30.2：User Agent & Identity Policy

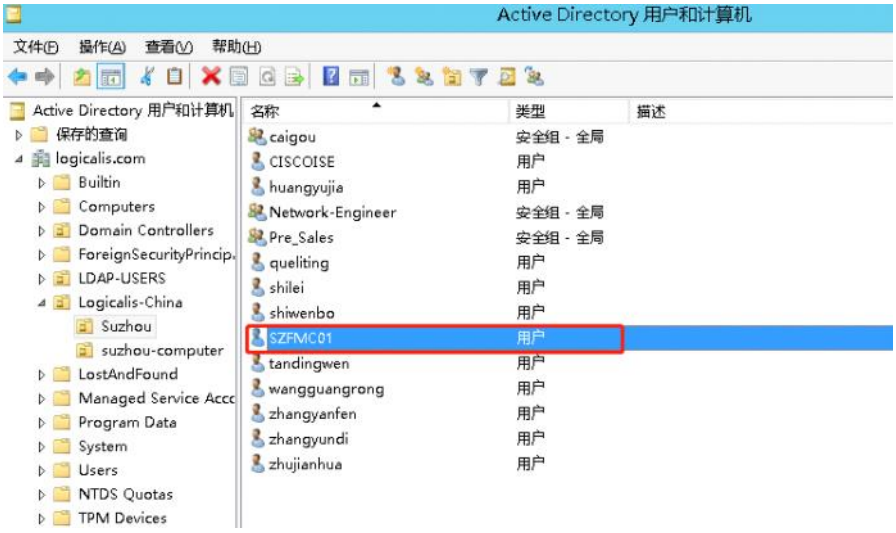
2020年1月31日 15:54

目录

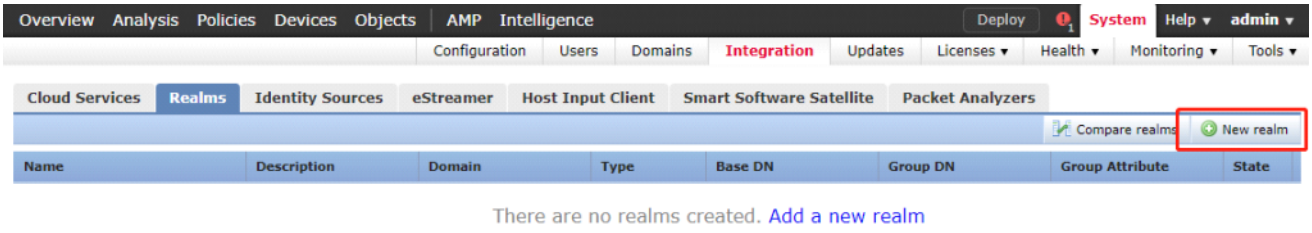
1：FMC关联AD获取用户信息

https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/create_and_manage_realms.html

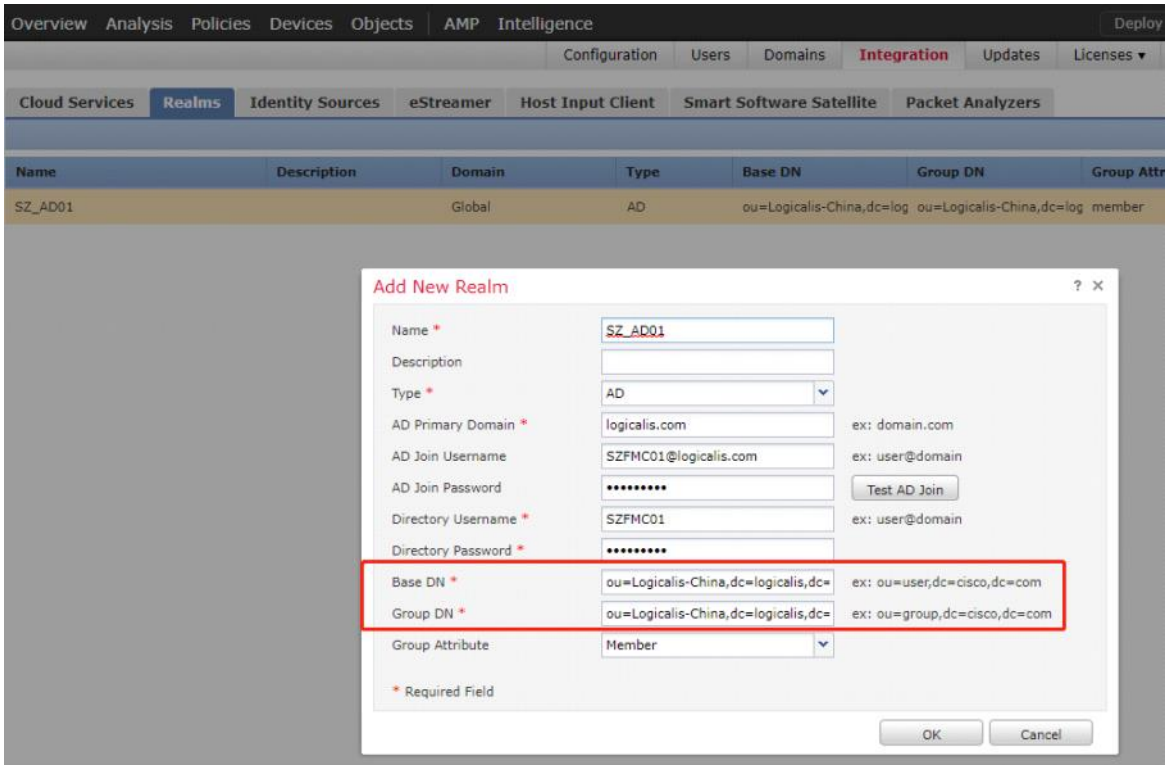
1.1：AD给FMC建立一个AD账户，普通domain-user账户即可



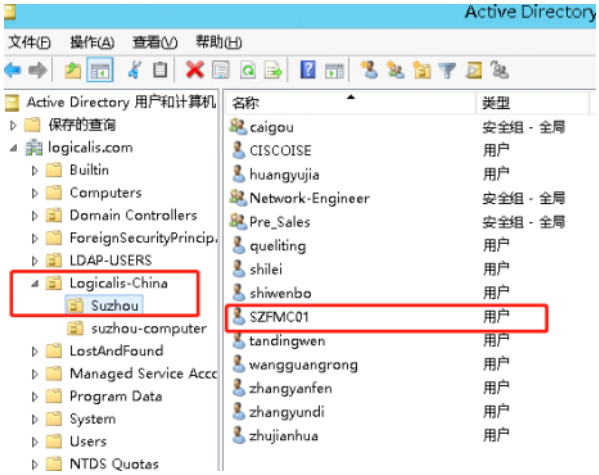
1.2：AD创建领域



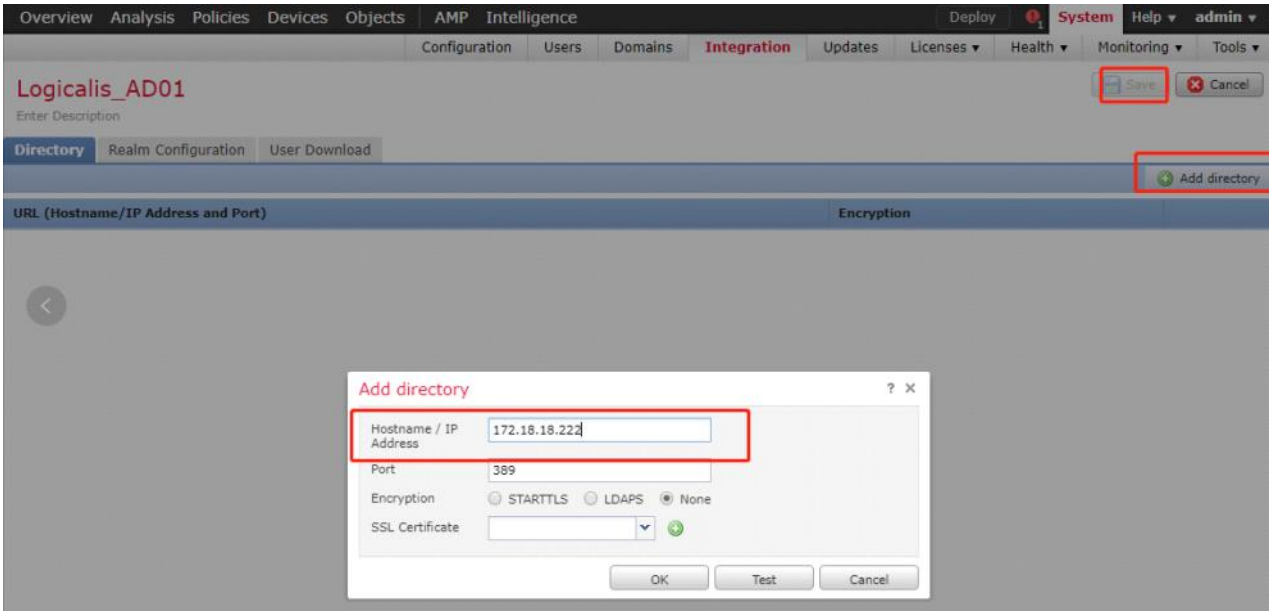
填写加域的域信息和域账户信息



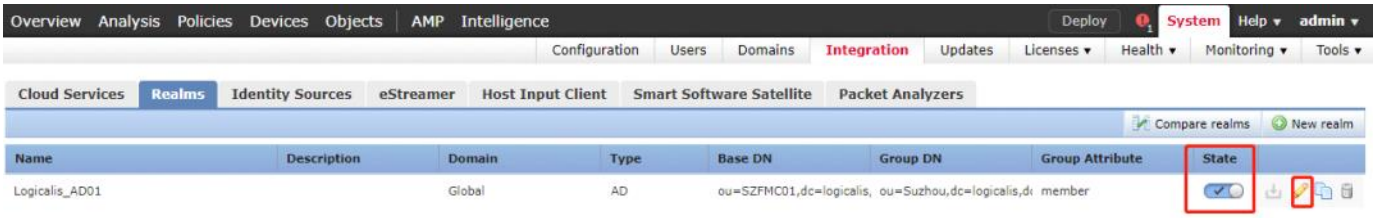
ou=Logicalis-China,dc=logicalis,dc=com
（如果你的OU是有子OU的，请填写父OU，比如这里父OU就是logicalis-China，子OU是苏州）



