Cisco APIC, Identity Server Groups, and AD Attribute for Microsegmentation

Revised: June 23, 2022,

New and Changed Information

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Table 1: New Features and Changed Behavior in Cisco APIC

Cisco APIC Release Version	Feature	Description
Release 3.2(2)	Support for identity-based (Active Directory) server groups.	Active Directory (AD) use groups can be used by a tenant for identity-based uEPGs, which allows control of traffic flow between EPGs based on AD security groups.
	Support for AD attribute for microsegmentation (uSeg) EPGs.	The AD attribute enables you to match VMs to uSeg EPGs using user groups.

AD-Based Microsegmentation

Microsegmentation (uSeg) with the Cisco Application Centric Infrastructure (ACI) enables you to automatically assign endpoints to logical security zones called endpoint groups (EPGs). These EPGs are based on various network-based or virtual machine (VM)-based attributes.

Beginning with Cisco APIC Release 3.2(2), identity servers, such as Active Directory (AD), can be used by a tenant for identity-based microsegmentation. This allows you to apply forwarding and security policies to entire group of VMs based on the security groups configured on the AD server.

This chapter contains information specific to using AD-based microsegmentation, for a complete overview of microsegmentation with Cisco ACI, see *Microsegmentation with Cisco ACI* .

Before this feature can be used in APIC, a device called ISE-PIC (Identity Service Engine, Passive Identity Connector) has to be installed and configured in your environment. ISE-PIC monitors all the events, users, and groups belonging to your AD domain and builds an inventory of them for APIC.

Keep in mind, before you configure ISE PIC and APIC, you must have a Microsoft AD server 2008 R2 or above already set up for your domain.

Note Configuring identity server groups and uSeg EPGs with the AD attribute are beta features in this release of Cisco APIC.

Configuring ISE-PIC for Identity-Based Microsegmentation

This section provides an overview of how to configure ISE-PIC for use with APIC's identity-based micro-segmentation.

Before you begin

- You must have installed ISE-PIC 2.0 or later, as described in *ISE-PIC Installation and Administrator Guide*

- You must have installed APIC 3.2(2) or later, as described in *Cisco APIC Basic Configuration Guide*
- You must also have an Active Directory (AD) server already configured for your domain.

Procedure

Step 1 Log in to your ISE-PIC.

Step 2 Configure the ISE-PIC to connect to your AD server.

a) Navigate to **Providers** > **Active Directory**.
b) Click **Add** to add a *Join Point* to communicate with your existing AD server.
c) Provide a *Join Point Name* and the *Active Directory Domain*
d) Click **Submit**.
e) Click **Yes** when prompted if you would like to join all ISE Nodes to the active directory domain.
f) Provide AD login credentials when prompted to allow ISE-PIC to create a computer account in AD.

Once completed, the ISE-PIC will display *Completed* in the **Node Status**.

After you complete these steps, the **ISE Node**'s status will change to *Operational*.

Step 3 Configure the Active Directory instance for PassiveID.

a) Navigate to **Providers** > **Active Directory** > **PassiveID**.
b) Click **Add DCs**
c) Select the Domain Controller you want to monitor and click **OK**.
d) In the PassiveID screen, select the domain controller you just added, then click **Config WMI**.

At this point, the ISE-PIC is configured to monitor the domain controler remotely via WMI. You can check the status of the domain controller on the dashboard using the **Providers** screen.

Step 4 Configure Active Directory Groups.

a) Navigate to **Providers** > **Active Directory** > **Groups**.
b) Choose **Add** > **Select Groups From Directory** to add the AD groups to ISE-PIC, then select the groups you want to add.
c) Navigate to **Providers** > **Active Directory** > **Advanced**.
d) Configure the **User session aging time** to specify the amount of time that ISE-PIC will keep the session alive (consider the user active) before issuing an automatic log off.

Step 5 Navigate to **Settings** > **System Time** and configure the NTP server.

It is recommended that you use the same NTP server for APIC, ISE-PIC, and AD server to keep the time synchronized between all devices.

Step 6 Create the certificates to be used by APIC.

a) Navigate to **Subscribers** > **Certificates**.
b) Generate a pxGrid certificate to be used for authentication between the ISE-PIC and APIC

For **Certificate Download Format**, select *PKCS12 format*

After you have created the certificate, you will need to import it into your APIC, as described in the following steps.

Step 7 Log in to your APIC.

Step 8 Create a certificate authority.

You can skip this step if you already have a certificate authority configured in your environment.

a) Navigate to **Admin** > **AAA** > **Public Key Management**.
b) Tight-click on the **Certificate Authorities** and choose **Create Certificate Authority**
c) In the same **Public Key Management** folder, right-click **Key Rings** and choose **Create Key Ring**

Then configure a key ring selecting the certificate authority you configured in the previous step (you can skip this step if you already have a key ring configured).

