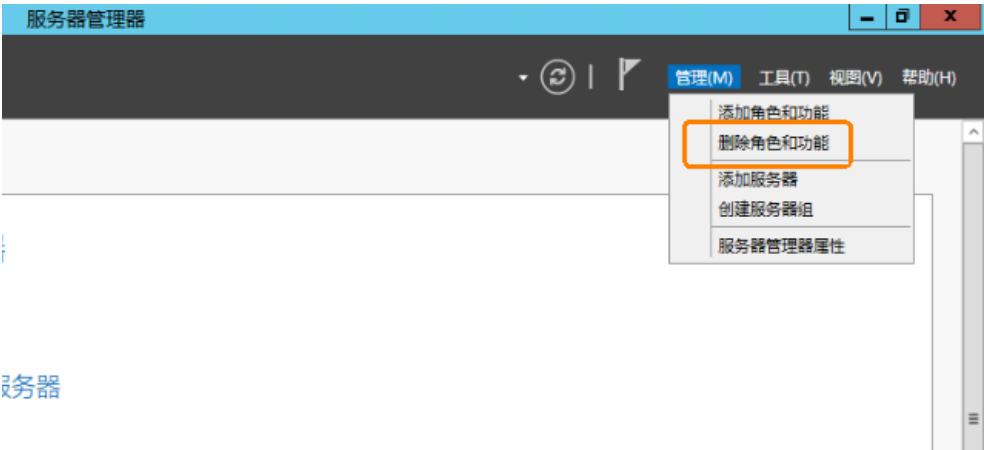
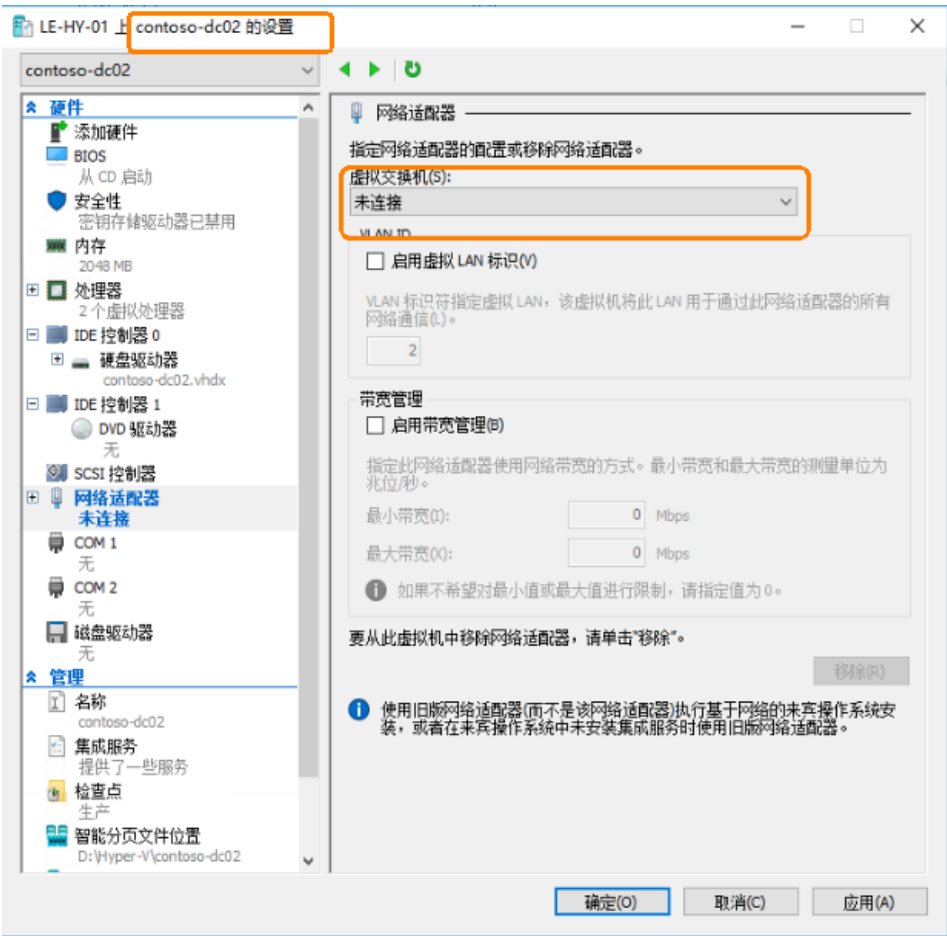


