This Assessment has been truncated to show sample data.

Technical Review

Prepared for:
BIG

Prepared by:
Copper Mountain Consulting
02/01/2025

Technical Assessment

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.

Scan Date: 02/01/2025

Table of Contents

1 - Discovery Tasks

This table contains a listing of all tasks which were performed as part of this assessment. Items which do not contain a check were not performed.

	TASK	DESCRIPTION
✓	Detect Azure Environment	Scan for Azure AD and infrastructure components.
✓	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.
✓	SQL Server Analysis	Lists the SQL Servers and associated database(s).
✗	Internet Domain Analysis	Queries company domain(s) via a WHOIS lookup.

	TASK	DESCRIPTION
✓	Missing Security Updates	Identifies computers missing security updates.
✓	System by System Event Log Analysis	Discovers the file system and app event log errors for servers.
✓	External Security Vulnerabilities	Lists the security holes and warnings from External Vulnerability Scan.

2 - Assessment Summary

AZURE ACTIVE DIRECTORY	
Azure AD Domains	5
Azure AD Applications	14
Azure AD Web URLs	6
Azure AD Organization Contacts	100
Azure AD Service Plans	69
Azure AD Subscribed SKUs	15
Azure AD Groups - Cloud Only	119
Azure AD Groups - On Premise Synced	0
Azure AD Users	258
Azure AD Devices	331
Azure AD User Devices	320

AZURE AD DEVICES BY OS	
Android 9	1
Windows 10	330

AZURE INFRASTRUCTURE	
Azure AD Domains	5
SharePoint Site Collections	0

AZURE INFRASTRUCTURE

SharePoint Web URLs	0
Teams	33
Azure Virtual Machines	0
Azure Cloud Services	0
Azure Cloud Service Roles	0
Azure Cloud Service Slots	0
Azure Entity Relationships	0
Azure Load Balancers	0
Azure Resource Groups	0
Azure Subscriptions	2
Azure SQL Servers	0
Azure Databases	0

ACTIVE DIRECTORY DOMAIN

Domain Controllers	2
Number of Organizational Units	13

ACTIVE DIRECTORY USERS

# Enabled	148
Last Login Within 30 Days	101
Last Login Older Than 30 Days	47
# Disabled	103

ACTIVE DIRECTORY USERS

Last Login Within 30 Days	4
Last Login Older Than 30 Days	99

ACTIVE DIRECTORY SECURITY GROUPS

Groups with Users	152
# Total Groups	209

ACTIVE DIRECTORY COMPUTERS

Total Computers	366
Last Login Within 30 Days	149
Last Login Older Than 30 Days	217

ACTIVE DIRECTORY COMPUTERS BY OS

Other	3
macOS	1
pc-linux-gnu	1
Windows 10 Enterprise LTSC	1
Windows 10 IoT Enterprise LTSC	5
Windows 10 IoT Enterprise LTSC Version 21H2	2
Windows 10 Pro	84
Windows 10 Pro for Workstations	4
Windows 10 Pro for Workstations Version 21H2	1

ACTIVE DIRECTORY COMPUTERS BY OS

Windows 10 Pro for Workstations Version 22H2	3
Windows 10 Pro N	1
Windows 10 Pro N Version 22H2	1
Windows 10 Pro Version 21H2	1
Windows 11 Pro	26
Windows 11 Pro for Workstations	1
Windows 11 Pro for Workstations Version 23H2	1
Windows 11 Pro Version 24H2	1
Windows 7 Professional	3
Windows Server 2008 R2 Enterprise	1
Windows Server 2008 R2 Standard	1
Windows Server 2012 R2 Standard	1
Windows Server 2016 Standard	1
Windows Server 2019 Datacenter	1
Windows Server 2022 Standard	4

MISCELLANEOUS

Non-A/D Systems	43
MX Records	0
MS SQL Servers	14
Web Servers	42

MISCELLANEOUS

Printers	33
Exchange Servers	0
Network Shares	56
Installed Applications	880
Potential Insecure Listening Ports	9
External Network Security (High Risk)	17
External Network Security (Medium Risk)	94

LOCAL ACCOUNTS

# Enabled	31
Last Login Within 30 Days	2
Last Login Older Than 30 Days	29
# Disabled	47
Last Login Within 30 Days	0
Last Login Older Than 30 Days	47

3 - Azure: BIG

3.1 - Organization

The organization is the highest-level entity in the Microsoft Cloud and represents the owner of the Azure AD environment. Below is a listing of the general contact information of the organization along with the configured technical notification email. Please ensure the information is accurate and up to date to avoid misdirected notices and delays in communication of key account and infrastructure issues.

Display Name	BIG
Street	
State	
City	
Postal Code	
Country	US

Technical Notifications sent to:

-

3.2 - Domains

The organization can support multiple domains both external and internal. Domains are required to be verified before they can be actively used. Verification can be done through multiple techniques, including special external DNS records. The primary default domain is highlighted in bold. Authentication be managed directly by Azure AD or federated.

DOMAIN	PARENT DOMAIN	AUTHENTICATION TYPE	IS ADMIN MANAGED	IS DEFAULT	IS INITIAL	IS ROOT	IS VERIFIED

DOMAIN	PARENT DOMAIN	AUTHENTICATION TYPE	IS ADMIN MANAGED	IS DEFAULT	IS INITIAL	IS ROOT	IS VERIFIED
BIG.com		Managed	Yes	Yes	No	Yes	Yes
BIG.mail.onmicrosoft.com		Managed	Yes	No	No	Yes	Yes
BIG.microsoftonline.com		Managed	Yes	No	No	Yes	Yes
BIG.onmicrosoft.com		Managed	Yes	No	Yes	Yes	Yes

3.3 - Supported Services

One or more services can be supported by the Azure AD environment per domain. The table below lists all managed domains and the supported services. The most common supported service is Email, which allows the sending and receiving of emails both internally and externally.

DOMAIN	SUPPORTED SERVICES
BIG.com	Email; Email Internal Relay Only; Org Id Authentication
BIG.microsoftonline.com	Email Internal Relay Only
BIG.onmicrosoft.com	Email; Office Communications Online
little.com	Email; Office Communications Online; Org Id Authentication; Intune

3.4 - On Premise Sync

Some configurations of Azure AD involve on-premise domain controllers where settings from the cloud are synced to and from. If On Premise Sync is enabled, the last time is documented here. If the last sync time is greater than 15 days, it is highlighted in red, possibly indicating syncing issues or a misconfiguration and should be investigated.

PROPERTY	SETTING
On Premise Sync Enabled	Yes
On Premise Sync Last Synced	01/31/2025 2:55:43 PM -06:00

3.5 - Applications

Beyond standard Microsoft services, the Microsoft Cloud and Azure AD can support custom applications. These applications become part of the Azure AD and may have direct access to certain resources that are part of the Microsoft Cloud infrastructure. It is important to periodically review applications to ensure that the minimum necessary are installed and configured properly.