For more detailed information about ISE pxGrid certificates, see Deploying Certificates with pxGrid

Step 9 Navigate to **Fabric** > **Fabric Policies** > **Policies** > **Global Policies** > **DNS Profiles**.

You can modify the default DNS profile and add DNS provider and DNS Domain associated with the AD domain you plan to use.

Identity Server Groups

The following sections provide information on how to set up and configure the APIC for identity-based microsegmentation, specifically how to create identity server groups. You can use the APIC GUI, the NX-OS style CLI, or REST API to make all the necessary setup and configuration changes.

Configuring an Identity Server Group Using the GUI

You can use the APIC GUI to configure an AD server group.

Before you begin

You must have a tenant configured. For tenant configuration information, see the *Cisco APIC Basic Configuration Guide*.

Procedure

Step 1 Log in to the Cisco APIC.

Step 2 Click **Tenants** and then click the tenant where you plan to use the AD attribute for a microsegmentation (uSeg) EPG.

Step 3 In the tenant navigation pane, select **Services**, then right-click **Identity Server Groups (Beta)** and choose **Create Identity Server Group**.

Step 4 In the **Create Identity Server Group** dialog box, read and accept the user agreement for the beta feature.

Step 5 In the **Name** field, enter the name for the Identity Server Group.

Step 6 (Optional) In the **Security Domain** area, click the plus icon, and select (or create) a security domain.

Step 7 In the **Servers** area, click the plus icon, and then enter the fully-qualified domain name (FQDN) of the ISE-PIC server and key ring you have created in Configuring ISE-PIC for Identity-Based Microsegmentation, on page 2.

Group inventory is synchronized every 8 hours. Synchronization can also be triggered manually from the GUI by clicking the identity server icon.

Step 8 Click **OK** and then click **Submit** to save the changes .

What to do next

If you want to define an AD attribute for uSeg EPG, follow the instructions in the section Microsegmentation EPGs with AD Group Attribute , on page 6 in this document.

Configuring an AD Server Group Using the NX-OS Style CLI

Before you begin

You must have a tenant configured. For tenant configuration information, see the *Cisco APIC Basic Configuration Guide*.

Procedure

Configure the ISE Auth server group under a given Tenant.

In the following commands, provide the following parameters for your environment:

- Name of the ISE server
- Management EPG
- Key Ring

Example:

```
Dev8-IFC1(config)#tenant common
Dev8-IFC1(config-tenant)# authsvrgrp ISE
Dev8-IFC1(config-tenant-authsvrgrp)# authsvr ISE_Server demo-ise1.isedemo2.local
uni/tn-mgmt/out-vmm/instP-extMgmt demo
```

What to do next

If you want to define an AD attribute for a uSeg EPG, follow the instructions in the section Microsegmentation EPGs with AD Group Attribute , on page 6 in this document.

Configuring an AD Server Group Using REST API

Before you begin

You must have a tenant configured. For tenant configuration information, see the *Cisco APIC Basic Configuration Guide*.

Procedure

Step 1 Configure a Certificate Authority (CA).

```
POST: <host info>/api/node/mo/uni.xml
```

Example:

```
<polUni>
<aaaUserEp>
    <pkiEp>
        <pkiTP certChain="-----BEGIN CERTIFICATE-----
        MIIFqDCCA5CgAwIBAgIQLN2SDaZqS6acY4ou6PmGMDANBgkqhkiG9w0BAQsFADAz
        MTEwLwYDVQQDDChDZXJ0aWZpY2F0ZSBTZXJ2aWNlcyBOb2RlIENBIC0gZGVtby1p
        c2UxMB4XDTE4MDQwOTIzNTU1MVoXDTIzMDQxMDIzNTU0MFowOzE5MDcGA1UEAwww
        Q2VydGlmaWNhdGUgU2VydmljZXMgRW5kcG9pbnQgU3ViIENBIC0gZGVtby1pc2Ux
        MIICIjANBgkqhkiG9w0BrzQDb+Wp47NV0ndrWWmKg2kV6PE4GJ15i3YLdYI=
```

```
        -----END CERTIFICATE-----" name="isedemo2-TP" />
    </pkiEp>
</aaaUserEp>
</polUni>
```

Step 2 Configure a key ring.

```
POST: <host info>/api/node/mo/uni.xml
```

Example:

```
<polUni>
<aaaUserEp>
    <pkiEp>
        <pkiKeyRing cert="-----BEGIN CERTIFICATE-----
        MIIEzzCCAregAwIBAgIQWcBwaqWzSCe9GCZzeRQ6hjANBgkqhkiG9w0BAQsFADA7
        MTkwNwYDVQQDDDBDZXJ0aWZpY2F0ZSBTZXJ2aWNlcyBFbmRwb2ludCBTdWIgQ0Eg
        LSBkZWrm4OdVZLOlOWgyGZtwBFtHeTvISJ0r/VsBVRMrpx4WB+q1QDLzkD
        -----END RSA PRIVATE KEY-----" name="isedemo2" tp="isedemo2-TP" />
    </pkiEp>
</aaaUserEp>
</polUni>
```

