT-1, ECAT-2
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.5

**Long Name:** A directory synchronization or maintenance application is not configured to collect audit data.

**Checks:**

- With the assistance of the application SA, determine the auditing components of the synchronization or maintenance application.
  - When supported by the product, review the audit configuration settings for the product.
  - Alternatively review logs or other evidence that indicates that audit data is being collected.
- If the synchronization or maintenance application is not configured to collect audit data, then this is a Finding.

DS05.0260 Synch\Maint Audit Data Tools

<b>STIG ID \ V-Key</b>	<b>DS05.0260 \ V0011791</b>
<b>Severity</b>	Cat III
<b>Short Name</b>	Synch\Maint Audit Data Tools
<b>IA Controls</b>	ECRG-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.5

**Long Name:** Tools are not installed to support reviewing audit data from a directory synchronization or maintenance application.

**Checks:**

- With the assistance of the application SA, invoke the tool used to review the audit data for the synchronization or maintenance application.
  - If the audit data is collected in a Windows Event Log, then the Event Viewer would be used for this demonstration.
- If no tools are installed to allow the audit data to be reviewed, then this is a Finding.

DS05.0290 Synch\Maint Audit Data Access Permissions

<b>STIG ID \ V-Key</b>	<b>DS05.0290 \ V0011792</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Synch\Maint Audit Data Access Permissions
<b>IA Controls</b>	ECTP-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.5

**Long Name:** Directory synchronization or maintenance audit data files do not have proper access permissions (ACLs).

**Checks:**

Note: This check is Not Applicable if the audit data is collected in a Windows Event Log. [Windows Event Log access control is reviewed in the Windows Checklist.]

- With the assistance of the application SA, determine the directories containing audit data files for the synchronization or maintenance application.
- Using the locations determined, compare the ACLs of the directories to the specifications in Checklist appendix A.1.5.
- If the actual permissions are not at least as restrictive as those in the appendix, then this is a Finding.

DS05.0300 Synch\Maint Application Account Membership

<b>STIG ID \ V-Key</b>	<b>DS05.0300 \ V0011793</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Synch\Maint Application Account Membership
<b>IA Controls</b>	ECLP-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.6

**Long Name:** An account used for a directory synchronization or maintenance application is a member of a Windows built-in administrative group.

**Checks:**

- With the assistance of the application SA, identify the application account(s) used to access directory data for any synchronization or maintenance application. [Retain this account information for use in a subsequent check.]
- For *\*each\** application account that is a local (*\*not\** AD domain) user account,
  - At a command line prompt enter: “net user *account*”  
where *account* is the synch\maint application account.
  - Note the Full Name and Group Membership information.
- For *\*each\** application account that is a domain user account,
  - At a command line prompt enter: “net user *account* /domain”  
where *account* is the synch\maint application account.
  - Note the Full Name and Group Membership information.
- If any synchronization or maintenance application account is a member of the Administrators, Domain Admins, Enterprise Admins, or Schema Admins groups, then this is a finding.

DS05.0310 Synch\Maint Application Account Dedication

<b>STIG ID \ V-Key</b>	<b>DS05.0310 \ V0011794</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	Synch\Maint Application Account Dedication
<b>IA Controls</b>	ECLP-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.6

**Long Name:** An account used for a directory synchronization or maintenance application is not dedicated for that function.

**Checks:**

- Refer to the list of application accounts obtained in check DS05.0300.
- For \*each\* application account:
  - Examine the Full Name information to determine if the account may be assigned as a user account (instead of an application account).
  - If the information is ambiguous, ask the SA to confirm whether the account is assigned as a user or application account.
- If any synchronization or maintenance application account is assigned as a user account, then this is a finding.

## 5.6 Active Directory Application Mode Instance

The checks in this section apply to ADAM Instance assets and are performed on **each** system on which ADAM is installed.

### DS15.0100 ADAM Host OS

<b>STIG ID \ V-Key</b>	<b>DS15.0100 \ V0008343</b>
<b>Severity</b>	Cat I
<b>Short Name</b>	ADAM Host OS
<b>IA Controls</b>	ECAR-1, ECAR-2, ECAR-3
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.5

**Long Name:** ADAM is installed on a host OS that does not support adequate auditing for ADAM.

**Checks:**

- Execute the Windows version reporter (“Start”, “Run...”, “winver.exe”).
- If the “About Windows” window indicates Windows XP, then this is a finding.

DS15.0110 ADAM Service Account

<b>STIG ID \ V-Key</b>	<b>DS15.0110 \ V0008344</b>
<b>Severity</b>	Cat II
<b>Short Name</b>	ADAM Service Account
<b>IA Controls</b>	ECLP-1
<b>MAC /Conf</b>	1-CSP, 2-CSP, 3-CSP
<b>References</b>	AD STIG 2.3.3.6

**Long Name:** An ADAM service account is a member of a Windows built-in administrative group.

**Checks:**

- A. Determine ADAM service accounts
- Start the Services console (“Start”, “Run...”, “services.msc”)
  - Identify the individual services for ADAM instances.  
These names are usually of the form “ADAM\_instance”, where *instance* is the name chosen during installation.
  - For *each* ADAM instance service:
    - Note the entry in the LogOnAs field.
  - If the service account used for all ADAM instances is the Network Service account, then there is *no* Finding.
- B. Check ADAM service accounts group membership
- For *each* ADAM service account that is a local (*not* domain) user account,
    - At a command line prompt enter: “net user *account*”  
where *account* is the ADAM service account.
    - Note the Group Membership information.
  - For *each* ADAM service account that is a domain user account,
    - At a command line prompt enter: “net user *account* /domain”  
where *account* is the ADAM service account.
    - Note the Group Membership information.
  - If any ADAM service account is a member of the Administrators, Domain Admins, Enterprise Admins, or Schema Admins groups, then this is a finding.

