Network Assessment
Risk Report
Sample Client

Prepared by:
PDC Technologies

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.

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

Issue: We discovered 23 active user accounts that have not logged in within the past 30 days.
Recommendation: Active accounts that are not in use may pose an inherent security risk, especially those that have been used for a prolonged period of time and should be addressed with a User Audit. These accounts should be reviewed and disabled or removed if they are no longer needed. The accounts could be used by a malicious attacker both internally and externally. The National Institute of Standards (NIST) recommends disabling any account with 90 days of inactivity. We suggest reviewing active users and disabling or removing accounts which are no longer needed.

Inactive Computers

Issue: 87 computers were found as having not checked in during the past 30 days.
Recommendation: By itself, this does not pose a serious threat, but proper organization and management is essential for good network administration and to providing accurate domain statistics and information. Inactive computers in active directory may represent computers that are no longer in use. While this poses limited risk to the organization, we recommend a more detailed and thorough review of Active Directory to identify machines that have not reported in and removing all defunct entries.

Organizational Units

Issue: We discovered 16 populated Organizational Units.
Recommendation: It's a good idea to periodically 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. Organization Units (OU) are the building blocks of good network security in an Active Directory environment. While there is no correct answer to the proper number of OUs required, having too few is an indicator that the OU structure may not be in line with the security needs of the company. We suggest reviewing the business organizational structure and security needs to ensure the proper Organizational Units (OU) structure is in place.

Password Strength Risks

Issue: Local Account Passwords on 7 computers 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.
Recommendation: Inadequate or weak passwords on local accounts can allow a hacker to compromise the system. It can also lead to the spread of malicious software that can cause business and productivity affecting issues. We recommend placing adequate password strength requirements in place and remediate the immediate password issues on the identified systems.

Password Policies

Issue: 29 enabled domain users have passwords that are set to never expire.
Recommendation: The best practice for passwords is to change them on a routine basis. While convenient (and in the case of Service Accounts appropriate), account passwords that are set to never

expire pose a significant security risk. We advise identifying if the accounts listed have a legitimate need for having the password never expire (as in the case of Service Accounts) or should have its policies modified.

Insecure Listening Ports

Issue: 28 computers were found to be 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 typically 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.

Operating System Support

Issue: 40 computers were found to be using an Operating System that is in Extended Support. 6 computers were found to be using an Operating System that is no longer supported by the manufacturer and should be upgraded.

Recommendation: Extended Support means patching and other updates will be unavailable in the near future. Operating system versions that are no longer supported pose a significant security risk as security holes will no longer be addressed. OSes in Extended Support are nearing end of life and should be upgraded before the end of life. We propose reviewing the function and criticality of computers in Extended Support and upgrading systems that are no longer supported.

Critical Patches Missing

Issue: 44 computers were detected as having 1 or more missing critical patches.

Recommendation: Maintaining properly patched systems reduces the risk of infection via malware or viruses and improves performance and stability. Unpatched systems are also less protected against malicious software attacks. This can pose a significant risk to your network. We strongly recommend applying missing patches on identified computers immediately.

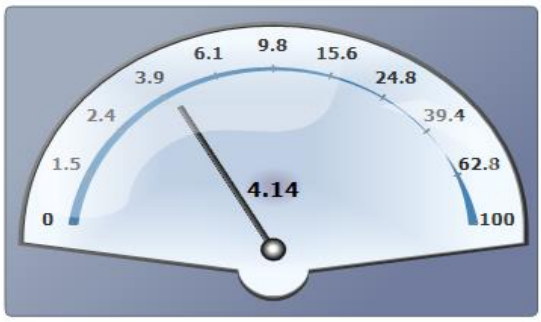
Endpoint Security

Issue: Anti-virus and anti-spyware was scanned for but not detected on 31 computers.

