Active Directory Integrations

Introduction

Elastic Stack security features can be configured to authenticate users through Active Directory by using LDAP to communicate with the directory. Active Directory realms are similar to LDAP realms, as they both store users and groups in a hierarchical structure, which includes containers such as organizational units (OU), organizations (O), and domain components (DC).

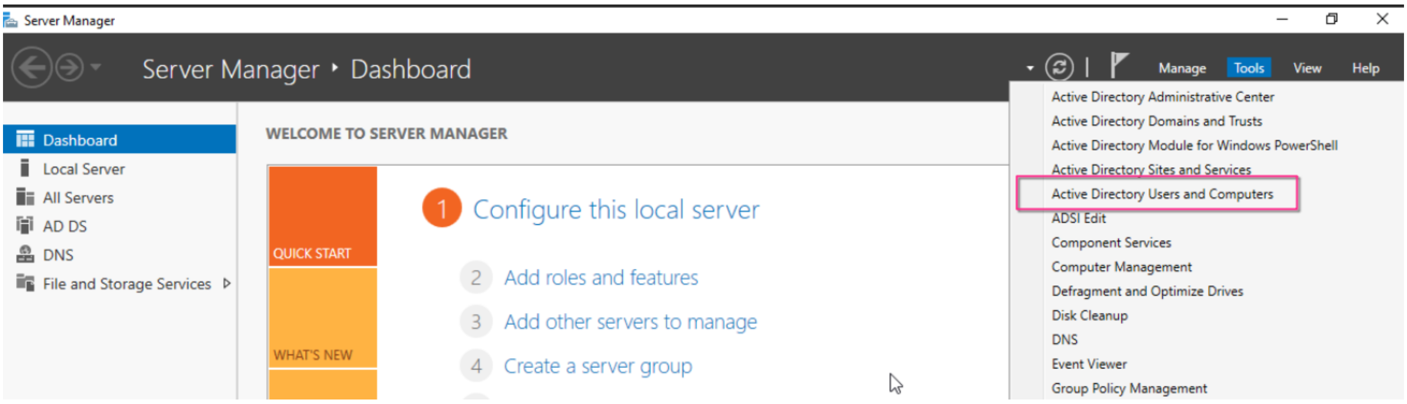
The security features support authentication based on Active Directory security groups, but not distribution groups. When authenticating users, the username entered must match the sAMAccountName or userPrincipalName, not the common name (cn). The realm authenticates users via an LDAP bind request, searches for their entry in Active Directory, and retrieves their group memberships from the tokenGroups attribute to assign appropriate roles.

I. Active Directory Information Lookup

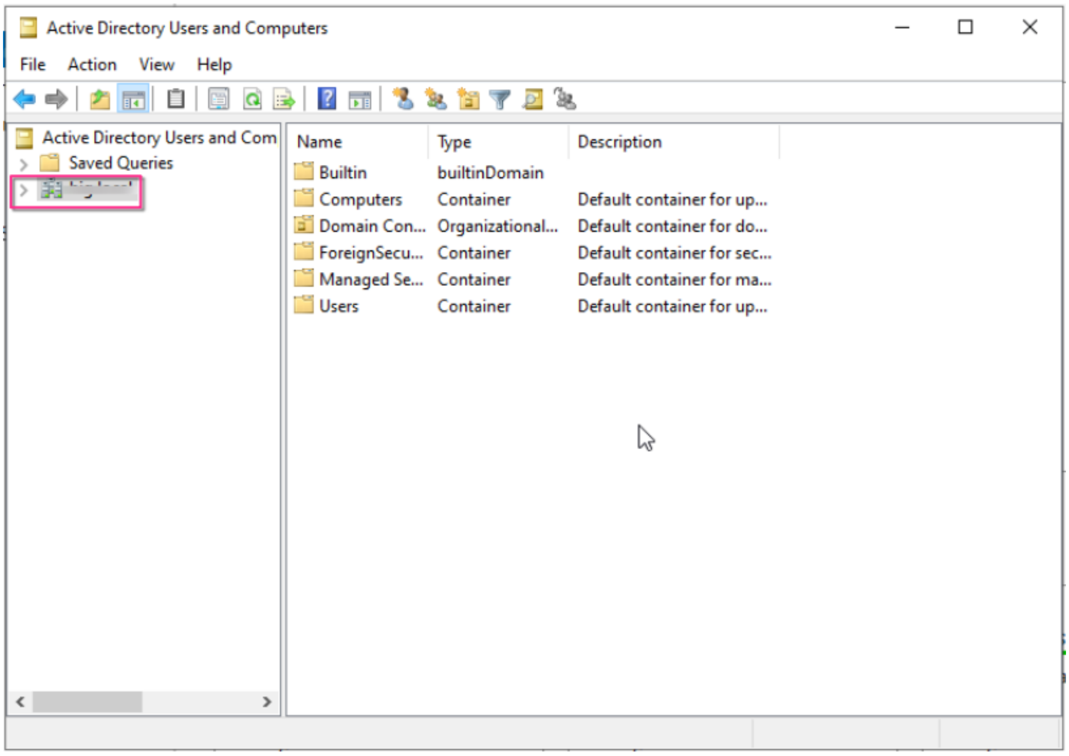
Finding the Base DN (Distinguished Name)