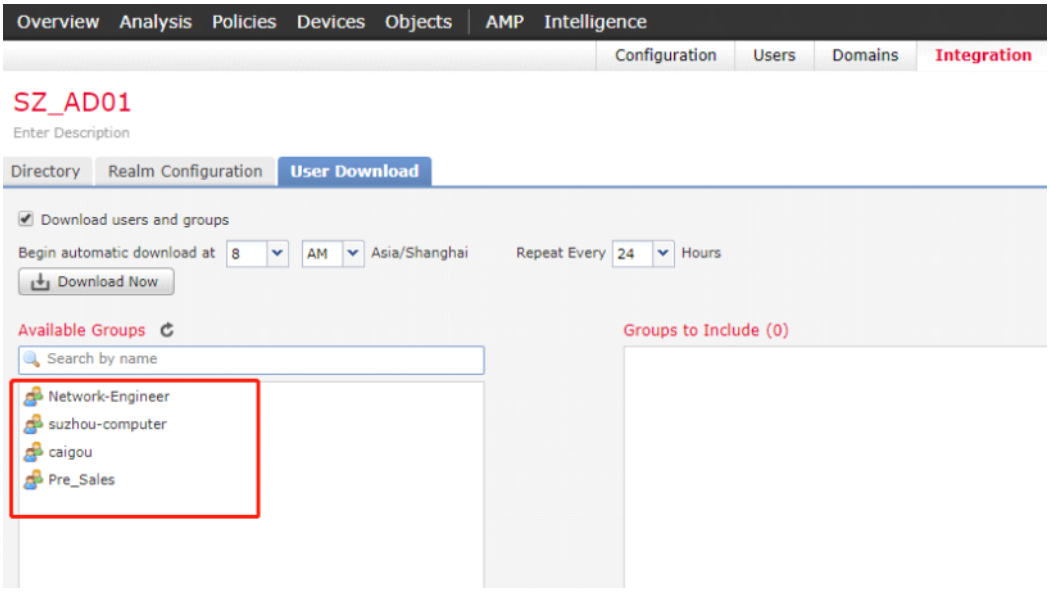
1.3：之前只是加域，现在要指定关联的AD服务器地址



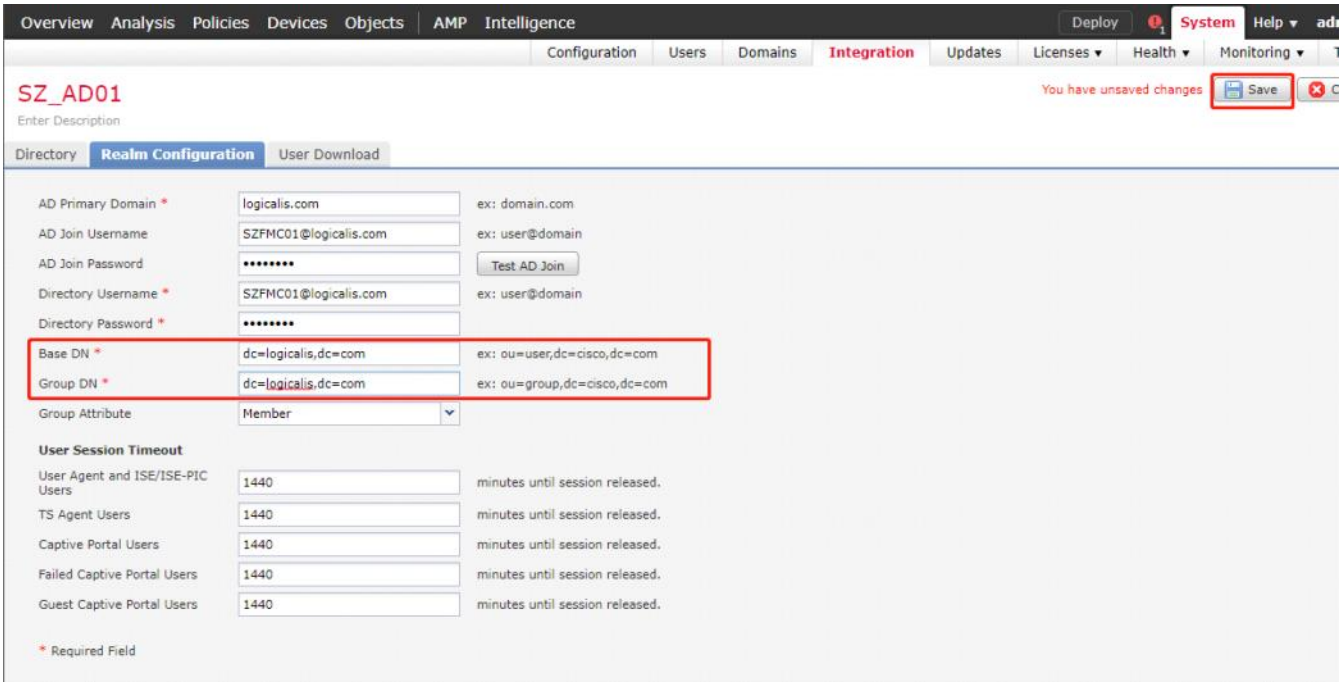
1.4：开启和AD连接并编辑获取组信息

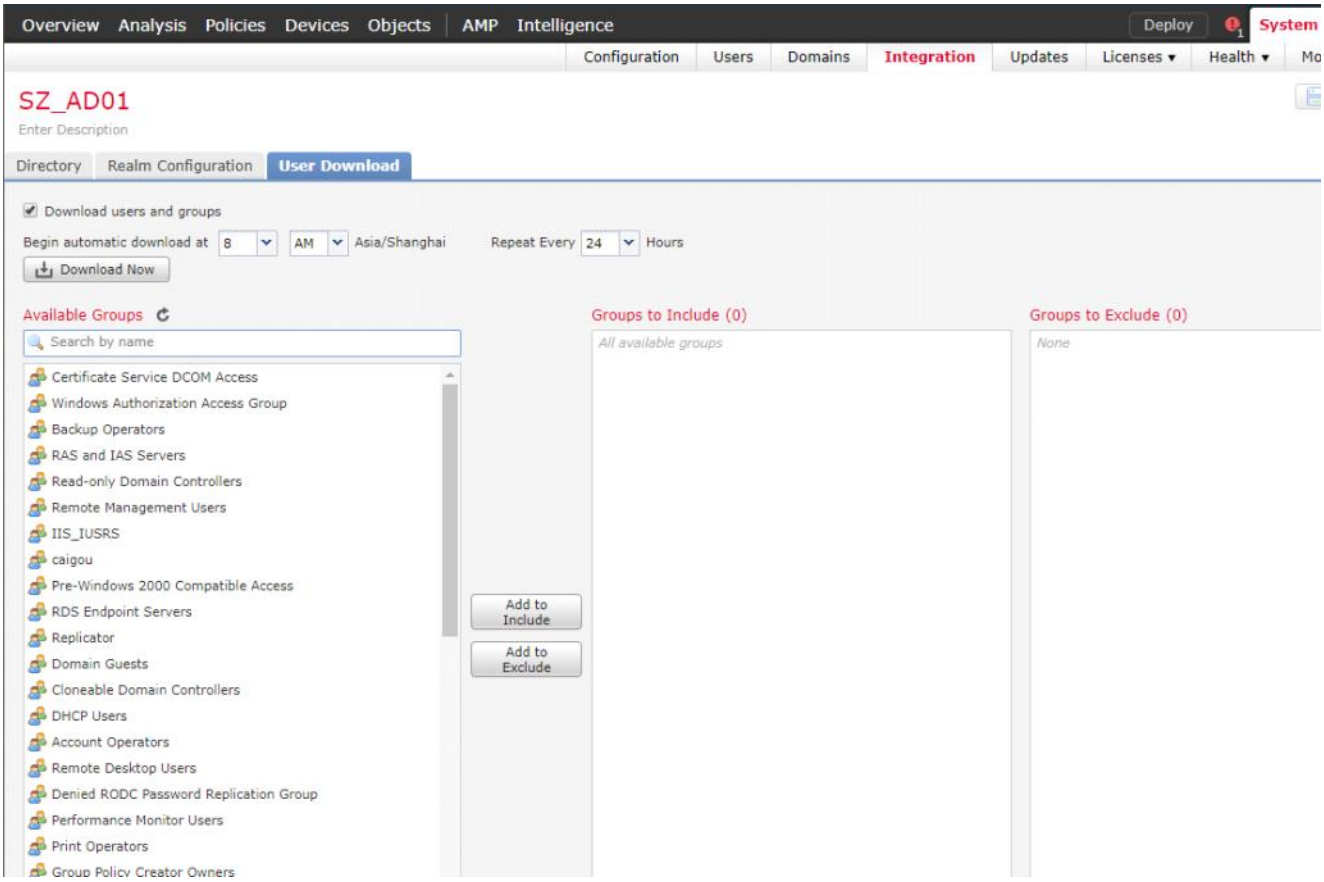


1.5：可以看到，可以从Logicalis-China这个OU获取用户组信息。



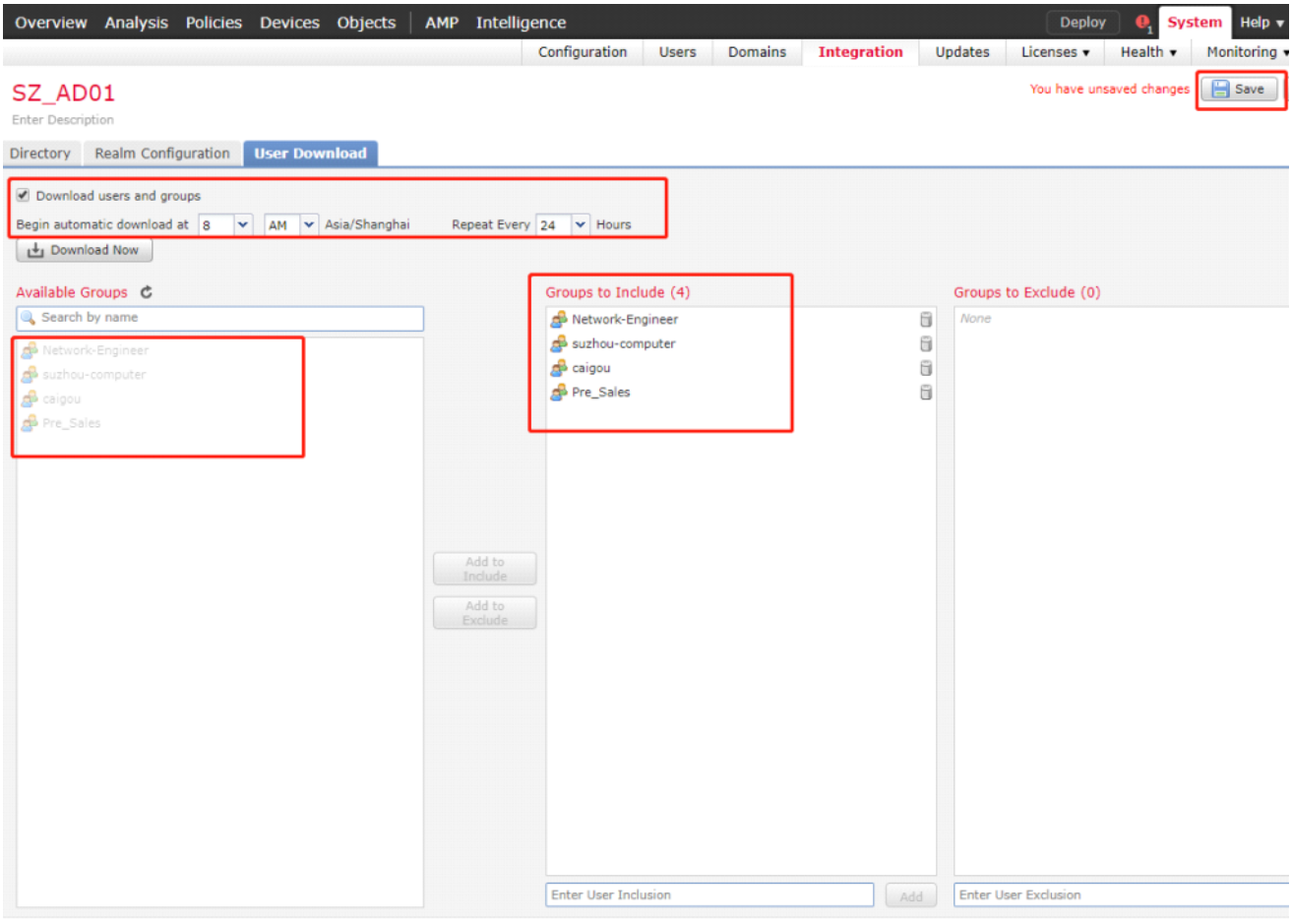
1.6：（可选）获取所有AD上所有OU的组信息，只需要把OU去掉只保留DC即可





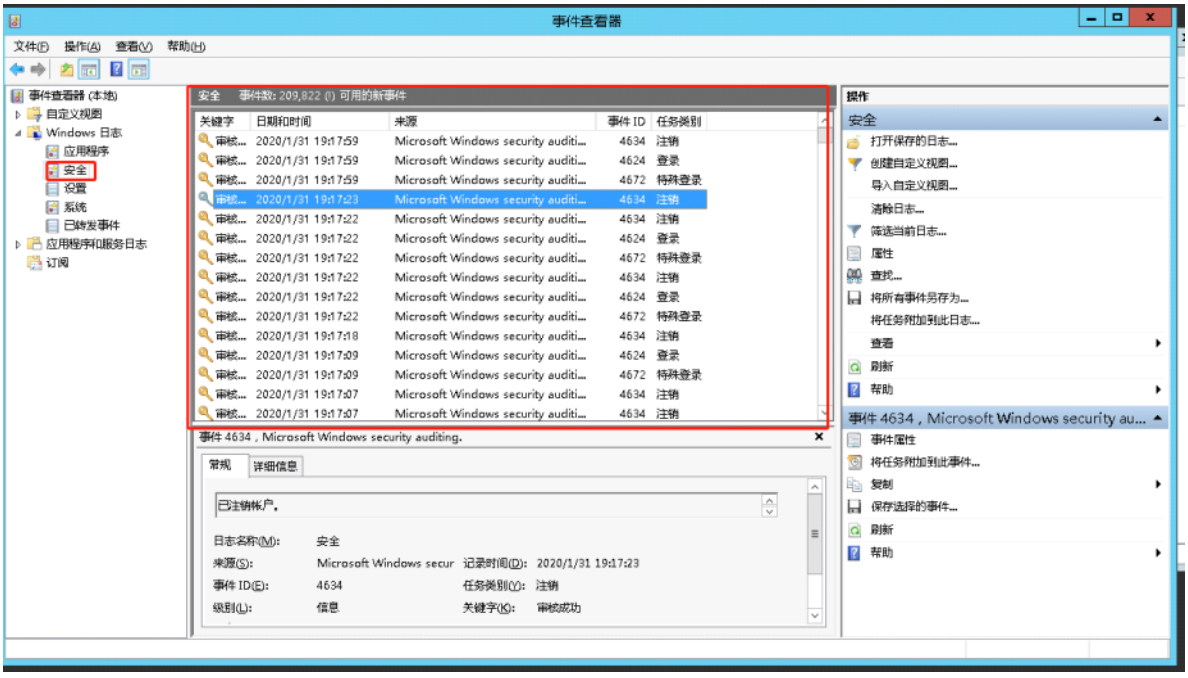
1.7：设置自动从AD获取组信息的更新时间，也可以现在更新，并将AD的用户组添加到本地

同时，这里还可以直接下include里面添加单个用户，或者排除单个用户



2：配置AD

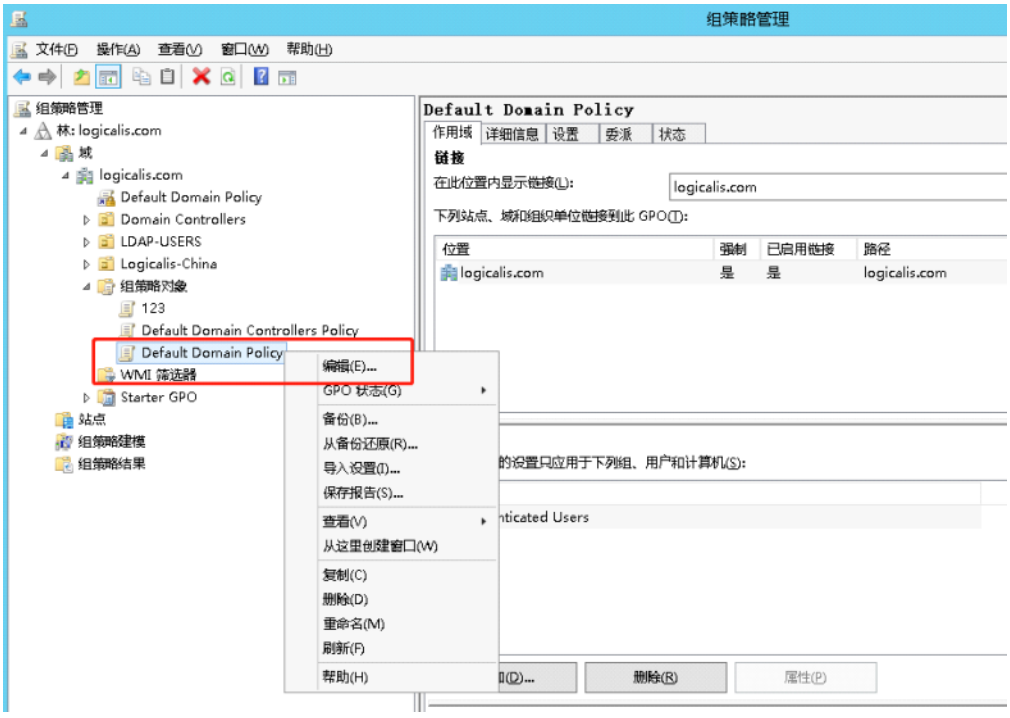
2.1：开启AD的日志记录（默认开启），没开启则没安全日志



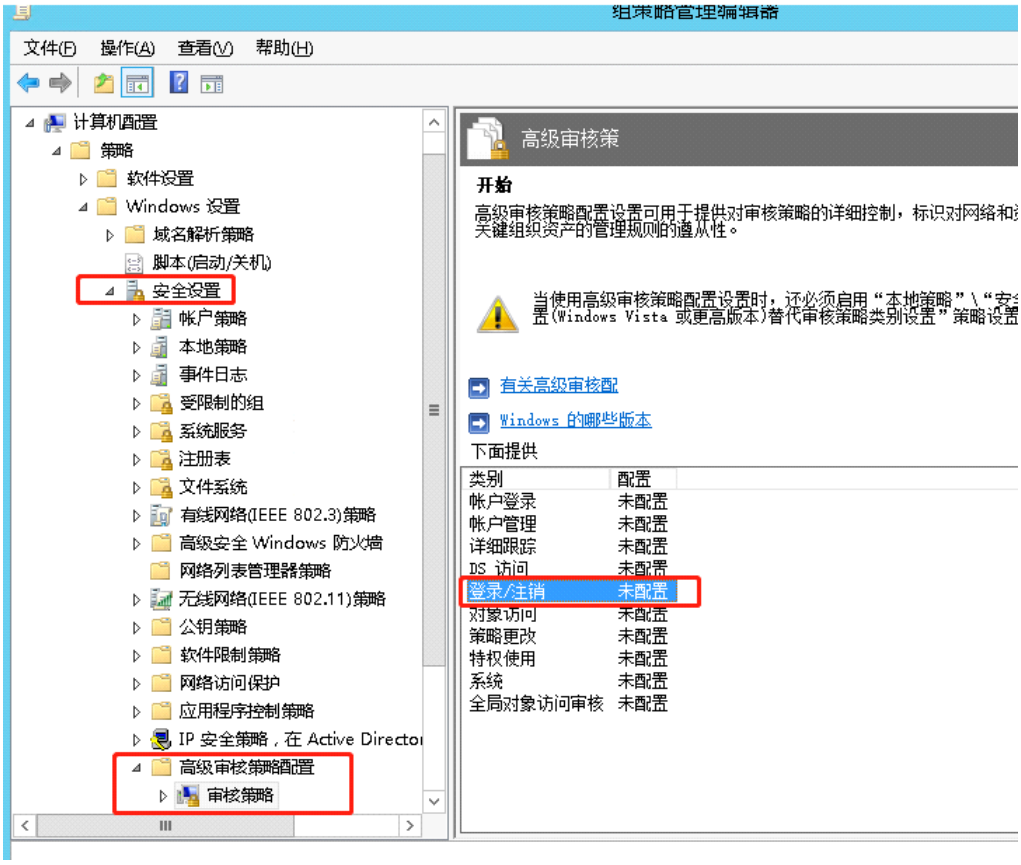
2.2：允许WMI通过AD服务器的防火墙（默认不用配）

如果Active Directory服务器正在运行Windows Server 2008或Windows Server 2012，请参阅在MSDN上设置远程WMI连接或更多信息。

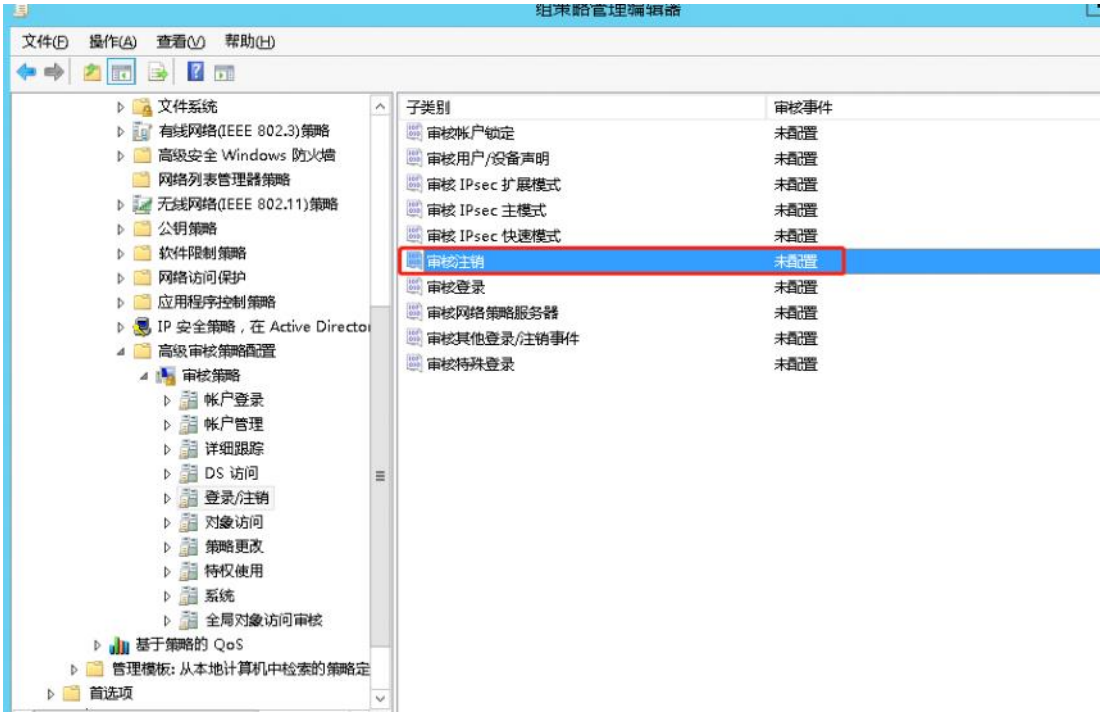
2.3：在Windows 2012 Server上启用登录/注销事件的审核：



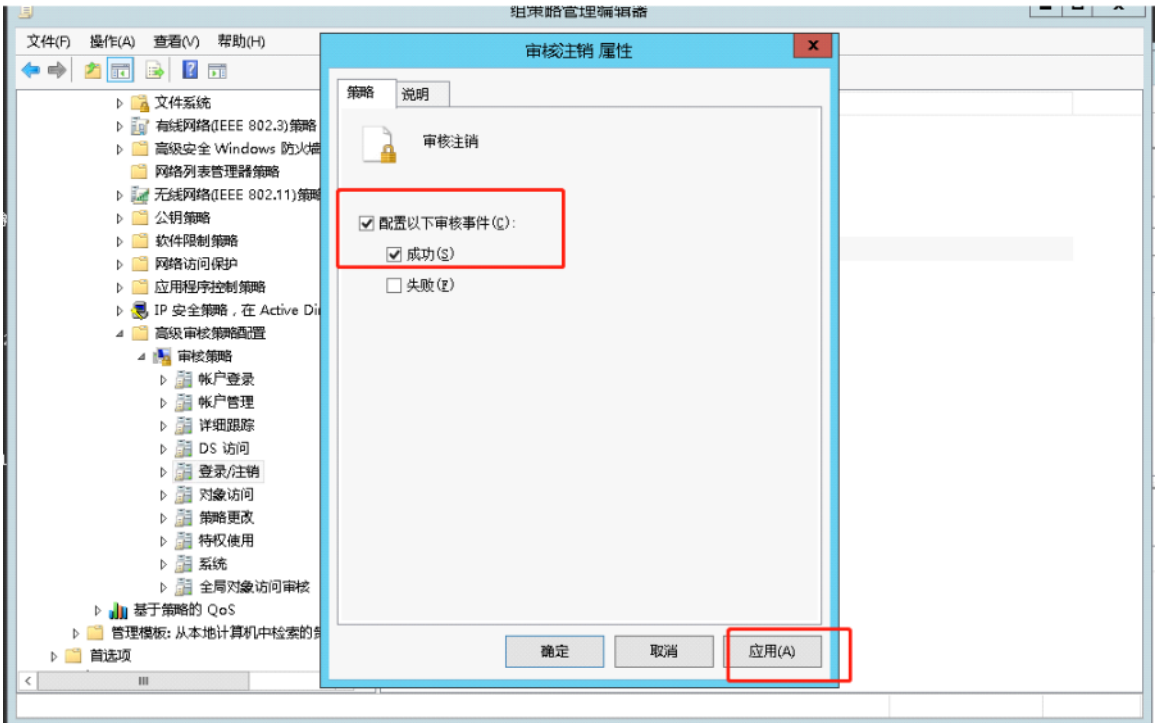
计算机配置>策略> Windows设置>安全设置>高级审核策略配置>审核策略>登录/注销。