DISPLAY NAME	APP ID	SIGN IN AUDIENCE	IS FALLBACK PUBLIC CLIENT	CLIENT SECRET EXPIRES
Barracuda Essentials for Outlook	2bb9e6d9-ea40-4af7-8863-8f5bbb98afe2	My Org		
SharePoint Online Client Extensibility Web Application Principal	5a60b5b8-ed5e-4aef-8b20-fefa5db5e83d	My Org		02/24/2072 12:22:45 AM +00:00
SharePoint Online Client Extensibility Web Application Principal Helper	a4a3e60a-60bd-4b42-8a79-989ae546c09c	My Org		

3.6 - Web URLs

Web URLs can be published by Azure AD for custom applications. Three primary URLs can be specified including a Home Page URL, Redirect URIs, and a Logout URL. These are typically configured by the administrator when installing the application. Periodic audits of Web URLs are highly recommended to avoid misconfiguration due to human error and to ensure malicious applications do not direct users to non-approved sites.

APPLICATION	HOME PAGE URL	REDIRECT URIS	LOGOUT URL
SharePoint Online Client Extensibility		https://BIG-	

APPLICATION	HOME PAGE URL	REDIRECT URIS	LOGOUT URL
Web Application Principal		admin.sharepoint.com/_forms/spfxsinglesignon.aspx	
SharePoint Online Client Extensibility Web Application Principal Helper		https://BIG-admin.sharepoint.com/_forms/spfxsinglesignon.aspx	

3.7 - Organization Contacts

Organization contacts represent external email addresses that are managed and can be used in the Azure AD environment. These entities exist alongside standard users and groups and are often seen globally. It is important to ensure organization contacts are configured to the proper external email addresses and authorized.

DISPLAY NAME	MAIL	MAIL NICKNAME	GIVEN NAME	SURNAME

3.8 - Proxy Addresses

The following table lists proxy addresses for various mail accounts. If Azure AD is being synchronized with an external Active Directory, a set of Azure AD settings govern whether the addresses are synchronized or not. Proxy addresses can contain various address entry types including SMTP addresses, X500 addresses, SIP addresses, as well as others.

LABEL	DISPLAY NAME	DESCRIPTION	MAIL	PROXY ADDRESSES

3.9 - Service Plans

The following table lists the various service plans available the organization and their provisioning status. Plans can be applied to company, group, or user levels as indicated in the table below. Success indicates that the plan was properly provisioned and is available for use with the target entities. Please note that the availability of a plan does not mean the actual use of licenses of the plans.

SERVICE PLAN NAME	PROVISIONING STATUS	APPLIES TO
ATP_ENTERPRISE	Success	Company
BI_AZURE_P0	Success	User
BI_AZURE_P2	Success	User
SHAREPOINT_PROJECT	Success	User
SHAREPOINTENTERPRISE	Success	User

3.10 - Subscribed SKUs

The following table lists the Subscribed SKUs along with their current license consumption. High consumption may be an indicator that additional licenses may be required in the near future.

PRODUCT NAME	CAPABILITY STATUS	CONSUMED UNITS	PREPAID UNITS			SERVICE PLANS	APPLIES TO
			ENABLED	SUSPENDED	WARNING		
Microsoft Defender for Office 365 (Plan 1)	Enabled	97	102	0	0	ATP_ENTERPRISE	User
Office 365 E3	Enabled	101	105	0	0	Bing_Chat_Enterprise CDS_O365_P2 CLIPCHAMP ContentExplorer_Standard Deskless DYN365_CDS_O365_P2 EXCHANGE_S	User

3.11 - Groups

Groups are used for various purposes in the Microsoft Cloud, including mail distribution groups, security groups, and Microsoft Teams. Groups that have the Mail Enabled property active can be emailed internally and externally depending on the visibility. Traditional Active Directory groups can be mapped to Azure AD groups by looking at the Mail Enabled and Security Enabled settings. Security groups will have Mail Enabled set to

No and Security Enabled set to Yes. Mail Enabled security groups will have Mail Enabled set to Yes and Security Enabled set to Yes. Distribution groups have Mail Enabled set to Yes and Security Enabled set to No.

The list of groups should be reviewed on a periodic basis to ensure settings and visibility are configured properly, as well as to reduce the number of groups to the minimum necessary to avoid security risks.

3.11.1 - Cloud Only

DISPLAY NAME	DESCRIPTION	MAIL	MAIL ENABLED	MAIL NICKNAME	SECURITY ENABLED	VISIBILITY

3.11.2 - On Premise Synced

On Premise Synced Groups Table is unavailable.

3.12 - Users

Users represent the base level accounts in Azure AD. Users are typically associated with people, but may be used for shared accounts, emails accounts, and users required for application access. The management of users to the minimum necessary is crucial to the security of any environment. The user list should be reviewed periodically to ensure that no terminated users or unnecessary accounts are still active in the list of users.

Users shown having MFA Enabled may be different from amounts reported by Microsoft because of differences in calculations.

Last login date based on data collected and synced with Microsoft. Logins within the last 24 hours may not have synced prior to scan.

Premium subscription to Azure Active Directory required to retrieve additional user data including MFA enabled/disabled and Last Login details.

Note: This table lists only accounts that have administrative access through a built-in administrator role. Some accounts may be given specific administrative privileges through custom roles and permissions.

DISPLAY NAME	GIVEN NAME	SURNAME	JOB TITLE	ADMIN	GLOBAL ADMIN	MFA ENABLED	MAIL	ENABLED/ DISABLED	LAST LOGIN
				No	No			Enabled	
				No	No			Enabled	
				No	No			Disabled	
				No	No			Enabled	
				No	No			Enabled	
				Yes	No			Disabled	
			IT Systems Administrator	Yes	Yes			Enabled	
			Director of Hardware Engineering	No	No			Enabled	
			Field Application Engineer	No	No			Enabled	
				No	No			Enabled	
			General Manager	Yes	Yes			Enabled	
				Yes	Yes			Enabled	

3.13 - Guest Users

A guest is a user who isn't considered internal to the company, such as an external collaborator, partner, or customer. Guest users utilize their own work, school, or social identities or credentials to access your apps and services, regardless of whether they have an Azure AD account.

The Guest user list should be reviewed periodically to ensure that only authorized users are listed.

Guest Users Table is not available.

3.14 - Devices

The following list of devices have been registered directly with Azure AD. Please note that some devices may be registered with on premise Active Directory environments and may not appear in the list of Azure AD devices. Devices must be registered by the device owner, who themselves must be an Azure AD user.