Method 1: Using Active Directory GUI

1. Open "Active Directory Users and Computers"

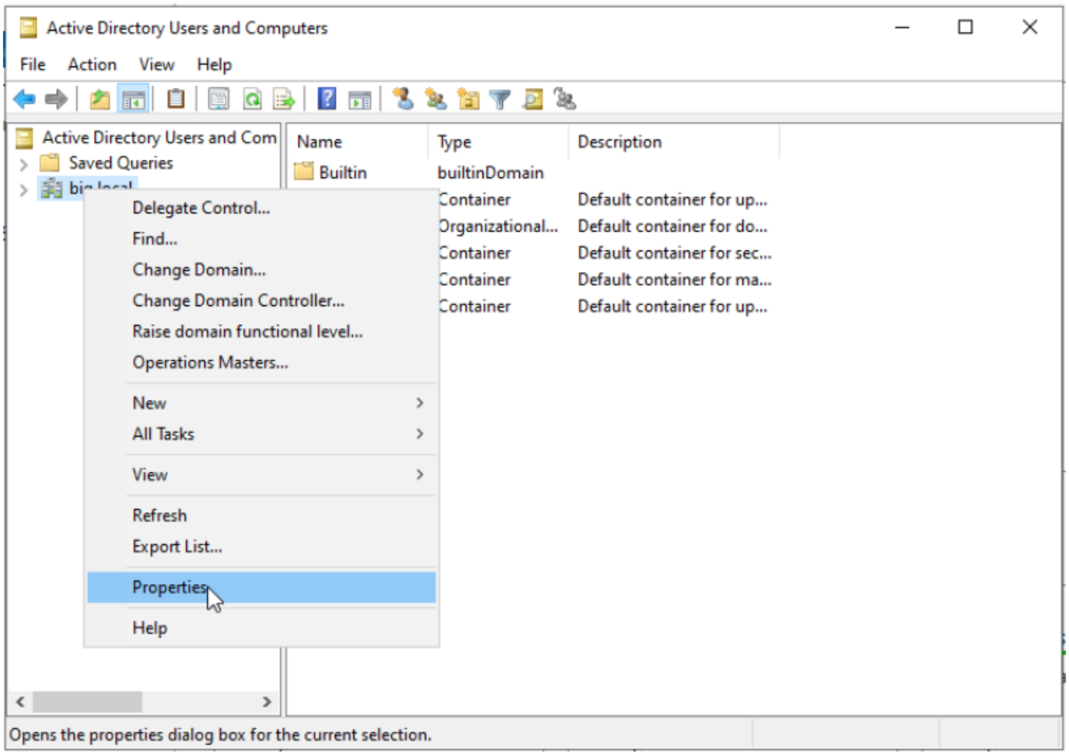

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management

2. Right-click on your domain


Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
[redacted]

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...
Users	Container	Default container for up...