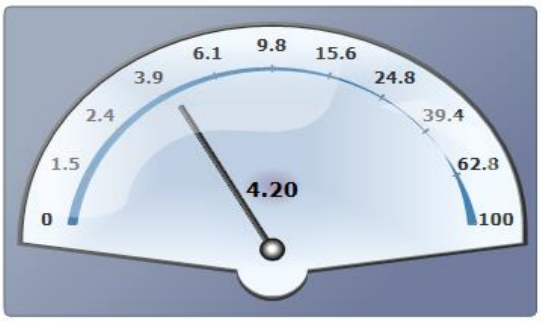
Recommendation: Without adequate anti-virus and anti-spyware protection on all workstations and servers, the risk of acquiring malicious software is significant. Since this can lead to both security and productivity issues, we strongly recommend assuring anti-virus and anti-spyware are deployed to all possible endpoints.

Internet Speed Test Results

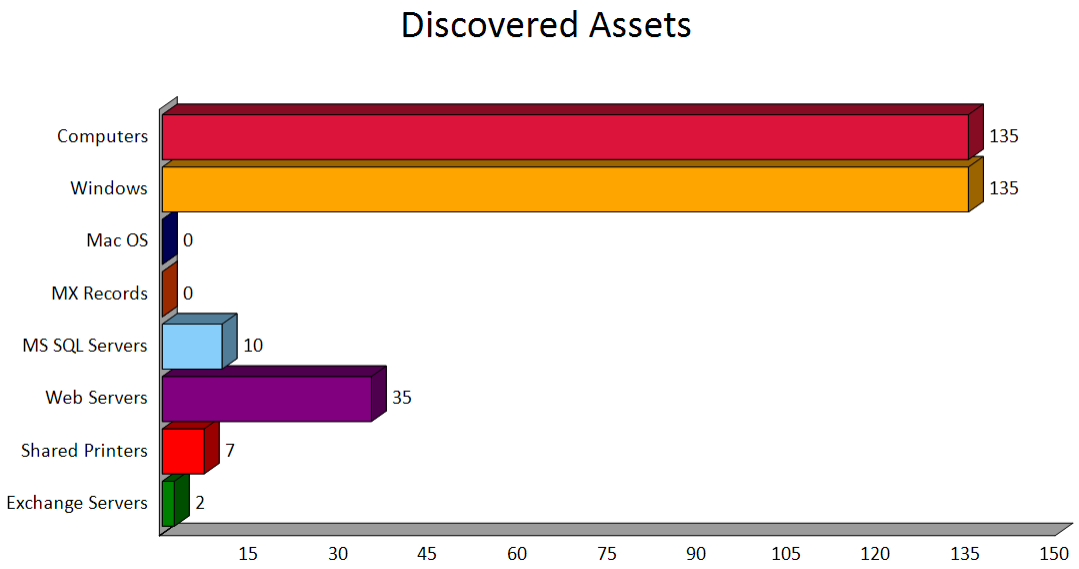
Download Speed: **4.14 Mb/s**



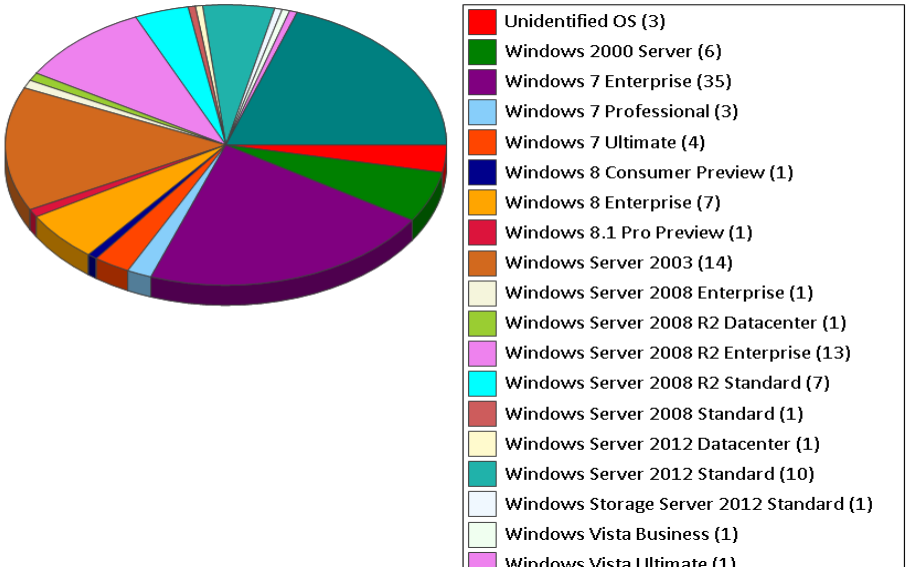
Upload Speed: **4.20 Mb/s**



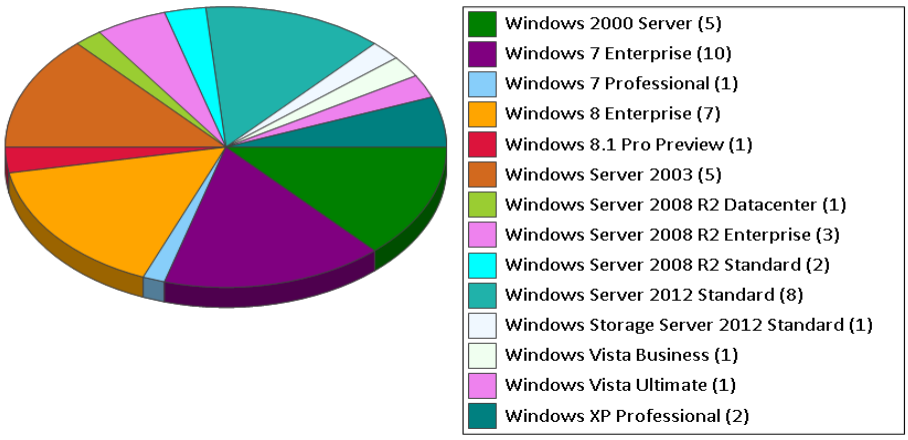
Asset Summary: Discovered Assets



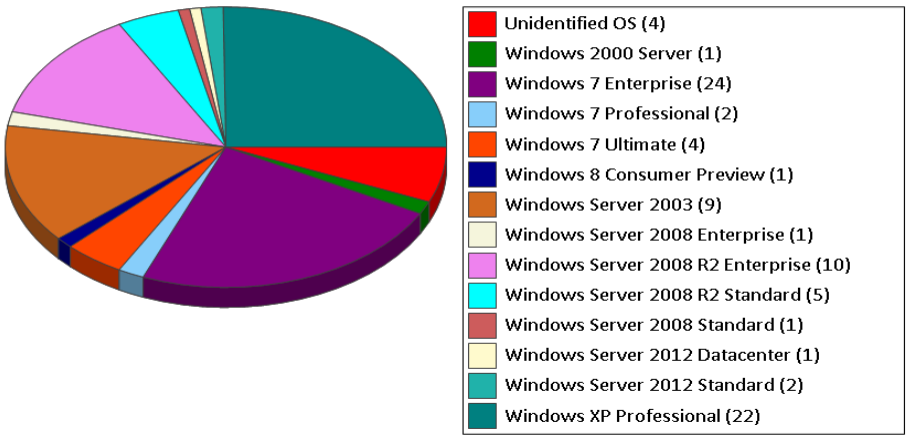
Asset Summary: Computers



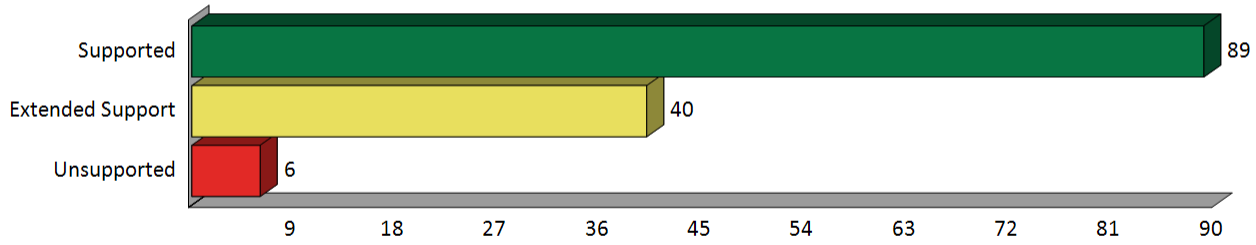
Active Computers by Operating System (48)



