THE CASSID GROUP

Simple. Solutions.

Network Assessment

Change Report

Prepared for: Customer

Prepared by: The Cassid Group

XX/XX/2018

Scan Date: XX/XX/2018

Table of Contents

NOTE: This change report only shows detail for items that are different between the two assessments. Sections where no changes were made will not contain data, and will instead report *No Change*.

Discovery Tasks

Each task which performed during the network assessment process is detailed below. Entries which do not have a ✓ were not performed.

	Task	Description
✓	Detect Domain Controllers	Identifies Domain Controllers and Online status.
✓	FSMO Role Analysis	Enumerates FSMO roles at the site.
✓	Enumerate Organization Units and Security Groups	Lists the Organizational units and Security Groups with members.
✓	User Analysis	List of users in AD, status, and last login/use. Helps identify potential security risks.
✓	Detect Local Mail Servers	Mail server(s) found on the network.
✓	Detect Time Servers	Time server(s) found on the network.
✓	Discover Network Shares	Comprehensive list of Network Shares by Server.
✓	Detect Major Applications	Major apps / versions and count of installations.
✓	Web Server Discovery and Identification	List of web servers and type.
✓	System by System Event Log Analysis	Last 5 System and App Event Log errors for servers.
✓	Detailed Domain Controller Event Log Analysis	List of event log entries from the past 24 hours for the Directory Service, DNS Server and File Replication Service event logs.
✓	Network Discovery for Non-A/D Devices	List of non AD devices responding to network requests.
✓	SQL Server Analysis	List of SQL Servers and associated database(s).
	Internet Domain Analysis	“Whois” check for company domain(s).
✓	Password Strength Analysis	Uses MBSA to identify computers with weak passwords that may pose a security risk.
✓	Missing Security Updates	Uses MBSA to identify computers missing security updates.
✓	Internet Access and Speed Test	Test of internet access and performance.
	External Security Vulnerabilities	List of Security Holes and Warnings from External Vulnerability Scan.

1. Assessment Summary – Changes from previous scan

The summary from the previous and current assessment, as well as the change, is listed below. Any row highlighted yellow indicates a change.

Domain	Previous	Current	Change
Domain Controllers	3	3	0
Number of Organizational Units	22	22	0
Users			
# Enabled	90	92	2
Last Login within 30 days	36	38	2
Last Login older than 30 days	36	38	2
# Disabled	21	21	0
Last Login within 30 days	0	0	0
Last Login older than 30 days	21	21	0
Security Group			
Groups with Users	36	36	0
# Total Groups	65	65	0
Computers in Domain			
Total Computers	72	75	3
Last Login within 30 days	34	35	1
Last Login older than 30 days	38	40	2
Windows 2000 Professional	2	4	2
Windows 7 Professional	7	7	0
Windows Server 2003	6	7	1
Windows Server 2008 R2 Enterprise	1	1	0
Windows Server 2008 R2 Standard	3	3	0
Windows Server® 2008 Enterprise	5	5	0
Windows XP Professional	48	48	0
Miscellaneous			
Non-A/D Systems	24	24	0
MX Records	0	0	0
MS SQL Servers	8	9	1
Web Servers	26	28	2
Printers	8	9	1
Exchange Servers	2	2	0

Network Shares	198	211	13
Installed Applications	822	822	0
Potential or Severe Security Risks	19	21	2
Potential Insecure Listening Ports	12	13	1

2.1 Domain Controllers

All Domain Controllers which were added, removed, or modified between the previous and current assessments are listed below.
There are 3 domain controllers:

Change Status	Domain Controller	Status
No Change		

2.2 FSMO Roles

The FSMO Roles are a set of roles needed to operate a Windows domain. Any FSMO Roles which were added, removed, or modified between the previous and current assessment are listed below.

Role	Role	Domain Controller	Best Practice
No Change			

2.3 Organizational Units

Any organizational units which were added, removed, or modified between the previous and current assessment are listed below.

- **CustDomain.com**

2.4 Group Policy Objects

Any Organization Units (OU) and applied group policies which were added, removed, or modified between the previous and current assessment are listed below.

No Change

2.5 Users

Any users which were added, removed, or modified between the previous and the current assessment are listed below.
113 total users

Change Status	User	Display Name	Enabled	Last Login
Added	Administrator2	Administrator2	Enabled	12/17/2011 4:11:03 PM
Added	Barbara	Barbara Whitman	Enabled	12/12/2011 12:09:11 PM

2.6 Security Groups

Any security groups which were added, removed, or modified between the previous and the current assessment are listed below.

