



**THE  
IT GUYS I/O LLC**

One Call. Problem Solved

# Network Assessment

## Client Risk Report



**CONFIDENTIALITY NOTE:** The information contained in this report is for the exclusive use of the client specified above and may contain confidential, privileged, and non-disclosable information. If you are not the client or addressee, you are strictly prohibited from reading, photocopying, distributing, or otherwise using this report or its contents in any way.

Scan Date: 2020/01/18

Prepared for: Your Company

Prepared by: The IT Guys I/O

2021/02/03

# Table of Contents

---

<b>01</b>	Discovery Tasks
<b>02</b>	Risk Score
<b>03</b>	Issues Summary
<b>04</b>	Internet Speed Test Results
<b>05</b>	Asset Summary: Total Discovered Assets
<b>06</b>	Asset Summary: Active Computers
<b>07</b>	Asset Summary: All Computers
<b>08</b>	Asset Summary: Inactive Computers
<b>09</b>	Asset Summary: Users
<b>10</b>	Asset Summary: Storage
<b>11</b>	Server Aging

# 12

## Workstation Aging

---

# Discovery Tasks

The following discovery tasks were 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	Lists the users in AD, status, and last login/use, which helps identify potential security risks.
✓ Detect Local Accounts	Detects local accounts on computer endpoints.
✓ Detect Added or Removed Computers	Lists computers added or removed from the Network since the last assessment.
✓ Detect Local Mail Servers	Detects mail server(s) on the network.
✓ Detect Time Servers	Detects server(s) on the network.
✓ Discover Network Shares	Discovers the network shares by server.
✓ Detect Major Applications	Detects all major apps / versions and counts the number of installations.
✓ Detailed Domain Controller Event Log Analysis	Lists the event log entries from the past 24 hours for the directory service, DNS server and file replication service event logs.
✓ Web Server Discovery and Identification	Lists the web servers and type.
✓ Network Discovery for Non-A/D Devices	Lists the non-Active Directory devices responding to network requests.
✓ Internet Access and Speed Test	Tests Internet access and performance.
✓ Internet Domain Analysis	Queries company domain(s) via a WHOIS lookup.
✓ Missing Security Updates	Identifies computers missing security updates.
✓ System by System Event Log Analysis	Discovers the five system and app event log errors for servers.
✓ External Security Vulnerabilities	Lists the security holes and warnings from External Vulnerability Scan.

# Risk Score

The Risk Score is a value from 0 to 100, where 100 represents significant risk and potential issues. The score is risk associated with the highest risk issue.

**CURRENT**  
**97**

LOW

MEDIUM

HIGH

Several critical issues were identified. Identified issues should be investigated and addressed according to the Management Plan.

# Issues Summary

This section contains a summary of issues detected during the Network Assessment process, and is based on industry-wide best practices for network health, performance, and security. The Overall Issue Score grades the level of issues in the environment. An Overall Issue score of zero (0) means no issues were detected in the environment. It may not always be possible to achieve a zero score in all environments due to specific circumstances.

## Overall Issue Score

Current  3454

**Overall Issue Score:** Risk Score x Number of Incidents = Total points: Total percent (%)

### 1358 Unsupported operating systems (97 pts each)

**Current Score:** 97 pts x 14 = 1358: 39.32%

**Issue:** Computers found using an operating system that is no longer supported. Unsupported operating systems no longer receive vital security patches and present an inherent risk.

**Recommendation:** Upgrade or replace computers with operating systems that are no longer supported.

### 825 Few Security patches missing on computers. (75 pts each)

**Current Score:** 75 pts x 11 = 825: 23.89%

**Issue:** Security patches are missing on computers. Maintaining proper security patch levels helps prevent unauthorized access and the spread of malicious software. Few is defined as missing 3 or less patches.

**Recommendation:** Address patching on computers missing 1-3 security patches.

### 299 User has not logged on to domain in 30 days (13 pts each)

**Current Score:** 13 pts x 23 = 299: 8.66%

**Issue:** Users have not logged on to domain in 30 days. A user that has not logged in for an extended period of time could be a former employee or vendor.