DISPLAY NAME	OS NAME	OS VERSION	PHYSICAL IDS	PROFILE TYPE	TRUST TYPE	APPROXIMATE LAST SIGN IN	OWNER
CORP-D-0031	Windows	10.0.22631.3296	[USER-HWID]:f7244718-bf6a-49ec-93a2-26e521af71fd:6755466231811533	RegisteredDevice	Workplace	01/28/2025 7:00:22 PM -06:00	
CORP-L-0005	Windows	10.0.19045.3996	[USER-HWID]:cbd4d56e-1490-448a-aeae-b6f854e7caa3:6825824411359941	RegisteredDevice	Workplace	01/22/2025 9:41:28 AM -06:00	
CORP-L-0006	Windows	10.0.19045.4355	[USER-HWID]:724d7e90-2c82-4f23-baaa-81bf6f089df6:6966560311103419	RegisteredDevice	Workplace	01/31/2025 12:23:24 PM -06:00	
CORP-L-0006	Windows	10.0.19045.3996	N/A	RegisteredDevice	Workplace	06/11/2024 6:54:05 AM -05:00	
CORP-L-0007	Windows	10.0.19045.3996	[USER-HWID]:4547ce86-3b66-4b85-b68a-0989de502f9d:6966560305097431	RegisteredDevice	Workplace	01/20/2025 9:18:06 AM -06:00	
CORP-L-0008	Windows	10.0.19045.3	[USER-	RegisteredDevi	Workplace	01/03/2025	

DISPLAY NAME	OS NAME	OS VERSION	PHYSICAL IDS	PROFILE TYPE	TRUST TYPE	APPROXIMATE LAST SIGN IN	OWNER
		996	HWID]:3ffa87f1-58b6-47bf-99c2-49215a9f79c9:6896196228266096	ce		10:46:08 AM -06:00	
CORP-L-0009	Windows	10.0.19045.3996	[USER-HWID]:cc863591-61fc-48c5-bde5-7a25a9dea29e:6755463782138343	RegisteredDevice	Workplace	01/30/2025 9:06:52 PM -06:00	

3.15 - Azure Subscriptions

Azure Subscriptions

SUBSCRIPTION ID	DISPLAY NAME	UNIQUE KEY	STATE
	Azure subscription 1		Enabled
	Azure subscription 1		Enabled

3.16 - Azure Resource Groups

Azure Resource Groups

Azure Resource Group Data is not available.

3.17 - Azure Load Balancers

Azure Load Balancers

Azure Load Balancer Data is not available.

3.18 - Azure Virtual Machines

Azure Virtual Machines

Azure Virtual Machine Data is not available.

3.19 - Azure App Services

Azure App Services

Azure App Service Data is not available.

Azure Cloud Service Slots

Azure Cloud Service Slot Data is not available.

Azure Cloud Service Roles

Azure Cloud Service Role Data is not available.

3.20 - Azure SQL Servers

Azure SQL Servers

Azure SQL Server Data is not available.

3.21 - Azure Databases

Azure Databases

Azure Database Data is not available.

3.22 - Azure Cloud Services

Azure Cloud Services

Azure Cloud Service Data is not available.

4 - Domain: BIG.LOCAL

This section and corresponding sub-sections contain a comprehensive view of the domain.

4.1 - Domain Controllers

This section contains a listing of all domain controllers and their corresponding status.

DOMAIN CONTROLLER	STATUS
BIG-DC01	online
BIG-DC02	online

4.2 - FSMO Roles

This section contains a listing of all FSMO (Flexible Single Master Operation) roles, which are needed to operate a Windows domain.

ROLE	DOMAIN CONTROLLER	BEST PRACTICE
Infrastructure Master	BIG-DC01.BIG.LOCAL	Domain Specific
Domain Naming Master	BIG-DC01.BIG.LOCAL	Forest Wide
PDC Emulator	BIG-DC01.BIG.LOCAL	Domain Specific
Relative ID (RID) Master	BIG-DC01.BIG.LOCAL	Domain Specific
Schema Master	BIG-DC01.BIG.LOCAL	Forest Wide

4.3 - Organizational Units

This section contains a hierarchical view of all organizational units from within Active Directory.

- **BIG.local**
  - **BIG Company (18 Security Groups, 101 Users, 29 Computers)**
    - **BIG Computers (18 Security Groups, 29 Computers)**
      - **Disabled Computers (27 Computers)**
      - **TestComputers (2 Computers)**
    - BIG Security Groups
    - **BIG Service Accounts (2 Users)**
    - **BIG Users (2 Users)**
    - **Disabled Users (97 Users)**
  - **Consultant (5 Users)**
  - **Domain Controllers (2 Computers)**
  - **Just In Time Accounts (2 Users)**
  - **Security Groups (84 Security Groups)**
  - **User Groups (28 Security Groups)**

4.4 - Group Policy Objects

This section contains a hierarchical view of all group policy objects from within Active Directory. Policies highlighted in green represent enabled policies.

- **BIG.local**
    - **(WIP) Deploy Company Authorized Certificates**
    - **Allow Remote Support**
    - Alta mapped Drives
    - Bambu Software Deploy
    - **BIG Printers**
    - **BIG Printers Non Admin**
    - **CPU_Allow_Configure_NIC**
    - **Default Domain Policy**
    - Deploy Cyber Security Software Standard
    - Deploy FAE Programs and Policies
    - Deploy Software Engineer Programs
    - Deploy Software Engineering Environment (WIP)
    - Deploy Standard Software
    - **Deploy User Cyber Security Policies**
    - **Enable SNMP**
    - **FAE Computer Policy**
    - **Force USB Device Encryption**
    - **Hardware Engineering RD Computer Policy**
    - **Noynim_ Deploy Cyber Security Software Standard**

- **NOYNIM_Deploy FAE Programs and Policies**
- **NOYNIM_Deploy Software Engineer Programs**
- **NOYNIM_Deploy Standard Software**
- **NOYNIM_Publish Standard Software**
- **Production Computer Policy**
- Publish Standard Software
- **Server Audit Policy**
- **SNMP Settings**
- **Windows 10 Machine Update Policy**
- **Domain Controllers (1-GPO, 1-Enabled)**
    - **Default Domain Controllers Policy**

4.5 - Users

This section contains a list of accounts with information on each account. Disabled accounts are highlighted in gray. Inactive users, defined as those that have not logged in 30 days, are highlighted in the Last Login column in **RED BOLD.** Accounts where passwords are set to never expire are highlighted in the Password Expires column in RED. Users with passwords that have expired are indicated in the Password Expires column in **RED BOLD.**