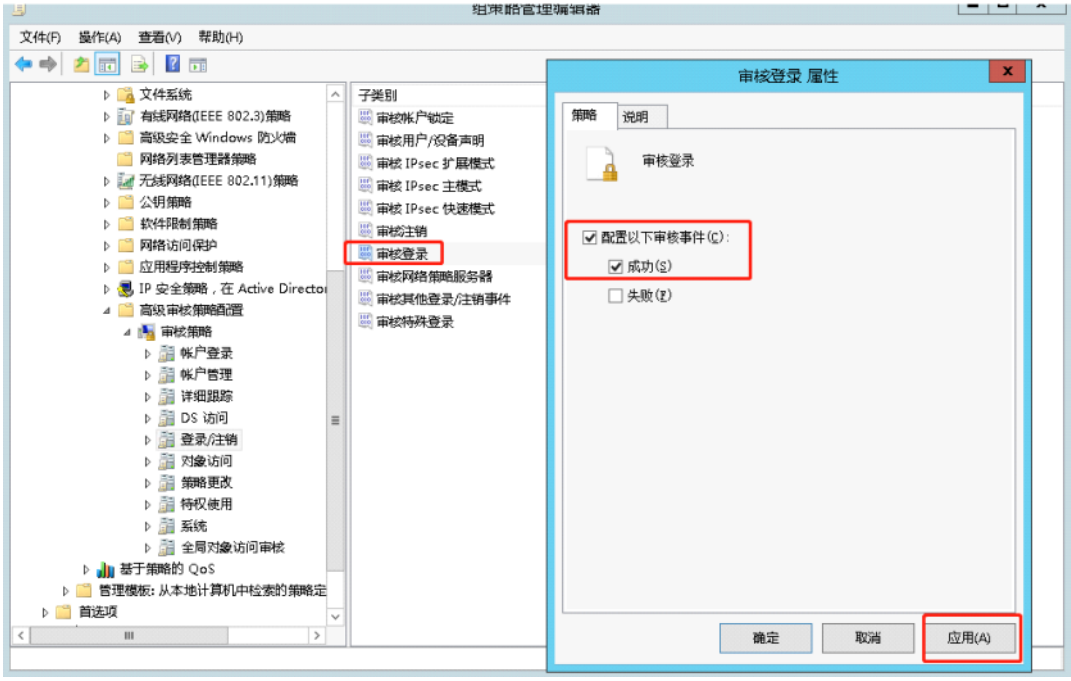
双击*Audit Logoff（审核注销）*



编辑注销属性”对话框中，选中“ *配置以下审核事件和成功”*



对“ *审计登录*”重复相同的任务



2.4：启用空闲会话超时（按需决定是否配置）☆

如何在组策略中有选择地启用空闲会话超时。这有助于防止代理由于主机上的多个会话而检测和报告无关的登录。

- 终端服务（Windows Server版本最高为2008）允许多个用户同时登录到服务器。启用空闲会话超时有助于减少登录到服务器的多个会话的实例。
- 远程桌面服务（Windows Server 2012及更高版本）允许一次允许一个用户远程登录工作站。但是，如果用户从远程桌面会话断开连接而不是注销，则该会话将保持活动状态。没有用户输入，活动会话最终将空闲。
- 如果一个会话闲置时，另一用户使用远程桌面服务登录到工作站，则可能有两次登录报告给管理中心。启用空闲会话超时会使这些会话在定义的空闲超时时间之后终止，这有助于防止主机上的多个远程会话。
- Citrix会话的功能类似于远程桌面服务会话。一台计算机上可以同时运行多个Citrix用户会话。启用空闲会话超时有助于防止主机上的多个Citrix会话，从而减少无关的登录报告。

请注意，根据配置的会话超时，可能仍然存在将多个会话登录到计算机的情况。

2.5：启用终端服务会话超时（按需决定是否配置）☆

本部分适用于Windows Server 2008之前的版本。

若要启用终端服务会话超时，请更新Windows Server 2008或Windows Server 2012的空闲终端服务会话超时和断开的终端服务会话超时的组策略设置，如在Microsoft TechNet上为终端服务会话配置超时和重新连接设置中所述。

组策略对象管理器中的路径为：

计算机配置\管理模板\ Windows组件\终端服务\终端服务器\会话时间限制

用户配置\管理模板\ Windows组件\终端服务\终端服务器\会话时间限制

将会话超时设置为比用户代理的注销检查频率短，以便空闲和断开连接的会话有机会在下一次注销检查之前超时。如果您有强制性的空闲会话或断开连接的会话超时，则将用户代理的注销检查频率设置为*比*会话超时长。有关配置注销检查频率的更多信息，请参阅“ 配置常规用户代理设置”。

完成后，继续“ 配置用户代理计算机”。

2.6：启用远程桌面会话超时（按需决定是否配置）☆

本节适用于Windows Server 2012及更高版本。

要启用远程桌面会话超时，请更新空闲远程会话超时和断开连接的会话超时的组策略设置。有关启用会话超时的更多信息，请参阅Microsoft TechNet上的会话时间限制。

将远程桌面超时设置为*短于*用户代理的注销检查频率，以便空闲和断开连接的会话有机会在下一次注销检查之前超时。如果您有强制性的空闲会话或断开连接的会话超时，则将用户代理的注销检查频率设置为*比*远程桌面超时长。有关配置注销检查频率的更多信息，请参阅“ 配置常规用户代理设置”。

组策略对象编辑器中的路径是：

用户配置\策略\管理模板\ Windows组件\远程桌面服务\远程桌面会话主机\会话时间限制

完成后，继续“ 配置用户代理计算机”。

3：配置User Agent的计算机条件

3.1：该计算机可以是以下任意计算机：

- （推荐）可访问Active Directory服务器的受信任网络上的某台计算机。此计算机应仅对网络管理员可用。我们推荐这种安装方法，因为它是最安全的。
- Active Directory服务器。**如果是ad安装agent，则登陆agent时 主机名=localhost，其余信息空。默认使用admin账户登陆读取WMI**

要使用户代理提供Active Directory域中所有计算机的登录和注销可见性，必须在每个域控制器上配置用户代理。例如，如果您的Active Directory域具有五个域控制器（每个域控制器安装在不同的主机上），则必须安装和配置用户代理软件五次，每个域控制器上一个。

3.2：安装User Agent条件

Windows计算机必须满足以下先决条件：

- 该计算机运行的是Windows Vista，Windows 7，Windows 8，Windows Server 2008或Windows Server2012。出于安全原因，我们建议您在域计算机上而非 Active Directory服务器计算机上安装用户代理。
- 该计算机安装了Microsoft.NET Framework 4.0版客户端配置文件和Microsoft SQL Server Compact（SQL CE）4.0版。
  - 在Microsoft.NET Framework版本4.0客户端配置文件可再发行组件包可从Microsoft下载网站（）。 dotNetFx40_Client_x86_x64.exe
  - 可从Microsoft下载站点获得SQL Server Compact 4

4：AD为user agent创建用户并分配权限

账户属性

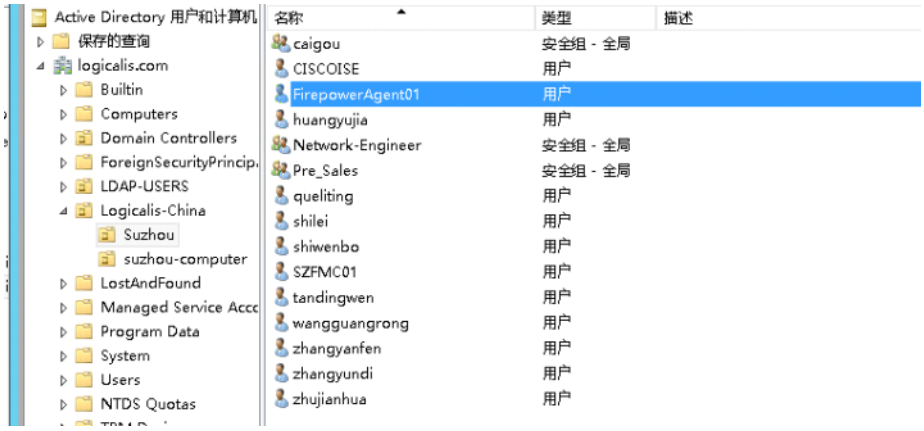
- 要在非Active Directory服务器的其他计算机上运行用户代理，该用户必须是域用户。
- 要在Active Directory服务器上运行用户代理，该用户应为本地帐户。（否则Agent登陆账户时无法读取security log）☆☆

☆**备注**：关于本地账户其实不是在AD上创建一个本地账域，域控是没法创建本地账户的，只是登陆agent时候填写localhost其余信息空，这样就默认使用本机administrator登陆了

授予该用户权限（两种办法）

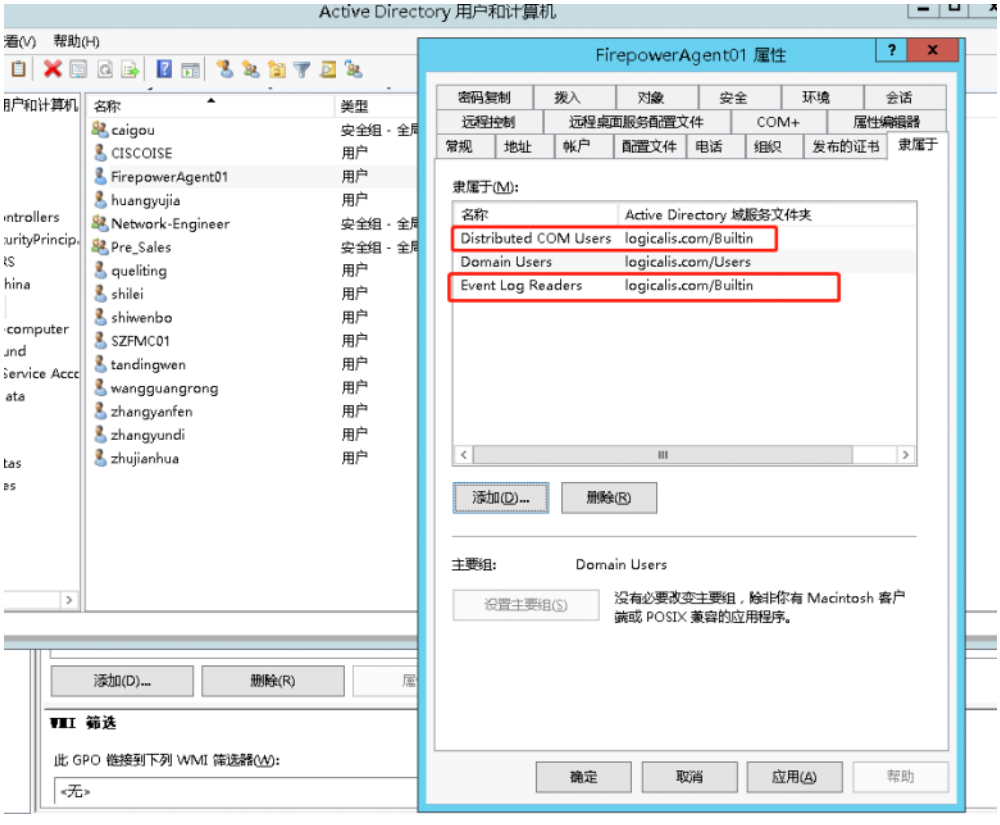
- 将本地用户添加到Active Directory服务器上的Domain Admins组。这种方法很简单，但是不建议使用，因为它的安全性较低。
- ☆推荐→ 为域用户提供运行用户代理的最小特权。（本章使用）☆