This page intentionally blank.

## APPENDIX A: OBJECT PERMISSIONS AND AUDIT SETTINGS

This appendix of the Checklist provides requirements for compliance with the *Active Directory STIG* for the ACLs of Windows file, registry, and AD objects and for audit settings for select AD objects.

### A.1 File and Directory Permissions

The permissions in this section refer to the ACL of the specified directories or files.

**Notes:** It is generally acceptable for an object's access control to be more restrictive than the settings specified in this document.

#### A.1.1 AD Data Permissions

##### AD Database, Log, and Work Files

Component	Object	Account Name	Type	Access
Database	...\ntds.dit	Administrators SYSTEM CREATOR OWNER* Local Service*	Allow Allow Allow	Full Control Full Control [None on file] Create Folders / Append Data
Log files and log reserve files	...\edb*.log, ...\res1.log ...\res2.log	Administrators SYSTEM CREATOR OWNER* Local Service*	Allow Allow Allow	Full Control Full Control [None on file] Create Folders / Append Data
Work files	...\temp.edb ...\edb.chk	Administrators SYSTEM CREATOR OWNER* Local Service*	Allow Allow Allow	Full Control Full Control [None on file] Create Folders / Append Data

The permissions for the account names with an asterisk in the table are only needed for Windows Server 2003.

##### FRS Directory

Component	Object	Account Name	Type	Access
FRS directory	...\Ntfrs	Administrators SYSTEM	Allow Allow	Full Control Full Control

**GPT (SYSVOL) Directories**

Component	Object	Account Name	Type	Access
GPT parent directory	...\SYSVOL	Administrators	Allow	Full Control Read, Read & Execute, List Folder Contents [None on dir.] Read, Read & Execute, List Folder Contents Full Control
		Authenticated Users	Allow	
		CREATOR OWNER Server Operators	Allow	
GPT policies directory	...\SYSVOL\ domain\Policies	Administrators	Allow	Full Control Read, Read & Execute, List Folder Contents [None on dir.] Read, Read & Execute, List Folder Contents, Modify, Write Read, Read & Execute, List Folder Contents Full Control
		Authenticated Users	Allow	
		CREATOR OWNER Group Policy Creator Owners	Allow	
		Server Operators	Allow	
		SYSTEM	Allow	

**A.1.2 Windows Support Tools Permissions**

Object	Account Name	Type	Access
...\%ProgramFiles%\ Support Tools\	Administrators	Allow	Full Control Full Control Read, Execute  With propagation
	SYSTEM	Allow	
	[Other IAO-authorized groups]	Allow	

**A.1.3 Synchronization\Maintenance Software Permissions**

Component	Account Name	Type	Access
Synch\Maint Software and Config Files	Administrators	Allow	Full Control
	[App account]	Allow	Read, Execute
	[App SAs]	Allow	Full Control
	SYSTEM	Allow	Full Control

### A.1.4 Synchronization\Maintenance Data Permissions

Component	Account Name	Type	Access
Synch\Maint Data Files	Administrators	Allow	Full Control
	[App account]	Allow	Full Control
	[App SAs]	Allow	Full Control
	[IAO-approved users]	Allow	Read, Execute
	SYSTEM	Allow	Full Control

### A.1.5 Synchronization\Maintenance Audit Data Permissions

Component	Account Name	Type	Access
Synch\Maint audit data	Administrators	Allow	Read, Execute
	[App account]	Allow	Full Control
	[App SAs]	Allow	Read, Execute
	[Auditors group]	Allow	Full Control
	SYSTEM	Allow	Full Control

## A.2 Registry Key Permissions

At this time there are no specific registry key permission checks for compliance with the *Active Directory STIG*.

It is assumed that the registry key permission checks in the applicable Windows Security Checklist have been applied.

## A.3 AD Object Permissions

The permissions in this section refer to the ACL of the specified AD database objects.

**Notes:** It is generally acceptable for an object's access control to be more restrictive than the settings specified in this document.

### Group Policy Objects

Object	Account Name	Type	Access
[Group Policy - e.g., Default Domain]	Administrators	Allow	Full Control
	Creator Owner	Allow	Full Control
	SYSTEM	Allow	Full Control
	ENTERPRISE DOMAIN CONTROLLERS*	Allow	Read
	Authenticated Users [or other user groups]	Allow	Read Apply Group Policy

Notes: - Groups containing authenticated users (such as the Authenticated Users group), other locally created user groups, and individual users \*may\* have the Read and Apply Group Policy permissions set to Allow or Deny.

- The Anonymous Logon, Guests, or any group that contains those groups (in which users are not uniquely identified and authenticated) must *\*not\** have any access permissions unless the group and justification is explicitly documented with the IAO.
- Other access permissions that allow the objects to be *\*updated\** are considered findings unless specifically documented by the IAO.
- The permissions for the account names with an asterisk in the table are only needed for Windows Server 2003.

