



Network Assessment
Executive Summary
BC Systems

Prepared by:
PerformancelT Managed Services

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.

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	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.
✓	Event Log Analysis	Last 5 System and App Event Log errors for servers.
✓	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.
✓	Internet Access and Speed Test	Test of internet access and performance.

Risk Score

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



Several critical issues were detected and should be investigated and corrected immediately. Review the summary issues on the following page and the full report for details.

Issues Summary

This section contains summary of issues detected during the Network Assessment. It is based on general best practices and may indicate existing issues or points of interest.

Inactive Users

We discovered 25 active users that have not logged in within the past 30 days. These accounts most likely need to be disabled or removed if the users are no longer active. Active accounts that are not in use may pose a security risk and should be addressed with a User Audit.

Inactive Computers

We discovered a total of 24 computers of which only 10 have registered with the domain controller in the past 30 days. There are 14 computers entries that may no longer be relevant. While not inherently harmful, the defunct systems should be removed from Active Directory routinely.

Organizational Units

We discovered 6 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

1 offline domain controller was discovered and should be investigated. An offline domain controller may be a remnant of decommissioning a server which was not properly removed from the domain. With only 1 online Domain Controller, there is a high risk of significant outage due to a lack of redundancy.

Password Strength Risks

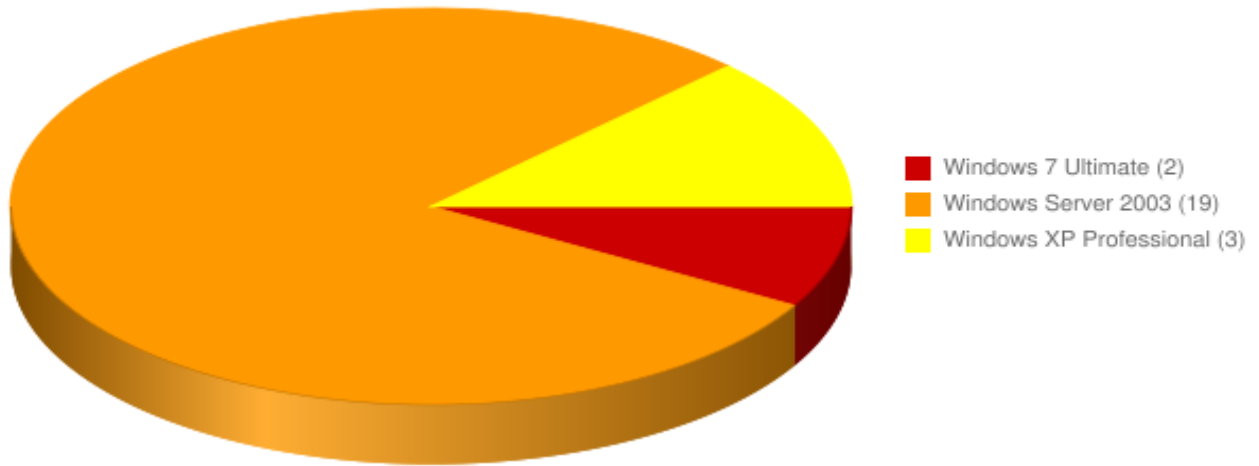
Passwords on 1 computer were found to be Potential Risks. 1 computer was found to have Severe Risks. These are systems where passwords are extremely weak or not set and should be rectified to prevent unauthorized access or the potential spread of viruses and worms.