Inactive Computers by Operating System (87)

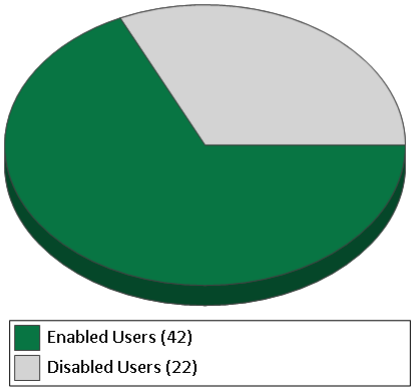


Operating System Support

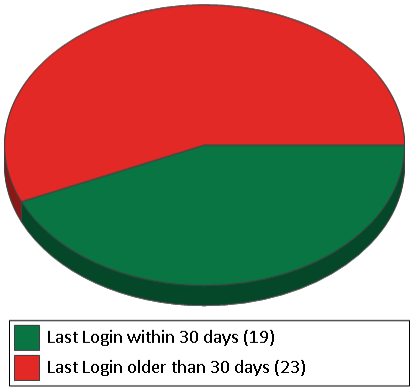


Asset Summary: Users

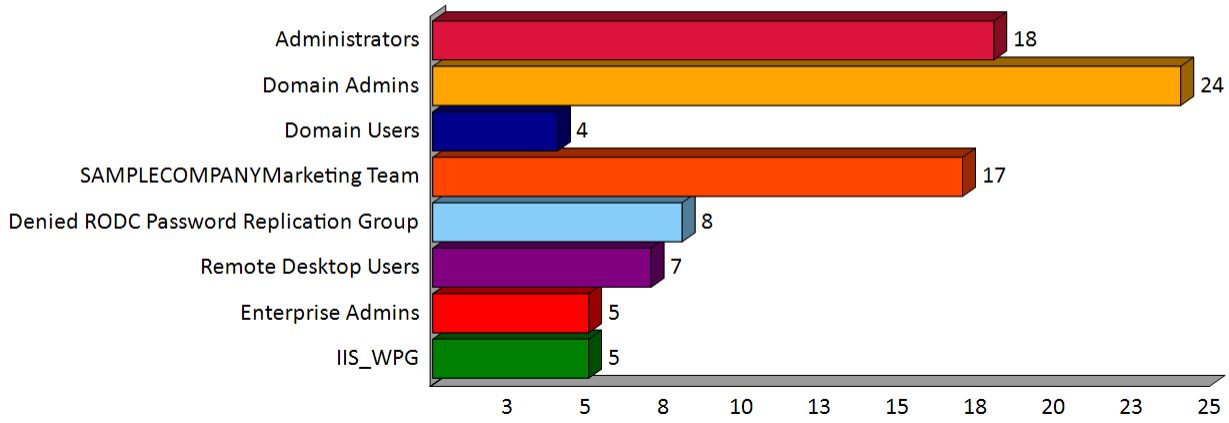
Total Users (64)



