Forcepoint Data Security Posture Management

Powered by Getvisibility

Setup LDAP AD Scan



Report

Forcepoint April 23, 2024

Table of Contents

INTRODUCTION	2
STEPS:	
DEFINITIONS	

Introduction

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 DDC/FDC UI and analytics.

Steps:

1. Go to Administration > Data Sources > LDAP

Forces Powered	point DSPM Dashboard 🔻	Analytics DSPM Administration				© •
DATTERN MATCHING	20 AWSIAM	Connection scans				
C€ : DATA SOURCES	awss3	Scan users and trustees to determine roles and	permissions			
4	20 Azure AD	NEWSCAN				
24	C Azure Blob				Search connections by name	۵ 🕸
USER MANAGEMENT	Azure Files	Name	Tatal seanned	Shaku		
% NETWORK	C OneDrive	AD.	iotai scanneo	Status		_
SETTINGS	SharePoint Online	AD	51	() Finished		=
&			Showing 1 to 1 of 1	entries < 1 >		
WEBHOOKS	20 LDAP					
	Constant SharePoint On- Premise					
	EQ SMB					
	20 Google IAM					
	C Google Drive					

Figure 1.

2. Select New Scan.

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

Name		Username admin@doma	in.com	Password	
P Address					
0.0.0.0					
Certificate (optional)					
Port	Inactivity	0	Search base		
389	90		DC-aws-gv,D	C-local	
Data Owner		Geographic Lo	ocation		
	~	Select count	ries		~

Figure 2.

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 DDC will start searching from.
- Data Owner: Select from the drop-down.
- **Geographical location**: Select from the drop-down.

In this example: DC stands for Domain Component. An attribute used to represent domain levels.

aws-gv is the name of the first-level domain.

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, From the burger menu, select Start trustee scan.

			Search connections by name	Q	\$
Name	Total scanned	Status			
AD	51	Finished			=
	Showing 1 to 1 of 1 entries < 1 >				
			(2 Start trustee	scan

Figure 3.

DDC has now begun discovering trustees and assessing permissions on files. An overview of the results can be found on the **Explore Trustees** page.

Forcepoint Powered by Getvi	DSPM isibility	Dashboard	d 🔹 Analytics										
O AN PROGRESS	Finde	everything using GC	j.										۹
													CLEAR SEARCH
2Q DOPLORE													۲
TRUSTEES		Source	Display	Туре	Groups	Enabled	Active	Top Leve	Passwor	Last Login	Created	Last Mo	Actions
LEEK SURVEY	2	ldap	Administrators	group		\oslash	Ø	Ø	Never	Never	Jan 21, 2021	Jan 21, 2021, 12:24:42 AM	:24 Q
	2	Idap	Replicator	group		\odot	\odot		Never	Never	Jan 21, 2021	Jan 21, 2021, 12:24:42 AM	:84 Q
	2	ldap	Network Configur	group		\odot	\odot		Never	Never	Jan 21, 2021	Jan 21, 2021, 12:08:50 AM	124 Q
	2	ldap	Performance Log l	group		\odot	\odot		Never	Never	Jan 21, 2021	Jan 21, 2021, 12:08:50 AM	184 Q
	2	ldap	Certificate Service	group		\odot	\oslash		Never	Never	Jan 21, 2021	Jan 21, 2021, 12:08:50 AM	:21 Q
	2	ldap	Access Control As	group		\odot	\oslash		Never	Never	Jan 21, 2021	Jan 21, 2021, 12:08:50 AM	121 0
	2	ldap	Storage Replica Ac	group		\odot	\odot		Never	Never	Jan 21, 2021	Jan 21, 2021, 12:08:50 AM	<i>18</i> 1 Q
	2	Idap	Domain Computer	group		\odot	\odot		Never	Never	Jan 21, 2021	Jan 21, 2021, 12:09:32 AM	:24 0
	2	ldap	Domain Admins	group	Denied RODC	\odot	Ø	\odot	Never	Never	Jan 21, 2021	Jan 21, 2021, 12:24:42 AM	: <u>81</u> 0

Figure 4.



forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

© 2024 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 Security Posture Management Powered by GetVisibility Setup LDAP AD Scan] [Status]23 Apr. 24