5-2：强制降级并清理AD残留信息

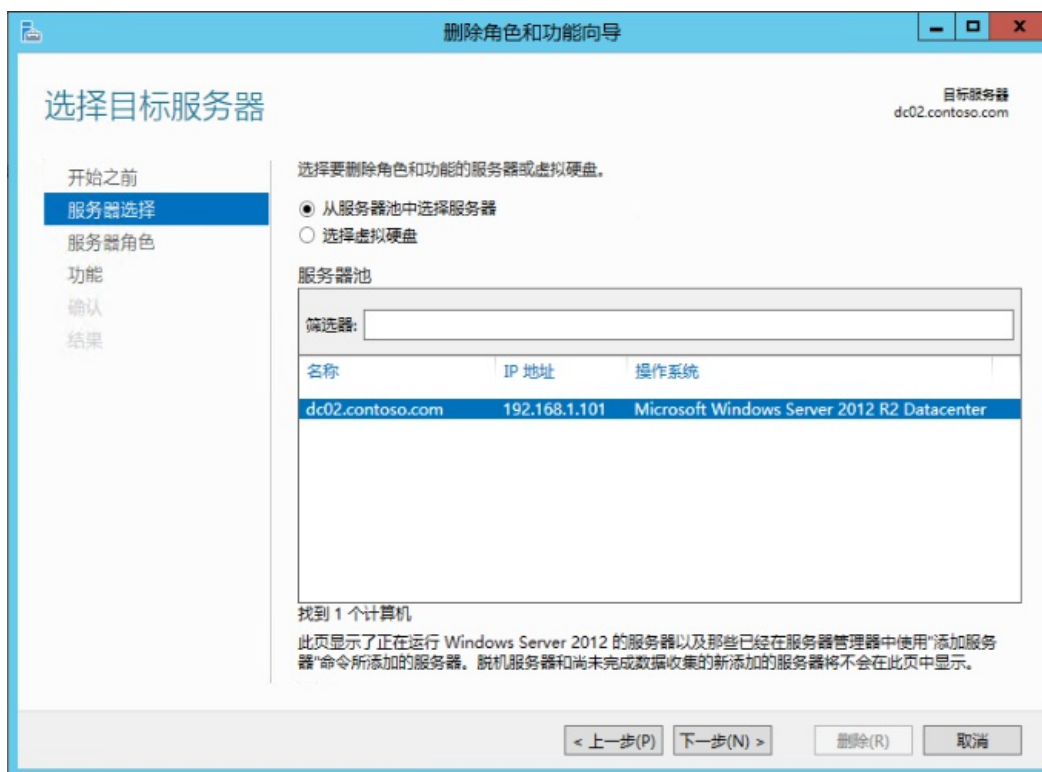
场景

一般用于域控制器无法正常在线下的情况，我们可以通过ntdsutil工具强制删除AD中的残留信息。

首先强制卸载DC（非必须）



服务器



Active Directory 域服务配置向导

凭据

警告

删除选项

新管理员密码

查看选项

降级

结果

目标服务器
dc02.contoso.com

提供执行此操作所需的凭据

CONTOSO\Administrator (当前用户)

更改(C)...

☐ 强制删除此域控制器(F)

⚠

无法联系其他域控制器，但其他域控制器对象位于目录中。如果你确定这是该域的最后一个域控制器并希望继续操作，请确认这是域中的最后一个域控制器。

☐ 域中的最后一个域控制器(L)

⚠

服务器将在降级操作后自动重新启动。重新启动后需要进行角色删除。

[详细了解 删除凭据](#)

< 上一步(P)

下一步(N) >

降级(D)

取消

Active Directory 域服务配置向导

凭据

警告

删除选项

新管理员密码

查看选项

降级

结果

目标服务器
dc02.contoso.com

提供执行此操作所需的凭据

CONTOSO\Administrator (当前用户)

更改(C)...