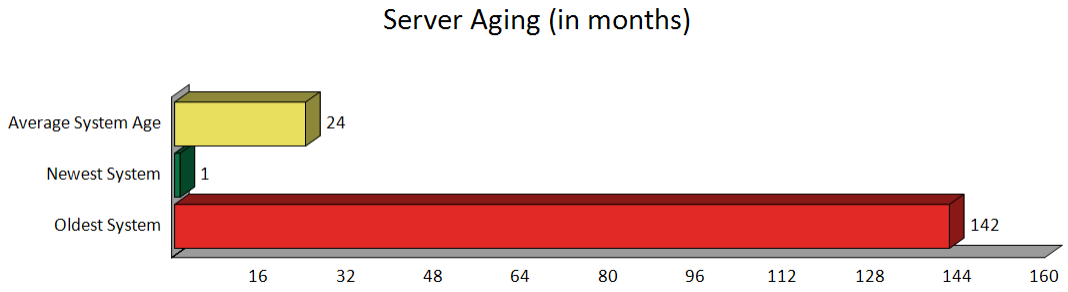
Enabled Users (42)



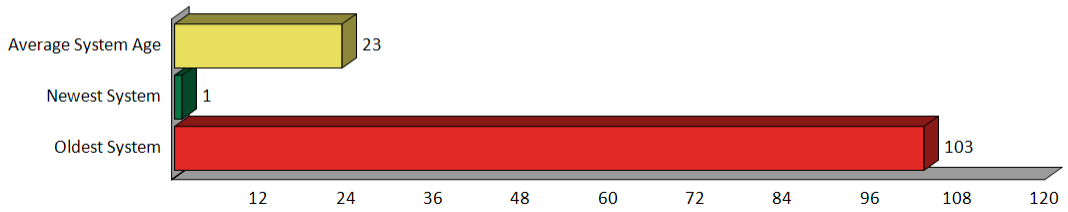
Security Group Distribution
(Admin Groups + Top 5 Non-Admin Groups)



