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.

Requirements

Elastic Agent must be installed. For more details and installation instructions, please refer to the Elastic Agent Installation Guide.

Installing and managing an Elastic Agent:

There are several options for installing and managing Elastic Agent:

Install a Fleet-managed Elastic Agent (recommended):

With this approach, you install Elastic Agent and use Fleet in Kibana to define, configure, and manage your agents in a central location. We recommend using Fleet management because it makes the management and upgrade of your agents considerably easier.

Install Elastic Agent in standalone mode (advanced users):

With this approach, you install Elastic Agent and manually configure the agent locally on the system where it’s installed. You are responsible for managing and upgrading the agents. This approach is reserved for advanced users only.

Install Elastic Agent in a containerized environment:

You can run Elastic Agent inside a container, either with Fleet Server or standalone. Docker images for all versions of Elastic Agent are available from the Elastic Docker registry, and we provide deployment manifests for running on Kubernetes.

Please note, there are minimum requirements for running Elastic Agent. For more information, refer to the Elastic Agent Minimum Requirements.

How to add configurations to Elastic Integration

I. Active Directory Base DN

- **Definition**: The Base DN (Distinguished Name) specifies the starting point in the Active Directory hierarchy for user and group searches.
- **Format**: It typically represents the container or organizational unit (OU) where your user accounts are located.
- **Example**: If your AD users are in the "Users" OU under the domain "example.com", the Base DN might look like:
  - `CN=Users,DC=example,DC=com`

Note: Refer to Step **I. Active Directory Information Lookup** for information on how to properly setup the configuration.

II. Active Directory URL

- **Definition**: The URL of your Active Directory server, specifying either an unsecured LDAP or secure LDAPS connection.
- **Format**:
  - **LDAP (insecure)**: `ldap://your-ad-server.example.com:389`
  - **LDAPS (secure)**: `ldaps://your-ad-server.example.com:636`
- **Example**:
  - `ldap://ad.example.com:389`

Note: Refer to Step **II. Finding Active Directory URL** for information on how to properly setup the configuration.

III. Active Directory User

- **Definition**: The username of the service account that Elastic Stack will use to authenticate and query AD. This account should have sufficient privileges to search for users and groups.
- **Format**:
  - It can be in the form of a **fully qualified domain username**: `username@example.com`
  - Or a **Distinguished Name (DN)**: `CN=ServiceAccount,OU=ServiceAccounts,DC=example,DC=com`
- **Example**:
  - `CN=serviceaccount,OU=ServiceAccounts,DC=example,DC=com`

Note: Refer to Step **III. Navigate to Users** for information on how to properly setup the configuration.

IV. Active Directory User Password

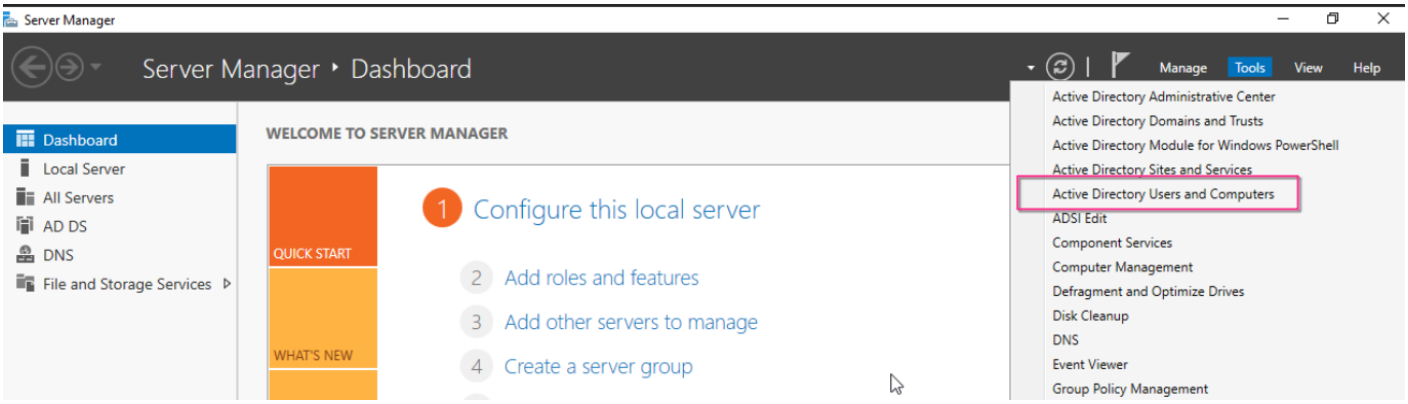
- **Definition**: The password for the AD user account used for the connection.
- **Example**:
  - `MySecurePassword123`