☒ 强制删除此域控制器(F)

⚠

除非这是域中的最后一个域控制器，否则，你必须在删除元数据后手动执行清理。

⚠

服务器将在降级操作后自动重新启动。重新启动后需要进行角色删除。

[详细了解 删除凭据](#)

< 上一步(P)

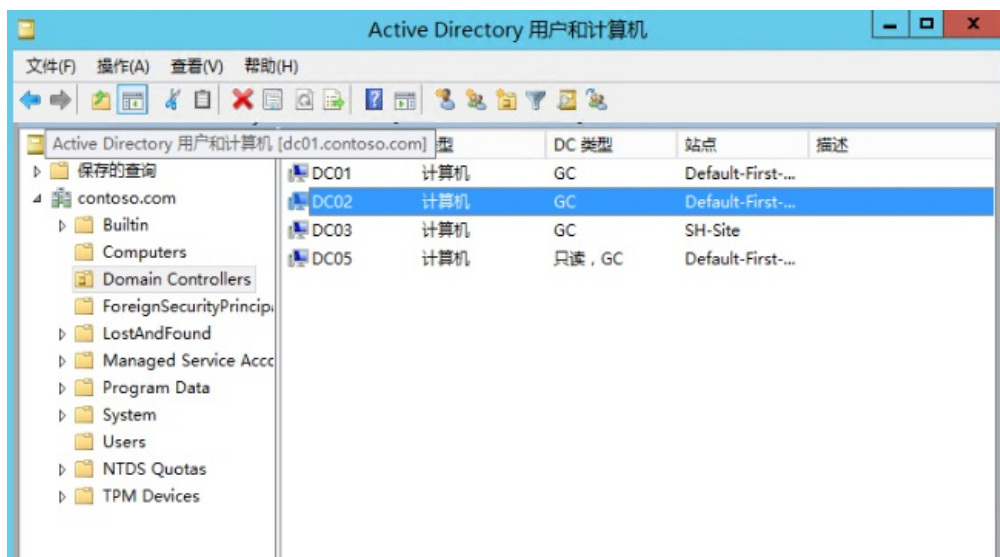
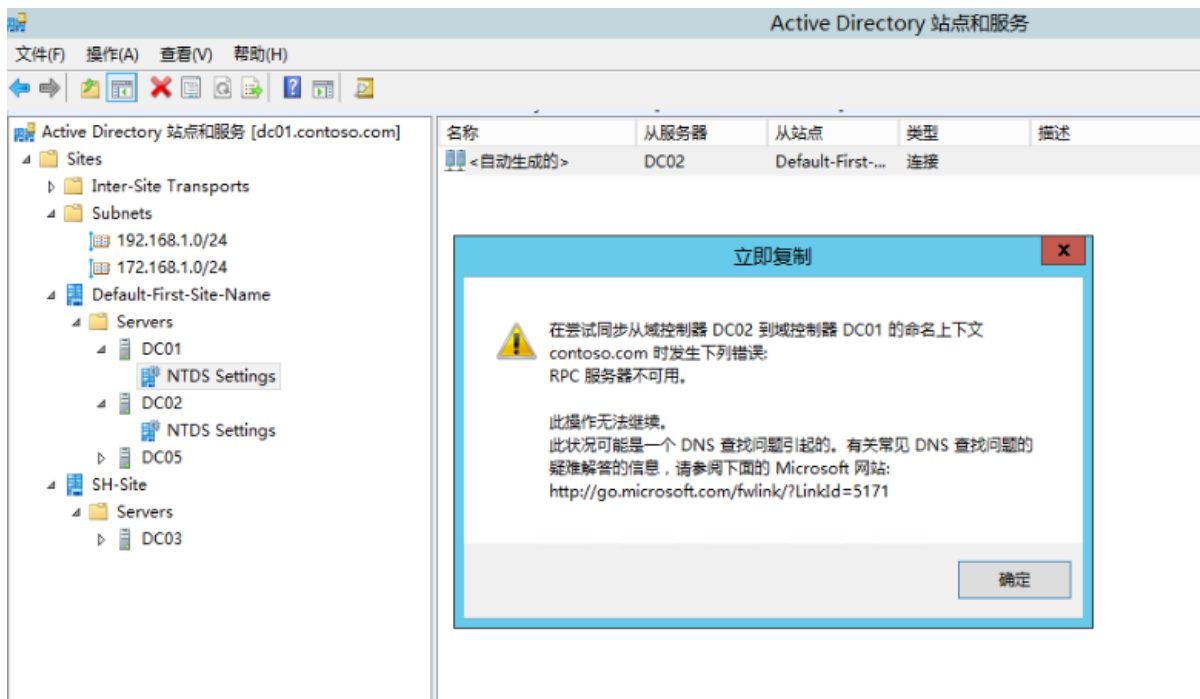
下一步(N) >