**Recommendation:** Disable or remove user accounts for users that have not logged on to active directory in 30 days.

## 272 Potential disk space issue (68 pts each)

**Current Score:** 68 pts x 4 = 272: 7.87%

**Issue:** 4 computers were found with significantly low free disk space.

**Recommendation:** Free or add additional disk space for the specified drives.

## 270 Insecure listening ports (10 pts each)

**Current Score:** 10 pts x 27 = 270: 7.82%

**Issue:** Computers are using potentially insecure protocols.

**Recommendation:** There may be a legitimate business need, but these risks should be assessed individually. Certain protocols are inherently insecure since they often lack encryption. Inside the network, their use should be minimized as much as possible to prevent the spread of malicious software. Of course, there can be reasons these services are needed and other means to protect systems which listen on those ports. We recommend reviewing the programs listening on the network to ensure their necessity and security. See Listening Ports sheets in Excel Export for details.

## 180 User password set to never expire (30 pts each)

**Current Score:** 30 pts x 6 = 180: 5.21%

**Issue:** User accounts with passwords set to never expire present a risk of use by unauthorized users. They are more easily compromised than passwords that are routinely changed.

**Recommendation:** Investigate all accounts with passwords set to never expire and configure them to expire regularly.

## 90 Anti-spyware not up to date (90 pts each)

**Current Score:** 90 pts x 1 = 90: 2.61%

**Issue:** Up to date anti-spyware definitions are required to properly prevent the spread of malicious software. Some anti-spyware definitions were found to not be up to date.

**Recommendation:** Ensure anti-spyware definitions are up to date on specified computers.

## 90 Anti-virus not up to date (90 pts each)

**Current Score:** 90 pts x 1 = 90: 2.61%

**Issue:** Up to date anti-virus definitions are required to properly prevent the spread of malicious software. Some anti-virus definitions were found to not be up to date.

**Recommendation:** Ensure anti-virus definitions are up to date on specified computers.

## 40 Operating system in Extended Support (20 pts each)

**Current Score:** 20 pts x 2 = 40: 1.16%

**Issue:** Computers are using an operating system that is in Extended Supported. Extended Support is a warning period before an operating system is no longer supported by the manufacturer and will no longer receive support or patches.

**Recommendation:** Upgrade computers that have operating systems in Extended Support before end of life.

## 30 Inactive computers (15 pts each)

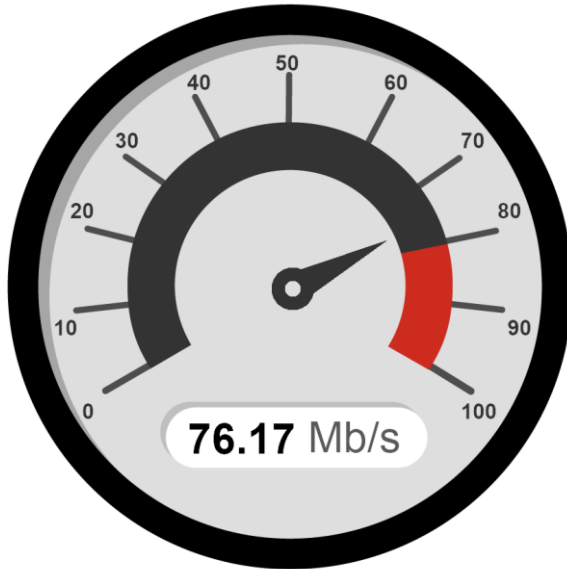
**Current Score:** 15 pts x 2 = 30: 0.87%

