



**Southern New England
Computer Services**

Network Assessment

Risk Report

**Prepared by: SNECS, LLC
Prepared for: Sample Client**

6/29/2013

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

NETWORK ASSESSMENT

Discovery Tasks

The following discovery tasks were performed:

✓	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, which 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-Active Directory 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

Risk Score

The Risk Score is a value from 1 to 10, where 10 represents significant risk and potential issues.



Several critical issues were identified (summarized on the next page). Identified issues should be investigated and addressed immediately.

If additional information is needed, please consult the Full Detail Report.



NETWORK ASSESSMENT

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.

Inactive Users

We discovered 4 active user accounts that have not logged in within the past 30 days. These accounts should be reviewed and disabled or removed if they are no longer needed. Active accounts that are not in use may pose a security risk and should be addressed with a User Audit.

Inactive Computers

4 computers were found as having not checked in during the past 30 days. This poses no threat, but organization is essential to proper network management and providing accurate domain statistics.

Organizational Units

We discovered 3 populated Organizational Units. You should review the details of the Organization Units to ensure they align with your business and operational needs. Proper alignment is crucial to ensuring security and access policies are adhered to properly.

Domain Controllers

With only 1 online Domain Controller, there is a heightened risk of business downtime, loss of data, or service outage due to a lack of redundancy.

Password Strength Risks

Local Account Passwords on 1 computer were found to have a Potential Risk. 0 computers were found to have a Severe Risk. These are systems where passwords are extremely weak or are not required and should be rectified to prevent unauthorized access or the potential spread of viruses and worms.

Password Policies

16 enabled domain users have passwords that are set to never expire.

Operating System Support

6 computers were found to be using an Operating System that is in Extended Support which means patching and other updates will be unavailable in the near future.

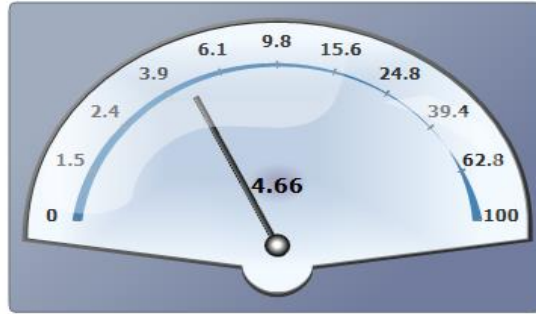
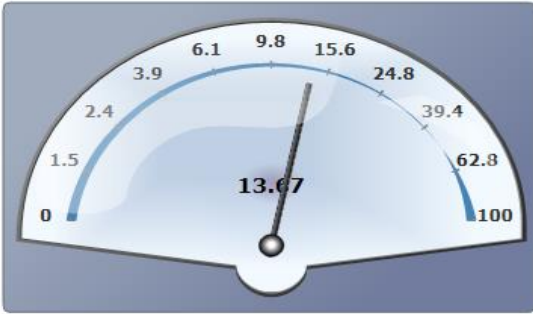
Endpoint Security

Anti-virus and anti-spyware was scanned for but not detected on 1 computer.