### Organizational Unit (OU) Objects

Object	Account Name	Type	Access
[Organizational Unit - e.g., Domain Controllers]	Administrators	Allow	Full Control
	Creator Owner	Allow	Full Control
	SYSTEM	Allow	Full Control
	Authenticated Users [or other user groups]	Allow	Read

If an IAO-approved distributed administration model [help desk or other user support staff] is implemented, permissions above Read may be allowed for groups documented by the IAO.

### A.4 AD Object Audit Settings

The audit settings in this section refer to the settings of the specified AD database objects.

**Notes:** It is generally acceptable for an object's audit settings to be more inclusive than the settings specified in this document.

### Group Policy Objects [Includes Site, Default Domain, and OU GPOs]

Type	Account	Access	Scope
Fail	Everyone	[All access types]	Object and all child objects
Success	Everyone	Modify Permissions Write All Properties	groupPolicyContainer objects

Note: The best method of **applying** audit settings for all the Group Policy Objects is by configuring the settings on the Policies container (within the domain's System container) and specifying inheritance.

### Domain Object

Type	Account	Access	Scope
Fail	Everyone	[All access types]	<i>Domain object only</i>
Success	Everyone	Write All Properties Modify Permissions Modify Owner	<i>Domain object only</i>
Success	Administrators	All Extended Rights	<i>Domain object only</i>
Success	Domain Users	All Extended Rights	<i>Domain object only</i>

**Infrastructure Object**

Type	Account	Access	Scope
Fail	Everyone	[All access types]	Infrastructure object only
Success	Everyone	All Extended Rights Write All Properties	Infrastructure object only

**AdminSDHolder Object**

Type	Account	Access	Scope
Fail	Everyone	[All access types]	AdminSDHolder object only
Success	Everyone	Modify Permissions Modify Owner Write All Properties	AdminSDHolder object only

**RID Manager\$ Object**

Type	Account	Access	Scope
Fail	Everyone	[All access types]	RID Manager\$ object only
Success	Everyone	All Extended Rights Write All Properties	RID Manager\$ object only

**Domain Controllers OU Object**

Type	Account	Access	Scope
Fail	Everyone	[All access types]	Domain Controllers OU and all child objects
Success	Everyone	Modify Permissions Modify Owner Create All Child Objects Delete Delete All Child Objects Delete Subtree	Domain Controllers OU only
Success	Everyone	Write All Properties	Domain Controllers OU and all child objects

This page intentionally blank.

## APPENDIX B: DOCUMENTATION

This appendix of the Checklist provides information about the documentation associated with a review of an AD environment. The initial section describes documentation to be obtained prior to the review trip. Subsequent sections offer examples of documentation used to satisfy requirements.

### B.1 Pre-Trip Information Gathering

This section of the appendix provides guidance about information to gather in advance of a review trip. The SRR Team Lead or Reviewer should obtain as much information as possible prior to arrival on-site. The information obtained will greatly assist the Reviewer in completing the checks and reduce the time required to complete the review.

The SRR Team Lead or Reviewer contacts the site being reviewed to identify the Point of Contact (POC) who will provide the required Pre-Trip AD information. This POC is responsible for ensuring the questions in Section B.1.1, *Pre-Trip Interview Questions* are completely answered, and for providing the required documents and procedures listed in Section B.1.2, *Pre-Trip Documentation*.

#### B.1.1 Pre-Trip Interview Questions

The SRR team members must make every attempt to answer the questions listed below prior to arriving on-site. The Team Lead, Reviewer, and site POC should work as a team to capture the required information to the fullest extent possible.

- a. How many Windows Domain Controllers are on-line at the site?
- b. Are there any Windows NT domain controllers in the AD domain?
- c. Does the site administer the AD domain?  
If not, provide POC information (name, phone number, and email address) of the responsible party.
- d. Does the site administer the AD forest?  
If not, provide POC information (name, phone number, and email address) of the responsible party.
- e. Does the site administer domain controllers at remote locations?  
If so, identify the locations for which the site is responsible.
- f. Does the site have a directory service synchronization or maintenance application product such as CPS Systems SimpleSync, Microsoft Identity Integration Server (MIIS) or Microsoft Identity Integration Feature Pack (IIFP) installed on any systems?
- g. Does the site have Active Directory Application Mode (ADAM) installed on any systems?

### **B.1.2 Pre-Trip Documentation**

The SRR team members must make every attempt to obtain copies of the documents and procedures listed below prior to arriving on-site. The SRR team members work with the site POC to capture the required information to the fullest extent possible.

#### Documents:

- a. Network diagram displaying AD architecture (forest hierarchy) including the location of Flexible Single-Master Operations (FSMO) domain controllers. The location of premise routers and any Intrusion Detection Systems should also be displayed.
- b. Password Policy
- c. List of accounts assigned to AD privileged groups including Domain Admins, Enterprise Admins, Schema Admins, Group Policy Creator Owners, and Incoming Forest Trust Builders
- d. List of accounts that are not members of the AD privileged groups, but do have (delegated) permission to create or change AD objects
- e. List of AD trust relationships, their characteristics, and the access requirement(s) that the trusts support
- f. Trust relationship documentation

#### Procedures:

- a. Standard Operating Procedures (SOP) for data backup
- b. Supplemental INFOCON response procedures, including any AD trust-specific actions
- c. Configuration management procedures that apply to AD schema updates
- d. Disaster recovery procedures, including any AD-specific actions

The SRR team members will obtain copies of all listed documentation and procedures for examination. The Team Lead or Reviewer should request the documentation from the site's POC in any one of the following formats, listed in the order of preference:

- CD-ROM
- Diskette
- Signed, encrypted e-mail
- Paper.

