Forcepoint

Forcepoint Data Visibility

Powered by GetVisibility

Setup LDAP/Active Directory Scan

Forcepoint

Report

Forcepoint 16 July 2023 Forcepoint Proprietary

Table of Contents

SETUP LDAP/ACTIVE DIRECTORY SCAN	2
DEFINITIONS	3
Full Walkthrough	4

Setup LDAP/Active Directory Scan

This feature gathers permissions and access rights for groups, users, and other entities (trustees) on an LDAP server. When used with a corresponding CIFS/SMB server, users can review file permissions and access from the Focus UI and reports.

1. Go to Administration > Connections > LDAP.

GETV	Gettvisibility Doubloard + Agent + Administration + Lagont [+				
	Вох	Connection scans			
DATTERN MATCHING	CIFS Google Drive	Scin users and trustees to determine notes and permissions			
26 USER	LDAP	NEW SCAN SUBAR			
NETWORK	SharePoint On-Premise		٩		
SETTINGS	SharePoint Online	Name Puth No convectors have been cristed yet			
ИЗ WEBHOOKS	Request connector	Showing 1 to 20 of 0 entries < >			
ANGLAGE SETTINGS					

Figure 1: LDAP

2. Select NEW SCAN SHARE

-	-					
OPS .	Connection scame	-				
Gaogie Orive	Manuscent and transvers to dee	Kar and ad balance is demonstrate add produces				
1044	Contraction in the					
OneDrive		_			-	
Bardwid Do Pennis		New LEAP year share			× .	
Marshold Dollow	Rama	Name	Usemane	Password		
C brand terretor						
		IP Address				
					-	
		Certificate lopitorul				
		Prof.	Institute #	South		
		249	10	DC-see-gs.DC-local		

Figure 2: NEW SCAN SHARE

3. Enter the details of the LDAP to scan and select SAVE.

New LDAP scan share		×
Name GV LDAP	Username	Password
IP Address Certificate (optional)		
Port 389	Inactivity @ 90	Search DC=aws-gv,DC=local
		CANCEL SAVE

Figure 3: Enter the details

Definitions

- → Name: Give a name to the scan to identify it later
- → Username: The user must be an admin level and have access to all the LDAP utilities to be scanned. The username should be entered in the format user@domain.com.
- → **Password:** Password for the admin user.
- → **IP Address:** The IP Address of the server where the LDAP is installed.
- → Certificate (Optional): If the server you wish to scan uses LDAPS (LDAP over SSL/TLS) enter your certificate text here. Otherwise leave it blank.
- → Port: 389 is the default port for LDAP, however for Secure LDAP 636 is used.
- → Inactivity: This defines inactive users. Default is 90 days.
- → Search: This is the point in the LDAP directory where Focus will start searching from. In this example:
 - 1. DC stands for Domain Component. An attribute used to represent domain levels.
 - 2. aws-gv is the name of the first-level domain.
 - 3. local is the top-level domain.

Together, DC=aws-gv, DC=local represents the domain aws-gv.local.

4. Back on the LDAP connections page, icons to Delete, Edit, and Scan are shown. Select Scan.

	Search connections by name
Name Path	
GV LDAP	ā / @
Showing 1 to 20 of 1 entries < 1 >	

Figure 1: LDAP connections page

Focus has now begun discovering trustees and assessing permissions on files. An overview of the results can be found on the

Company Overview page.

GETVISIBILITY Dashboard - Agent - Administration -					
O SCAN PROGRESS					
	Files & Folders	Users & Groups			
Q COMPANY OVERVIEW	* 345,161	* 3,156			
EQ EXPLORE	Found Files # 345,161 191.55 GB Classified Files # 226,824 33.02 GB	Groups # 1,072 Users # 2,084			
REPORTS	PII Files # 86,144 13.87 GB	Active Users 4 Inactive Users			
DATA RISK SURVEY		<pre># 2,080 Suspended Users # 2,008</pre>			

5. For more detailed information select from one of the hyperlinked: Groups, Users, Active Users, Inactive Users, or Suspended Users, to view tables.

Refer the demo.

Conversely, the permissions for particular files can be checked. Navigate to the Explore page and under the Actions on each applicable file, select Open Permissions.

Refer the Demo.

For more information about the security of the Active Directory, navigate to Reports and select User Access Report. This pdf report shows information on: Users in the most Groups, Enabled Inactive Users, Domain Administrators, and Users with Outdated Passwords.

Refer the Demo.

Full Walkthrough

Refer the demo for full walkthrough.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

© 2023 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners. [Forcepoint Data Visibility Powered by GetVisibility Setup LDAP/Active Directory Scan] [Status]16 Jul. 24