Internet Speed Test Results

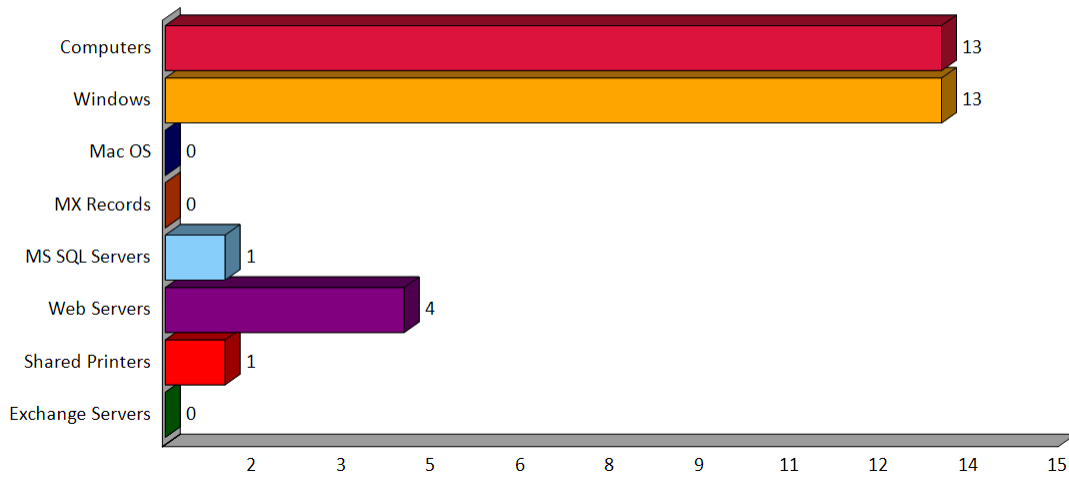
Download Speed: **13.67 Mb/s**

Upload Speed: **4.66 Mb/s**



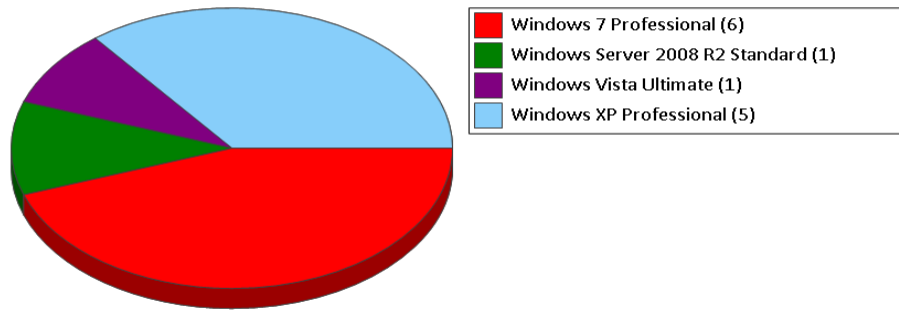
Asset Summary: Discovered Assets

Discovered Assets

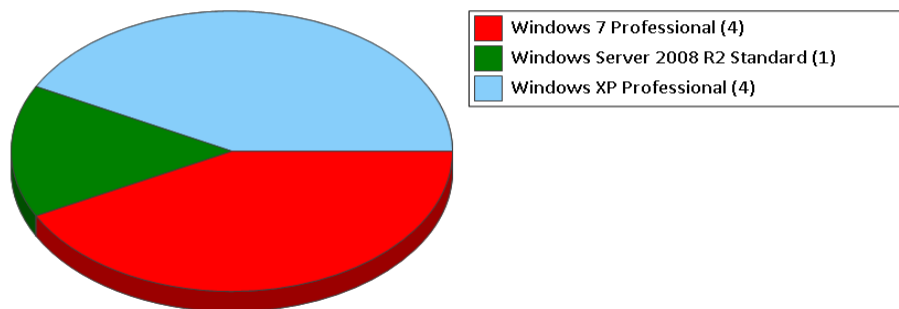


Asset Summary: Computers

Total Computers by Operating System (13)

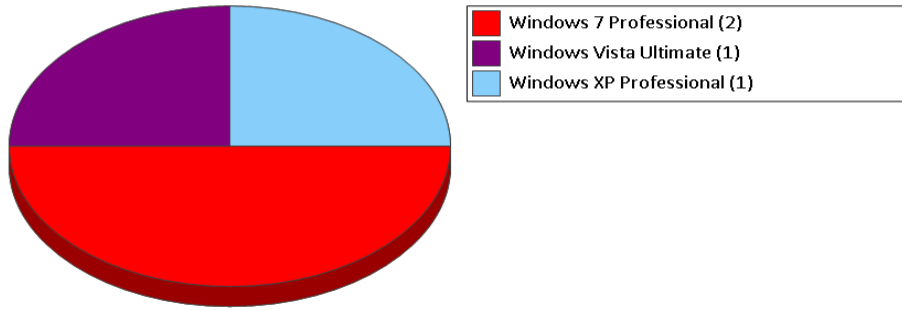


Active Computers by Operating System (9)

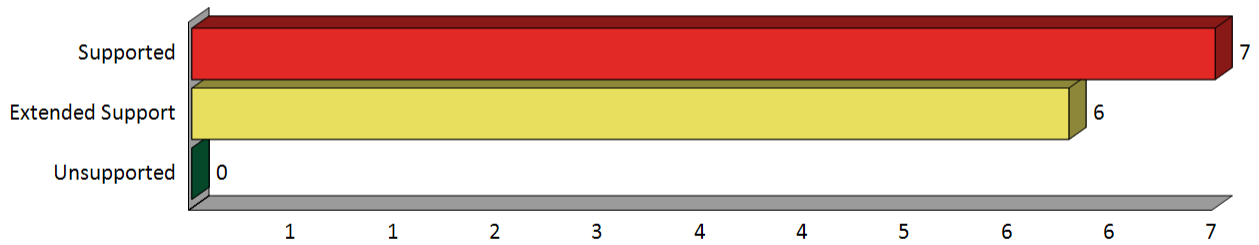


NETWORK ASSESSMENT

Inactive Computers by Operating System (4)

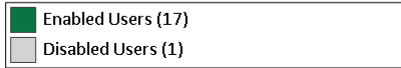
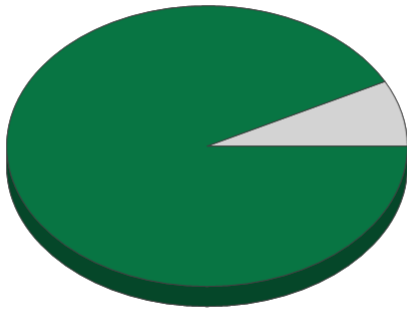