Insecure Listening Ports

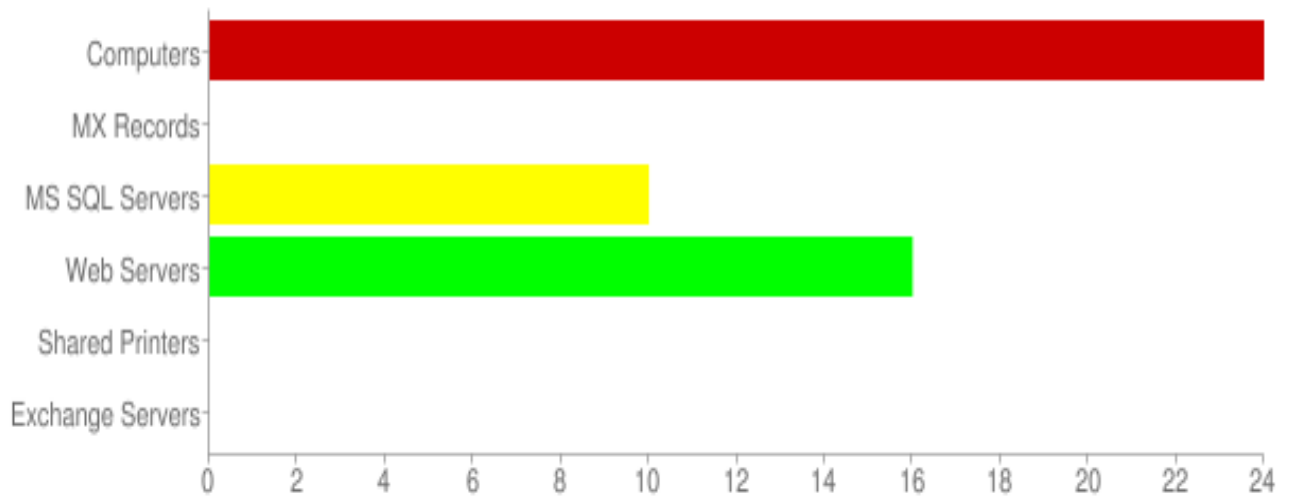
5 computers were detected as using potentially insecure protocols. There may be a legitimate need to use these protocols, but risks should be assessed to prevent unauthorized access.

Asset Summary

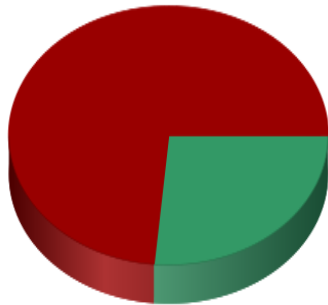
Computers by Operating System (24)



Discovered Assets

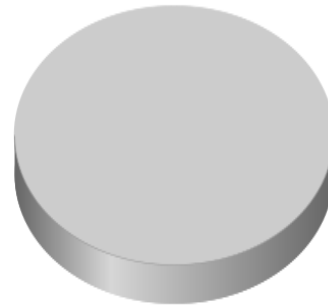


Enabled Users (34)



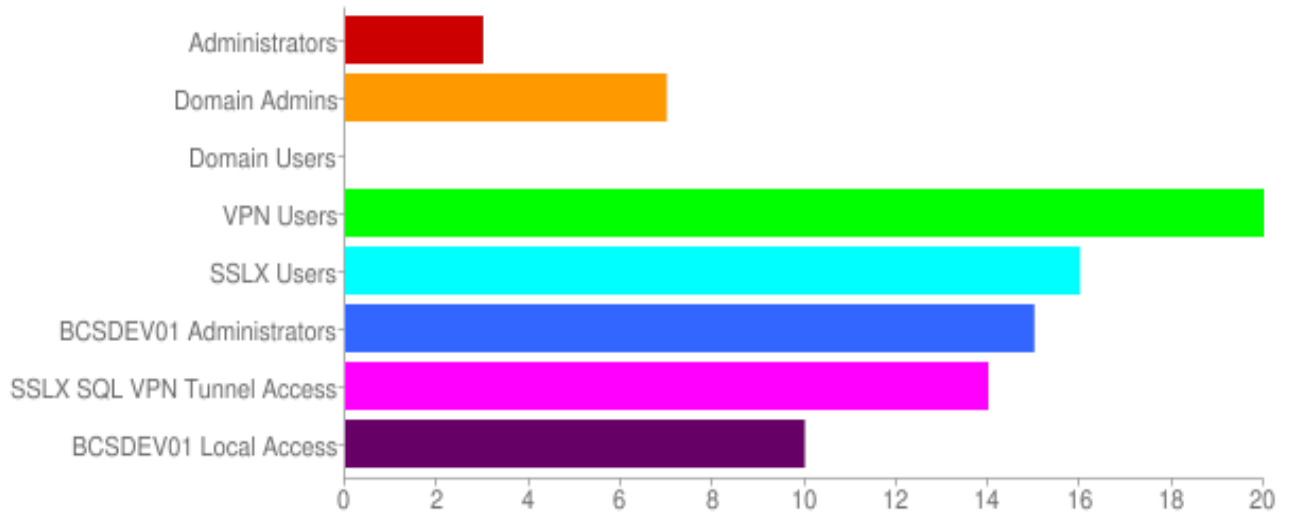
■ Last Login within 30 days (9)
■ Last Login older than 30 days (25)

Disabled Users (2)