## B.2 AD Documentation Examples

This section of the appendix provides examples of documentation that could be used to meet requirements for compliance with the *Active Directory STIG*.

### B.2.1 Trust Relationship Documentation

The following subsections provide examples of documentation to satisfy trust relationship requirements. Note that some trust attributes are relevant only to specific configurations as follows:

- Selective Authentication is not applicable (N/A) for realm trusts or any incoming trusts.
- SID Filtering is not applicable (N/A) for realm trusts or any incoming trusts.

#### B.2.1.1 Example Trust Relationship Documentation - Child Domain

The following example documents trust relationships for a domain that has established two unidirectional external trusts with one other domain and a realm trust with a Kerberos domain.

AD Trust Relationship Documentation							
A. Domain NetBIOS name: <u>NORTH</u>						Verified: <u>Mar 2006</u>	
Fully Qualified Domain Name: <u>NORTH.AOFN21.DISA.MIL</u>							
B. Classification: <u>Unclass</u>							
C. MAC: <u>II</u> Confidentiality: <u>Sensitive</u>							
D. Trusts Defined:							
Type	Other Party (NetBIOS\FQDN)	MAC	Classif.	Direction	Transitive	Selective Auth	SID Filtering
<u>External</u>	<u>MEFN19 \ MEFN19.USN.MIL</u>	<u>II</u>	<u>Unclass</u>	<u>Outgoing</u>	<u>N/A</u>	<u>Yes</u>	<u>Yes</u>
<u>External</u>	<u>MEFN19 \ MEFN19.USN.MIL</u>	<u>II</u>	<u>Unclass</u>	<u>Incoming</u>	<u>N/A</u>	<u>N/A</u>	<u>N/A</u>
<u>Realm</u>	<u>UNI91</u>	<u>II</u>	<u>Unclass</u>	<u>Outgoing</u>	<u>No</u>	<u>N/A</u>	<u>N/A</u>

E. Access Requirements:	
<b>Other Party</b> (NetBIOS\FQDN)	<b>Access Requirements</b>
<u>MEFN19 \ MEFN19.USN.MIL</u>	- <u>NORTH users access personnel files in the MEFN19 domain.</u> - <u>MEFN users access inventory files in the NORTH domain.</u>
<u>UNI91</u>	- <u>UNI91 (Solaris) users access inventory files in the NORTH domain.</u>

### B.2.1.2 Example Trust Relationship Documentation - Forest Root Domain

The following example documents trust relationships for a forest root domain that has established a bidirectional forest trust with another forest and an incoming forest trust with a DMZ-based forest.

AD Trust Relationship Documentation							
A. Domain NetBIOS name: <u>VCFN</u>						Verified: <u>Jan 2006</u>	
Fully Qualified Domain Name: <u>VCFN.DISA.MIL</u>							
B. Classification: <u>Unclass</u>							
C. MAC: <u>II</u> Confidentiality: <u>Sensitive</u>							
D. Trusts Defined:							
Type	Other Party (NetBIOS\FQDN)	MAC	Classif.	Direction	Transitive	Selective Auth	SID Filtering
<u>Forest</u>	<u>AOFN21 \ AOFN21.DISA.MIL</u>	<u>II</u>	<u>Unclass</u>	<u>Both</u>	<u>N/A</u>	<u>Yes</u>	<u>Yes</u>
<u>Forest</u>	<u>VCDMZF \ VCDMZF.DISA.MIL</u>	<u>II</u>	<u>Unclass</u>	<u>Incoming</u>	<u>N/A</u>	<u>N/A</u>	<u>N/A</u>
E. Access Requirements:							
<b>Other Party</b> (NetBIOS\FQDN)		<b>Access Requirements</b>					
<u>AOFN21 \ AOFN21.DISA.MIL</u>		- <u>VCFN users access Target Practice application hosted in AOFN21 forest.</u> - <u>AOFN21 users access color laser printers in VCFN forest.</u>					
<u>VCDMZF \ VCDMZF.DISA.MIL</u>		- <u>VCDMZF is a DMZ forest that may be accessed by VCFN administrators.</u>					

## APPENDIX C: VMS PROCESS GUIDANCE

This appendix provides guidance for entering and accessing the asset information in VMS for the items covered by the Checklist. There are three review subjects covered in the Checklist:

- Active Directory Implementation - This subject covers checks for AD Domain Controllers, AD Domains, and the AD Forest that make up an implementation of Active Directory.
- Synchronization\Maintenance Application - This subject covers checks for an individual installation of an application used to perform synchronization or maintenance on one or more Active Directory implementations.
- ADAM - This subject covers checks for an individual installation of ADAM as a directory service.

To understand how to access the VMS data, it is helpful to know how the data is organized. The following table summarizes this VMS data organization.