Active Users

USERNAME	DISPLAY NAME	ENABLED	PASSWORD LAST SET	PASSWORD EXPIRES	LAST LOGIN
.\JENKINS	N/A	enabled	N/A	N/A	N/A
.\NTP	N/A	enabled	N/A	N/A	N/A
BIG.LOCAL\		enabled	09/05/2024 11:12:43 AM	03/04/2025 11:13:59 AM	01/31/2025 2:50 PM
BIG.LOCAL\		enabled	09/05/2024 11:08:07 AM	03/04/2025 11:09:23 AM	01/31/2025 1:38 PM
BIG.LOCAL\		enabled	10/28/2024 2:47:45 PM	<never>	01/31/2025 8:35 AM
BIG.LOCAL\	QA	enabled	06/04/2013 5:01:11 PM	<never>	02/01/2025 12:01 AM
BIG.LOCAL\		enabled	12/16/2024 8:04:21 AM	06/14/2025 8:05:37 AM	01/31/2025 8:02 AM
BIG.LOCAL\		enabled	02/04/2019 9:04:27 AM	<never>	01/31/2025 3:49 AM
BIG.LOCAL\		enabled	11/04/2024 6:34:40 AM	05/03/2025 6:35:56 AM	01/30/2025 5:36 PM
BIG.LOCAL\		enabled	10/07/2024 1:43:59 PM	04/05/2025 1:45:15 PM	01/31/2025 1:30 PM
BIG.LOCAL\		enabled	12/30/2024 8:11:43 AM	06/28/2025 8:12:59 AM	01/30/2025 5:12 PM

Inactive Users

USERNAME	DISPLAY NAME	ENABLED	PASSWORD LAST SET	PASSWORD EXPIRES	LAST LOGIN
BIG.LOCAL		disabled	01/23/2025 8:09:47 AM	<never>	**01/30/2025 8:56 AM**
BIG.LOCAL\		disabled	06/17/2024 12:11:51 PM	12/14/2024 12:13:07 PM	**06/17/2024 12:12 PM**
BIG.LOCAL\admin	admin	enabled	01/28/2013 3:59:43 PM	<never>	**03/30/2017 3:49 PM**
BIG.LOCAL\		disabled	01/29/2014 4:13:34 PM	07/28/2014 4:14:50 PM	**02/13/2014 4:45 AM**
BIG.LOCAL\		disabled	04/08/2022 10:47:08 AM	<never>	**04/13/2022 3:35 PM**
BIG.LOCAL\		disabled	11/26/2023 9:48:12 PM	05/24/2024 9:49:28 PM	**11/27/2023 8:13 AM**
BIG.LOCAL\		disabled	06/21/2017 10:00:22 AM	12/18/2017 10:01:38 AM	**09/14/2017 1:29 PM**

4.6 - Service Accounts

This section contains a list of service accounts with information on each account.

Enabled Service Accounts

USERNAME	DISPLAY NAME	ENABLED	PASSWORD LAST SET	PASSWORD EXPIRES	LAST LOGIN
.\JENKINS	N/A	enabled	N/A	N/A	N/A
.\NTP	N/A	enabled	N/A	N/A	N/A
BIG.LOCAL\Administrator	Administrator	enabled	12/06/2013 2:29:23 PM	<never>	02/01/2025 4:00 AM
BIG.LOCAL\cwienke		enabled	12/18/2023 7:45:28 AM	<never>	01/31/2025 2:40 PM
BIG.LOCAL\FogBugz		enabled	01/26/2015 9:51:55 PM	<never>	01/27/2025 1:12 PM
BIG.LOCAL\qa		enabled	06/04/2013 5:01:11 PM	<never>	02/01/2025 12:01 AM

Disabled Service Accounts

USERNAME	DISPLAY NAME	ENABLED	PASSWORD LAST SET	PASSWORD EXPIRES	LAST LOGIN
BIG.LOCAL\NoynimAdmin	NoynimAdmin	disabled	07/30/2024 11:03:50 AM	01/26/2025 11:05:06 AM	**10/07/2024 3:45 PM**

4.7 - Security Groups

This section contains a listing of all security groups from Active Directory with detailed information on group membership by user account.

GROUP NAME	MEMBERS
Access Control Assistance Operators *(BIG.local/Builtin/Access Control Assistance Operators)* 0 Total: 0 Enabled, 0 Disabled	

4.8 - Active Directory Computers

This section contains a listing of all computers from Active Directory. Computers which have not logged in for over 30 days are marked as inactive computers and highlighted in red. Disabled computers are highlighted in gray.

Active Computers

COMPUTER NAME	IP ADDRESS(ES)	NETMASK	CIDR	DNS ENTRY	ENABLED	OPERATING SYSTEM	LAST LOGIN
	192.168.128.66				enabled	Windows 10 Pro	01/31/2025 8:47:45 PM
	10.0.0.18				enabled	Windows 10 Pro	01/31/2025 8:29:22 AM
	10.0.0.96				enabled	Windows 10 Pro	01/31/2025 5:36:14 PM
	10.10.00.169				enabled	Windows 10 Pro	01/31/2025 3:54:19 PM
	10.10.00.41				enabled	Windows 10 Pro	01/31/2025 3:26:36 PM
	fe80::d0db:ed22:2a08:2ff0%11,10.10.00.199	255.255.255.0	10.10.00.0/24		enabled	Microsoft Windows Server 2008 R2 Standard	02/01/2025 5:04:04 AM

Inactive Computers

	IP ADDRESS(ES)	NETMASK	CIDR	DNS ENTRY	ENABLED	OPERATING SYSTEM	LAST LOGIN
					disabled	Windows 7 Professional	**11/05/2012 3:10:03 AM**
	10.10.00.44			23348-002.BIG.local	enabled	Windows 7 Professional	**10/29/2012 12:33:26 PM**
					disabled	Windows 7 Ultimate N	**11/05/2012 11:31:22 AM**
					disabled	Windows 7 Professional	**11/05/2012 5:19:06 PM**

4.9 - Server Aging

This section is an indicator of the age of the active servers based on the date their operating system was installed. The actual age of the server may vary if the operating system was re-installed for any reason. Older systems are highlighted in red and much older systems are bolded. Excludes computers that we were unable to retrieve an OS Install Date.

COMPUTER	OPERATING SYSTEM	OS INSTALL DATE	AGE (MONTHS)
	Windows Server 2008 R2 Standard	05/17/2012 4:21:29 PM	153
	Windows Server 2022 Standard	07/07/2023 3:59:50 PM	19
	Windows Server 2022 Standard	11/25/2024 5:44:14 PM	3
	Windows Server 2022 Standard	12/28/2023 2:29:03 PM	14
	Windows Server 2022 Standard	12/28/2023 3:34:15 PM	14
	Windows Server 2012 R2 Standard	02/06/2018 6:40:25 PM	84
	Windows Server 2008 R2 Enterprise	01/15/2011 8:38:40 PM	169
	Windows Server 2019 Datacenter	09/26/2019 3:38:56 PM	65
	Windows Server 2016 Standard	01/26/2018 4:25:42 PM	85

4.10 - Workstation Aging

This section is an indicator of the age of the active workstations based on the date their operating system was installed. The actual age of the workstation may vary if the operating system was re-installed for any reason. Older systems are highlighted in red and much older systems are bolded. Excludes computers that we were unable to retrieve an OS Install Date.