4.1：创建一个User agent使用的AD账户



4.2：将用户添加到两个组中

- Distributed COM Users
- Event Log Readers

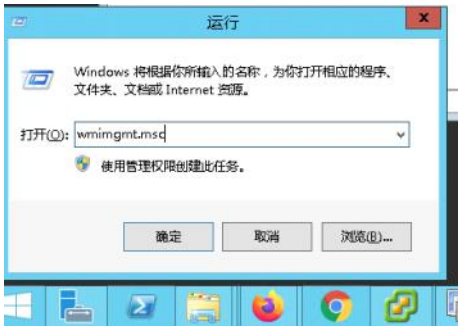


4.3：使用Windows Management Instrumentation（WMI）控制台向用户授予对该 Root\CIMV2节点的以下权限

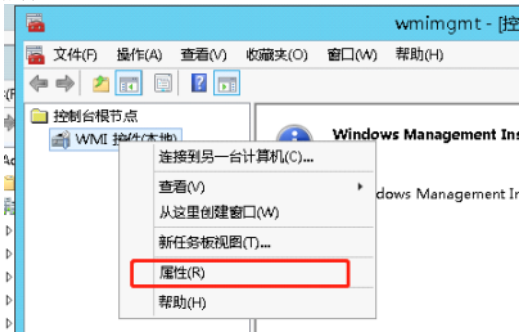
- Execute Methods

- Enable Account
- Remote Enable
- Read Security

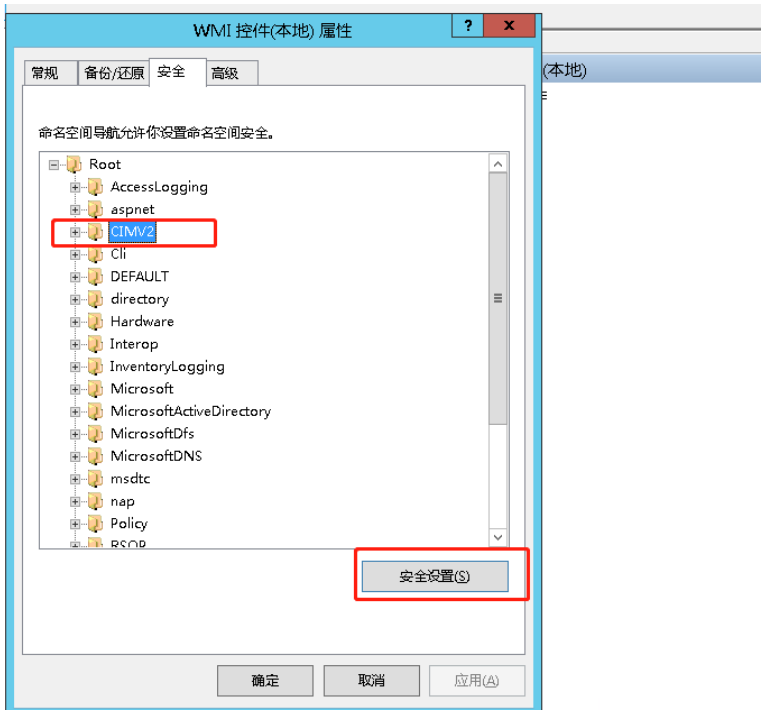
windows开始 → 运行 → 输入wmimgmt.msc



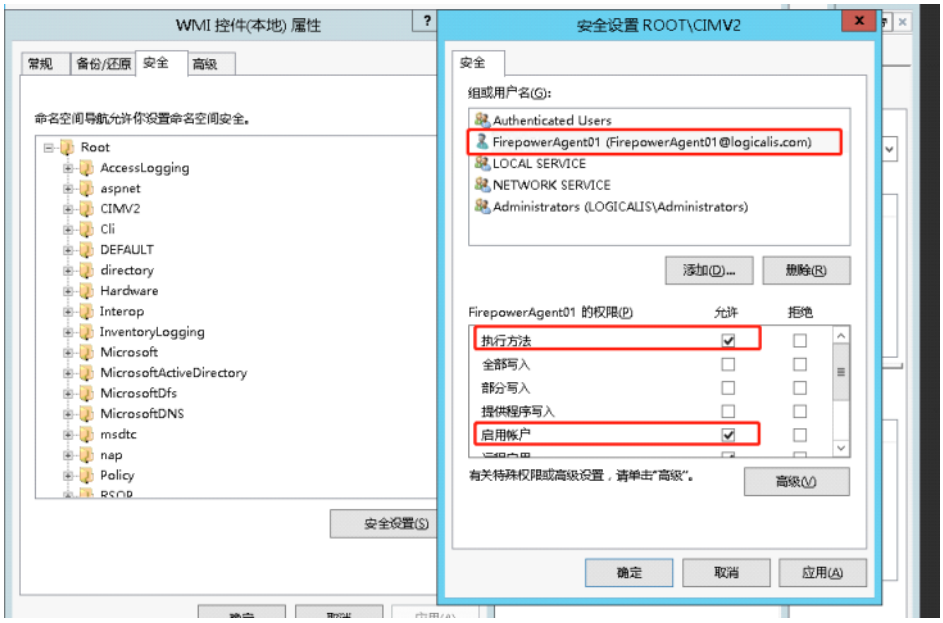
选择属性

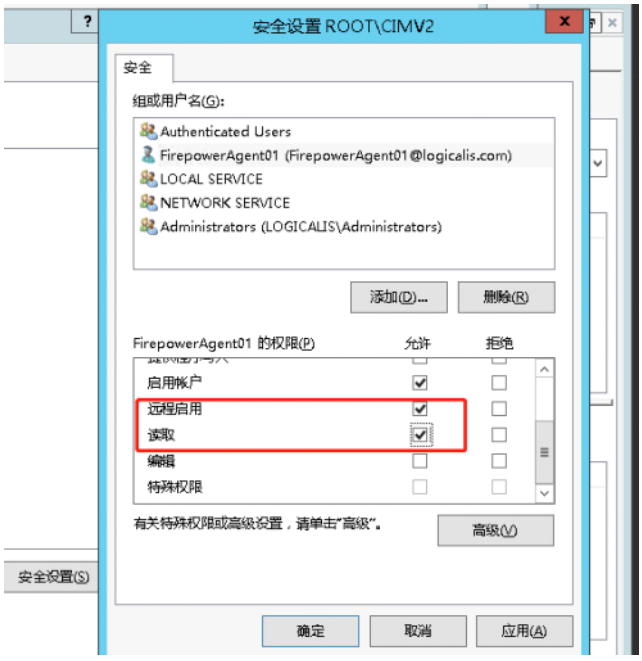


选择CIMV2的安全设置



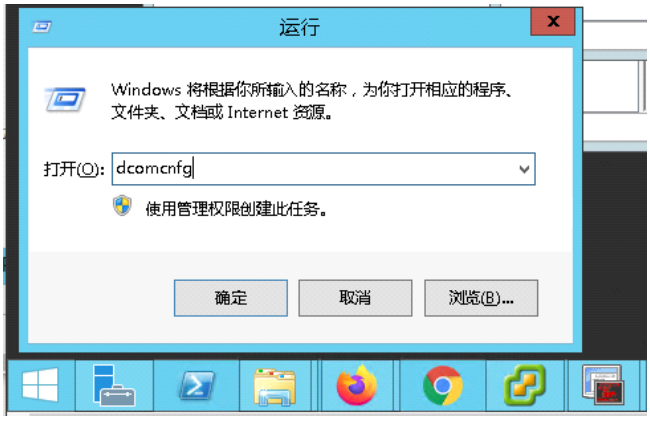
添加Agent的AD账户并添加四个权限



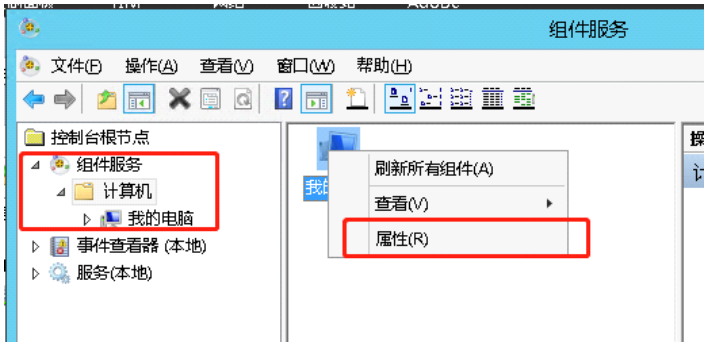


4.4：允许用户代理访问分布式组件对象管理（DCOM）

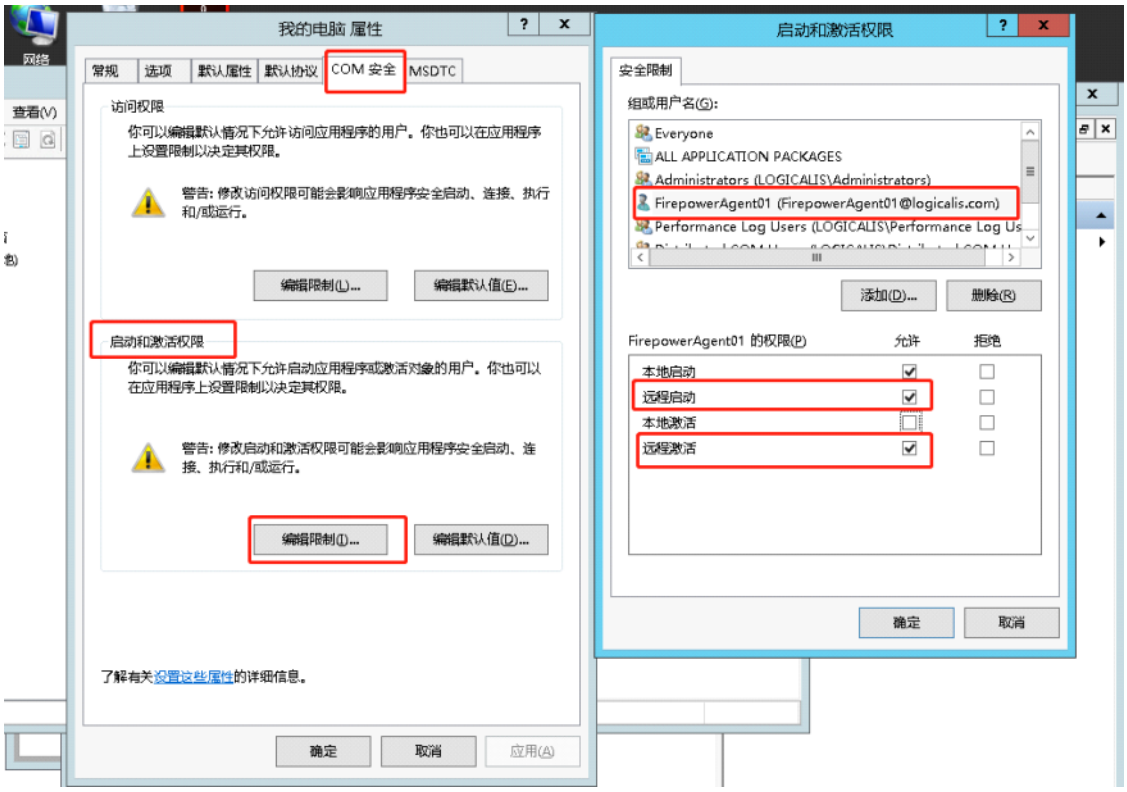
开始 → 运行 → dcomcnfg



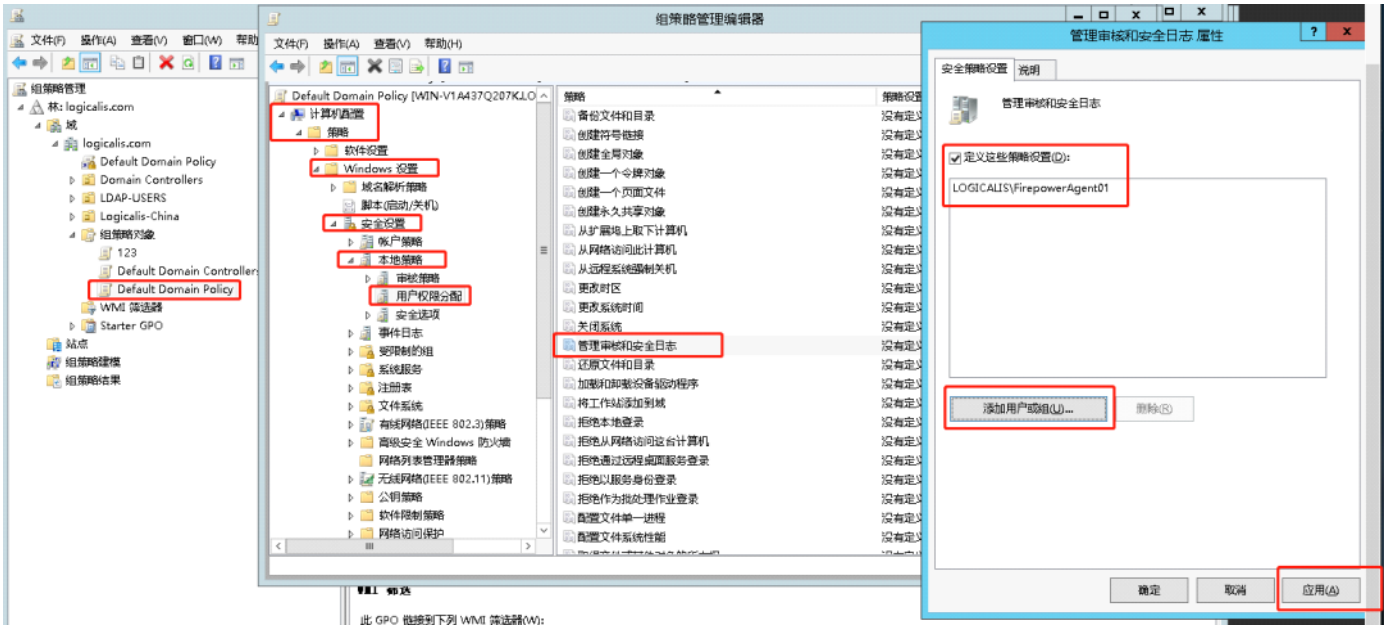
右键单击我的电脑，然后单击属性



为Agent账户添加进去，并赋予远程机动和激活权限



4.5：配置组策略允许Agent账户访问AD的安全日志



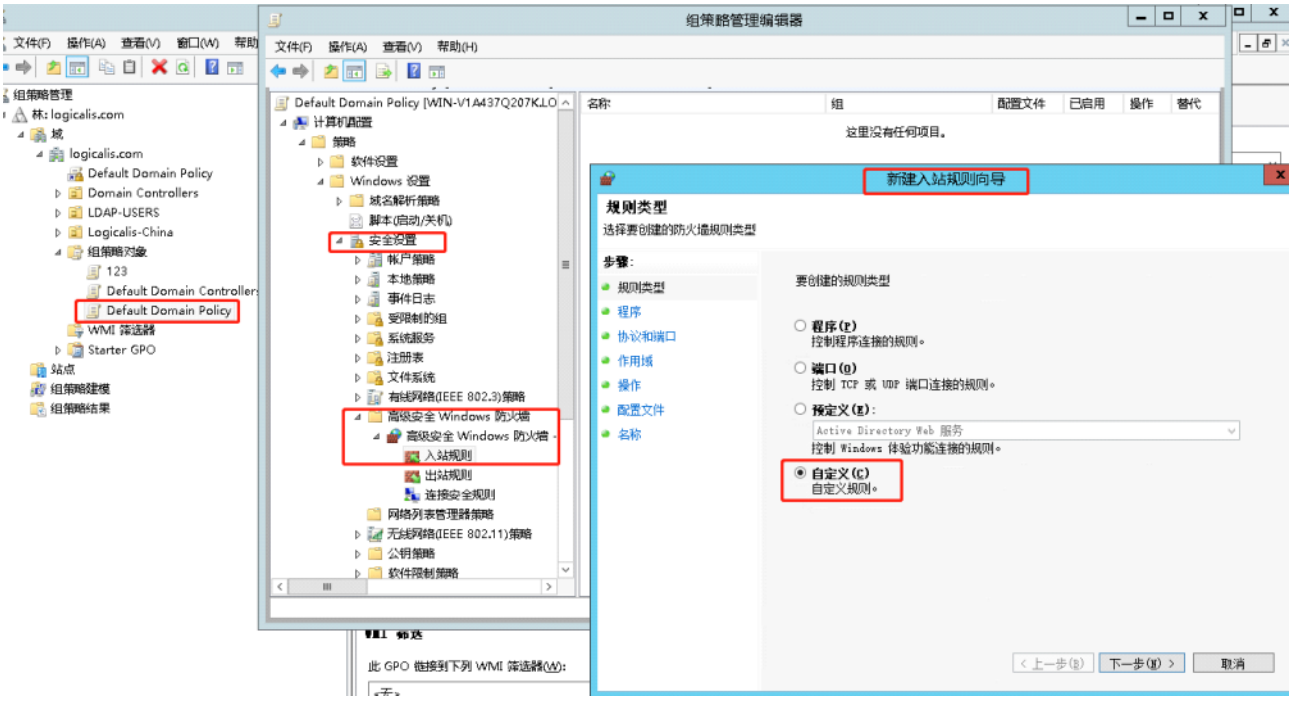
5：（可选）配置AD防火墙策略允许上述配置的流量通过☆

如果使用AD装Agent，此步骤可以跳过，如果使用非域PC装Agent获取AD的WMI，则需要配置两条防火墙策略

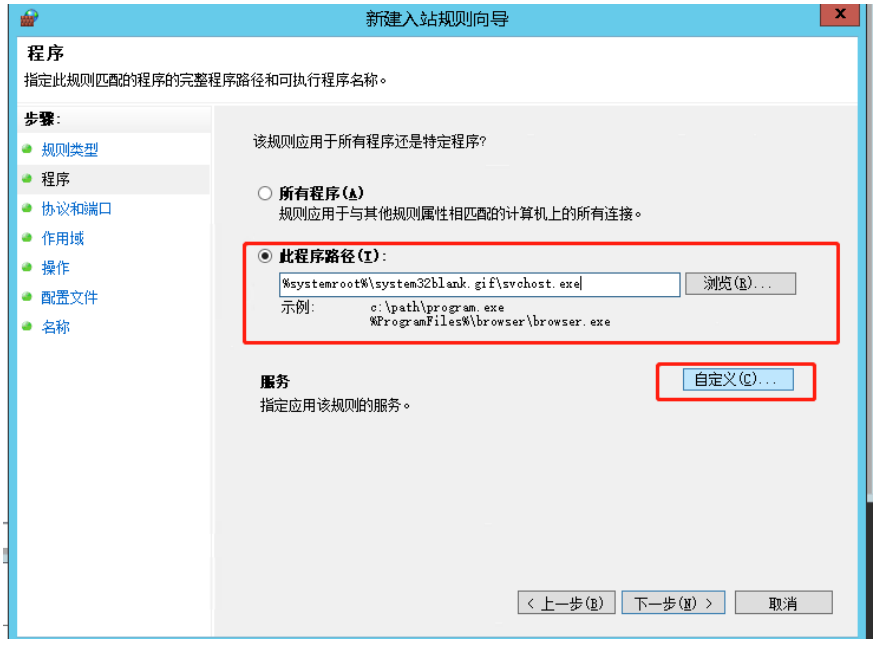
- 第一条规则允许传入RPC终结点映射程序服务的流量，该服务以动态分配的端口号作为响应，客户端必须使用该端口号与该服务进行通信。
- 第二条规则允许将网络流量发送到动态分配的端口号。

5.1：创建GPO防火墙规则以允许RPC通信，请执行以下操作：

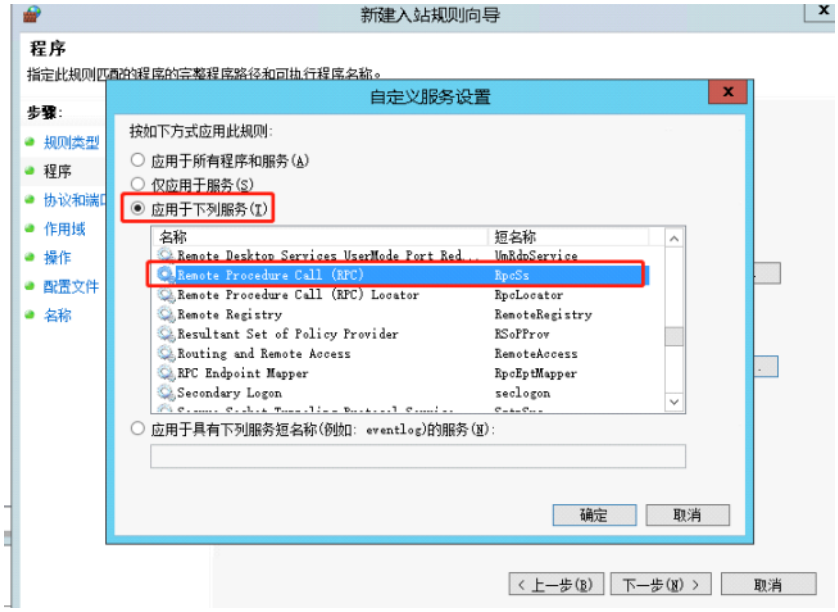
5.1.1：使用组策略编辑，创建AD的防火墙入站规则，选择自定义



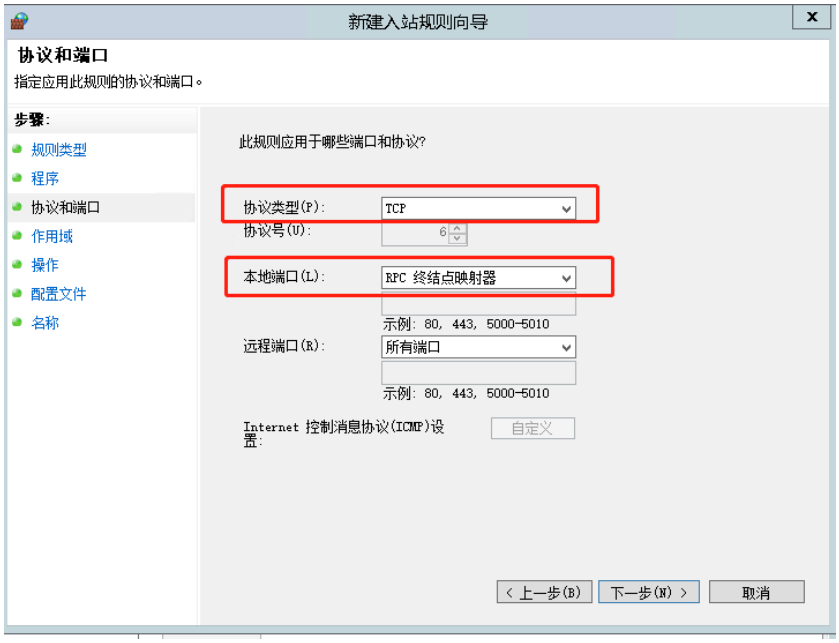
5.1.2：输入路径：%systemroot%\system32\svchost.exe　　并点击自定义