**Issue:** Computers have not checked in during the past 30 days

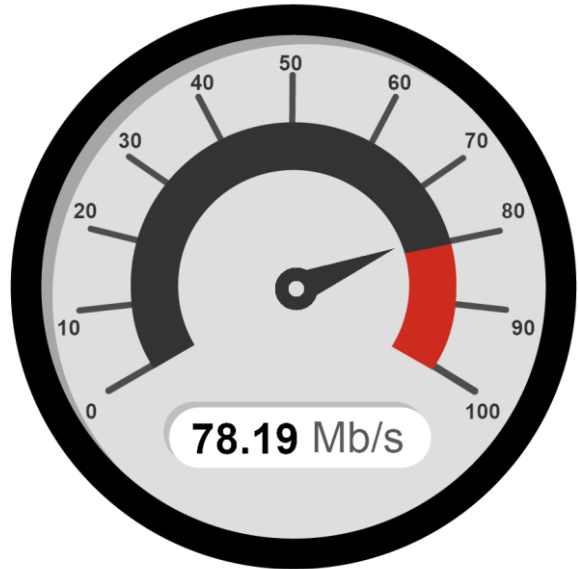
**Recommendation:** Investigate the list of inactive computers and determine if they should be removed from Active Directory, rejoined to the network, logged into by authorized users, or powered on.

# Internet Speed Test Results

Download Speed: **76.17 Mb/s**

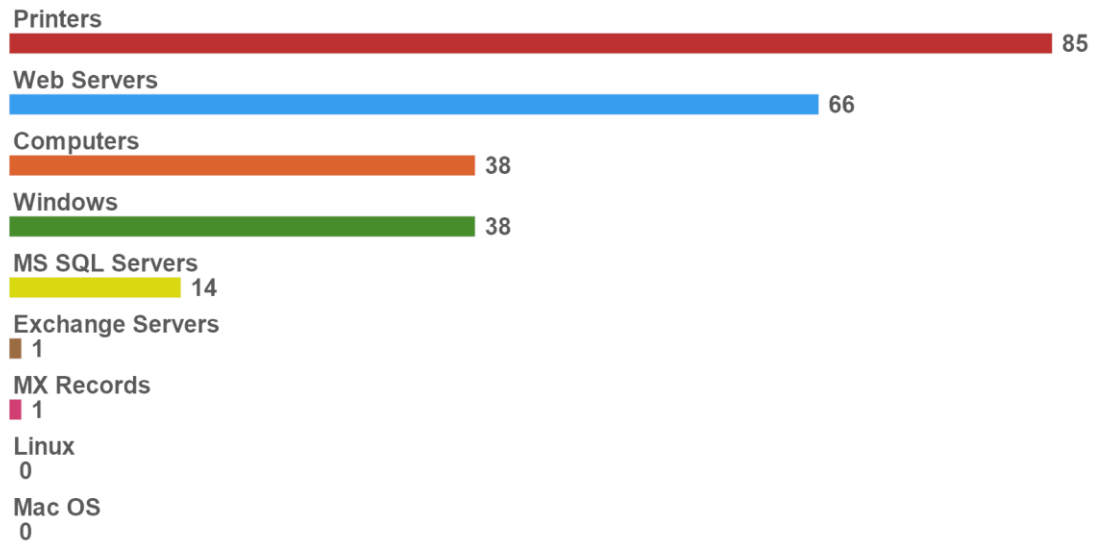


Upload Speed: **78.19 Mb/s**



# Asset Summary: Total Discovered Assets

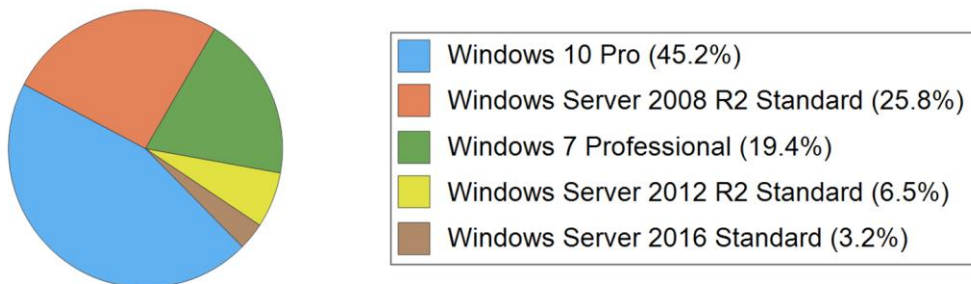
## Total Discovered Assets



# Asset Summary: Active Computers

Active Computers are defined as computers that were either actively responding at the time of the scan or have checked in with Active Directory within the past 30 days.