Step 3 Configure an AD server group.

```
POST: <host info>/api/node/mo/uni.xml
```

Example:

```
<polUni>
<fvTenant name="common">
    <authSvrGroup name="group1" mode="AD">
        <authSvr name="demo-ise1" hostOrIp="demo-ise1.isedemo2.local">
            <authRsSvrToMgmtEPg tDn="uni/tn-mgmt/out-vmm/instP-extMgmt"/>
            <authUsrAccP keyRingDn="uni/userext/pkiext/keyring-isedemo2"/>
       </authSvr>
   </authSvrGroup>
</fvTenant>
</polUni>
```

What to do next

If you want to define a DNS attribute for a uSeg EPG, follow the instructions in the section Microsegmentation EPGs with AD Group Attribute , on page 6 in this document.

Microsegmentation EPGs with AD Group Attribute

Defining an AD attribute for a uSeg EPG enables you to put VMs matching AD security groups that you previously identified into the uSeg EPG. You can define an AD attribute for a uSeg EPG in the APIC GUI, NX-OS style CLI, or REST API.

Configuring a uSeg EPG with the AD Attribute Using the GUI

Before you begin

Read and understand the guidelines and fulfill the prerequisites in the "Microsegmentation with Cisco ACI" chapter of the *Cisco ACI Virtualization Guide*.

Procedure

Step 1 Follow the procedure "Configuring Microsegmentation with Cisco ACI Using the GUI" in the "Microsegmentation with Cisco ACI" chapter of the *Cisco ACI Virtualization Guide* through Step 11.

Step 2 Instead of Step 12, perform the following steps:

a) From the **Select a type...** drop-down list, choose **AD Group (Beta)**.
b) Select the **AD Controller**.
c) Select the **AD Domain**.
d) Select the **AD Group**.
e) Click **Submit**.

Step 3 Complete Step 13 and the rest of the procedure.

After a uSeg EPG has been configured with the AD attribute, you will be able to see the classified end points move to the **Tenants** > **Tenant Name** > **Application Profiles** > **ApplicationProfile** > **uSeg EPGs** folder in the UI.

Alternatively, you can also view the classified microsegmentation end points under **Tenants** > **Tenant common** > **Services** > **Identity Server Groups (Beta)** > **ServerGroup** > **ISEPIC** > **Classified EPGs**.

Configuring a uSeg EPG with the AD Attribute Using the NX-OS Style CLI

Before you begin

Read and understand the guidelines and fulfill the prerequisites in the "Microsegmentation with Cisco ACI" chapter of the *Cisco ACI Virtualization Guide*.

Procedure

Create the AD-based attribute matching a specific Active Directory group under a given Tenant

Example:

```
Dev8-IFC1(config)# tenant BlueCorp
Dev8-IFC1(config-tenant)# application AP1
Dev8-IFC1(config-tenant-app)# epg useg1
Dev8-IFC1(config-tenant-app-uepg)# attribute 1 match idgrp ?
  adepg/authsvr-common-ISE-ISE_Server/grpcont/dom-isedemo2.local/grp-Builtin
  adepg/authsvr-common-ISE-ISE_Server/grpcont/dom-isedemo2.local/grp-Users
  adepg/authsvr-common-ISE-ISE_Server/grpcont/dom-isedemo2.local/grp-cisco
Dev8-IFC1(config-tenant-app-uepg)# attribute 1 match idgrp
adepg/authsvr-common-ISE-ISE_Server/grpcont/dom-isedemo2.local/grp-cisco
```

Configuring a uSeg EPG with the AD Attribute Using REST API

Before you begin

Read and understand the guidelines and fulfill the prerequisites in the "Microsegmentation with Cisco ACI" chapter of the *Cisco ACI Virtualization Guide*.

Procedure

Configure a uSeg EPG with the AD attribute.

Example:

```
<polUni>
    <fvTenant name="cisco">
        <fvCtx name="HRNet" />
        <!-- bridge domain -->
        <fvBD name="BD1">
            <fvRsCtx tnFvCtxName="HRNet" />
            <fvSubnet ip="1.1.1.1/24" />
        </fvBD>
        <fvAp name="web" >
            <fvAEPg descr="" dn="uni/tn-cisco/ap-web/epg-TEST"
              isAttrBasedEPg="yes" matchT="AtleastOne" name="TEST">
                <fvRsBd tnFvBDName="BD1" />
                <fvCrtrn match="any" name="default" prec="0">
                    <fvIdGroupAttr name="match-Eng"
                      selector="adepg/authsvr-common-sg1-ISE_1/grpcont/dom-cisco.com/grp-Eng">
                </fvIdGroupAttr>
                </fvCrtrn>
            </fvAEPg>
        </fvAp>
    </fvTenant>
</polUni>
```

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.