I. Active Directory Information Lookup

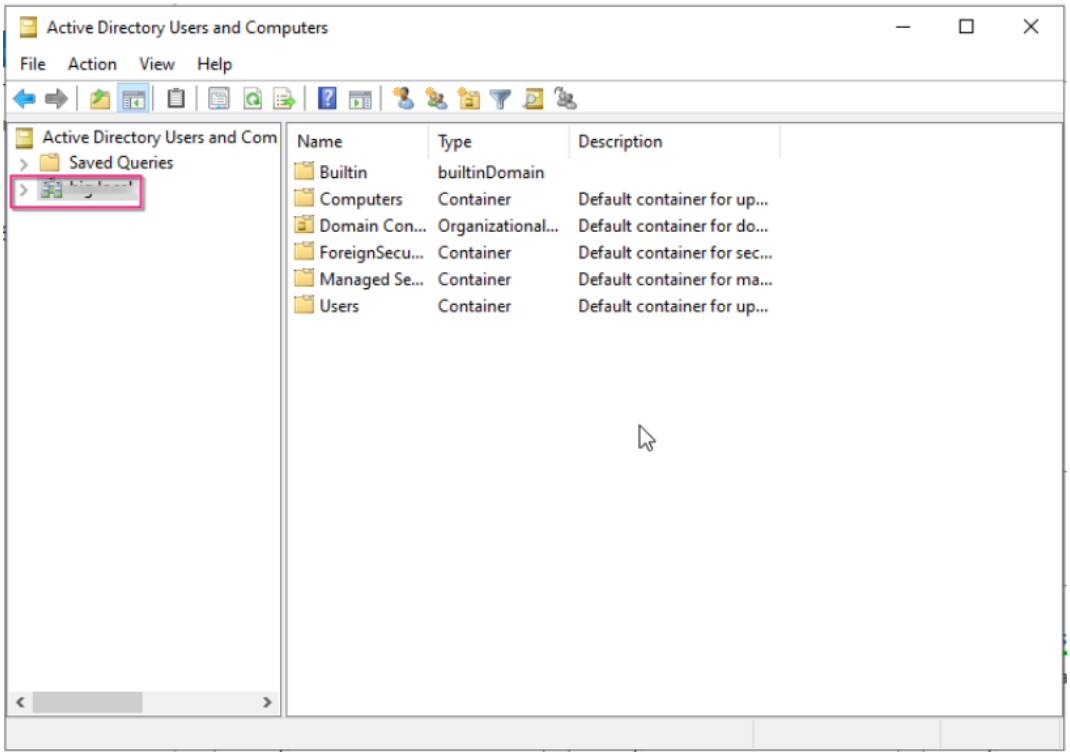
Finding the Base DN (Distinguished Name)

Method 1: Using Active Directory GUI

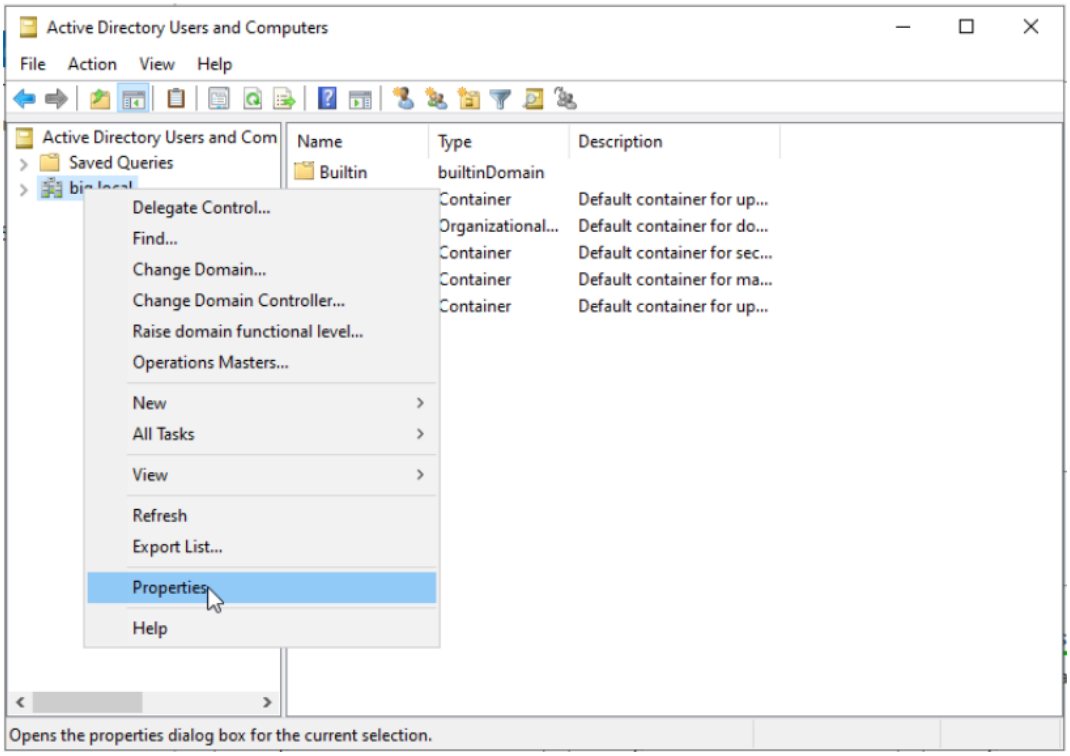
1. Open "Active Directory Users and Computers"