COMPUTER	OPERATING SYSTEM	OS INSTALL DATE	AGE (MONTHS)
	Windows 10 IoT Enterprise LTSC Version 21H2	12/10/2019 12:12:00 AM	62
	Windows 10 Pro for Workstations Version 22H2	06/12/2020 7:55:34 AM	56
	Windows 10 Pro for Workstations Version 22H2	07/14/2020 4:53:52 PM	55
	Windows 10 Pro Version 21H2	07/17/2020 4:51:18 PM	55
	Windows 10 Pro for Workstations Version 22H2	09/15/2020 6:24:08 PM	53
	Windows 10 Pro N Version 22H2	09/20/2020 11:53:26 PM	53
	Windows 10 Pro for Workstations Version 21H2	06/01/2023 9:58:44 AM	20
	Windows 11 Pro for Workstations Version 23H2	03/14/2024 3:49:42 PM	11
	Windows 10 IoT Enterprise LTSC Version 21H2	03/31/2024 11:58:45 PM	11
	Windows 11 Pro Version 24H2	01/30/2025 2:34:27 PM	1

4.11 - Domain DNS

This section contains a listing of all IP addresses and hostnames from DNS, with conflicting entries highlighted in red.

IP ADDRESS	HOSTNAME
10.0.0.7	.BIG.local
10.0.0.13	.BIG.local
10.0.0.16	.BIG.local
10.0.0.18	.BIG.local
10.0.0.30	.BIG.local
10.0.0.34	.BIG.local
10.0.0.45	.BIG.local
10.0.0.45	.BIG.local
10.0.0.49	.BIG.local
10.0.0.96	.BIG.local
10.0.0.100	.BIG.local
10.10.00.55	.BIG.local
10.10.00.55	.BIG.local
10.10.00.56	.BIG.local
10.10.00.56	.BIG.local
10.10.00.56	.BIG.local
10.10.00.56	.BIG.local
10.10.00.57	.BIG.local

5 - Non A/D Devices

This section contains a listing of all devices which were not joined to a domain or workgroup.

IP ADDRESS	COMPUTER NAME	LISTENING PORT(S)	DEVICE TYPE
10.10.00.5		HTTP (80/TCP)	
10.10.00.6		SSH (22/TCP), DNS (53/TCP), HTTP (80/TCP), HTTP (8080/TCP)	Linux beaglebone 4.14.108-ti-r108 #1 SMP PREEMPT Tue Jun 18 05:11:38 UTC 2019 armv7l
10.10.00.8	POLYCOM_64167F7CA5C2.BIG.LOCAL		
10.10.00.17	POLYCOM_64167F7D4B28.BIG.LOCAL		
10.10.00.20		SSH (22/TCP), HTTP (80/TCP), HTTPS (443/TCP)	1.3.6.1.4.1.674.10892.5
10.10.00.24	POLYCOM_64167F7ADF29.BIG.LOCAL		
10.10.00.26	POLYCOM_64167F7D4348.BIG.LOCAL		
10.10.00.29			
10.10.00.35	POLYCOM_64167F7D4732.BIG.LOCAL		
10.10.00.45		RDP (3389/TCP), VNC (5900/TCP)	
10.10.00.53	HP23BCD8.BIG.LOCAL	HTTP (80/TCP), HTTPS (443/TCP), HTTP (8080/TCP)	HP ETHERNET MULTI-ENVIRONMENT
10.10.00.62	POLYCOM_64167F7D45D9.BIG.LOCAL		
10.10.00.64		RDP (3389/TCP)	
10.10.00.70		SSH (22/TCP), HTTPS (443/TCP)	gunicorn

IP ADDRESS	COMPUTER NAME	LISTENING PORT(S)	DEVICE TYPE
10.10.00.79		RDP (3389/TCP)	
10.10.00.96		SMTP (25/TCP), HTTP (80/TCP), SQLServer (1433/TCP), RDP (3389/TCP)	
10.10.00.98		HTTP (80/TCP), HTTPS (443/TCP), HTTP (8080/TCP)	HP HTTP Server; OfficeJet Pro 7740 series - G5J38A; Serial Number: CN7AQ250NN; Built: Fri Jan 10, 2025 11:12:15AM {EDWINXPP1N002.2502B.00}
10.10.00.100		RDP (3389/TCP)	
10.10.00.101		RDP (3389/TCP)	
10.10.00.107	POLYCOM_64167F7AD75D.BIG.LOCAL		
10.10.00.113		SSH (22/TCP), HTTP (80/TCP), HTTPS (443/TCP), VNC (5900/TCP)	lighttpd/1.4.23
10.10.00.117			
10.10.00.118		HTTP (80/TCP), HTTPS (443/TCP)	nginx

* Indicates that the device was scanned more than one time during the network scanning process.

6 - Servers

This section and corresponding sub-sections contain a comprehensive listing of servers by type, which are then categorized by domain or workgroup membership.

6.1 - MS SQL Servers

BIG.LOCAL

MS SQL SERVER NAME	INSTANCE	VERSION	# OF DATABASES	ACTIVE SQL AGENT JOBS?
	MSSQL.1	9.00.3042.00	<unknown>	<unknown>
	SQLEXPRESS	9.00.3042.00	<unknown>	<unknown>
	SQLSERVER2008R2	10.50.6000.34	<unknown>	<unknown>
	MSSQL.1	9.00.3042.00	<unknown>	<unknown>
	SQLEXPRESS	9.00.3042.00	<unknown>	<unknown>
	LITTLE	14.0.1000.169	<unknown>	<unknown>
	IDFDASH	15.0.2000.5	<unknown>	<unknown>
	SQLSERVER2022	16.0.1000.6	<unknown>	<unknown>
	SQLEXPRESS	9.00.3042.00	<unknown>	<unknown>
	SQLEXPRESS	15.0.2000.5	<unknown>	<unknown>
	SQLEXPRESS	9.00.5000.00	<unknown>	<unknown>
	LITTLE	14.0.1000.169	<unknown>	<unknown>

MS SQL SERVER NAME	INSTANCE	VERSION	# OF DATABASES	ACTIVE SQL AGENT JOBS?
	SOLIDWORKS	15.0.2000.5	<unknown>	<unknown>
	LITTLE	15.0.2000.5	<unknown>	<unknown>