Change Status	Group	Members
Added	Front Desk Rotation *(CustDomain.com/Builtin/Front Desk Rotation)* 3 Total: 3 Enabled, 0 Disabled	**Enabled**: Tom Whiteman (Unchanged) , Sandy Rogers (Unchanged) , Christina Mason (Unchanged)

2.7 Computers in Domain

Any computers which were added, removed, or modified between the previous and the current assessment are listed below.

Change Status	Computer Name	IP Address(es)	DNS Entries	Operating Systems	Last Login
Deleted	Sarah-W2K	179.14.217.19	Sarah-W2K.CustDomain.com	Windows 2000 Professional	**<never>**
Deleted	JDUNCAN3			Windows XP Professional	**<never>**
Added	CS-SRV02	179.14.217.33	CS-SRV02.CustDomain.com	Windows Server 2003	12/12/2011 2:12:20 PM
Added	James-W2K	179.14.217.49	James-W2K.CustDomain.com	Windows 2000 Professional	**<never>**
Added	James-Laptop	179.14.217.53	James-Laptop.CustDomain.com	Windows 2000 Professional	**<never>**
Added	David-W2K	179.14.217.19	Sarah-	Windows 2000	**<never>**

			W2K.CustDomain.com	Professional	
Added	MARKW2			Windows XP Professional	**<never>**

2.8 Domain Service: DHCP

Any DHCP services which were added, removed, or modified between the previous and the current assessment are listed below.

Served By:	
Errors (last 24 hours)	

2.9 MS SQL Servers

Any MS SQL Servers which were added, removed, or modified between the previous and the current assessment are listed below.

Change Status	Computer Name	Instance	Version	# of Databases	Active SQL Agent Jobs?
Added	James-Laptop	ACT7	9.00.3042.00	<unknown>	<unknown>

2.10 Web Servers

Any Web Servers which were added, removed, or modified between the previous and the current assessment are listed below.

Change Status	Computer Name	Listening Port	Server Type
Added	James-Laptop	80/TCP	Microsoft-IIS/6.0
Added	CS-SRV02	80/TCP	Cherokee/0.7.2 (Debian GNU/Linux)

2.11 Time Servers

Any time servers which were added, removed, or modified between the previous and the current assessment are listed below.

Change Status	Time Server Name	IP Address
No Change		

2.12 Printers

Any printers which were added, removed, or modified between the previous and the current assessment are listed below.

Change Status	Printer Name	Printer Server	Location	Comment
Added	SRV01-RICOH 7770 PCL 4	TS		

2.13 Exchange Servers

Any Exchange Servers which were added, removed, or modified between the previous and the current assessment are listed below.

Change Status	Computer Name	Server Type
No Change		

2.14 Network Shares

Any Network Shares which were added, removed, or modified between the previous and the current assessment are listed below.

Hosted By	Share UNC
No Change	

2.15 Major Applications

A count of previous and current computers for each application installed, as well as the changed quantities, is listed below. Any changed row is highlighted.

Application Name	Version	# Computers (Previous)	# Computers (Current)	Change
32 Bit HP CIO Components Installer	3.1.1	1	2	1
Adobe AIR	2.7.0.19530	1	2	1
Adobe Flash Player 10 ActiveX	10.2.152.32	2	3	1
Adobe Reader X (10.1.0)	10.1.0	1	2	1

APC PowerChute Business Edition Agent	1	2	3	1
ATI Display Driver		3	4	1
Automise Runtime 3.0.0.494	3.0.0.494	10	11	1
Brother Bradmin Light 1.18.0001	1.18.0001	1	2	1
Dell MFP 1125 WebPackage	1.00.0000	1	2	1
FreeMyIT Agent	2.0.0018	1	2	1
Hewlett-Packard Survey Utility		1	2	1
HP Array Configuration Utility CLI	7.85.18.0	3	4	1
HP Array Configuration Utility	7.85.18.0	3	4	1
HP Array Diagnostic Utility	7.85.16.0	3	4	1
HP Insight Management Agents	7.90.0.0	2	3	1
HP LighCS-Out Online Configuration Utility	1.5.1.1	2	3	1
HP ProLiant Integrated Management Log Viewer	5.13.0.0	2	3	1
HP ProLiant Remote Monitor Service	5.11.3.0	2	3	1
HP ProLiant Smart Array Device Manager Extension	6.4.0.32	2	3	1
HP Protect Your Data		4	5	1
HP System Management Homepage	2.1.10	2	3	1
HP Version Control Agent	2.1.9.790	2	3	1
HPInsightDiagnostics	7.9.0	2	3	1
Internet Explorer Q903235		1	2	1
Java(TM) 6 Update 13	6.0.130	2	3	1
Java(TM) 6 Update 3	1.6.0.30	3	4	1
Kardin Budget System	32.18	3	4	1
Kardin Consolidation System	32.17	1	2	1
KBOX	4.3.20024	1	2	1
Kiwi Syslog Daemon 8.3.4 (Standard Edition)	8.3.4 (Standard Edition)	1	2	1
KONICA MINOLTA C360Series		1	2	1
LiveUpdate 3.1 (Symantec Corporation)	3.1.0.90	3	4	1
MapMerge		3	4	1
Microsoft .NET Framework 1.1		15	16	1
Microsoft .NET Framework 2.0 Service Pack 2	2.2.30729	12	13	1
Microsoft .NET Framework 3.0 Service Pack 2	3.2.30729	12	13	1

