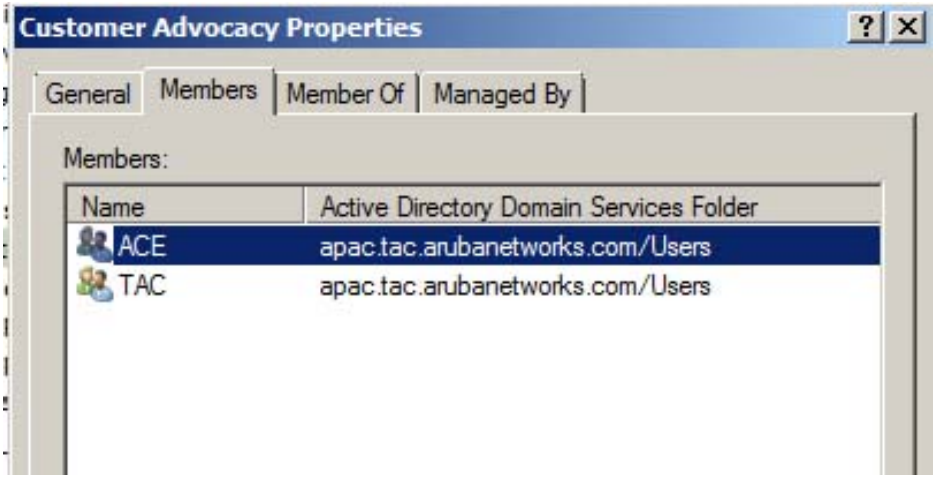
CPPM Nested AD Groups

A UserDN (Distinguished Name) in Active Directory (AD) can be part of a group which in turn as part of another group. For example, a user can be a member of the 'ACE' group while the group 'ACE' is part of the 'Customer Advocacy' group.

The following screenshot is from an AD (Windows 2008) showing the group 'Customer Advocacy' with its two members (ACE and TAC) which are also groups.



It is sometimes useful to define policy based on the 'Customer Advocacy' group which is also applicable to all users that are members of the 'ACE' group. A standard LDAP search using just the 'memberOf' attribute would not yield the desired result. Microsoft AD (Windows 2003 Server and up) supports an extension called LDAP_MATCHING_RULE_IN_CHAIN which is a "special extended match operator that walks the chain of ancestry in objects all the way to the root until it finds a match".

The default filter which returns all groups which a user DN is direct member of uses the following LDAP Filter Query:

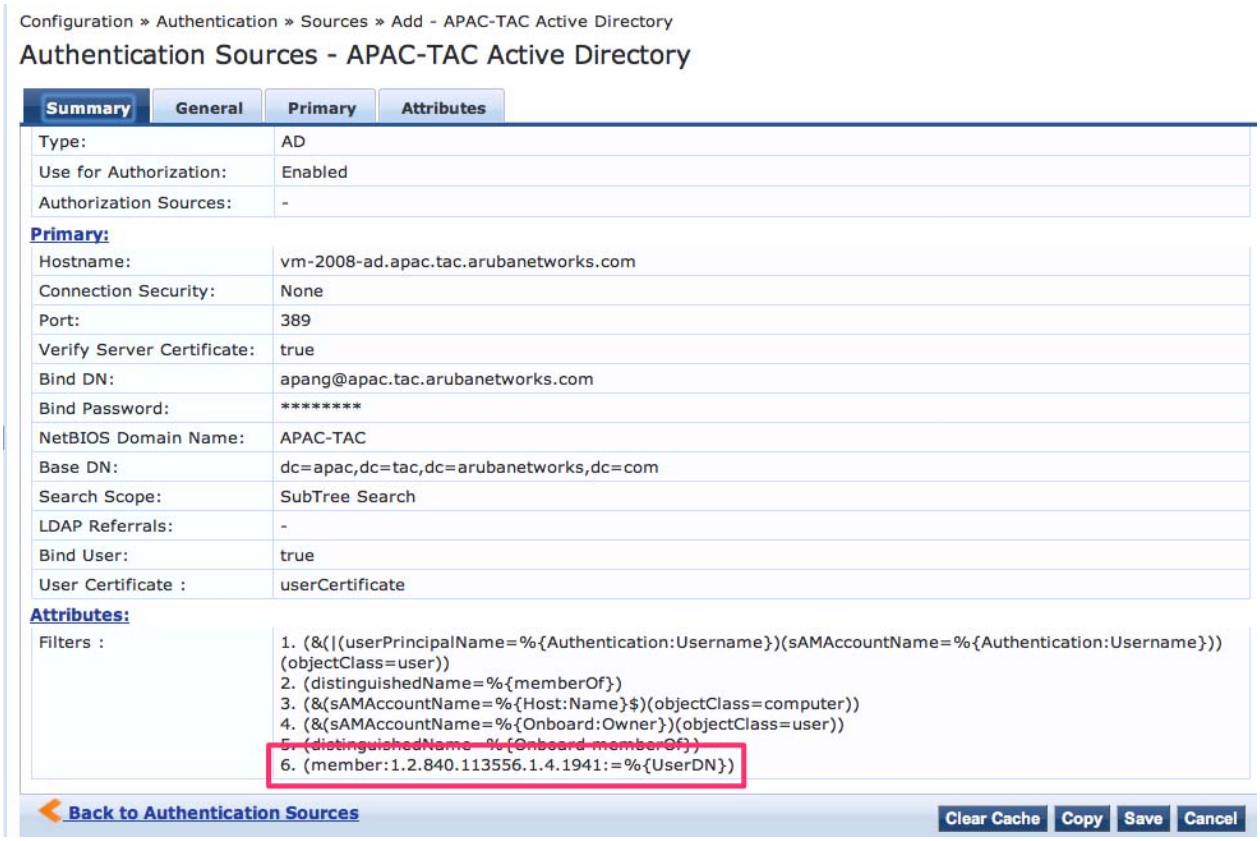
```
(distinguishedName=%{memberOf})
```

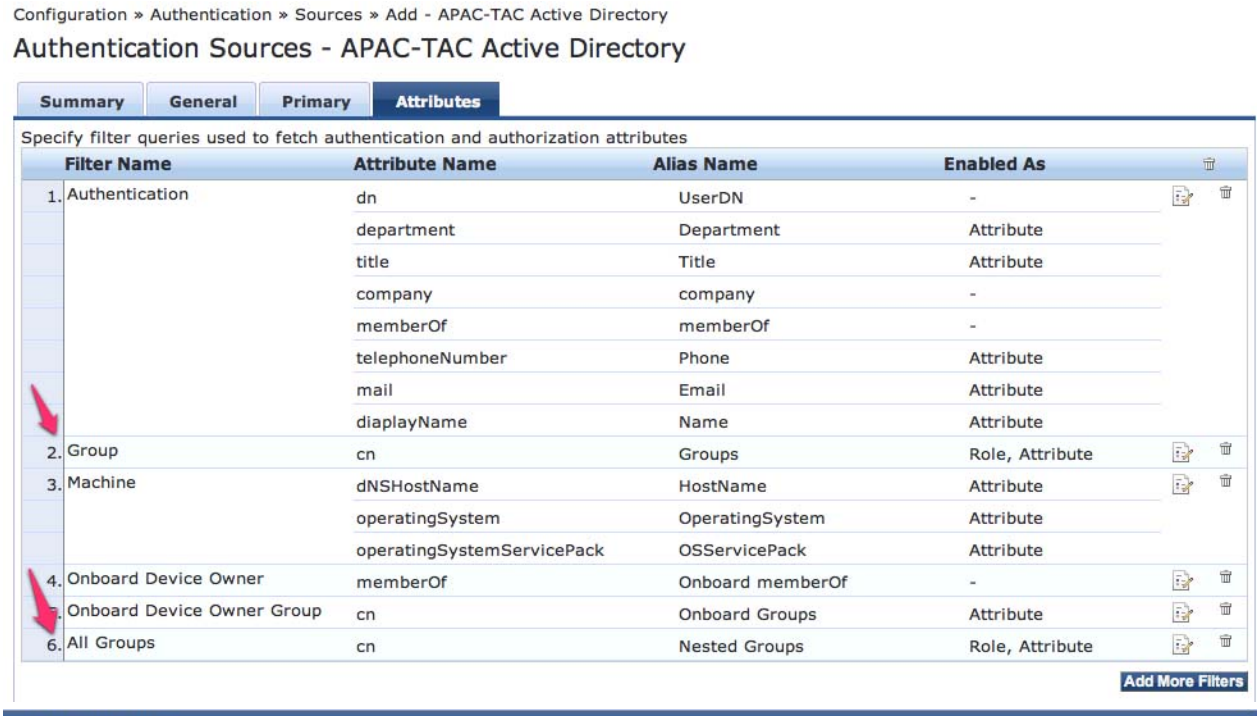
In order to return all groups that a UserDN is part of, we can use the following LDAP Filter Query:

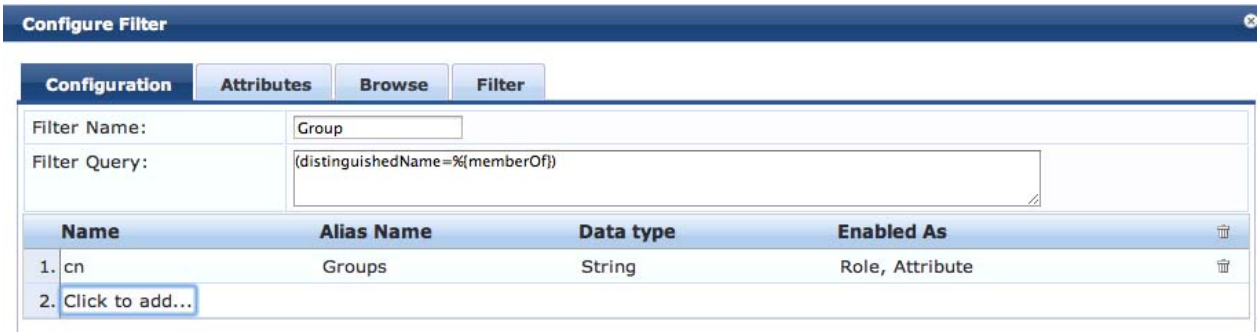
```
(member:1.2.840.113556.1.4.1941:=%{UserDN})
```

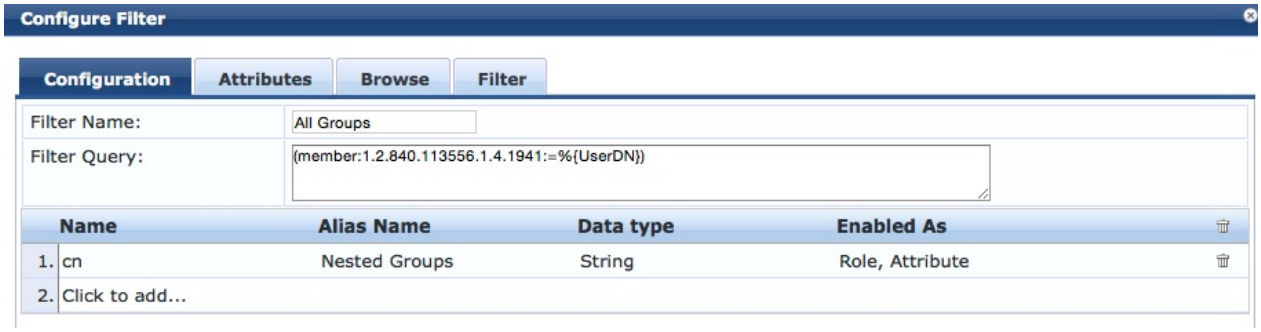
Below are the configuration steps in CPPM to implement the nested group requirement. Assuming that an Authentication Source on an Active Directory has already been defined. The step is ao add an extra filter which contains all of the groups (and their parent groups) that a UserDN is a member of.