6.2 - Web Servers

BIG.LOCAL

IP ADDRESS	WEB SERVER NAME	LISTENING PORT(S)	SERVER TYPE
10.10.00.15		80/TCP	Web Server
10.10.00.22		80/TCP, 443/TCP	nginx
10.10.00.23		80/TCP, 443/TCP	nginx
10.10.00.30		80/TCP, 443/TCP	
10.10.00.31		80/TCP, 443/TCP	Microsoft-IIS/10.0
10.10.00.52		80/TCP, 443/TCP, 8080/TCP	nginx
10.10.00.74		80/TCP, 443/TCP	
10.10.00.83		80/TCP, 443/TCP	nginx
10.10.00.86		80/TCP	
10.10.00.87		80/TCP	Microsoft-IIS/7.5
10.10.00.95		80/TCP	Microsoft-IIS/10.0
10.10.00.128		80/TCP	Microsoft-IIS/10.0

IP ADDRESS	WEB SERVER NAME	LISTENING PORT(S)	SERVER TYPE
10.10.00.136		8080/TCP	Jetty(9.4.z-SNAPSHOT)
10.10.00.140		80/TCP, 443/TCP	nginx
10.10.00.150		80/TCP, 443/TCP	
10.10.00.153		443/TCP	
10.10.00.155		80/TCP	GoAhead-Webs
10.10.00.170		80/TCP, 8080/TCP	
10.10.00.171		80/TCP	Microsoft-IIS/10.0
10.10.00.199		80/TCP, 8080/TCP	Apache/2.2.22 (Win32) PHP/5.2.14
10.10.00.214		80/TCP, 443/TCP	Microsoft-IIS/10.0
10.10.00.227		80/TCP	Microsoft-IIS/10.0
10.10.00.252		80/TCP	Microsoft-IIS/10.0

No Domain

IP ADDRESS	WEB SERVER NAME	LISTENING PORT(S)	SERVER TYPE
10.10.00.5		80/TCP	
10.10.00.6		80/TCP, 8080/TCP	Apache/2.4.25 (Debian)
10.10.00.20		80/TCP, 443/TCP	Apache
10.10.00.53		80/TCP, 443/TCP, 8080/TCP	HP HTTP Server; HP PageWide Pro 577 MFP - D3Q21A; Serial Number: CN94UJY0JX; Built: Fri Sep 06, 2024 07:18:49PM {MAHDWOPP1N001.2436C.00}

IP ADDRESS	WEB SERVER NAME	LISTENING PORT(S)	SERVER TYPE
10.10.00.70		443/TCP	gunicorn
10.10.00.96		80/TCP	
10.10.00.98		80/TCP, 443/TCP, 8080/TCP	HP HTTP Server; OfficeJet Pro 7740 series - G5J38A; Serial Number: CN7AQ250NN; Built: Fri Jan 10, 2025 11:12:15AM {EDWINXPP1N002.2502B.00}
10.10.00.113		80/TCP, 443/TCP	lighttpd/1.4.23
10.10.00.118		80/TCP, 443/TCP	nginx
10.10.00.123		80/TCP, 443/TCP	Apache
10.10.00.131		80/TCP, 8080/TCP	Apache/2.4.25 (Debian)
10.10.00.133		443/TCP	
10.10.00.139		80/TCP, 443/TCP, 8080/TCP	Virata-EmWeb/R6_2_1
10.10.00.254		80/TCP	

6.3 - Time Servers

Domain: BIG.LOCAL

TIME SERVER NAME	IP ADDRESS
BIg-DC02	10.10.00.128

6.4 - Exchange Servers

No Exchange Servers were discovered.

6.5 - DHCP Servers

BIG.LOCAL

IP ADDRESS(ES)	SERVER NAME	ERRORS (LAST 24 HOURS)
10.10.00.223	big-dc01.BIG.local	

6.6 - Hyper-V Servers

BIG.LOCAL

HOST	HYPER-V GUEST INFORMATION			
	NAME	STATE	OPERATING SYSTEM	NOTES
BIG-HV02 (Windows Server 2022 Standard)	build-3 (Build Server, Asset I-R-81)	Running	Windows 10 Pro	
	IDF Inspector Win10	Running	Windows 10 IoT Enterprise LTSC 2021	
	V-D-380 (jsie-dev) Development	Running	Windows 10 IoT Enterprise LTSC 2021	
	Build Server (Developer) TEMPLATE	Off		

6.7 - MacOS Database Servers

No macOS Database Servers were discovered.

7 - Printers

This section contains a listing of all printers categorized by a combination of domain or workgroup membership and method of access. Alerts for SNMP-enabled printers are also displayed in red.

BIG.LOCAL (from Active Directory)

IP ADDRESS	PRINTER NAME	ACCESSED FROM	LOCATION	COMMENT
10.10.00.136	Accounting-MFC (HP OfficeJet Pro 9010 series)		accounting-mfc	

BIG.LOCAL (from WMI)

IP ADDRESS	PRINTER NAME	ACCESSED FROM	LOCATION	COMMENT
10.10.00.150	HP Officejet Pro X576dw MFP PCL 6 (Network)			This is a web services printer

Networked (from SNMP)

IP ADDRESS	PRINTER NAME	HOSTNAME	DESCRIPTION	ALERTS
10.10.00.52	Accounting-MFC	ACCOUNTING-MFC.BIG.LOCAL	HP ETHERNET MULTI-ENVIRONMENT	65561 65561 65561 65561

BIG.LOCAL (from Shares)

SHARED PRINTER	USER/GROUP	SHARE PERMISSIONS		
		FULL CONTROL	CHANGE	READ

8 - Network Shares

This section contains a listing of all network shares categorized first by domain or workgroup membership, and then by machine.

BIG.LOCAL

HOSTED BY	SHARE UNC

No NFS Shares were discovered.

9 - Major Applications

This section contains a listing of major applications with corresponding version numbers and the number of computers the application was detected on. Applications that appear on more than three computers are highlighted in gray for easy recognition.

Domain BIG.local

Windows Applications

APPLICATION NAME	VERSION	# COMPUTERS	COMPUTERS
.NET Core SDK 1.0.0 (x64) Installer (x64)	4.0	2	
.NET Core SDK 1.0.4 (x64)	4.1	1	
3ware Disk Management Tools		3	
7-Zip 18.06 (x64)	18.06	1	
7-Zip 22.01 (x64 edition)	22.01	2	
7-Zip 23.01 (x64)	23.01	7	
7-Zip 9.20 (x64 edition)	9.20	4	
Accusoft PICVideo Motion JPEG 4	4.0	1	
AcquireNow	1.00	1	
Acronis True Image	22.6	1	
Acronis True Image	22.7	3	
Acronis True Image	23.2	1	

10 - Patch Summary

This section contains the patching status of computers determined through Windows Update. Windows Update checks the local computer for all non-hidden updates. Missing updates in both areas are highlighted in red. Security and critical updates are bolded.