## Active Computers by Operating System Total (31)



OPERATING SYSTEM (TOP FIVE)	TOTAL	PERCENT
Windows 10 Pro	14	45.2%
Windows Server 2008 R2 Standard	8	25.8%
Windows 7 Professional	6	19.4%
Windows Server 2012 R2 Standard	2	6.5%
Windows Server 2016 Standard	1	3.2%
<b>Total - Top Five</b>	<b>31</b>	<b>100%</b>

OPERATING SYSTEM (OTHER)	TOTAL	PERCENT
Total - Other	0	0%

<b>OVERALL TOTAL</b>	<b>31</b>	<b>100%</b>
----------------------	-----------	-------------

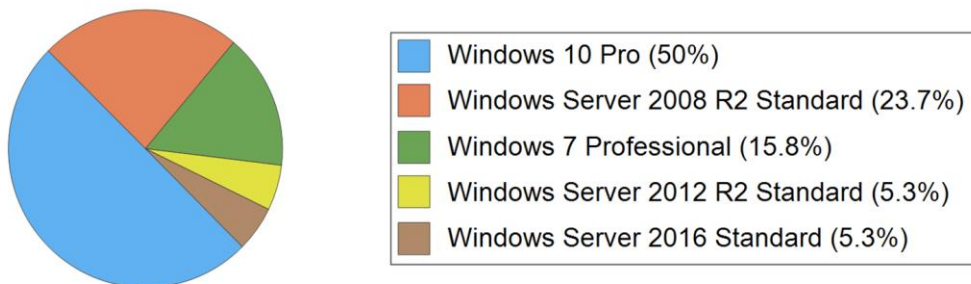
## Operating System Support



# Asset Summary: All Computers

The list of all computers includes computers that may no longer be active but have entries in Active Directory (in a domain environment).

**Total Computers by Operating System**  
 Total (38)



OPERATING SYSTEM (TOP FIVE)	TOTAL	PERCENT
Windows 10 Pro	19	50%
Windows Server 2008 R2 Standard	9	23.7%
Windows 7 Professional	6	15.8%
Windows Server 2012 R2 Standard	2	5.3%
Windows Server 2016 Standard	2	5.3%
<b>Total - Top Five</b>	<b>38</b>	<b>100%</b>

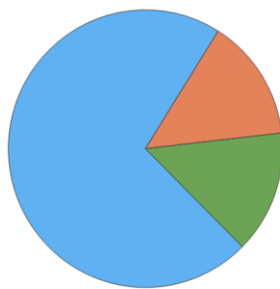
OPERATING SYSTEM (OTHER)	TOTAL	PERCENT
Total - Other	0	0%

<b>OVERALL TOTAL</b>	<b>38</b>	<b>100%</b>
----------------------	-----------	-------------

# Asset Summary: Inactive Computers

Inactive computers are computers that could not be scanned or have not checked into Active Directory in the past 30 days.

## Inactive Computers by Operating System Total (7)



Windows 10 Pro (71.4%)
Windows Server 2008 R2 Standard (14.3%)
Windows Server 2016 Standard (14.3%)

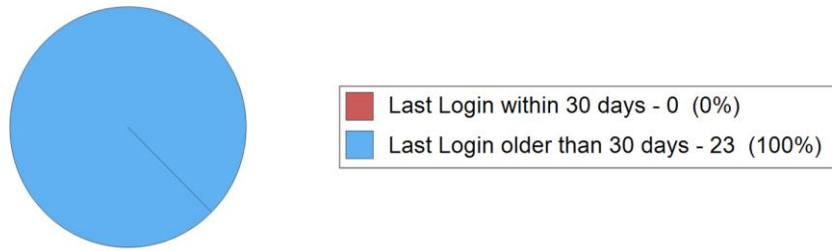
OPERATING SYSTEM (TOP FIVE)	TOTAL	PERCENT
Windows 10 Pro	5	71.4%
Windows Server 2008 R2 Standard	1	14.3%
Windows Server 2016 Standard	1	14.3%
<b>Total - Top Five</b>	<b>7</b>	<b>100%</b>