Review Subject	Items Included	VMS Asset Data Organization	VMS Asset Type
Active Directory Implementation	AD Domain Controller	Windows server OS Asset Posture <b>with</b> Domain Controller Role	Computing
	AD Domain	Active Directory Domain Asset	Non-Computing
	AD Forest	Active Directory Forest Asset	Non-Computing
Synch\Maint Application	Synch\Maint Application	Synch\Maint App Asset Posture	Computing
ADAM	ADAM Instance	ADAM Instance Asset Posture	Computing

**Note:** The path used to access asset data in the VMS application depends on the assigned role of the user:

- System Administrators (SAs) use the **Asset Finding Maint.** item on the VMS menu, select the **Assets / Findings** item, and navigate to assets under the **By Location** branch.
- Reviewers use the **Asset Finding Maint.** item on the VMS menu, select the **Assets / Findings** item, and navigate to assets under the **Visit** branch.

Because this is the significant detail in which the procedures vary between SAs and Reviewers, a single set of procedures is defined here and variations are noted where relevant.

### C.1 AD Implementation Data - AD Domain Controller, AD Domain, AD Forest

AD implementation data is expressed in VMS through three categories:

- The AD Domain Controller category is not explicitly defined in VMS. Rather, to take advantage of the existing VMS data, the asset data for AD Domain Controllers is stored under assets that are defined with a Windows server OS Asset Posture **and** the Domain Controller Role.
- AD Domain asset data is stored though the definition of an “Active Directory Domain” Non-Computing asset in VMS.
- AD Forest asset data is stored though the definition of an “Active Directory Forest” Non-Computing asset in VMS.

### C.1.1 AD Domain Controller Asset Data

As noted above, the asset data for AD Domain Controllers is stored in VMS under Computing (host) assets that are defined with a Windows server OS Asset Posture **and** the Domain Controller Role.

Because Asset Posture data is captured at the time a Windows domain controller is registered in VMS, no additional asset data needs to be entered to allow AD Domain Controller data (for an AD implementation review) to be stored. Please refer to the appropriate appendix in the *Windows 2000 Security Checklist* and the *Windows Server 2003 Security Checklist* documents for details on VMS procedures for defining and accessing the asset data.

### C.1.2 AD Domain Asset Data

Asset data for an AD domain is stored in VMS as a Non-Computing asset with the Asset Posture “Active Directory Domain”. Therefore it is necessary to define a new VMS asset the first time an AD domain is reviewed.

The following procedure describes the steps needed to access the AD domain VMS asset data.

1. Log on to the VMS application.
2. Select the **Asset Finding Maint.** menu item.
3. Select the **Assets / Findings** menu item.
4. [SAs] Expand the **By Location** branch, navigate to the correct location, and expand the location.  
[Reviewers] Expand the **Visit** branch, navigate to the correct visit, and expand the visit.
5. Expand the **Non-Computing** item.
6. If a new Active Directory Domain asset needs to be created:
  - a. Select the **Create Non-Computing Asset** icon.
  - b. Enter the asset information on the **General** tab:
    - It is highly recommended that the format “AD-Domain(*fully-qualified-domain-name*)” be used in the **Display Name** field so that future automation efforts are more easily implemented. The *fully-qualified-domain-name* is the DNS-style name of the domain. An example of this format is: “AD-Domain(aofn21.disa.mil)”.
    - The **Classification**, **MAC**, and **Confidentiality** fields should reflect the highest levels for any of the servers or workstations that are members of the AD domain.
  - c. Enter the asset information on the **Systems / Enclaves** tab:
    - Determine the enclave in which the asset resides. For registered enclaves, select the enclave from the **Available Enclaves** list. If the enclave is not present, ensure that the IAM or Team Lead works with the appropriate site personnel to request an enclave.
  - d. Enter the asset information on the **Additional Details** tab.

- e. Enter the asset information on the **Asset Posture** tab:
  - In the **Available:** field, expand **Non-Computing**, scroll to and expand the **Directory Services** item, select **Active Directory Domain**, and select the add button (>>).
- f. Select the **Save** button.
7. Ensure that the correct Active Directory Domain asset is selected.
8. Use the Navigation tree to select a Vulnerability and access the **Status, Details, Comments, Programs, or POA&M** information.
9. If any updates are made, be sure to click the **Save** button before leaving the Vulnerability.

### C.1.3 AD Forest Asset Data

Asset data for an AD forest is stored in VMS as a Non-Computing asset with the Asset Posture "Active Directory Forest". Therefore it is necessary to define a new VMS asset the first time an AD forest is reviewed.

The following procedure describes the steps needed to access the AD forest VMS asset data.

1. Log on to the VMS application.
2. Select the **Asset Finding Maint.** menu item.
3. Select the **Assets / Findings** menu item.
4. [SAs] Expand the **By Location** branch, navigate to the correct location, and expand the location.  
[Reviewers] Expand the **Visit** branch, navigate to the correct visit, and expand the visit.
5. Expand the **Non-Computing** item.
6. If a new Active Directory Forest asset needs to be created:
  - a. Select the **Create Non-Computing Asset** icon.
  - b. Enter the asset information on the **General** tab:
    - It is highly recommended that the format "AD-Forest(*fully-qualified-domain-name*)" be used in the **Display Name** field so that future automation efforts are more easily implemented. The *fully-qualified-domain-name* is the DNS-style name of the forest root domain. An example of this format is: "AD-Forest(aofn21.disa.mil)".  
Note: The forest root domain will \*also\* be defined in VMS as an AD Domain asset, so it is essential to have a unique **Display Name** value to avoid confusion.
    - The **Classification, MAC, and Confidentiality** fields should reflect the highest levels for any of the servers or workstations that are members of the AD forest.
  - c. Enter the asset information on the **Systems / Enclaves** tab:
    - Determine the enclave in which the asset resides. For registered enclaves, select the enclave from the **Available Enclaves** list. If the enclave is not present, ensure that the IAM or Team Lead works with the appropriate site personnel to request an enclave.
  - d. Enter the asset information on the **Additional Details** tab.
  - e. Enter the asset information on the **Asset Posture** tab:
    - In the **Available:** field, expand **Non-Computing**, scroll to and expand the **Directory Services** item, select **Active Directory Forest**, and select the add button (>>).