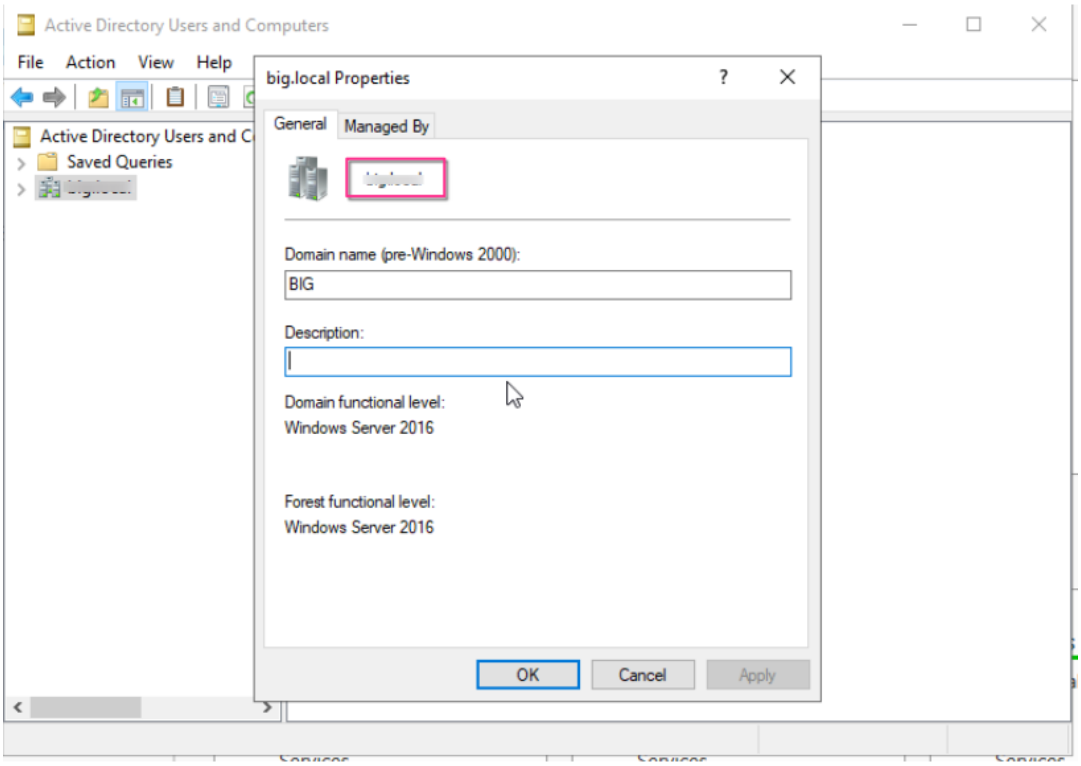
3. Select "Properties"



Name	Type	Description
Builtin	builtinDomain	
	Container	Default container for up...
	Organizational...	Default container for do...
	Container	Default container for sec...
	Container	Default container for ma...
	Container	Default container for up...

Opens the properties dialog box for the current selection.

4. Look for the "Distinguished Name" field



big.local Properties

[redacted]

Domain name (pre-Windows 2000):
BIG

Description:

Domain functional level:
Windows Server 2016

Forest functional level:
Windows Server 2016

Method 2: Using PowerShell

1. Open PowerShell with administrator privileges
2. Run the command:

```
Get-ADDomain | Select-Object DistinguishedName
```