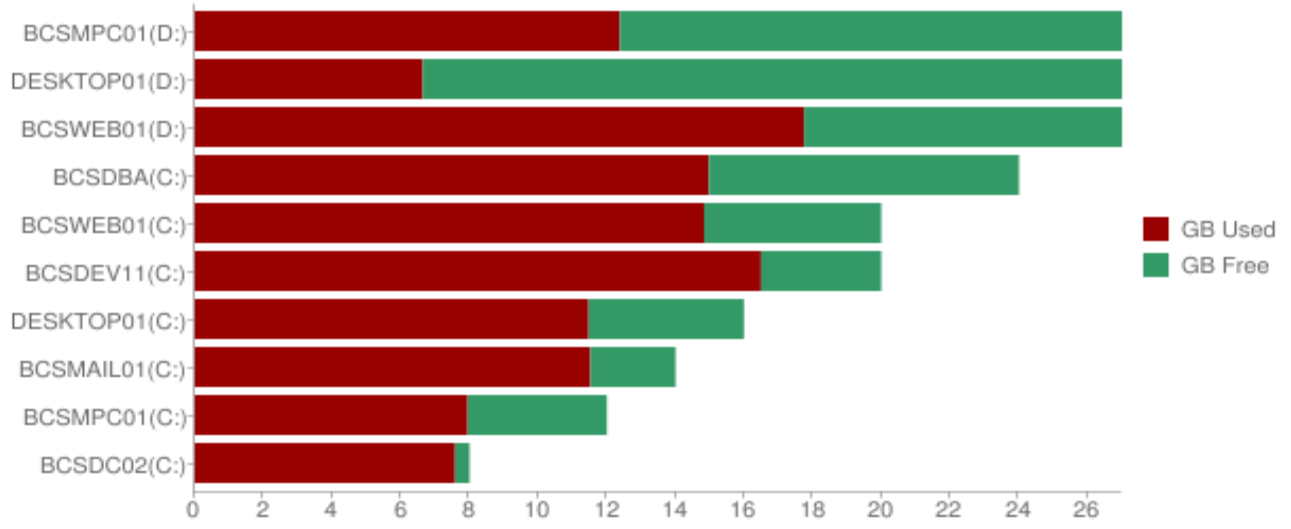


■ Last Login within 30 days (0)
■ Last Login older than 30 days (2)

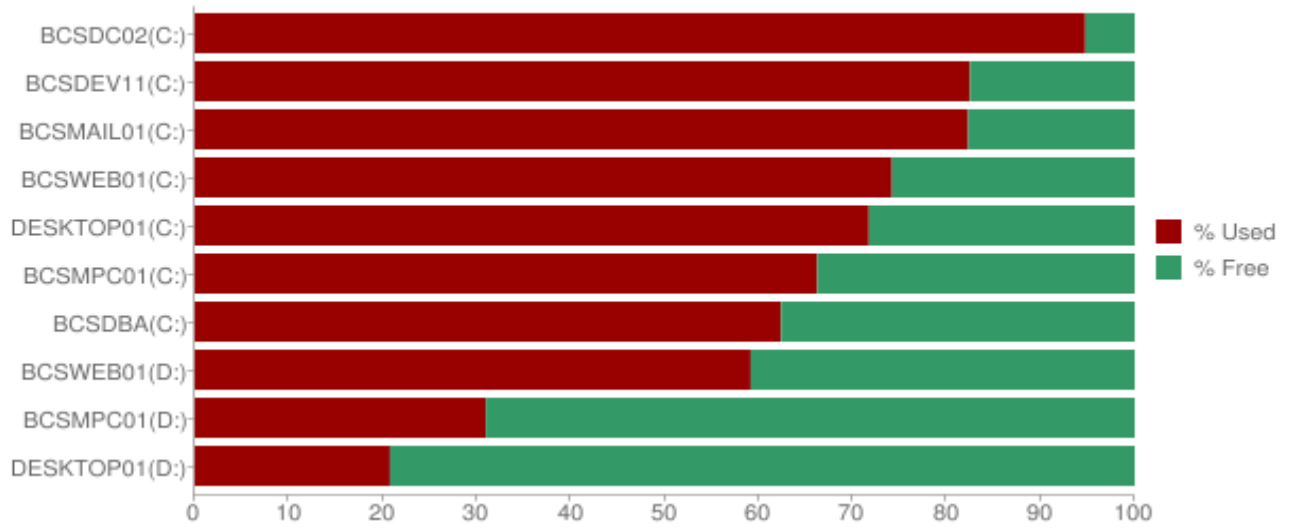
User Security Role Distribution (Admin and Top 5)



Top 10 Drive Capacity



Top 10 Drive % Used



Top 10 Drive Free Space