Windows Updates

IP ADDRESS	COMPUTER NAME	ISSUE	RESULT	ASSESSMENT
10.10.00.199		Feature Packs, Windows Server 2008 R2	Failed (non-critical)	1 update is missing.
		Microsoft SQL Server 2012, Service Packs	Failed (non-critical)	1 update is missing.
		Security Updates, Windows Server 2008 R2	**Failed (critical)**	**1 security update is missing.**
		Update Rollups, Windows Server 2008 R2	Failed (non-critical)	1 update is missing.
		Updates, Windows Server 2008 R2	Failed (non-critical)	1 update is missing.
10.10.00.223		Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Microsoft Server operating system-21H2, Security Updates	Failed (non-critical)	1 security update is missing.
		Update Rollups, Windows Server 2016, Windows Server 2019, Windows Server, version 1903 and later	Failed (non-critical)	1 update is missing.
169.254.1.2, 10.10.00.128		Drivers: hp - Printer - 6/21/2019 12:00:00 AM - 8.0.1329.6720	Failed (non-critical)	1 update is missing.
		Drivers: Intel - System - 9/1/2016 12:00:00 AM - 11.6.0.1026	Failed (non-critical)	1 update is missing.

IP ADDRESS	COMPUTER NAME	ISSUE	RESULT	ASSESSMENT
		Security Updates	Failed (non-critical)	1 security update is missing.

11 - Endpoint Security and Backup

This section contains a listing of detected anti-virus, anti-spyware, firewall, and backup information as detected through *Security Center* and/or *Installed Services* for major vendors. This list is categorized by domain or workgroup membership.

The 'Name' column contains either the name of the product, None indicating the that machine returned information but no product was found, or <empty> indicating that information was not obtainable. Additionally, a status of ✓ indicates 'yes', × indicates 'no', or <empty> indicates that a status was not available.

BIG.LOCAL

COMPUTER NAME	ANTI-VIRUS			ANTI-SPYWARE			FIREWALL		BACKUP	
	NAME	ON	CURRENT	NAME	ON	CURRENT	NAME	ON	NAME	CURRENT
ALTA	Symantec Endpoint Protection	✓	N/A	Symantec Endpoint Protection	✓	N/A	Symantec Endpoint Protection	✓	None	
	Symantec Endpoint Protection.cloud	✓	N/A	Symantec Endpoint Protection.cloud	✓	N/A	Symantec Endpoint Protection.cloud	✓		
	Windows Defender	✓	×	Windows Defender	✓	×	Windows Firewall	✓		
BIG-DC01	Sentinel One	✓	N/A	Sentinel One	✓	N/A	Windows Firewall	×	None	
	Windows Defender	✓	✓	Windows Defender	✓	✓				
BIG-DC02	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
BIG-HV02	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
BIG-HV03	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	

N/A - No information available.

12 - Remote Listening Ports

This section contains a list of common ports/protocols assessed, and is categorized by domain or workgroup membership. Items with a red check indicate a potential risk.

BIG.LOCAL

IP ADDRESS	COMPUTER NAME	FTP (21/TCP)	SSH (22/TCP)	DNS (53/TCP)	HTTP (80/TCP)	HTTPS (443/TCP)	SQL SERVER (1433/TCP)	MYSQL (3306/TCP)	RDP (3389/TCP)	VNC (5900/TCP)	HTTP (8080/TCP)
10.10.00.202									✓		
10.10.00.208									✓		
10.10.00.213									✓		
10.10.00.214		✓			✓	✓	✓		✓		
10.10.00.218									✓		
10.10.00.223				✓					✓		
10.10.00.224									✓		
10.10.00.227					✓				✓		
10.10.00.229									✓		
10.10.00.230									✓		
10.10.00.252					✓				✓		

IP ADDRESS	COMPUTER NAME	FTP (21/TCP)	SSH (22/TCP)	DNS (53/TCP)	HTTP (80/TCP)	HTTPS (443/TCP)	SQL SERVER (1433/TCP)	MYSQL (3306/TCP)	RDP (3389/TCP)	VNC (5900/TCP)	HTTP (8080/TCP)
169.254.1.2					✓				✓		
169.254.141.71					✓	✓			✓		
172.19.96.1					✓	✓			✓	✓	
172.22.48.1									✓		
172.26.112.1									✓		
172.30.00.1									✓		
192.168.56.1									✓		

No Domain

IP ADDRESS	COMPUTER NAME	SSH (22/TCP)	SMTP (25/TCP)	DNS (53/TCP)	HTTP (80/TCP)	HTTPS (443/TCP)	SQL SERVER (1433/TCP)	RDP (3389/TCP)	VNC (5900/TCP)	HTTP (8080/TCP)
10.10.00.5					✓					
10.10.00.6		✓		✓	✓					✓
10.10.00.20		✓			✓	✓				
10.10.00.45								✓	✓	
10.10.00.53					✓	✓				✓

13 - Internet Access

This section lists the latency between the computer and both Google and Yahoo, as well as a trace route to Google for further diagnostics if needed.

INTERNET ACCESS

Latency Tests:

Retrieval time for Google.com: 70 ms
Retrieval time for Yahoo.com: 329 ms

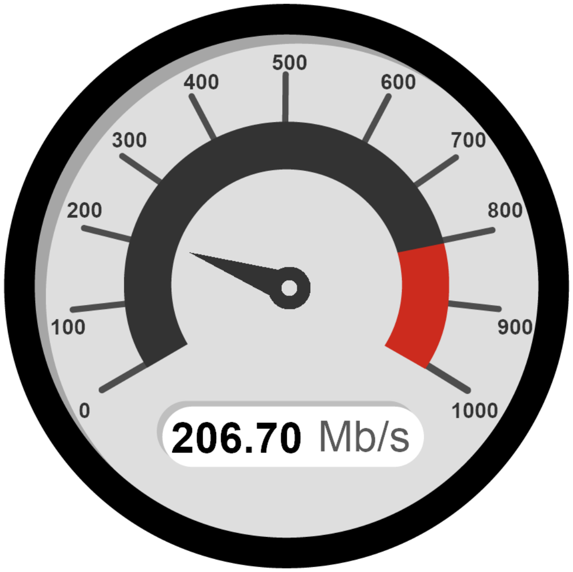
Internet trace route to Google.com:

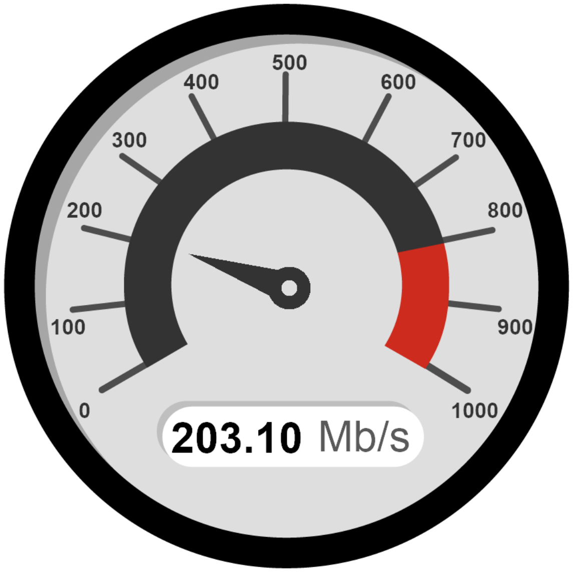
```
Tracing route to www.google.com [142.250.69.228] over a maximum of 30 hops:

13 ms10.10.
22 mseg-1-1-15-3994-soag02.louisville.co.denver.comcast.net [50.169.]
36 msbe-102-1-ceg01.louisville.co.denver.comcast.net [96.216.179.217]
411 msae-296-ar01.denver.co.denver.comcast.net [96.216.179.197]
52 msbe-501-arsc1.denver.co.denver.comcast.net [96.216.22.129]
65 msbe-36011-cs01.1601milehigh.co.ibone.comcast.net [96.110.43.241]
710 msbe-3211-pe11.910fifteenth.co.ibone.comcast.net [96.110.33.118]
84842 ms
94 ms216.239.40.57
106 ms142.251.61.181
116 msden08s05-in-f4.1e100.net [142.250.69.228]

Trace complete.
```

14 - External Speed Test

This section displays upload and download speed.

DOWNLOAD SPEED: 206.7 MB/S	UPLOAD SPEED: 203.1 MB/S





NDT SERVER	LOCATION	DOWNLOAD	UPLOAD
ndt-mlab1-chs02.mlab-oti.measurement-lab.org	Atlanta, Georgia	201.1 Mb/s	38.1 Mb/s
ndt-mlab1-den04.mlab-oti.measurement-lab.org	CLOSEST	205.0 Mb/s	203.1 Mb/s
ndt-mlab2-ord06.mlab-oti.measurement-lab.org	Chicago, Illinois	206.7 Mb/s	185.7 Mb/s
ndt-mlab2-dfw03.mlab-oti.measurement-lab.org	Dallas, Texas	202.6 Mb/s	197.2 Mb/s

NDT SERVER	LOCATION	DOWNLOAD	UPLOAD
ndt-mlab3-dub01.mlab-oti.measurement-lab.org	Dublin, Ireland	175.9 Mb/s	169.4 Mb/s
ndt-mlab1-fra04.mlab-oti.measurement-lab.org	Frankfurt, Germany	168.7 Mb/s	163.6 Mb/s
ndt-mlab1-lhr07.mlab-oti.measurement-lab.org	London, United Kingdom	167.7 Mb/s	3.7 Mb/s
ndt-mlab3-mad06.mlab-oti.measurement-lab.org	Madrid, Spain	113.6 Mb/s	163.1 Mb/s
ndt-mlab2-mia02.mlab-oti.measurement-lab.org	Miami, Florida	202.3 Mb/s	175.2 Mb/s
ndt-mlab3-mil07.mlab-oti.measurement-lab.org	Milan, Italy	154.7 Mb/s	73.7 Mb/s
ndt-mlab2-yul03.mlab-oti.measurement-lab.org	New York City, New York	202.6 Mb/s	55.3 Mb/s
ndt-mlab1-par09.mlab-oti.measurement-lab.org	Paris, France	174.2 Mb/s	63.5 Mb/s
ndt-mlab1-prg05.mlab-oti.measurement-lab.org	Prague, Czech Republic	117.7 Mb/s	149.4 Mb/s
ndt-mlab1-nuq08.mlab-oti.measurement-lab.org	San Francisco, California	203.9 Mb/s	179.1 Mb/s
ndt-mlab3-sea03.mlab-oti.measurement-lab.org	Seattle, Washington	91.4 Mb/s	60.0 Mb/s
ndt-mlab3-svg01.mlab-oti.measurement-lab.org	Stavanger, Norway	173.9 Mb/s	166.3 Mb/s
ndt-mlab1-syd03.mlab-oti.measurement-lab.org	Sydney, Australia	64.0 Mb/s	64.8 Mb/s
ndt-mlab1-hnd02.mlab-oti.measurement-lab.org	Tokyo, Japan	140.6 Mb/s	98.0 Mb/s

15 - External Security Vulnerabilities

This section contains an overview of external vulnerabilities detected during the scan, with items in red indicating a risk.

EXTERNAL IP ADDRESS	RISK	HIGH RISK	MEDIUM RISK	LOW RISK	PORT AND PROTOCOL
13.74.	**High**	**1**	0	0	**443/tcp (https)**, **443/tcp**, **80/tcp**
40.99.	Medium	0	1	1	**80/tcp (http)**, **80/tcp**
76.223.17.250 (ox.godaddy.com)	Low	0	0	1	, **443/tcp**, **80/tcp**
40.126.	Low	0	0	0	, **443/tcp**, **80/tcp**
65.141.	**High**	**16**	86	4	**80/tcp (http)**, **443/tcp (https)**, **444/tcp (snpp)**, **443/tcp**, **444/tcp**, **80/tcp**, **500/udp**
52.98.	Medium	0	3	2	**25/tcp (smtp)**, **80/tcp (http)**, **587/tcp (submission)**, **25/tcp**, **587/tcp**, **80/tcp**, **143/tcp**, **110/tcp**, **443/tcp**, **993/tcp**, **995/tcp**
198.49.	Medium	0	1	1	**80/tcp (http)**, **80/tcp**, **443/tcp**
50.169.	Medium	0	1	1	, **10443/tcp**, **500/udp**
198.185.	Medium	0	2	1	**80/tcp (http)**, **443/tcp (https)**, **443/tcp**, **80/tcp**
198.185.	Low	0	0	1	, **443/tcp**, **80/tcp**
198.49.	Low	0	0	1	, **443/tcp**, **80/tcp**
173.8.	Low	0	0	0	
66.77.	Low	0	0	0	
75.125.	Low	0	0	0	

16 - Local Accounts

This section contains a list of local accounts with information on each account.

COMPUTER NAME	ACCOUNT NAME	DISPLAY NAME	ENABLED	GROUPS	LAST LOGIN
QA-IDF-BASE			enabled	Users	**6/3/2018 3:22:46 PM**
QA-IDF-BASE			enabled	Users	**6/3/2018 3:23:28 PM**
QA-IDF-BASE			enabled		**9/11/2024 9:06:47 PM**
QA-IDF-BASE			enabled	Users	**2/10/2020 1:16:11 PM**
QA-IDF-BASE			enabled	Users	**6/3/2018 2:16:11 PM**
WMA-D-52			enabled	Administrators	**1/13/2020 10:41:41 AM**
WMA-D-52			disabled	System Managed Accounts Group	**<never>**
WMA-D-52			disabled	Guests	**<never>**
WMA-D-52			enabled	Users	1/29/2025 9:51:42 AM
WMA-D-52			disabled		**<never>**

17 - Additional Users

No Additional Users were found.

18 - Additional Assets

No Additional Assets were found.

19 - Additional Applications

No Additional Applications were found.