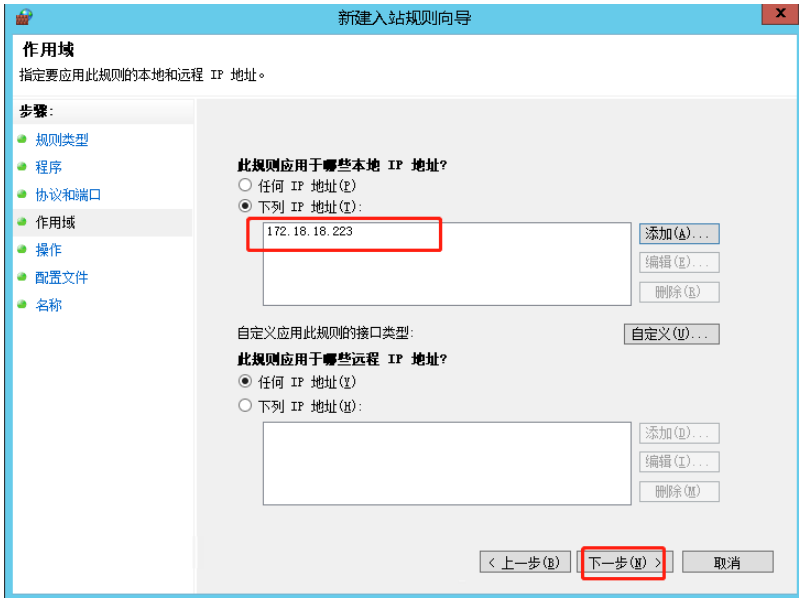
5.1.3：select　Remote Procedure Call (RPC)



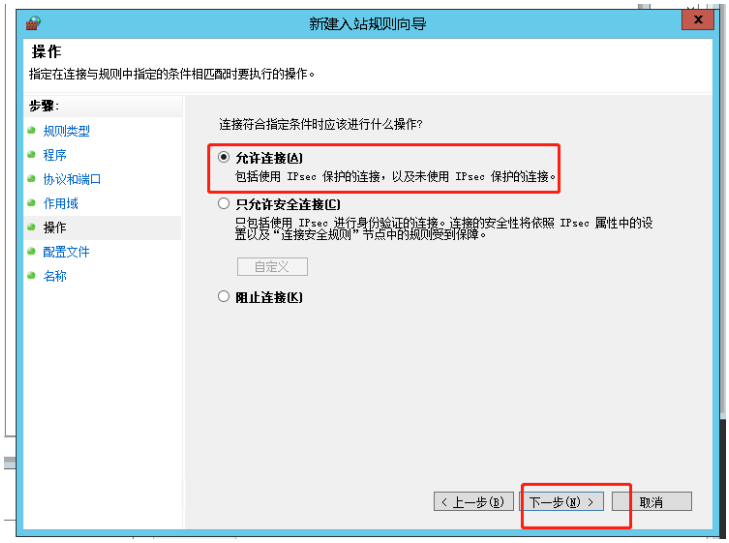
5.1.4：选择TCP协议，选择本地端口=RPC终点映射



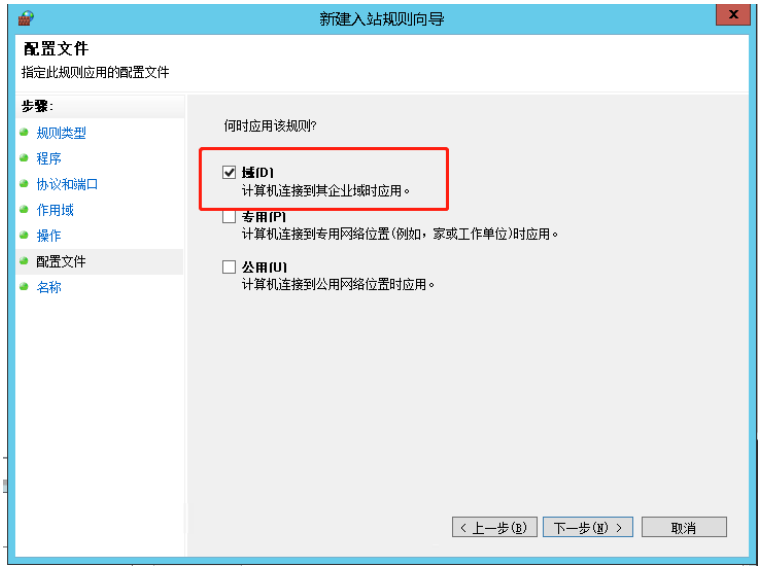
5.1.5：输入安装agent的PC电脑IP地址，这里其实应该是172.18.18.111



5.1.6：允许连接



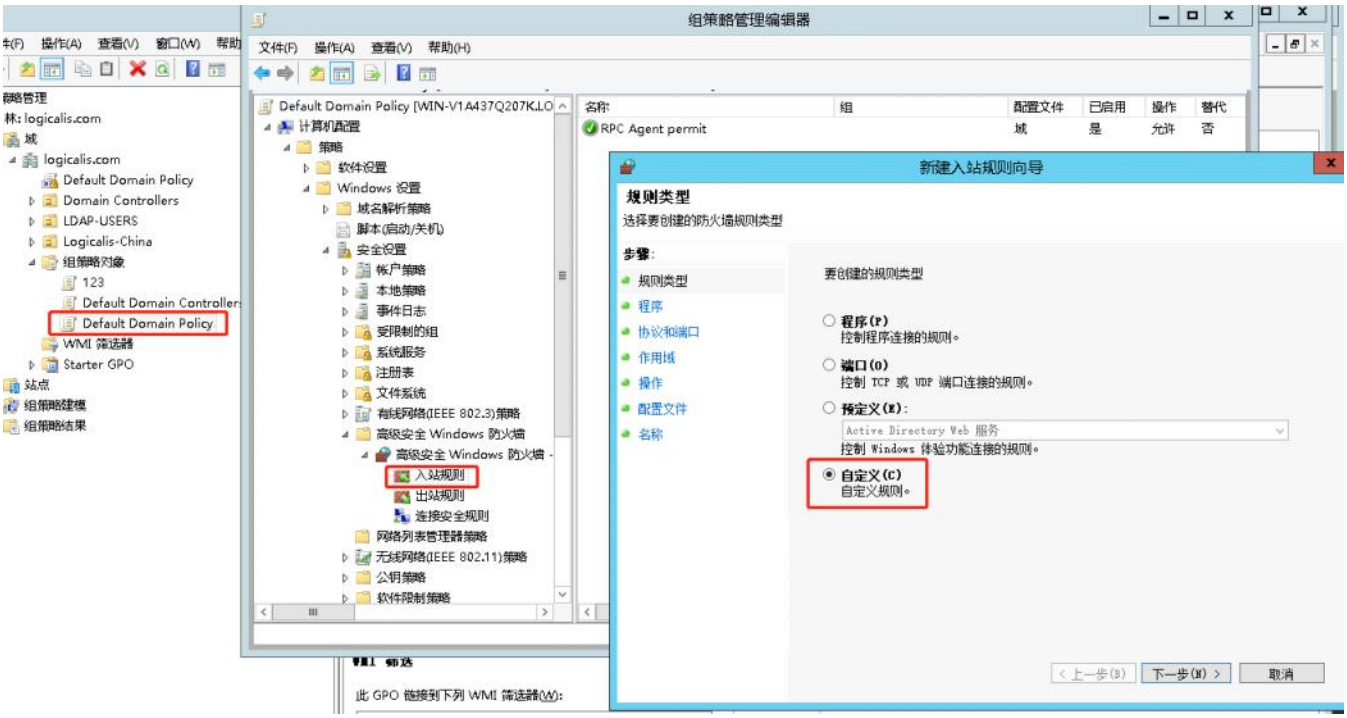
5.1.7：只选择域



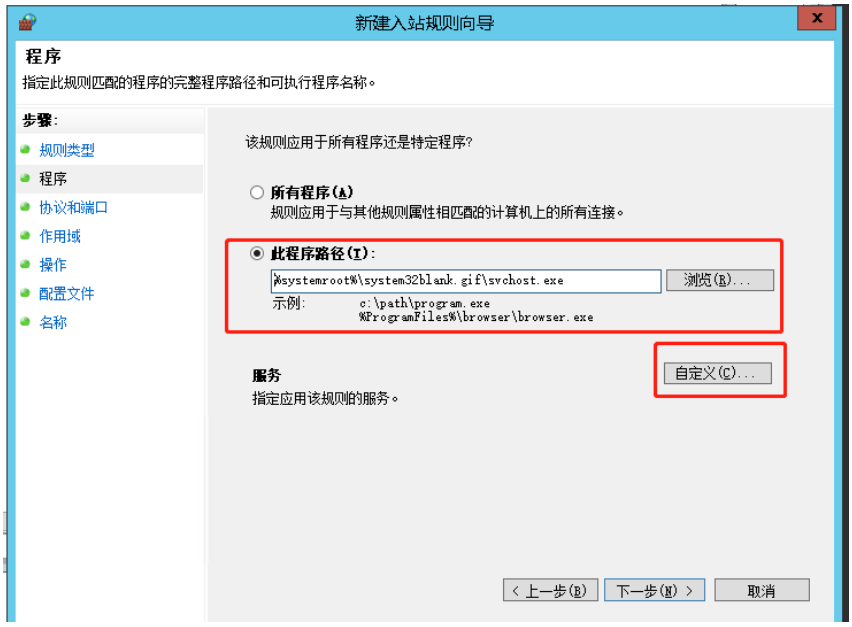
5.1.8：输入防火墙规则名称

5.2：创建GPO规则以允许动态映射端口，请执行以下操作：

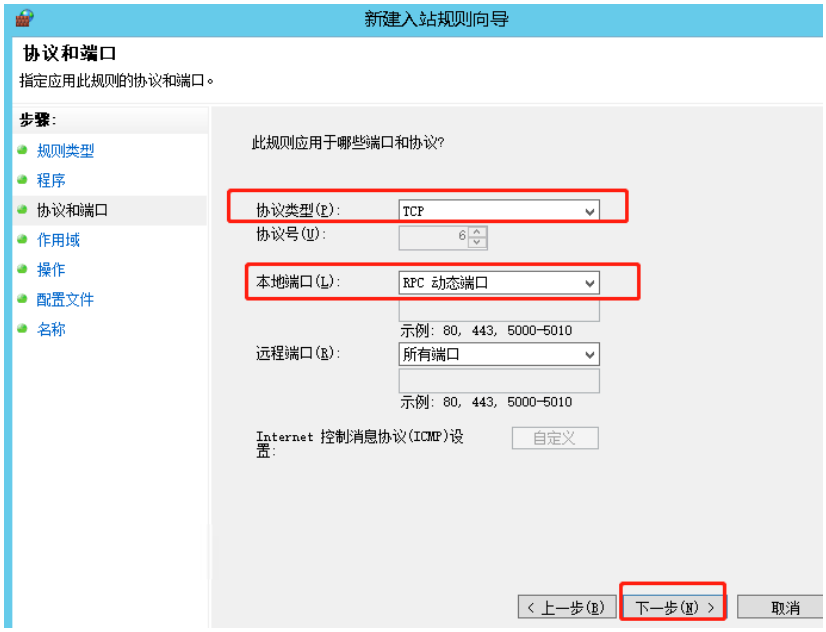
5.2.1：自定义入站规则



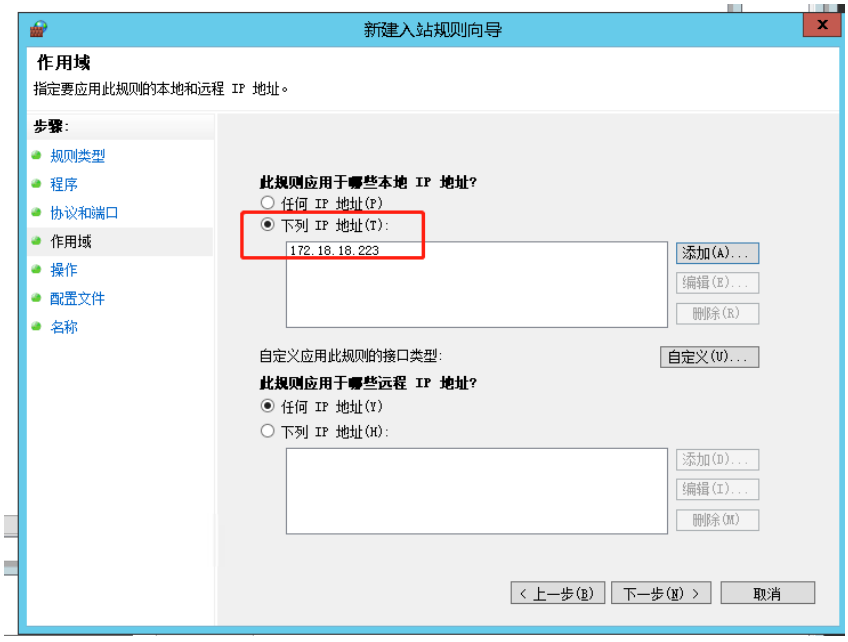
5.2.2：路径 %systemroot%\system32\svchost.exe



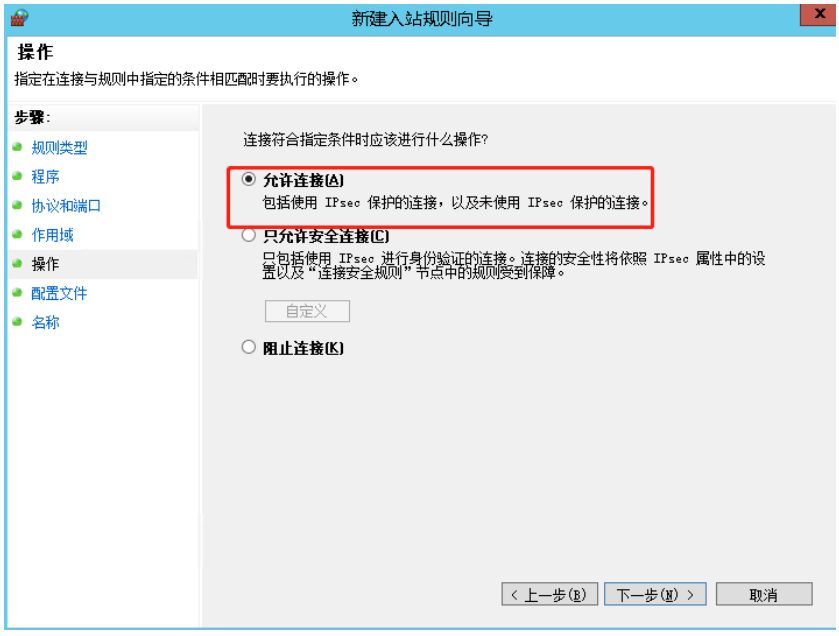
5.2.3：协议=TCP，本地端口这次选择=RPC动态端口

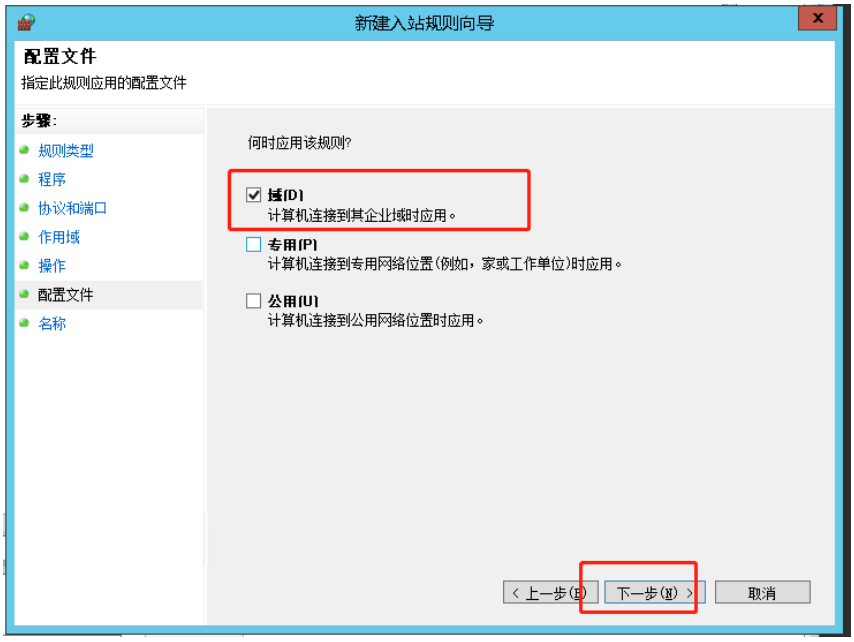


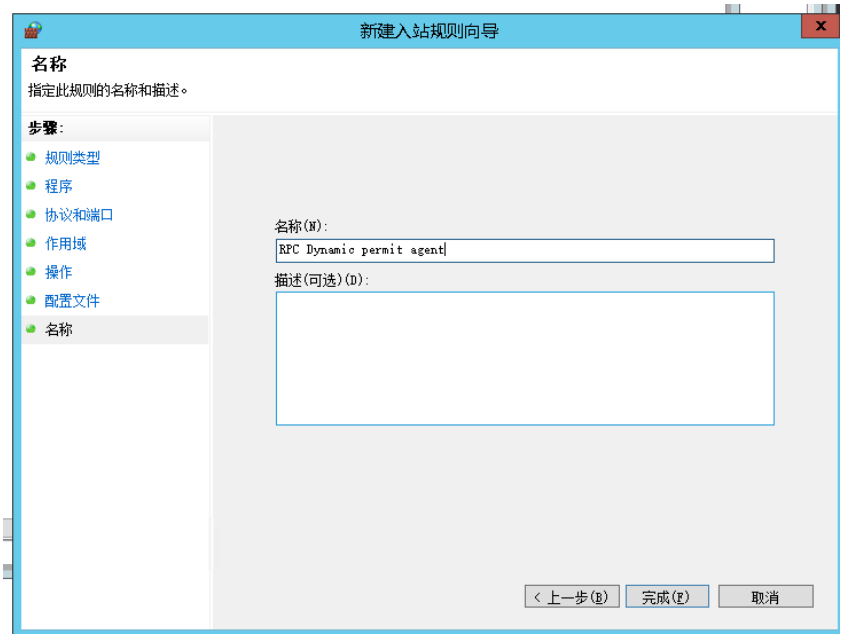
5.2.4：填写装Agent的PC地址，这里其实是172.18.18.111



5.2.5：允许连接







5.3：更新组策略

服务器更新组策略 ： gpupdate /force

6：User Agent安装

6.0：Agent下载地址

https://software.cisco.com/download/home/286259687/type/286271057/release/eNcore%20for%20Splunk