Microsoft .NET Framework 3.5 SP1		16	17	1
Microsoft Application Error Reporting	11.0.5228.1	3	4	1
Microsoft Baseline Security Analyzer 2.1	2.1.0000	1	2	1
Microsoft Internet Explorer Administration Kit 5		1	2	1
Microsoft Office 2000 Resource Kit Tools and Utilities	9.00.00.2010	1	2	1
Microsoft Office 2007 Service Pack 2 (SP2)		7	8	1
Microsoft Office Access 2007	12.0.6425.1000	2	3	1
Microsoft Office Access MUI (English) 2007	12.0.6425.1000	6	7	1
Microsoft Office Access Runtime (English) 2007	12.0.6425.1000	3	4	1
Microsoft Office Access Setup Metadata MUI (English) 2007	12.0.6425.1000	6	7	1
Microsoft Office Excel MUI (English) 2007	12.0.6425.1000	5	6	1
Microsoft Office Outlook MUI (English) 2007	12.0.6425.1000	6	7	1
Microsoft Office PowerPoint MUI (English) 2007	12.0.6425.1000	4	5	1
Microsoft Office Professional 2007	12.0.6425.1000	2	3	1
Microsoft Office Professional Edition 2003	11.0.8173.0	2	3	1
Microsoft Office Proof (English) 2007	12.0.6425.1000	8	9	1
Microsoft Office Proof (French) 2007	12.0.6425.1000	8	9	1
Microsoft Office Proof (Spanish) 2007	12.0.6425.1000	8	9	1
Microsoft Office Proofing (English) 2007	12.0.4518.1014	13	14	1
Microsoft Office Proofing Tools 2007 Service Pack 2 (SP2)		7	8	1
Microsoft Office Publisher MUI (English) 2007	12.0.6425.1000	4	5	1
Microsoft Office Shared MUI (English) 2007	12.0.6425.1000	8	9	1
Microsoft Office Shared Setup Metadata MUI (English) 2007	12.0.6425.1000	8	9	1
Microsoft Office Word MUI (English) 2007	12.0.6425.1000	5	6	1
Microsoft Software Update for Web Folders (English) 12	12.0.6425.1000	8	9	1
Microsoft SQL Server 2005 Express Edition (SQLEXPRESS)	9.2.3042.00	1	2	1
Microsoft SQL Server 2005		3	4	1
Microsoft SQL Server Native Client	9.00.3042.00	2	3	1
Microsoft SQL Server Setup Support Files (English)	9.00.3042.00	2	3	1
Microsoft SQL Server VSS Writer	9.00.3042.00	2	3	1
Microsoft VGX Q833989		1	2	1
Microsoft Windows Journal Viewer	1.5.2316.3	1	2	1

Microsoft XML Parser and SDK	4.10.9406.0	1	2	1
Microsoft XML Parser	8.70.1104.04	8	9	1
Pervasive PSQL v11 Server Engine (32-bit) SP1	11.10.051	1	2	1
Pervasive PSQL v11 Server Engine (32-bit)	11.10.051	1	2	1
ProactiveWatch Agent	2.0.0004	3	4	1
SHARP MX-M350/450 Series PCL/PS Printer Driver		3	4	1
SHARP PCL6 T1 Printer Driver	1.00.000	1	2	1
SKYLINE® 2012 Client	12	8	9	1
SKYLINE® 2012 Server	12	2	3	1
Symantec AntiVirus	10.1.5000.5	11	12	1
Symantec Backup Exec Remote Agent for Windows Systems	11.0.6235	3	4	1
VNC Free Edition 4.1.2	4.1.2	3	4	1
WebFldrs	9.00.3907	1	2	1
Windows Imaging Component	3.0.0.0	8	9	1
Windows Search 4.0	04.00.6001.503	11	12	1
Windows Server 2003 Service Pack 1 Administration Tools Pack	5.2.3790.1830	3	4	1
Windows Server 2003 Service Pack 2	20070217.021455	4	5	1
Windows Support Tools	5.2.3790	2	3	1
WinZip	8.1 (4331)	2	3	1