Note that set up the 'Group' and 'All Groups' filter to create CPPM 'Roles' automatically with the same name in addition to returning the results as attributes. This makes it simpler to created Enforcement Policies based on the automatically created roles (based on AD membership).

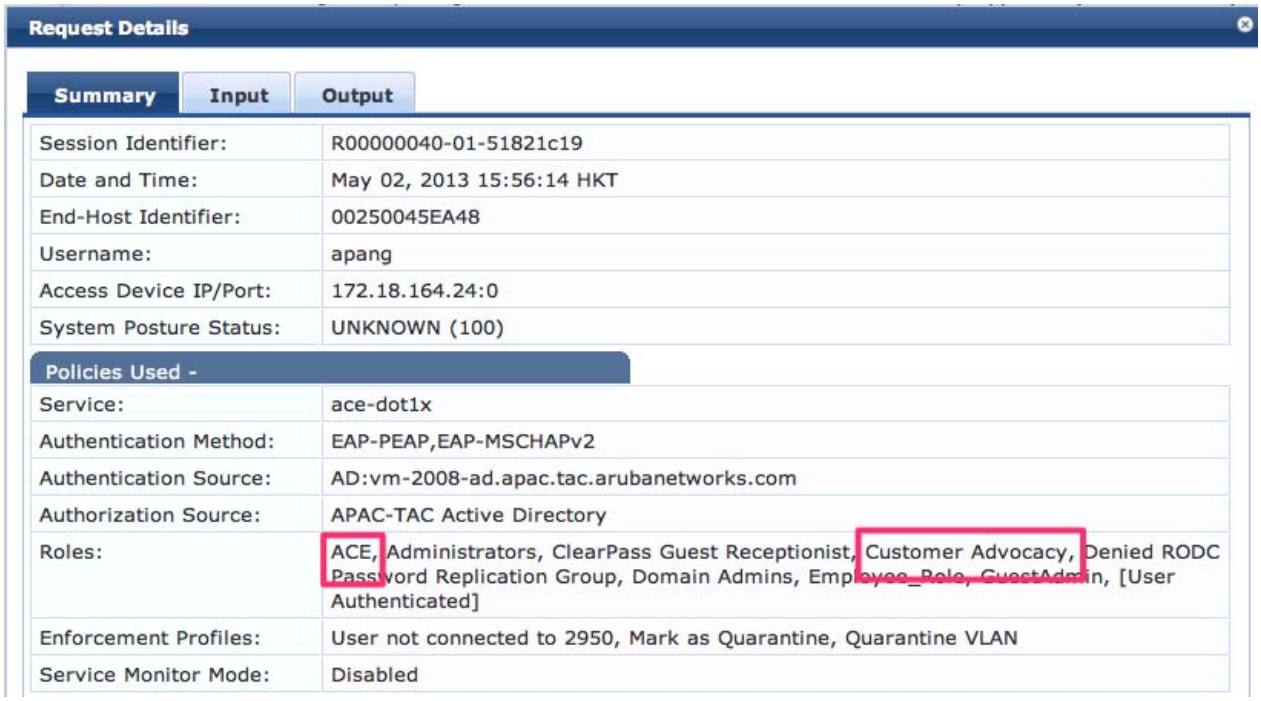

Configuration » Authentication » Sources » Add - APAC-TAC Active Directory
Authentication Sources - APAC-TAC Active Directory
Summary
General
Primary
Attributes
Type: AD
Use for Authorization: Enabled
Authorization Sources: -
Primary:
Hostname: vm-2008-ad.apac.tac.arubanetworks.com
Connection Security: None
Port: 389
Verify Server Certificate: true
Bind DN: apang@apac.tac.arubanetworks.com
Bind Password: ********
NetBIOS Domain Name: APAC-TAC
Base DN: dc=apac,dc=tac,dc=arubanetworks,dc=com
Search Scope: SubTree Search
LDAP Referrals: -
Bind User: true
User Certificate : userCertificate
Attributes:
Filters : 1. (&(|(userPrincipalName=%{Authentication:Username})(sAMAccountName=%{Authentication:Username}))(objectClass=user))
2. (distinguishedName=%{memberOf})
3. (&(sAMAccountName=%{Host:Name}$)(objectClass=computer))
4. (&(sAMAccountName=%{Onboard:Owner})(objectClass=user))
5. (distinguishedName=%{Onboard-memberOf})
6. (member:1.2.840.113556.1.4.1941:=%{UserDN})
Back to Authentication Sources
Clear Cache
Copy
Save
Cancel


Configuration » Authentication » Sources » Add - APAC-TAC Active Directory
Authentication Sources - APAC-TAC Active Directory
Summary
General
Primary
Attributes
Specify filter queries used to fetch authentication and authorization attributes
Filter Name
Attribute Name
Alias Name
Enabled As
1. Authentication dn UserDN -
department Department Attribute
title Title Attribute
company company -
memberOf memberOf -
telephoneNumber Phone Attribute
mail Email Attribute
diaplayName Name Attribute
2. Group cn Groups Role, Attribute
3. Machine dNSHostName HostName Attribute
operatingSystem OperatingSystem Attribute