6.1：安装用户代理的先决条件

Windows计算机必须满足以下先决条件：

- 该计算机运行的是Windows Vista，Windows 7，Windows 8，Windows Server 2008或Windows Server2012。出于安全原因，我们建议您在域计算机上而非 Active Directory服务器计算机上安装用户代理。
- 该计算机安装了Microsoft.NET Framework 4.0版客户端配置文件和Microsoft SQL Server Compact（SQL CE）4.0版。

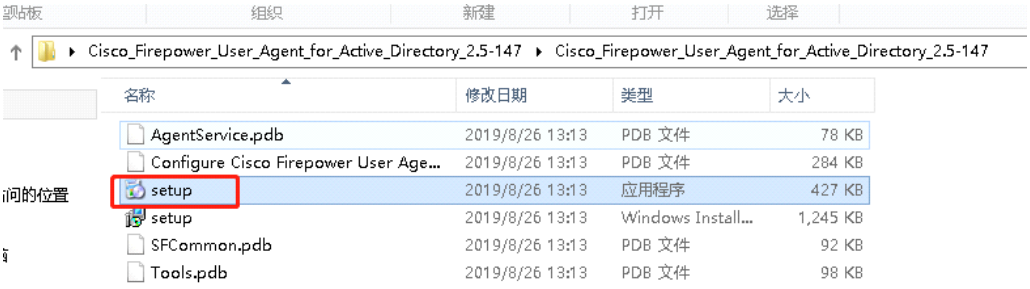
- 在Microsoft.NET Framework版本4.0客户端配置文件可再发行组件包可从Microsoft下载网站（）。 dotNetFx40_Client_x86_x64.exe

- 可从Microsoft下载站点获得SQL Server Compact 4

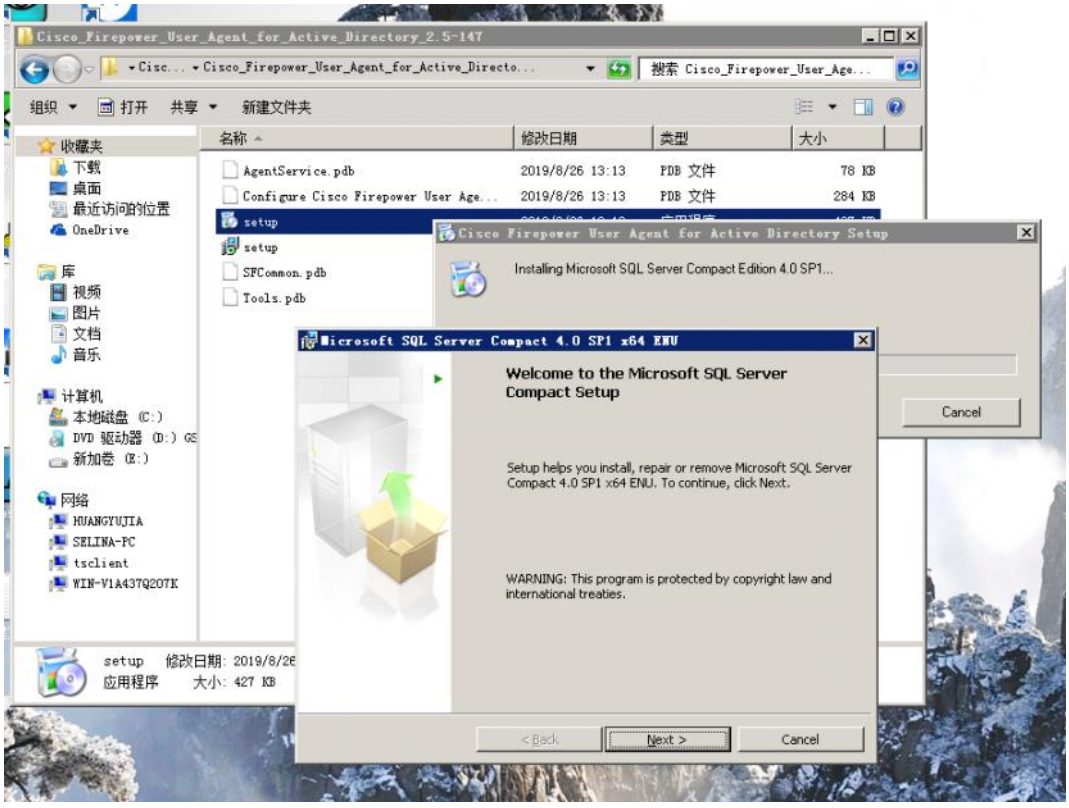
注意如果您没有.NET Framework，则在启动代理可执行文件（setup.exe）时，它会提示您下载它。有关更多信息，请参见安装用户代理。

6.2：进行安装（win7没问题，自动下载需要的插件）

6.2.1：双击setup.exe而*不是* setup.msi。setup.msi在安装用户代理之前不会检查必备软件，否则可能会导致安装或运行代理错误。

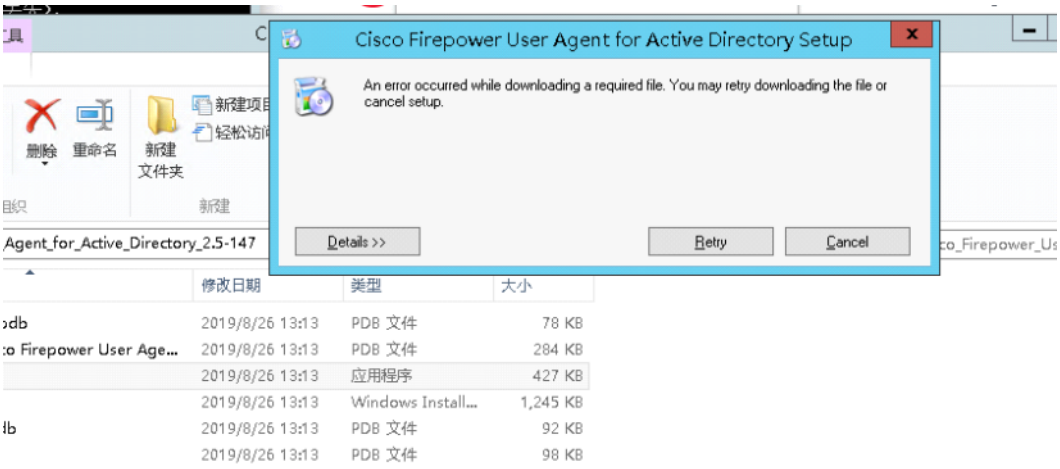


6.2.1：如果在安装代理的Windows计算机上没有Microsoft.NET Framework 4.0版客户端配置文件和SQL Server Compact 4.0，则会提示您下载适当的文件。下载并安装文件。



6.3：2012安装时候可能会报错（手动下载数据库）

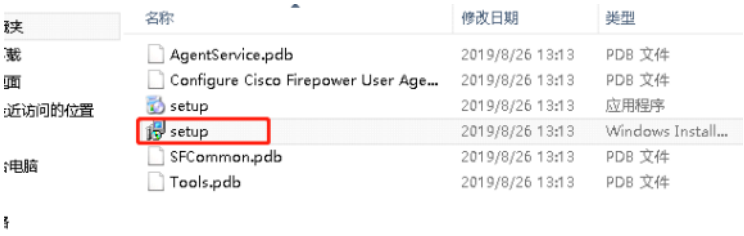
an error occurred while downloading a required file.you may retry downloading the file or cancel setup



6.3.1：手动去微软下载这两个进行安装

- - 在Microsoft.NET Framework版本4.0客户端配置文件可再发行组件包可从Microsoft下载网站（）。 dotNetFx40_Client_x86_x64.exe
- - 可从Microsoft下载站点获得SQL Server Compact 4

6.3.2：其实只需要装数据库4，数据库装完点击MSI文件安装 net4.0 2012默认就装了



7：User Agent配置连接AD☆☆

可以从用户代理向一台或多台Active Directory服务器添加连接，并配置以下内容：

- 代理是实时检索登录和注销数据还是定期轮询Active Directory服务器以获取数据。
- 代理多久轮询一次用户活动数据，或者在连接丢失时尝试与Active Directory服务器建立或重新建立实时连接。
- 代理报告用于登录到Active Directory服务器本身的IP地址。
- 代理与Active Directory服务器建立或重新建立连接时，代理检索到多少登录和注销数据。

当用户代理配置为实时检索数据并且实时监视不可用时，该代理会尝试轮询Active Directory服务器以获取数据，直到再次提供实时监视为止。

请注意，实时监视需要运行Windows Server 2008或更高版本的Active Directory服务器。

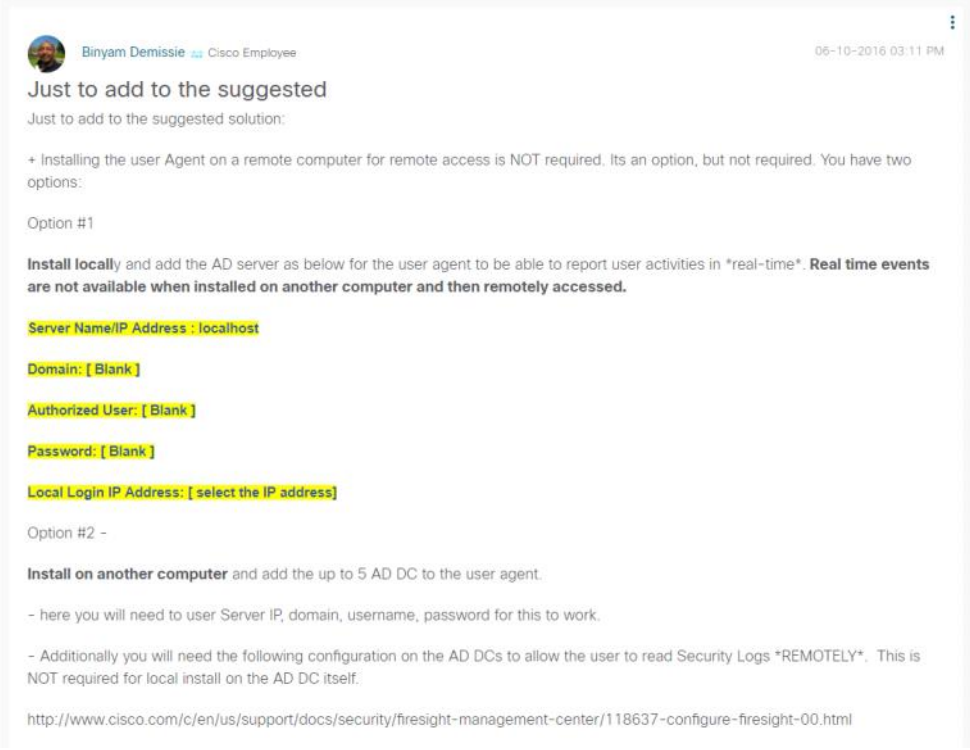
Active Directory服务器状态	Polling Availability轮询可用性	Real Time Availability实时可用性
available	该服务器可用于轮询。	该服务器可用于实时数据检索。
unavailable	该服务器不可用于轮询。	该服务器不可用于实时数据检索，或者该服务器配置为轮询。
pending	服务器配置已添加，但通讯尚未开始。	添加并保存服务器配置后，需要一些时间才能开始与用户代理进行通信。如果pending状态仍然存在，请检查用户代理与服务器之间的通信。
unknown	代理已启动并且状态不可用，或者代理尚未检查Active Directory服务器。	代理已启动并且状态不可用，或者代理尚未检查Active Directory服务器。

您不应将多个用户代理连接到同一Active Directory域控制器，因为当每个用户代理检测到另一个用户的连接时，该用户代理会报告无关的登录信息。

7.1：User Agent连接AD（AD自己装Agent连接AD）

7.1.1：输入AD的IP地址，域名，Agent的AD账户（分配权限的），注意，如果Agent装在AD上使用AD本地账户而不是域账户
如果使用域账户登陆agent，就会报错无法读取security -log，这里AD本地agent一定要用AD本地账户登陆

应该填写如下信息，主机名=localhost，其余信息=空，则调用本地账户读取WMI信息（可选输入账户密码）
https://community.cisco.com/t5/firepower/problem-agent-sourcefire/td-p/2728832



Binyam Demissie Cisco Employee 06-10-2016 03:11 PM

Just to add to the suggested

Just to add to the suggested solution:

+ Installing the user Agent on a remote computer for remote access is NOT required. Its an option, but not required. You have two options:

Option #1

Install locally and add the AD server as below for the user agent to be able to report user activities in *real-time*. **Real time events are not available when installed on another computer and then remotely accessed.**

Server Name/IP Address : localhost

Domain: [Blank]

Authorized User: [Blank]

Password: [Blank]

Local Login IP Address: [select the IP address]

Option #2 -

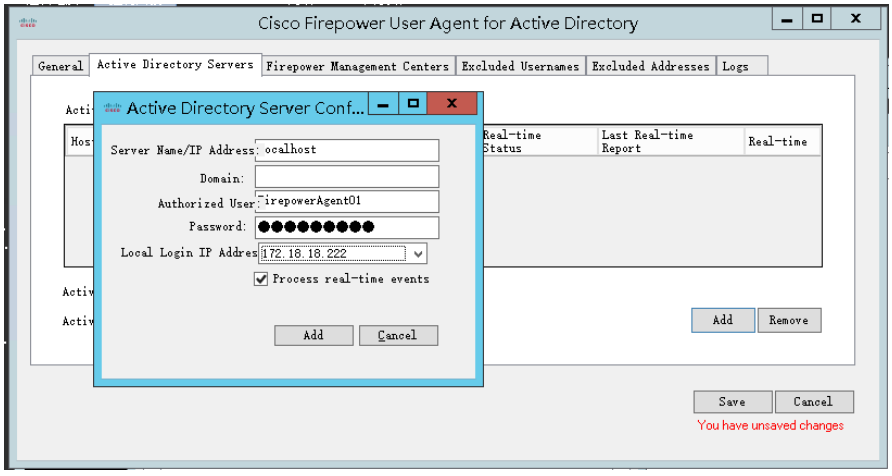
Install on another computer and add the up to 5 AD DC to the user agent.

- here you will need to user Server IP, domain, username, password for this to work.

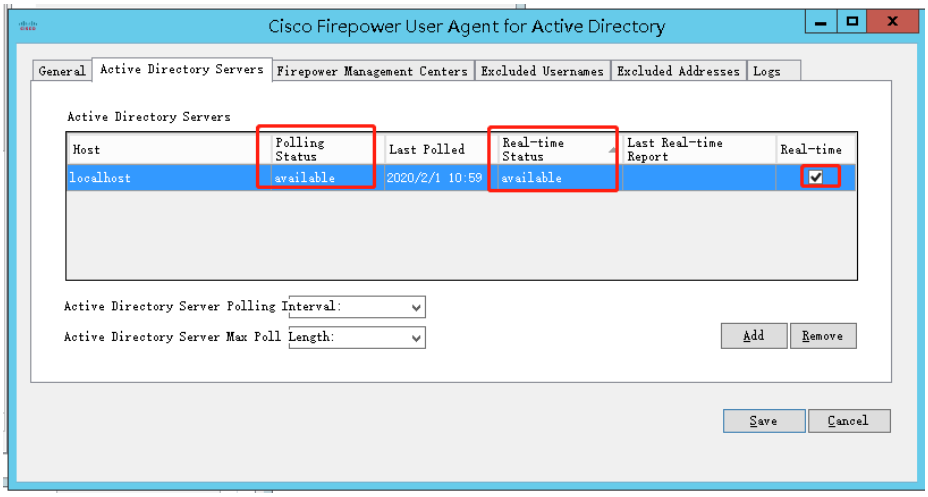
- Additionally you will need the following configuration on the AD DCs to allow the user to read Security Logs *REMOTELY*. This is NOT required for local install on the AD DC itself.

http://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/118637-configure-firesight-00.html

您可以选择添加用户名和密码。如果省略该信息，则无法检测到对Active Directory服务器进行身份验证的用户的注销。
无论是否输入用户名和密码，都可以轮询服务器。这里推荐你还是输入账户密码