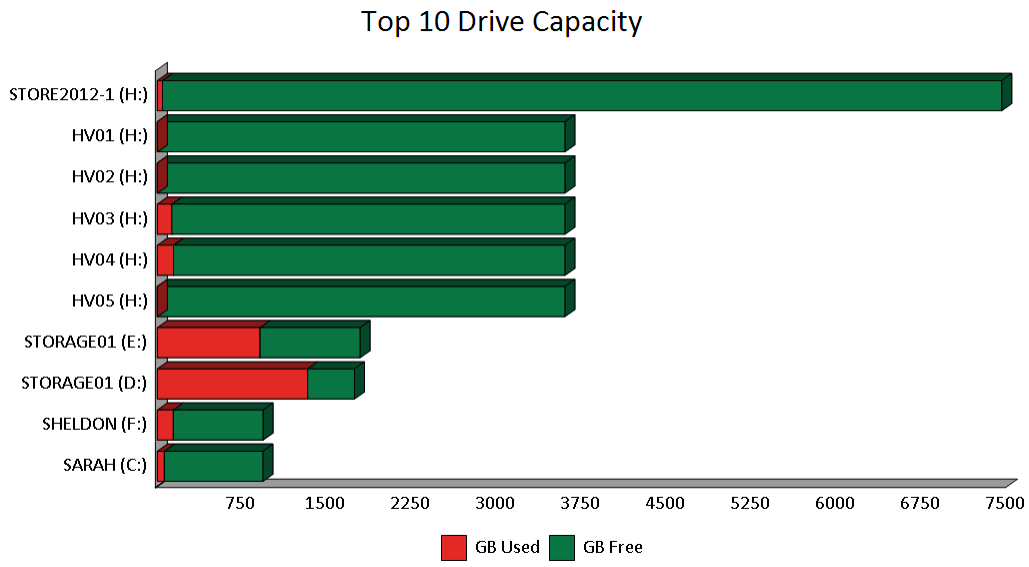
Server Aging

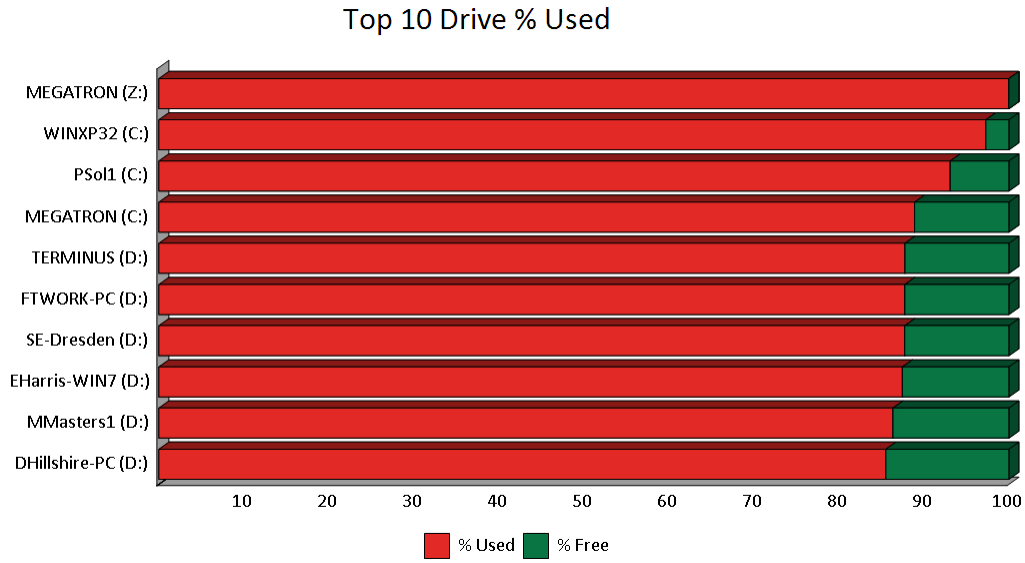


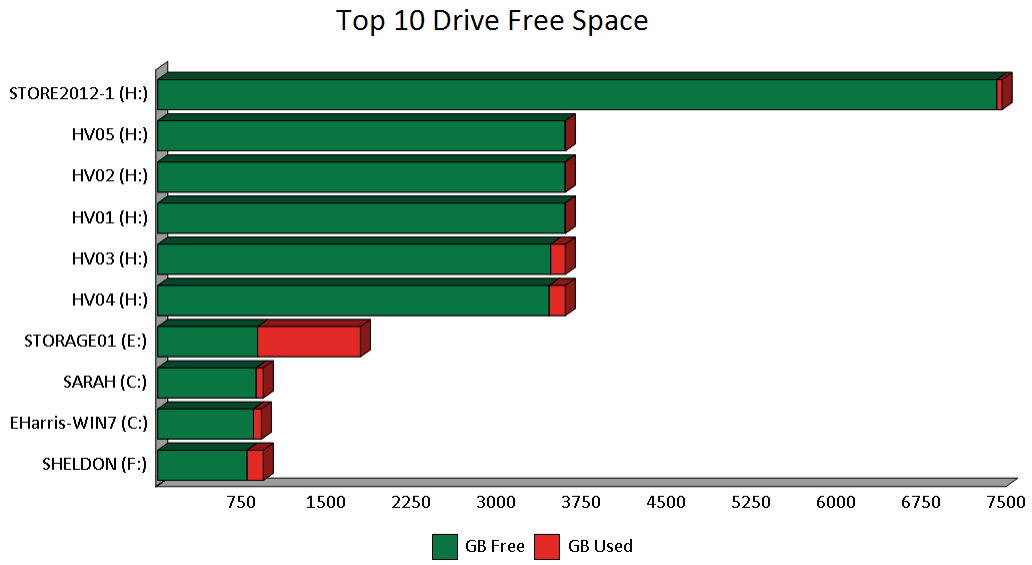
Workstation Aging



Asset Summary: Storage






Top 10 Drive Free Space
STORE2012-1 (H:)
HV05 (H:)
HV02 (H:)
HV01 (H:)
HV03 (H:)
HV04 (H:)
STORAGE01 (E:)
SARAH (C:)
EHarris-WIN7 (C:)
SHELDON (F:)
750
1500
2250
3000
3750
4500
5250
6000
6750
7500
GB Free
GB Used