- f. Select the **Save** button.
7. Ensure that the correct Active Directory Forest asset is selected.
8. Use the Navigation tree to select a Vulnerability and access the **Status, Details, Comments, Programs, or POA&M** information.
9. If any updates are made, be sure to click the **Save** button before leaving the Vulnerability.

## C.2 Synchronization\Maintenance Application Asset Data

Asset data for a Synchronization\Maintenance Application is stored in VMS as part of the Asset Posture information for a Computing (host) asset. Therefore it is necessary to add an Asset Posture item to the Computing (host) asset the first time the application is reviewed.

The following procedure describes the steps needed to access the Synchronization\Maintenance Application VMS data.

1. Log on to the VMS application.
2. Select the **Asset Finding Maint.** menu item.
3. Select the **Assets / Findings** menu item.
4. [SAs] Expand the **By Location** branch, navigate to the correct location, and expand the location.  
[Reviewers] Expand the **Visit** branch, navigate to the correct visit, and expand the visit.
5. Expand the **Computing** item, navigate to the correct host asset, and select it.
6. If a new Synchronization\Maintenance Application needs to be added:
  - a. Select the **Asset Posture** tab:
    - In the **Available:** field, expand **Computing**, expand **Application**, scroll to and expand the **Directory Service Unit** item, select **Synch \ Maint App**, and select the add button (>>).
  - b. Select the **Save** button.
7. Ensure that the correct host asset is selected.
8. Use the Navigation tree to select a Vulnerability and access the **Status, Details, Comments, Programs, or POA&M** information.
9. If any updates are made, be sure to click the **Save** button before leaving the Vulnerability.

### C.3 ADAM Instance Asset Data

Asset data for an ADAM Instance is stored in VMS as part of the Asset Posture information for a Computing (host) asset. Therefore it is necessary to add an Asset Posture item to the Computing (host) asset the first time the ADAM installation is reviewed.

The following procedure describes the steps needed to access the ADAM Instance VMS data.

1. Log on to the VMS application.
2. Select the **Asset Finding Maint.** menu item.
3. Select the **Assets / Findings** menu item.
4. [SAs] Expand the **By Location** branch, navigate to the correct location, and expand the location.  
[Reviewers] Expand the **Visit** branch, navigate to the correct visit, and expand the visit.
5. Expand the **Computing** item, navigate to the correct host asset, and select it.
6. If a new ADAM installation needs to be added:
  - a. Select the **Asset Posture** tab:
    - In the **Available:** field, expand **Computing**, expand **Application**, scroll to and expand the **Directory Service Unit** item, select **ADAM Instance**, and select the add button (>>).
  - b. Select the **Save** button.
7. Ensure that the correct host asset is selected.
8. Use the Navigation tree to select a Vulnerability and access the **Status, Details, Comments, Programs,** or **POA&M** information.
9. If any updates are made, be sure to click the **Save** button before leaving the Vulnerability.

This page intentionally blank.

## APPENDIX D: DIRECTORY INFORMATION GATHERING

This appendix of the Checklist describes tools and methods that could be used to gather directory information. This is certainly not an exhaustive list. It is intended to point out some of the simpler and less invasive tools that are available. Although multiple tools are described, the emphasis is on the simplest command line tools and methods.

### D.1 Active Directory

The tools and processes in this section are used to gather information about Active Directory implementations. SAs may consider compiling some of these tools into batch scripts that could be used to automate information gathering for their specific environment.

**Note:** Some of the procedures described here require that the user performing the actions is a member of the Domain Admins security group.

**Note:** Some of the tools described here require specific Windows releases or the installation of additional programs:

- Methods that are identified with “Windows Server 2003” use programs that are present on domain controllers that are running that release or later.
- Methods that are identified with “Windows Support Tools” use programs that are installed with the Windows Support Tools optional component. Although present on the OS server installation CD, these programs are not installed by default.
- Methods that are identified with “Script” use the Windows Script Host (WSH) to execute scripts written in the Microsoft Visual Basic Scripting Edition (VBScript) language. The scripts invoke the Active Directory Service Interfaces (ADSI) components to get information from AD. These components are present on all Windows 2000 and later releases, but it is possible that the execution of VBScript scripts is restricted or disabled on individual machines.

#### D.1.1 Identifying Domain Controllers

The following are methods to get a list of all the domain controllers in a domain.

##### Method 1: Microsoft Management Console

- a. Start the Active Directory Users and Computers console (“Start”, “Run...”, “dsa.msc”).
- b. Select and expand the left pane item that matches the name of the domain being reviewed.
- c. Select the Domain Controllers OU.
- d. Each domain controller is represented as an object in this OU.

Notes: This method assumes that domain controller computers are members of the Domain Controllers OU. This is the default AD configuration and Microsoft recommends strongly against changing it.