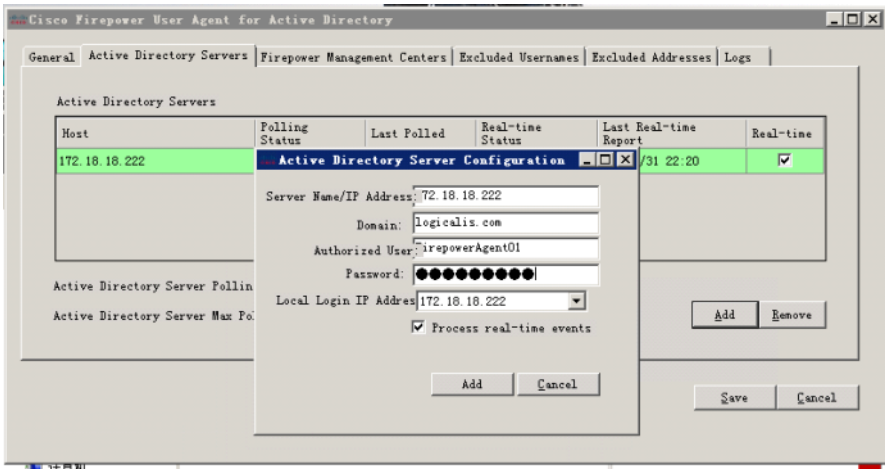


如果加完以后real-time实时更新pending，你可以点击编辑开关下实时更新，就变成available了

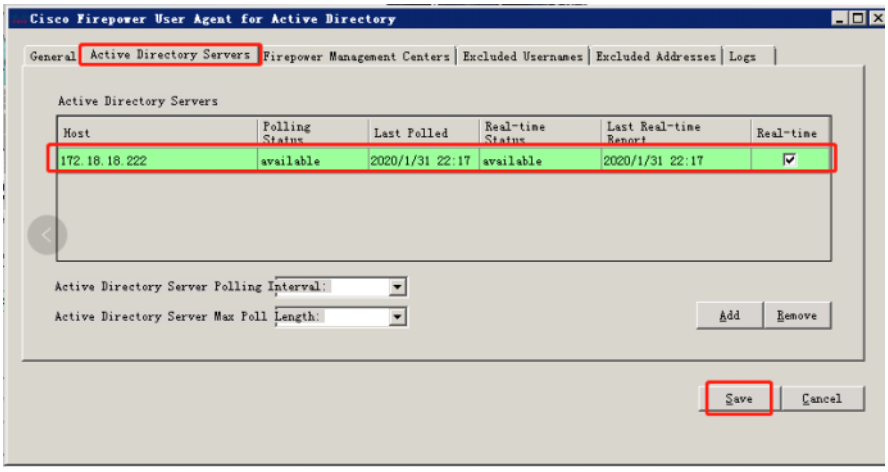


7.2：若是非AD的加域PC装agent，则使用FirepowerAgent01账户登陆

7.2.1：输入账户和域信息



7.2.2：SAVE保存，看到绿色，available可用

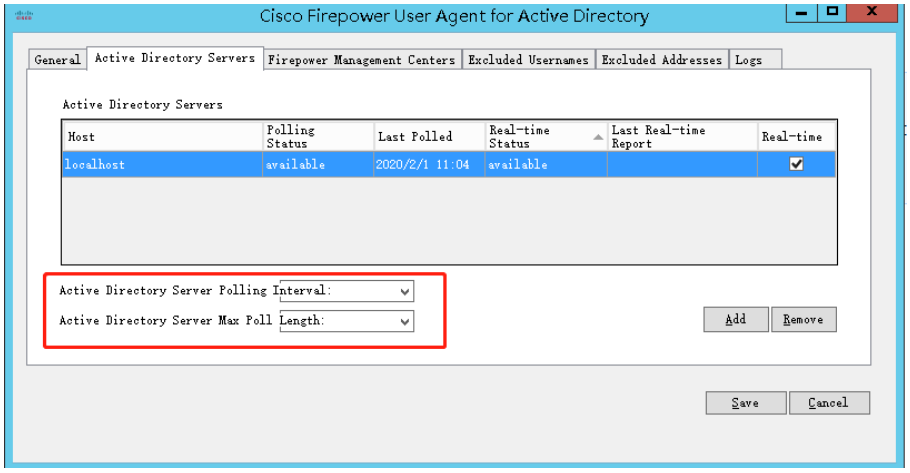


7.2.3：若pending，可以点击save，或者关闭agentPC的防火墙

7.3：（可选）更改AD查询的时间，或者继续添加AD

7.3.1：（可选）。更改代理自动轮询Active Directory服务器以获取用户登录数据的时间*间隔，然后* 从“ *Active Directory服务器轮询间隔”*列表中选择一个时间。

7.3.2：（可选）更改代理首次建立或重新建立连接以轮询Active Directory服务器以获取用户登录数据时所轮询的最长时间，请从*Active Directory服务器“最大轮询长度”* 列表中选择一个时间。

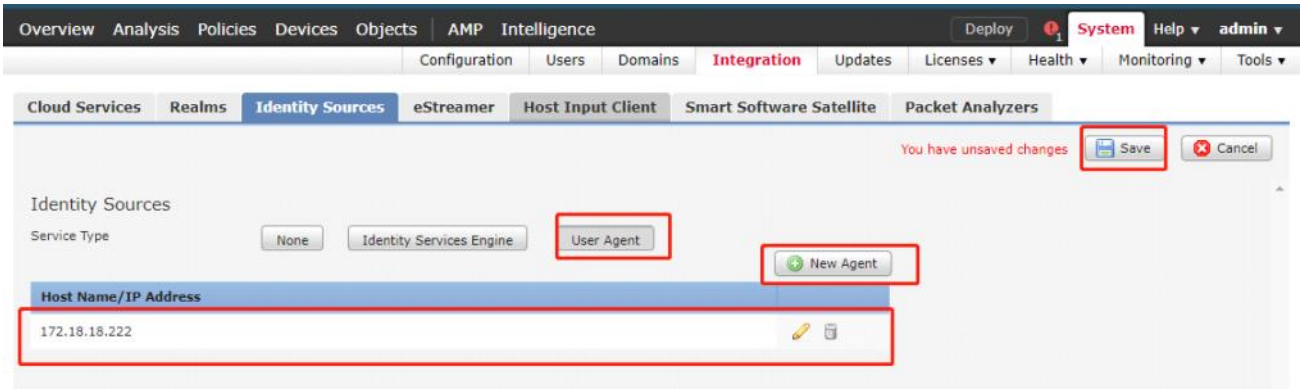


8：User Agent连接FMC

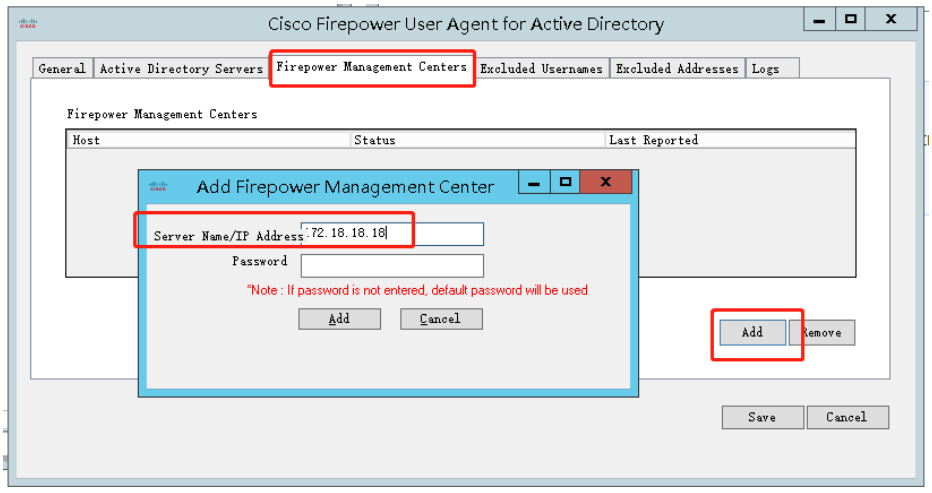
- 一个User Agent最多可以向5个FMC发送AD用户数据
- 如果用户代理无法在配置时连接到管理中心，则无法添加该管理中心。检查代理是否具有对管理中心的TCP / IP访问。

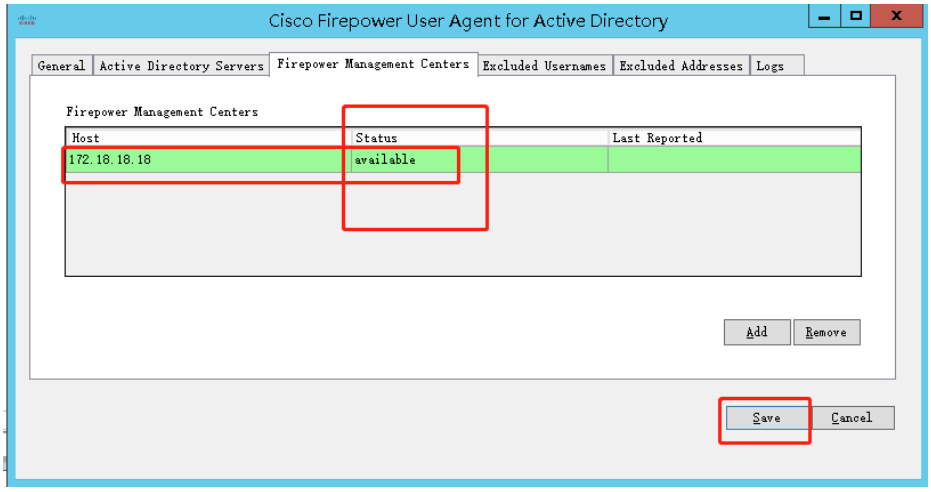
8.1：先配置FMC关联User Agent

如果不先在FMC上添加Agent，FMC是不会先接收代理指过来的，类似于白名单机制



8.2：配置User Agent添加FMC，无需填写密码，并Save





9：可选配置集合（正常无需配置）

9.1：User Agent关联FMC需要输入密码

请参阅《*Firepower管理中心配置指南*》中的《 Firepower管理中心CLI参考》中的章节。

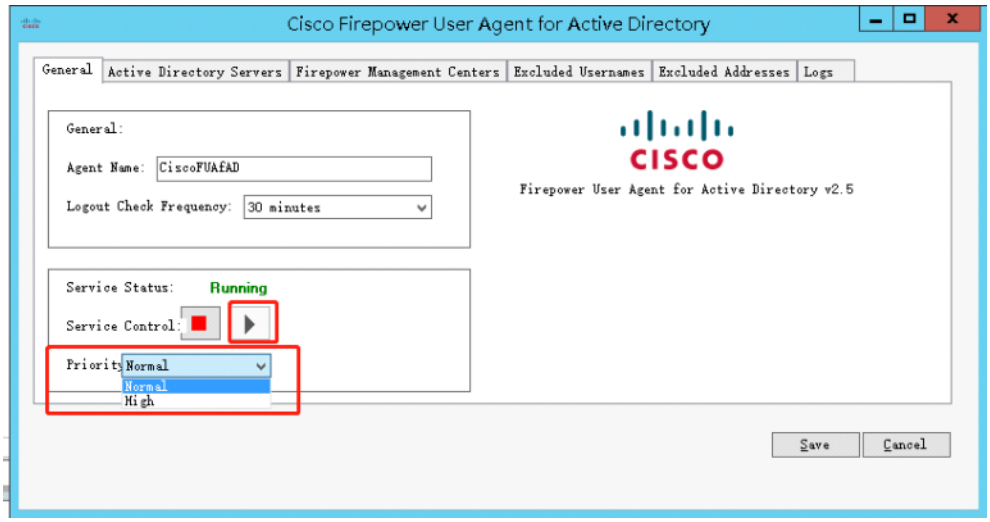
9.2：配置用户代理排除的用户名设置

轮询登录或注销事件时，最多可以定义500个要排除的用户名。如果代理通过排除的用户名检索登录或注销事件，则代理不会将事件报告给管理中心。
来自 <https://www.cisco.com/c/en/us/td/docs/security/firesight/user-agent/25/config-guide/Firepower-User-Agent-Configuration-Guide-v2-5/ConfigAgent.html#40929>

9.3：配置用户代理排除的地址设置

轮询登录事件时，最多可以配置100个要排除的IPv4和IPv6地址。
如果用户代理检索到包含排除的IP地址的登录或注销事件，则该代理不会将该事件报告给管理中心。
来自 <https://www.cisco.com/c/en/us/td/docs/security/firesight/user-agent/25/config-guide/Firepower-User-Agent-Configuration-Guide-v2-5/ConfigAgent.html#40929>

9.4：开关代理&设置优先级

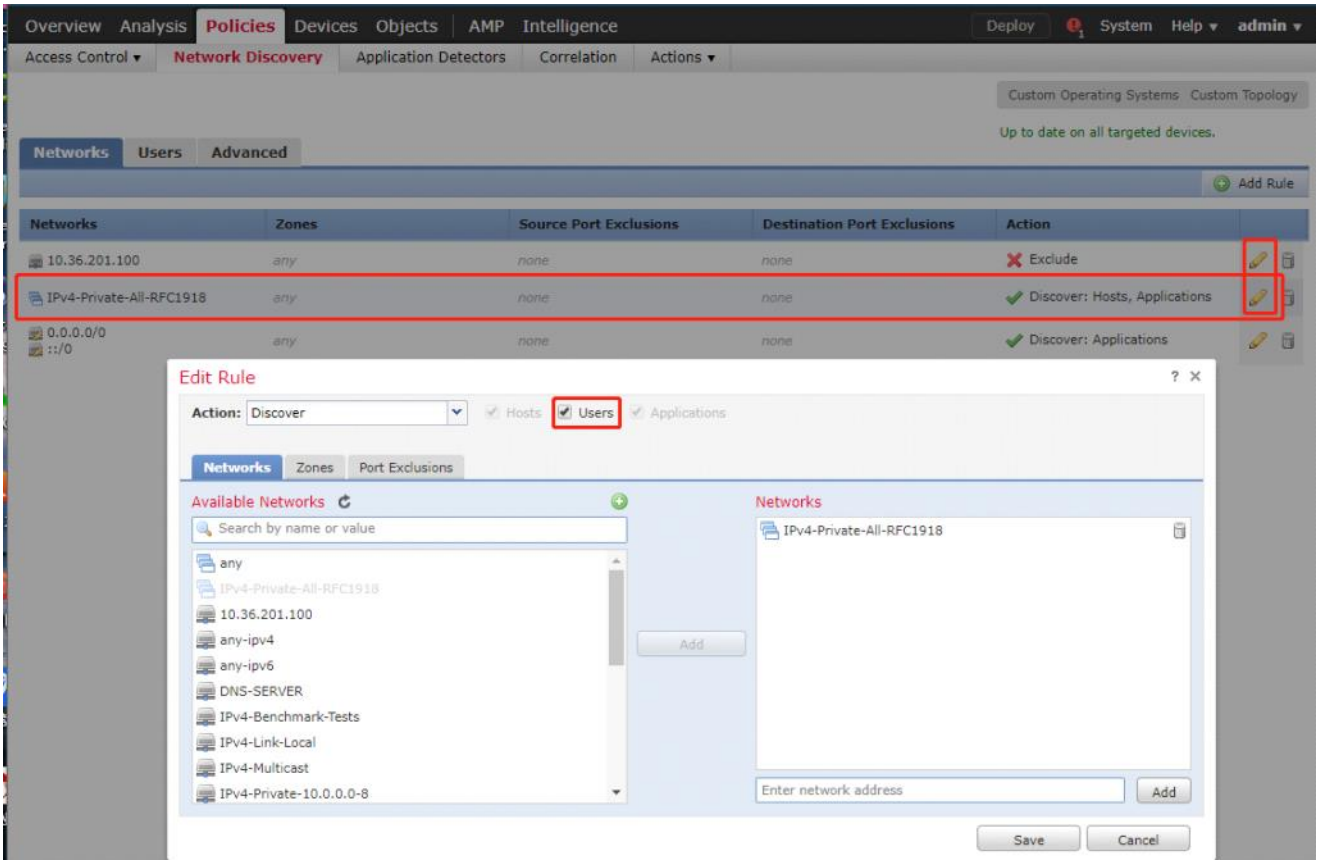


9.5：排错文档

https://www.cisco.com/c/en/us/td/docs/security/firesight/user-agent/25/config-guide/Firepower-User-Agent-Configuration-Guide-v2-5/ConfigAgent.html#40929

10：在Network Discovery里打开用户发现

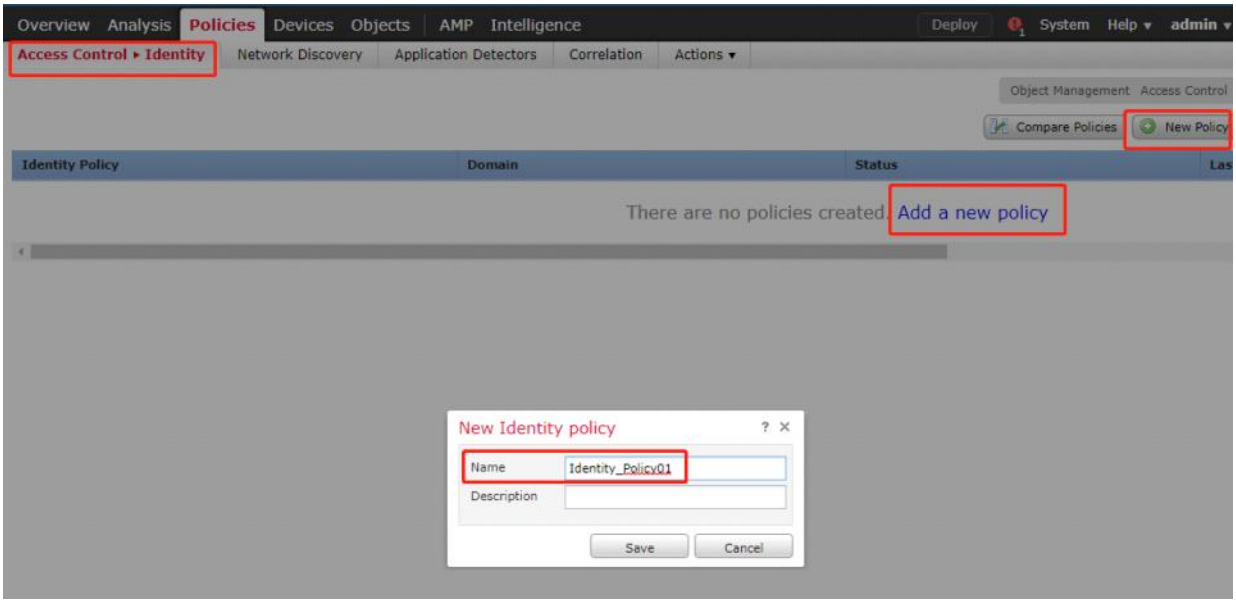
- 在默认的网络发现策略/自定义的网络发现策略中打开用户发现
- 这样可以让用户，应用，主机形成对应关系，在以后查看日志更明显