operatingSystemServicePack OSServicePack Attribute
4. Onboard Device Owner memberOf Onboard memberOf -
5. Onboard Device Owner Group cn Onboard Groups Attribute
6. All Groups cn Nested Groups Role, Attribute
Add More Filters


Configure Filter
Configuration
Attributes
Browse
Filter
Filter Name: Group
Filter Query: (distinguishedName=%{memberOf})
Name
Alias Name
Data type
Enabled As
1. cn Groups String Role, Attribute
2. Click to add...



Access Tracker showing user as part of the 'Customer Advocacy' group (of groups).



See Also

- Active_Directory

Reference

1. http://msdn.microsoft.com/en-us/library/windows/desktop/aa746475(v=vs.85).aspx
2. http://www.tek-tips.com/viewthread.cfm?qid=1442886

Article Sources and Contributors

CPPM Nested AD Groups *Source*: https://arubapedia.arubanetworks.com/arubapedia/index.php?oldid=67582 *Contributors*: Apang, Schoate

Image Sources, Licenses and Contributors

File:CPPM-Nested-AD-Group-AD.jpg *Source*: https://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:CPPM-Nested-AD-Group-AD.jpg *License*: unknown *Contributors*: Apang

File:CPPM-Nested-AD-Group-1.jpg *Source*: https://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:CPPM-Nested-AD-Group-1.jpg *License*: unknown *Contributors*: Apang

File:CPPM-Nested-AD-Group-2.jpg *Source*: https://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:CPPM-Nested-AD-Group-2.jpg *License*: unknown *Contributors*: Apang

File:CPPM-Nested-AD-Group-3.jpg *Source*: https://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:CPPM-Nested-AD-Group-3.jpg *License*: unknown *Contributors*: Apang

File:nestedgroup.png *Source*: https://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:nestedgroup.png *License*: unknown *Contributors*: Apang, Rwright

File:CPPM-Nested-AD-Group-Access-Tracker.jpg *Source*: https://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:CPPM-Nested-AD-Group-Access-Tracker.jpg *License*: unknown *Contributors*: Apang