2.16 Domain DNS

Any DNS entries which were added, removed, or modified between the previous and the current assessment are listed below. Change Status	IP	Host
No Change		

3. Internet Access

This is a comparison of the Internet Access times between the two reports.

Internet Access [Previous]	Internet Access [Current]
Latency Tests: Retrieval time for Google.com: 318 ms Retrieval time for Yahoo.com: 1535 ms ***Internet trace route to Google.com:*** Tracing route to www.google.com [74.125.157.147] over a maximum of 30 hops: 1 2 ms 107.7.15.129 2 50 ms 10.4.27.245 3 82 ms 97.67.118.1 4 34 ms te10-0-0d0.cir1.atlanta6-ga.us.xo.net [216.156.108.23] 5 21 ms 216.156.108.18.ptr.us.xo.net [216.156.108.18] 6 69 ms 72.14.233.56 7 44 ms 209.85.254.247 8 3128 ms 9 38 ms gy-in-f147.1e100.net [74.125.157.147] Trace complete.	***Latency Tests:*** Retrieval time for Google.com: 391 ms Retrieval time for Yahoo.com: 1530 ms ***Internet trace route to Google.com:*** Tracing route to www.google.com [74.125.157.147] over a maximum of 30 hops: 1 2 ms 107.7.15.129 2 52 ms 10.4.27.245 3 98 ms 97.67.118.1 4 24 ms te10-0-0d0.cir1.atlanta6-ga.us.xo.net [216.156.108.25] 5 22 ms 216.156.108.18.ptr.us.xo.net [216.156.108.18] 6 46 ms 72.14.233.56 7 36 ms 209.85.254.247 8 4898 ms 9 37 ms gy-in-f147.1e100.net [74.125.157.147] Trace complete.

4. Non A/D Devices

Any Non Active Directory devices which were added, removed, or modified between the previous and the current assessment are listed below.

Change Status	Computer Name	Listening Port	Server Type
No Change			

5. Internet Domain

Any Internet Domain additions, removals, or modifications between the previous and the current assessment are listed below.

No Change

6. System Password Strength Assessment

Any differences in system password strength between the previous and the current assessment are listed below.

IP Range for MBSA scan: 179.14.217.0-179.14.217.255

Change Status	Computer	IP	Assessment
No Change			

7. Patch Summary

Any differences in patching between the previous and the current assessment are listed below.

IP Range for Patch scan: 179.14.217.0-179.14.217.255

Computer	Issue	Score	Assessment
No Change			

8. Listening Ports

Computers or devices with a change of state for one or more listening reports are listed below. Potentially insecure ports are shown in Red.

Computer	FTP 21/TCP	SSH 22/TCP	Telnet 23/TCP	SMTP 25/TCP	DNS 53/TCP	HTTP 80/TCP	HTTPS 443/TCP	SQLServer 1433/TCP	RDP 3389/TCP	VNC 5900/TCP	HTTP 8080/TCP
James-Laptop				Added		Added			Added		
CS-SRV02						Added				Added	

Appendix I: Detailed Computer Analysis

Below is a list of the computer details for computers that have been added since the previous scan, or cases where there has been a change to system resources, scheduled tasks, etc. (Note: Event logs do not trigger this section of the change report.)

Computer Name	O/S	CPU	RAM	Analysis
David-W2K	Current: Windows 2000 Professional Previous: Windows XP Professional			***Scheduled Tasks:***
James-Laptop	Current: Windows 2000 Professional Previous: Windows XP Professional			***Scheduled Tasks:*** ***Listening Ports:***
James-W2K	Current: Windows 2000 Professional Previous: Windows XP Professional			***Scheduled Tasks:*** Current: netScan test run User_Feed_Synchronization-{C56CDDAE-B362-4994-BA6D-B9698B08FBE1} Previous: netScan test run User_Feed_Synchronization-{C56CDDAE-B362-4994-BA6D-B9698B08FBE1}
MARKW2	Current: Windows XP Professional Previous: Windows 2000 Professional			***Scheduled Tasks:***