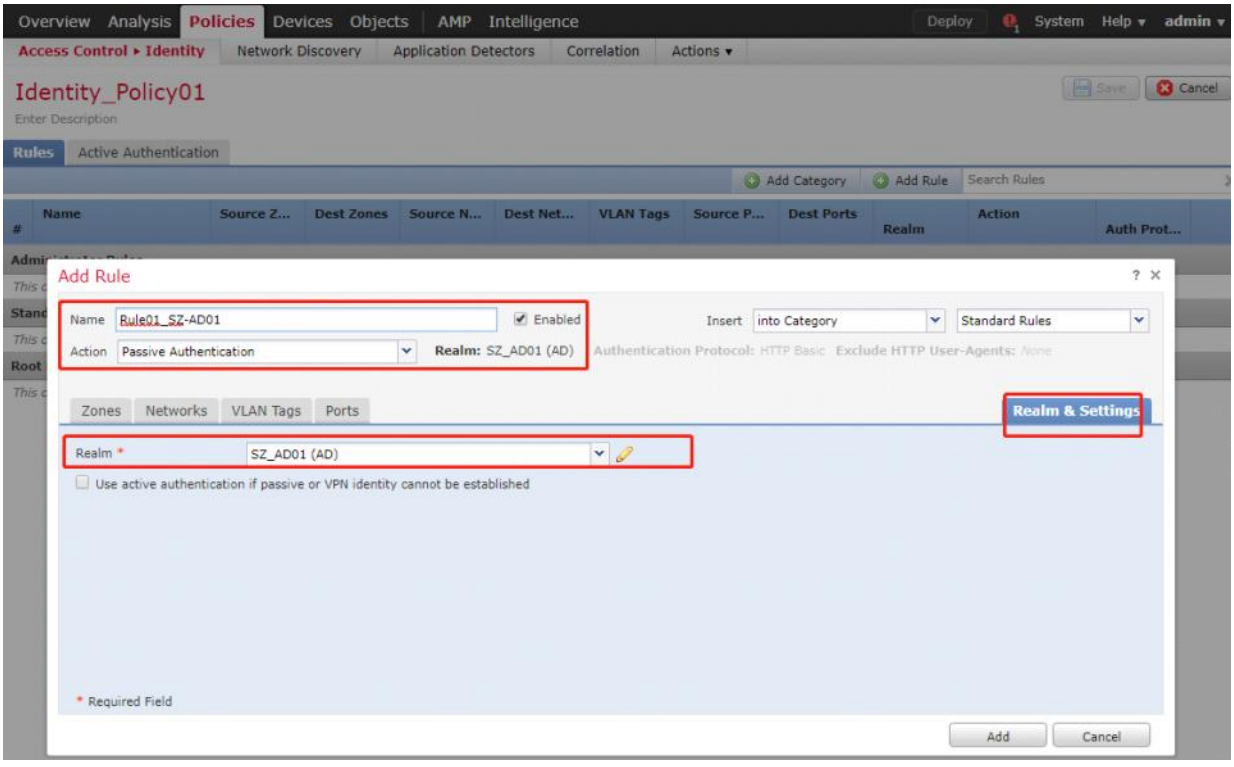
当你配置完networkdiscovery里添加user后，只要该用户登陆了加域PC，就会显示发现用户了
以后Firepower就可以看到该用户的事件。访问的URL/app等，而不单是基于IP，但我们还没对其做策略控制

11：配置Identity Policy

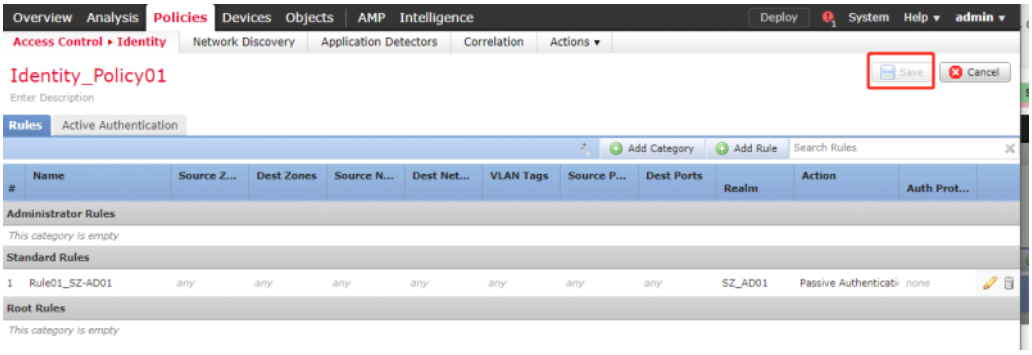
11.1：创建一个身份策略



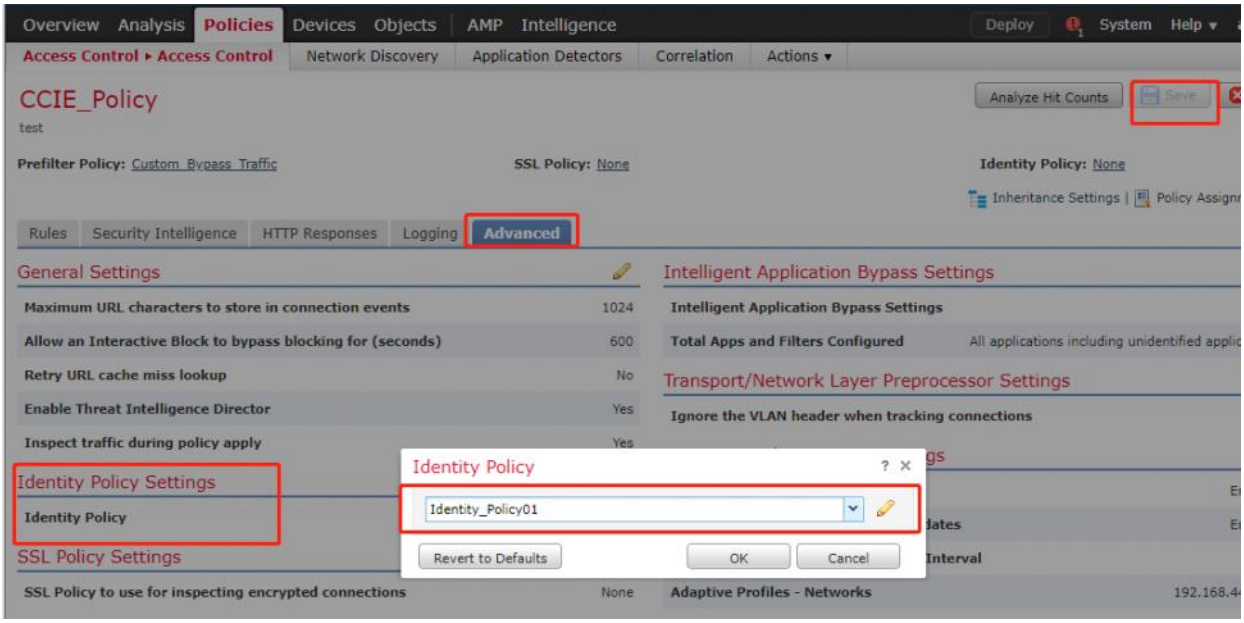
11.1.1：选择该策略=被动认证，即不认证，并将之前FMC上创建的Realm（领域，就是关联AD）添加到该策略中



11.1.2：保存



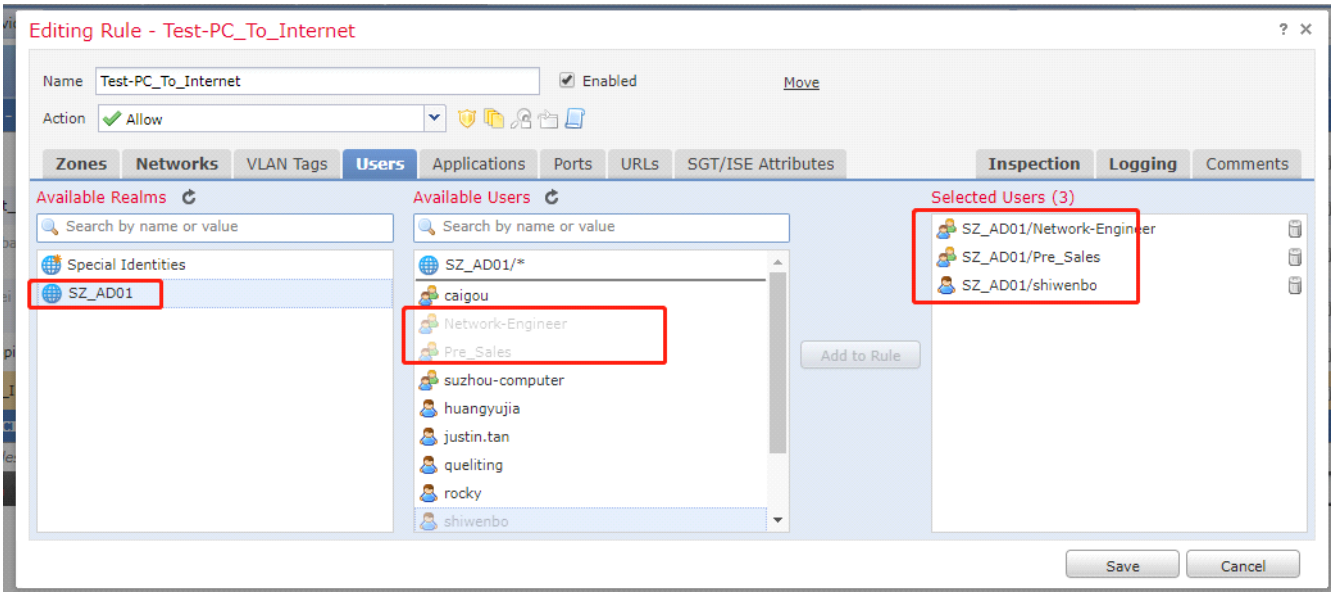
11.2：ACP的高级选项调用身份策略



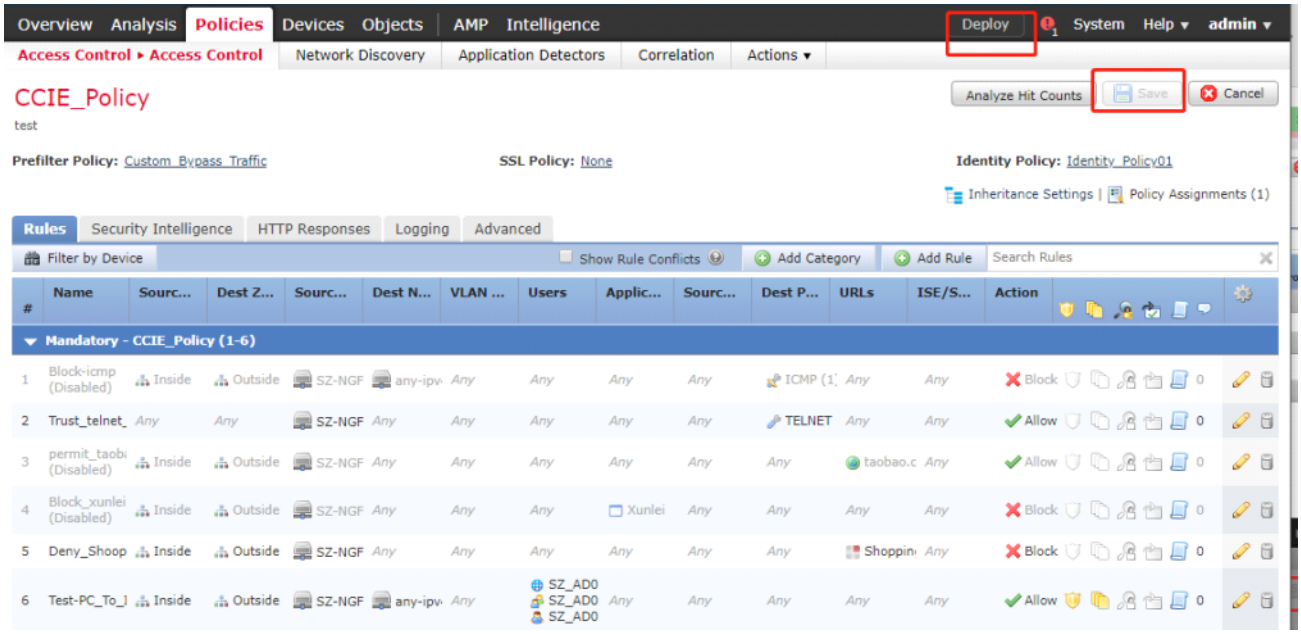
11.3：配置ACP里ACR访问控制规则☆

11.3.1：ACR控制规则里，选择获取用户/用户组信息的领域
并选择该策略生效的用户/用户组/整个Realms（甚至是整个AD）

注意：这条规则=不仅需要匹配该规则所有的网络IP/端口/应用这些条件。还需要源地址匹配用户组/用户才可以allow流量
如果该规则生效范围内有的IP是给非加域电脑使用，那么该策略不会放行这些非加域PC的流量

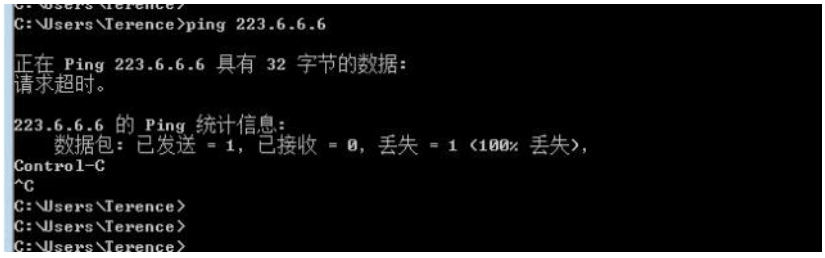


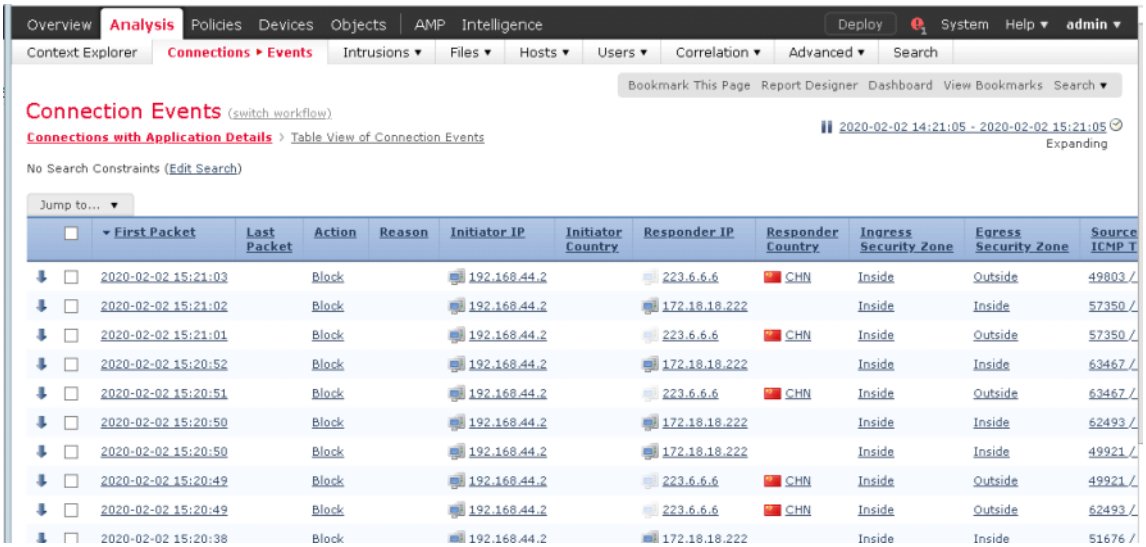
11.3.2：保存部署到FTD



12：验证

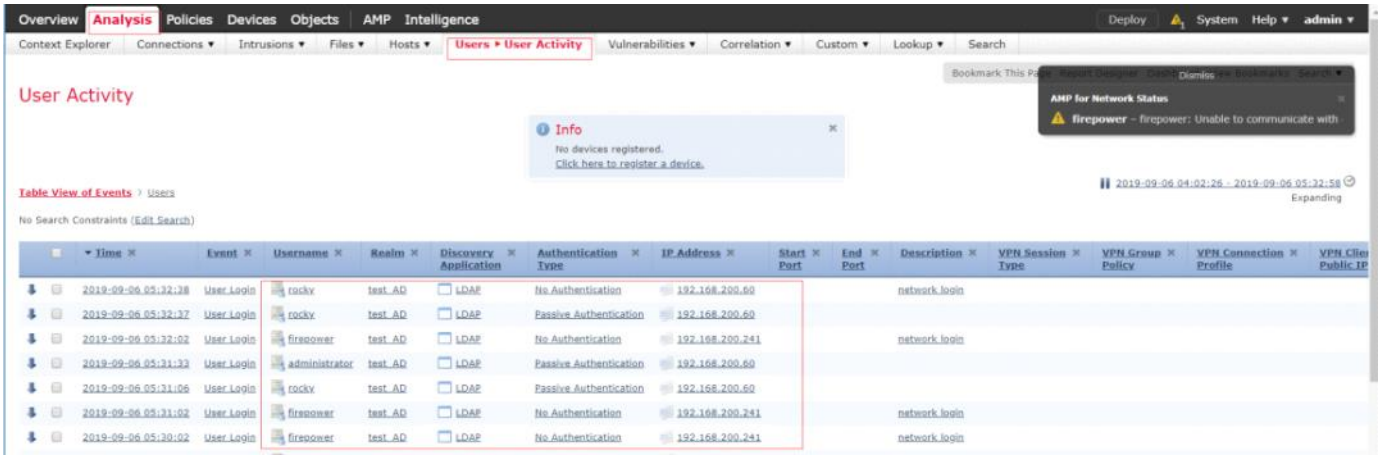
12.1：如果电脑没加域，经过firepower流量不放行





13.2：这时候用户使用域账户登陆电脑，防火墙就有事件了

- 加域电脑使用域账户登陆PC，连接网络，AD发现域账户登陆
- User Agent读取AD实时事件反馈给FMC，FMC知道该用户IP地址（network discovery）
- 则进行策略控制，我们的策略是放行，所以看事件就可以了，如果该网段有PC没加域，则无法通信



13：故障排查

该错误可能导致防火墙无法工作身份策略，导致流量中断。
AD2012，FMC/FTD 6.4.0.4，user agent 2.5（未解决，有哥们儿遇到与我联系）