3. The output will be in the format: "DC=company,DC=local"

II. Finding Active Directory URL

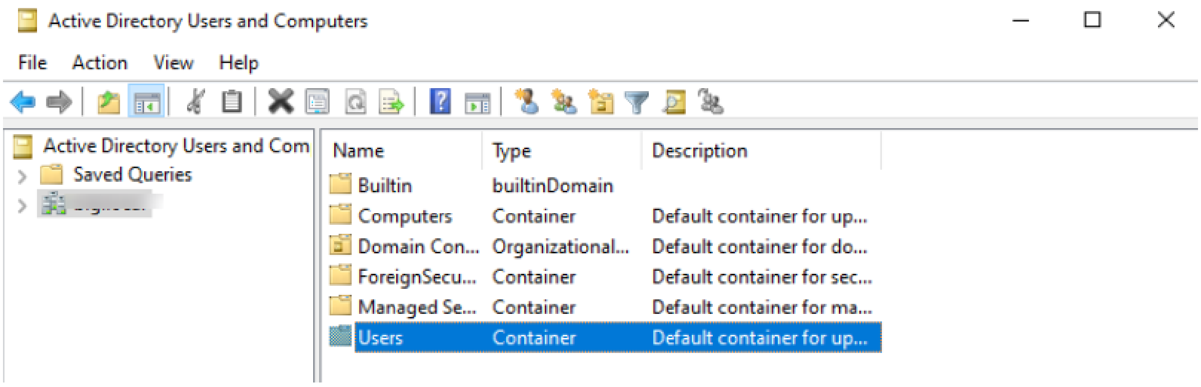
Method 1: PowerShell

1. Open PowerShell as administrator
2. Run the command:

```
Get-ADDomainController | Select-Object HostName
```

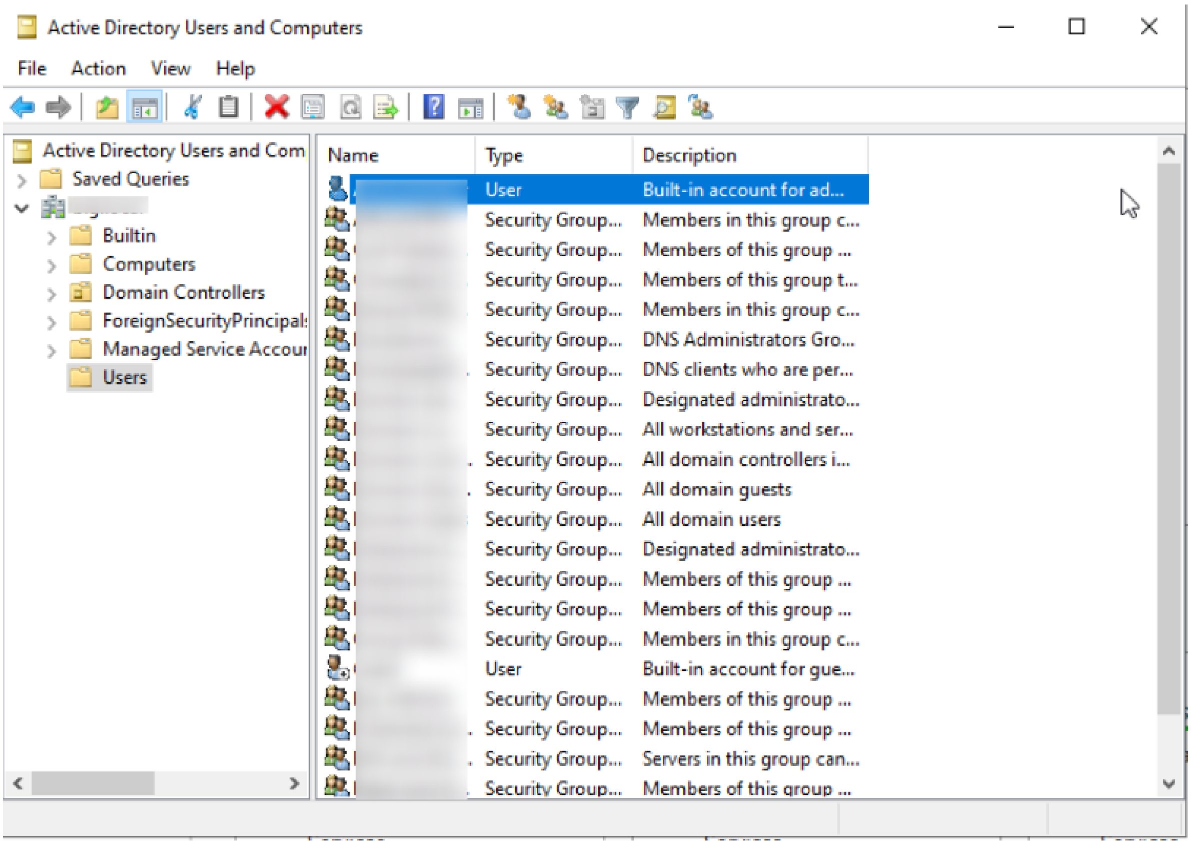
3. Take the DC name from the output
   - LDAP://servername.domain.com
   - LDAP://server-IP

III. Navigate to Users



- Active Directory Users and Com
  - Saved Queries
  - [redacted]

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...
Users	Container	Default container for up...



- Active Directory Users and Com
  - Saved Queries
  - [redacted]
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipal
    - Managed Service Accour
    - Users

Name	Type	Description
[redacted]	User	Built-in account for ad...
[redacted]	Security Group...	Members in this group c...
[redacted]	Security Group...	Members of this group ...
[redacted]	Security Group...	Members of this group t...
[redacted]	Security Group...	Members in this group c...
[redacted]	Security Group...	DNS Administrators Gro...
[redacted]	Security Group...	DNS clients who are per...
[redacted]	Security Group...	Designated administrato...
[redacted]	Security Group...	All workstations and ser...
[redacted]	Security Group...	All domain controllers i...
[redacted]	Security Group...	All domain guests
[redacted]	Security Group...	All domain users
[redacted]	Security Group...	Designated administrato...
[redacted]	Security Group...	Members of this group ...
[redacted]	Security Group...	Members of this group ...
[redacted]	Security Group...	Members in this group c...
[redacted]	User	Built-in account for gue...
[redacted]	Security Group...	Members of this group ...
[redacted]	Security Group...	Members of this group ...
[redacted]	Security Group...	Servers in this group can...
[redacted]	Security Group...	Members of this group ...

If you need further assistance, kindly contact our support at info@cytechint.com for prompt assistance and guidance.

Revision #4
Created 13 November 2024 10:21:44 by CyTech Admin
Updated 14 November 2024 08:19:02 by David Napoleon Romanillos