Operating System Support

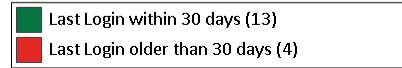
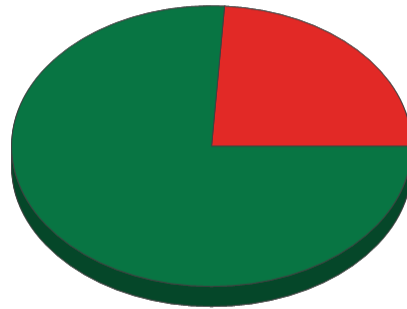


Asset Summary: Users

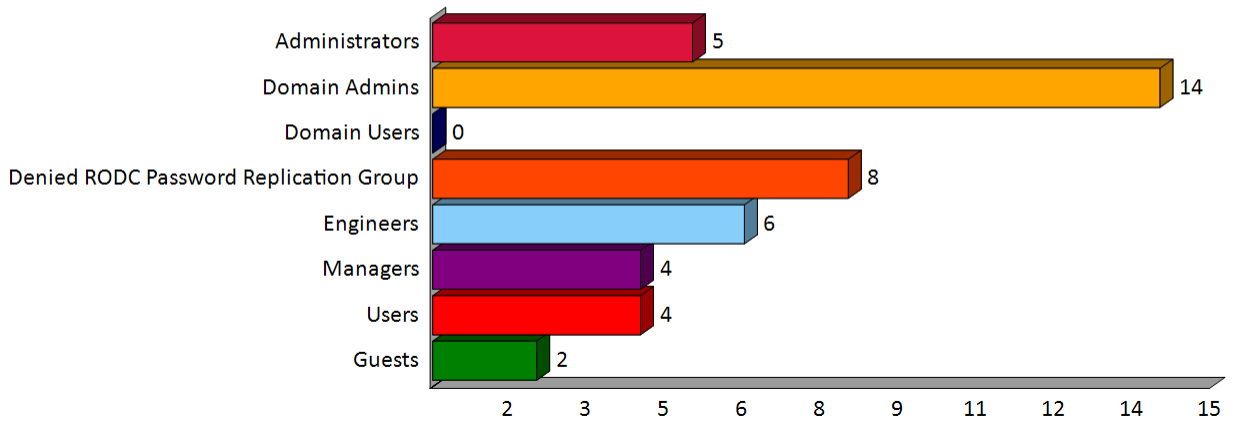
Total Users (18)



Enabled Users (17)

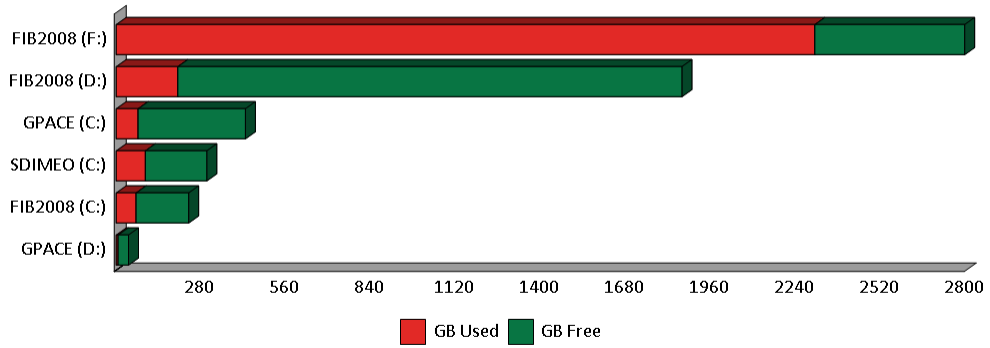


Security Group Distribution
 (Admin Groups + Top 5 Non-Admin Groups)

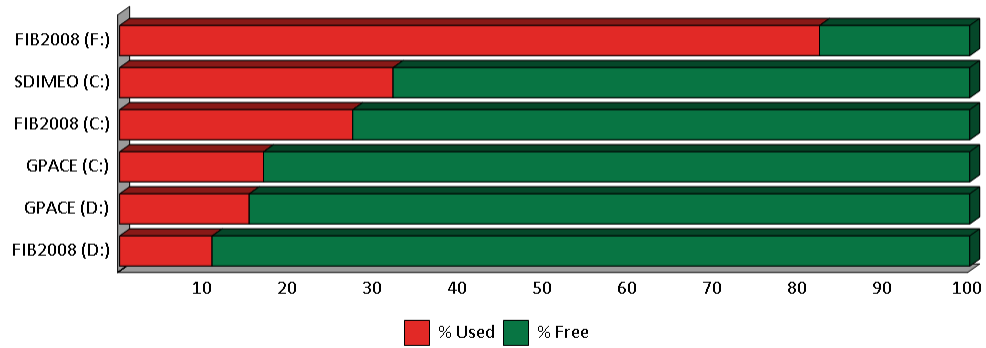


Asset Summary: Storage

Top 10 Drive Capacity



Top 10 Drive % Used





NETWORK ASSESSMENT

Top 10 Drive Free Space