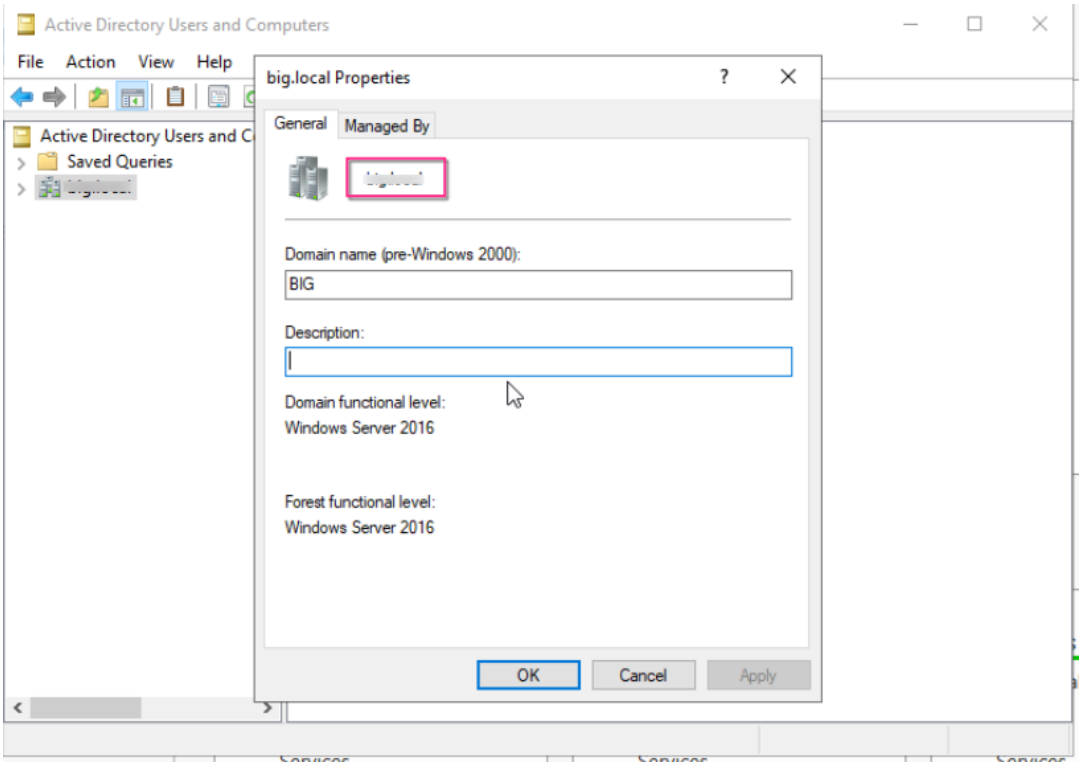
2. Right-click on your domain



3. Select "Properties"



4. Look for the "Distinguished Name" field



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

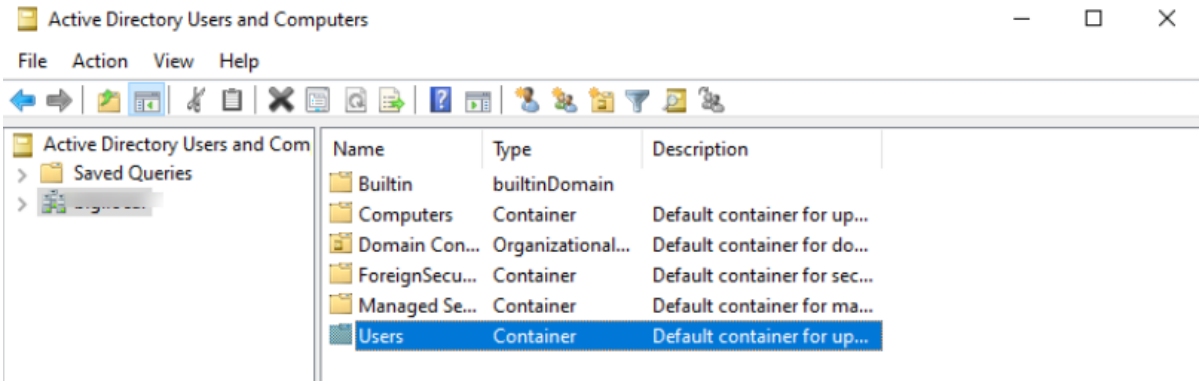
Method 1: PowerShell

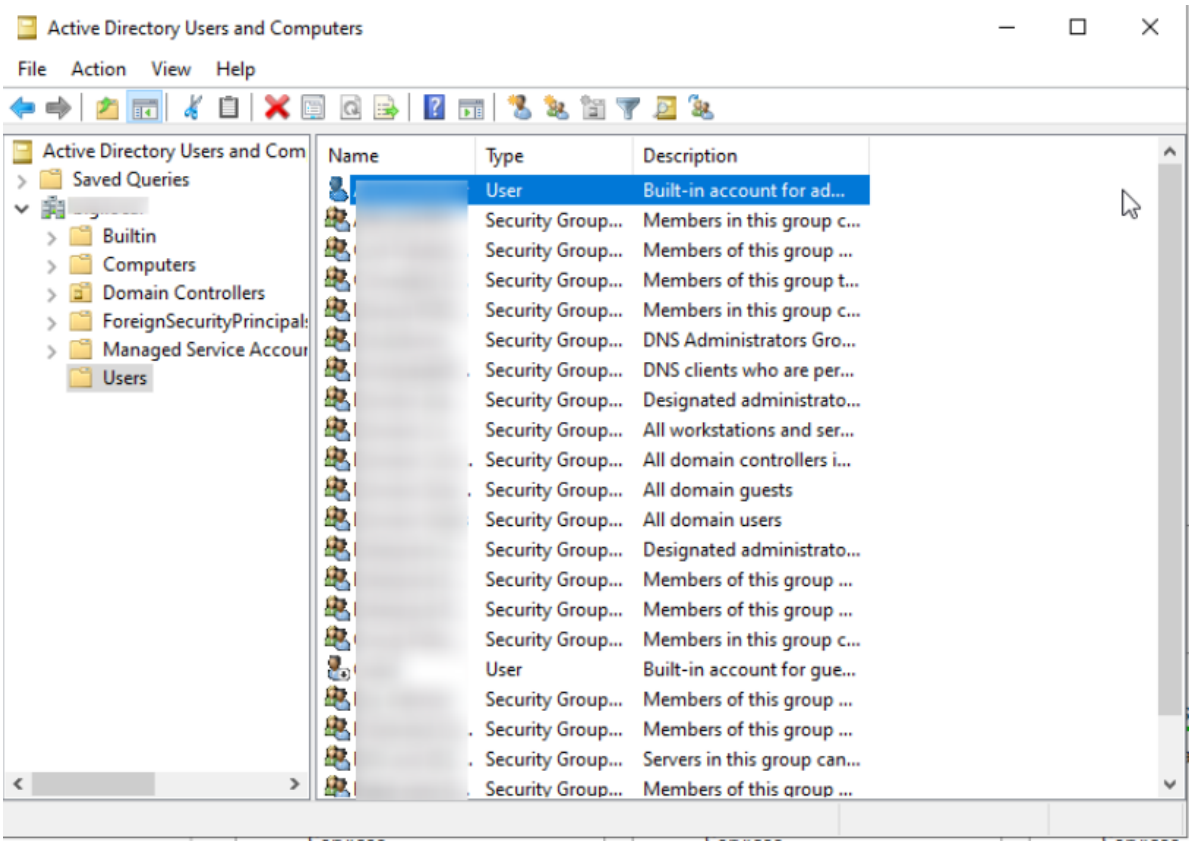
1. Open PowerShell as administrator
2. Run the command:

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

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

III. Navigate to Users





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

Revision #6
Created 13 November 2024 10:21:44 by CyTech Admin
Updated 15 November 2024 09:14:56 by David Napoleon Romanillos