OPERATING SYSTEM (OTHER)	TOTAL	PERCENT
<b>Total - Other</b>	<b>0</b>	<b>0%</b>

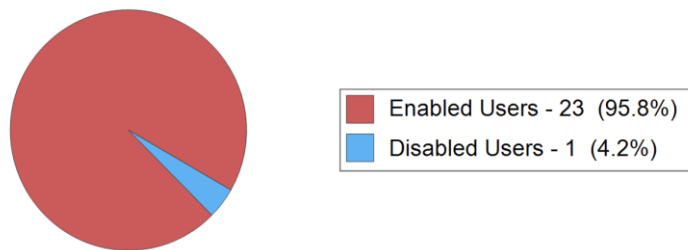
<b>OVERALL TOTAL</b>	<b>7</b>	<b>100%</b>
----------------------	----------	-------------

# Asset Summary: Users

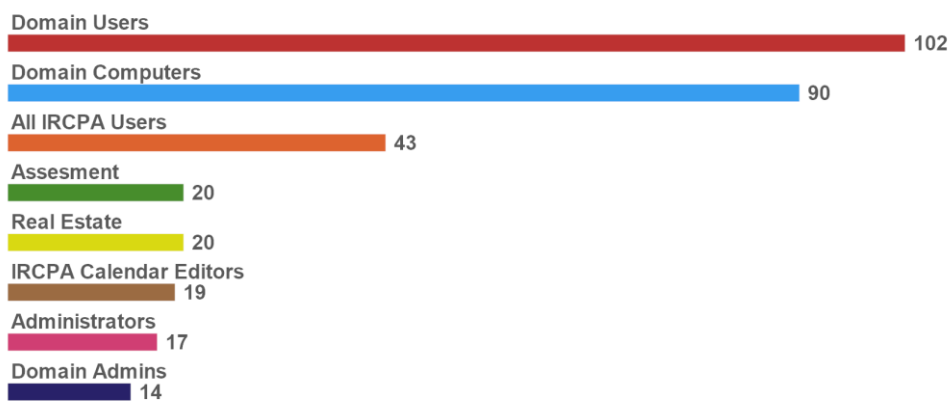
## Users Logged in



## Total Users

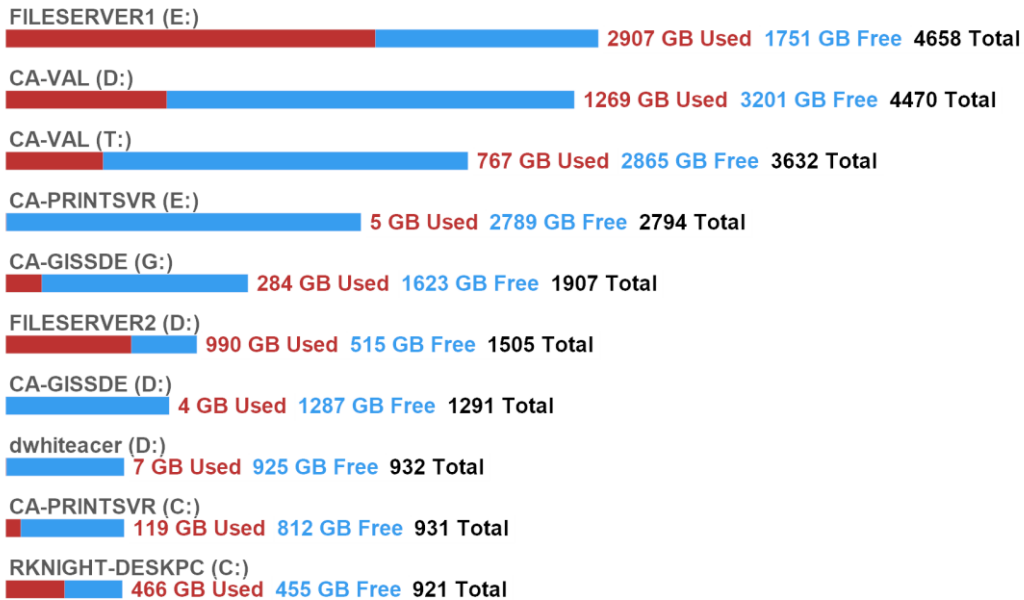


## Security Group Distribution (Admin Groups + Top 5 Non-Admin Groups)

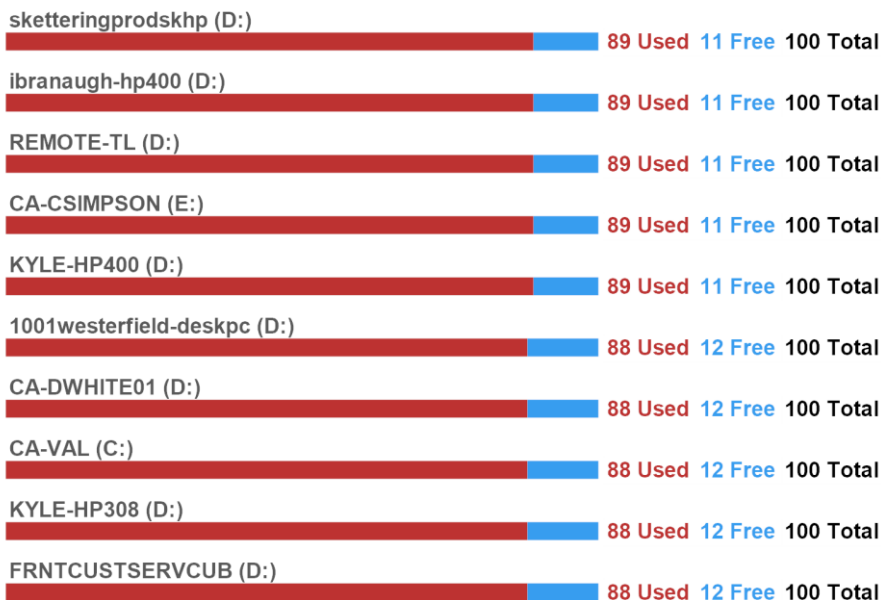


# Asset Summary: Storage

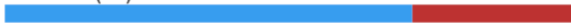









## Top 10 Drive Capacity



## Top 10 Drive % Used

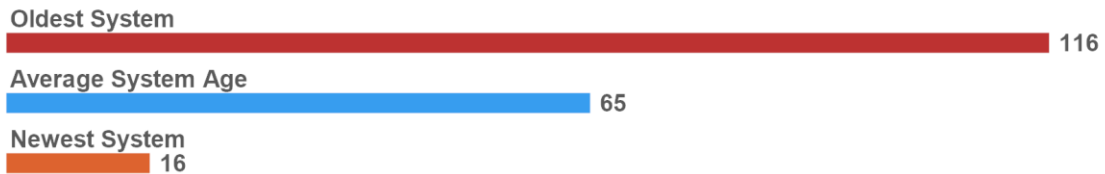


## Top 10 Drive Free Space

CA-VAL (D:)		3201 GB Free	1269 GB Used	4470 Total
CA-VAL (T:)		2865 GB Free	767 GB Used	3632 Total
CA-PRINTSVR (E:)		2789 GB Free	5 GB Used	2794 Total
FILESERVER1 (E:)		1751 GB Free	2907 GB Used	4658 Total
CA-GISSDE (G:)		1623 GB Free	284 GB Used	1907 Total
CA-GISSDE (D:)		1287 GB Free	4 GB Used	1291 Total
dwhiteacer (D:)		925 GB Free	7 GB Used	932 Total
gilesmsi (D:)		913 GB Free	1 GB Used	914 Total
KYLE-HP400 (C:)		842 GB Free	76 GB Used	918 Total
FRNTCUSTSERVCUB (C:)		840 GB Free	77 GB Used	917 Total

# Server Aging

## Server Aging (Number of months )



# Workstation Aging

## Workstation Aging (Number of months )