### Method 2: Windows "net" Command

- a. Open a Command Prompt window (“Start”, “Run...”, “cmd.exe”).
- b. Enter “net group "domain controllers"”.
- c. Each domain controller will be listed as a member of the OU.

Notes: This method assumes that domain controller computers are members of the Domain Controllers OU. This is the default AD configuration and Microsoft recommends strongly against changing it.

### Method 3: Windows Server 2003 "dsquery" command

- a. Open a Command Prompt window (“Start”, “Run...”, “cmd.exe”).
- b. Enter “dsquery server”
- c. The distinguished name of each domain controller will be listed.

### Method 4: Windows Support Tools "netdom" command

- a. Open a Command Prompt window (“Start”, “Run...”, “cmd.exe”).
- b. Enter “netdom query dc”
- c. The host name for each domain controller will be listed.

## **D.1.2 Determining “Immediate” Domain Structure**

The following are methods to determine the name of the “current” domain and the forest root domain. The “current” domain is the AD domain to which the logged-on user has been authenticated. Information is obtained by querying the AD database on the domain controller.

### Method 1: Microsoft Management Console

- a. Start the Active Directory Users and Computers console (“Start”, “Run...”, “dsa.msc”).
- b. By default the current domain will be listed in the left pane.
- c. Start the Active Directory Domains and Trusts console (“Start”, “Run...”, “domain.msc”).
- d. The left pane will contain an icon for each domain that represents the root of an item in the AD hierarchy. Expand each node in the left pane to locate the domain name obtained from the Active Directory Users and Computers console. This will display the relationship of the current domain to its root domain.

### Method 2: Script

- a. Create a script file (optionally named *dir\AD\_List\_DomNames.vbs*) with the following contents:

```
'List AD Domain Names - "Current" \ Forest Root
'
Option Explicit
Dim strAD_objdata
Dim objRootDSE
Dim strDefNC, strRootNC
Dim strdnsHostName
Dim strCurrDom, strRootDom
'
```

```
'Get "Current" Domain Name
Set objRootDSE = GetObject("LDAP://rootDSE")
strDefNC = objRootDSE.Get("defaultNamingContext")
'Get "Current" DC
strdnsHostName = objRootDSE.Get("dnsHostName")
'

'Get Root Domain Name
strRootNC = objRootDSE.Get("rootDomainNamingContext")
'

'Display the results
strAD_objdata = "Domain Name Data: "
strAD_objdata = strAD_objdata & vbcrLf & "- Root Domain: " & strRootNC
strAD_objdata = strAD_objdata & vbcrLf & "- ""Current"" Domain: " & strDefNC
strAD_objdata = strAD_objdata & vbcrLf
strAD_objdata = strAD_objdata & vbcrLf & """"Current"" Domain DC: "
strAD_objdata = strAD_objdata & vbcrLf & "- HostName: " & strdnsHostName
'

wscript.echo strAD_objdata
```

- b. Open a Command Prompt window (“Start”, “Run...”, “cmd.exe”).
- c. Execute the script file:  
    “wscript *dir*\AD\_List\_DomNames.vbs”
- d. The following items will be displayed in a dialog box:
  - The distinguished name of the forest root domain
  - The distinguished name of the current domain
  - The fully qualified host name of the domain controller where the query was performed.

**Note:** Execution of this script does not require special privileges beyond user authentication. Any user who has logged on to the domain can execute this script.

### Method 3: Windows Support Tools "ldp" command

- a. Start the ldp utility (“Start”, “Run...”, “ldp.exe”).
- b. From the Connection menu item, select Connect...
  - Leaving the Server field blank on the Connect dialog results in a connection to the current domain controller.
- c. Scan the RootDSE information in the right pane:
  - Find the defaultNamingContext entry.
    - The value for this entry is the distinguished name of the current domain.
  - Find the rootDomainNamingContext entry.
    - The value for this entry is the distinguished name of the forest root domain.
- d. Exit the ldp utility (Connection | Exit).

**Note:** This use of the ldp (or other LDAP-capable) utility does not, by itself, require special privileges. Any user who has network access to a domain controller and access to an LDAP utility can execute this particular query.

### D.1.3 Identifying Holders of FSMO Roles

The following are methods to determine the names of the domain controllers that hold FSMO roles in the domain. Depending on the size of the AD implementation, it is typical for one domain controller to host multiple FSMO roles.

- The RID Master, PDC Emulator, and Infrastructure Master roles must be present on a domain controller **in each AD domain**.
- The Domain Naming Master and Schema Master roles must be present on a domain controller **in each AD forest**.

#### Method 1: Microsoft Management Console

- e. Start the Active Directory Users and Computers console (“Start”, “Run...”, “dsa.msc”).
- f. Right-click the left pane item that matches the name of the domain being reviewed.
- g. Select the Operations Masters... menu item.
- h. The fully qualified host name(s) of the domain controller(s) holding the RID Master, PDC Emulator, and Infrastructure Master are displayed in the “Operations master” text boxes on the respective tabs of the Operations Masters dialog.
- i. Select the Close (2003) or Cancel (2000) button to terminate the Operations Masters dialog.
  
- j. Start the Active Directory Domains and Trusts console (“Start”, “Run...”, “domain.msc”).
- k. Right-click the “Active Directory Domains and Trusts” item in the left pane.
- l. Select the Operations Master... menu item.
- m. The fully qualified host name of the domain controller holding the Domain Naming Master FSMO role is displayed in the “Domain naming operations master” text box.
- n. Select the Close button to terminate the Operations Master dialog.
  
- o. Start a management console that is configured with the Active Directory Schema snap-in. (“Start”, “Run...”, *console-name.msc*).  
**Note:** This console must be manually configured and might only be configured on one server in the forest.
- p. Right-click the “Active Directory Schema” item in the left pane.
- q. Select the Operations Master... menu item.
- r. The fully qualified host name of the domain controller holding the Schema Master FSMO role is displayed in the “Current schema master” (2003) or “Current operations master” (2000) text box.
- s. Select the Close (2003) or Cancel (2000) button to terminate the Schema Master dialog.

## Method 2: Script

- a. Create a script file (optionally named *dir\AD\_List\_FSMOInfo.vbs*) with the following contents:

```
'List FSMO Role Holders
'
Option Explicit
Dim strAD_objdata
Dim objRootDSE, objSchemaNC, objConNC, objDefNC, objRIDC, objInfC
Dim objNTDS, objServer
Dim strSchNC, strSchCont, strSch_FSMO
Dim strConNC, strConCont, strDN_FSMO
Dim strDefNC, strDefCont, strPDCE_FSMO
Dim strRIDCont, strRID_FSMO
Dim strInfCont, strInf_FSMO
'
Set objRootDSE = GetObject("LDAP://rootDSE")
'
' Get Forest Schema Master
strSchNC = objRootDSE.Get("SchemaNamingContext")
Set objSchemaNC = GetObject("LDAP://" & strSchNC)
strSchCont = objSchemaNC.Get("fsmoRoleOwner")
Set objNTDS = GetObject("LDAP://" & strSchCont)
Set objServer = GetObject(objNTDS.Parent)
strSch_FSMO = objServer.Get("dnsHostName")
'
' Get Forest Domain Naming Master
strConNC = objRootDSE.Get("ConfigurationNamingContext")
Set objConNC = GetObject("LDAP://CN=Partitions," & strConNC)
strConCont = objConNC.Get("fsmoRoleOwner")
Set objNTDS = GetObject("LDAP://" & strConCont)
Set objServer = GetObject(objNTDS.Parent)
strDN_FSMO = objServer.Get("dnsHostName")
'
' Get Domain PDC Emulator
strDefNC = objRootDSE.Get("defaultNamingContext")
Set objDefNC = GetObject("LDAP://" & strDefNC)
strDefCont = objDefNC.Get("fsmoRoleOwner")
Set objNTDS = GetObject("LDAP://" & strDefCont)
Set objServer = GetObject(objNTDS.Parent)
strPDCE_FSMO = objServer.Get("dnsHostName")
'
' Get RID Master
Set objRIDC = GetObject("LDAP://CN=RID Manager$,CN=System," & strDefNC)
strRIDCont = objRIDC.Get("fsmoRoleOwner")
Set objNTDS = GetObject("LDAP://" & strRIDCont)
Set objServer = GetObject(objNTDS.Parent)
strRID_FSMO = objServer.Get("dnsHostName")
```

```
'
' Get Infrastructure Master
Set objInfC = GetObject("LDAP://CN=Infrastructure," & strDefNC)
strInfCont = objInfC.Get("fsmoRoleOwner")
Set objNTDS = GetObject("LDAP://" & strInfCont)
Set objServer = GetObject(objNTDS.Parent)
strInf_FSMO = objServer.Get("dnsHostName")
'

'Display all FSMOs
strAD_objdata = "FSMO Role Holder Data: "
strAD_objdata = strAD_objdata & vbcrlf & "- Schema Master:" & vtab & vtab & strSch_FSMO
strAD_objdata = strAD_objdata & vbcrlf & "- Domain Naming Master:" & vtab & strDN_FSMO
strAD_objdata = strAD_objdata & vbcrlf & "- PDC Emulator:" & vtab & vtab & strPDCE_FSMO
strAD_objdata = strAD_objdata & vbcrlf & "- RID Master:" & vtab & vtab & strRID_FSMO
strAD_objdata = strAD_objdata & vbcrlf & "- Infrastructure Master:" & vtab & strInf_FSMO
'

wscript.echo strAD_objdata
```

- b. Open a Command Prompt window (“Start”, “Run...”, “cmd.exe”).
- c. Execute the script file:  
    “wscript *dir*\AD\_List\_FSMOInfo.vbs”
- d. The fully qualified host names for each of the domain controllers holding a FSMO role will be displayed in a dialog box.

**Note:** Execution of this script does not require special privileges beyond user authentication. Any user who has logged on to the domain can execute this script.

#### Method 3: Windows Support Tools "netdom" command

- a. Open a Command Prompt window (“Start”, “Run...”, “cmd.exe”).
- b. Enter “netdom query fsmo”
- c. The fully qualified host names for each of the domain controllers holding a FSMO role will be displayed.

#### Method 4: Windows Server 2003 "dsquery" command

- a. Open a Command Prompt window (“Start”, “Run...”, “cmd.exe”).
- b. Enter “dsquery server -hasfsmo *fsmo-role*” for each role, where *fsmo-role* is “rid”, “pdc”, “infr”, “name”, and “schema”.
- c. The distinguished name for the domain controller holding the specified FSMO role will be displayed.