降级(D)

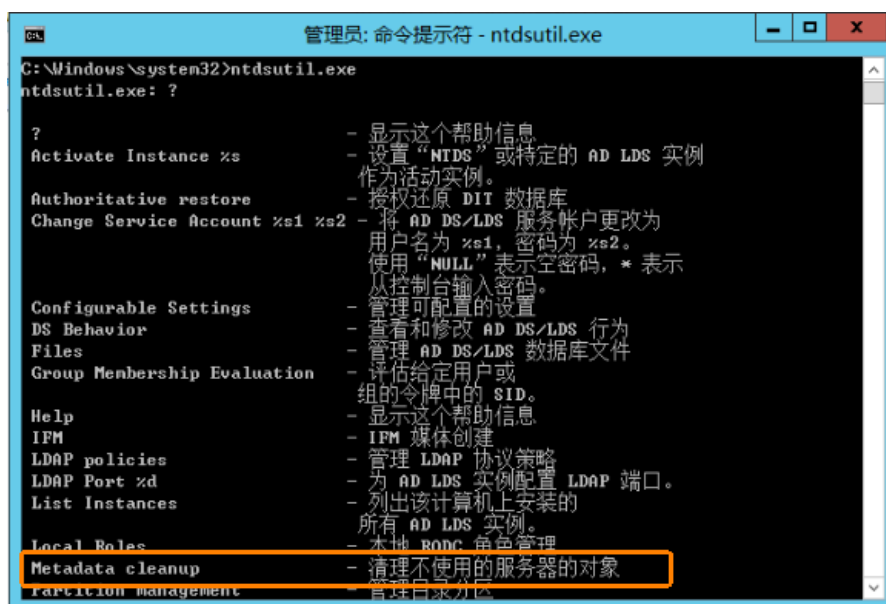
取消



虽然这台机器上的DC角色已经卸载，但是如果我们来到online的DC上，还是可以看到DC02的信息的，因为这台DC并没有从AD的数据库里面完全清除掉，如图。



然后到其他正常的AD上删除刚才强制卸载的DC的残留信息



```
管理员: 命令提示符 - ntdsutil.exe

Snapshot - 快照管理
SSL Port %d - 为 AD LDS 实例配置 SSL 端口。

ntdsutil.exe: metadata cleanup
metadata cleanup: ?

? - 显示这个帮助信息
Connections - 连接到一个特定 AD DC/LDS 实例
help - 显示这个帮助信息
Quit - 返回到上一个菜单
Remove selected domain - 删除所选域的 AD DS 对象
Remove selected Naming Context - 为选定的命名上下文删除对象
Remove selected server - 从所选服务器上删除对象
Remove selected server %s - 从所选服务器上删除对象
Remove selected server %s on %s - 从所选服务器上删除对象
Select operation target - 选择的站点, 服务器, 域, 角色和命名上下文

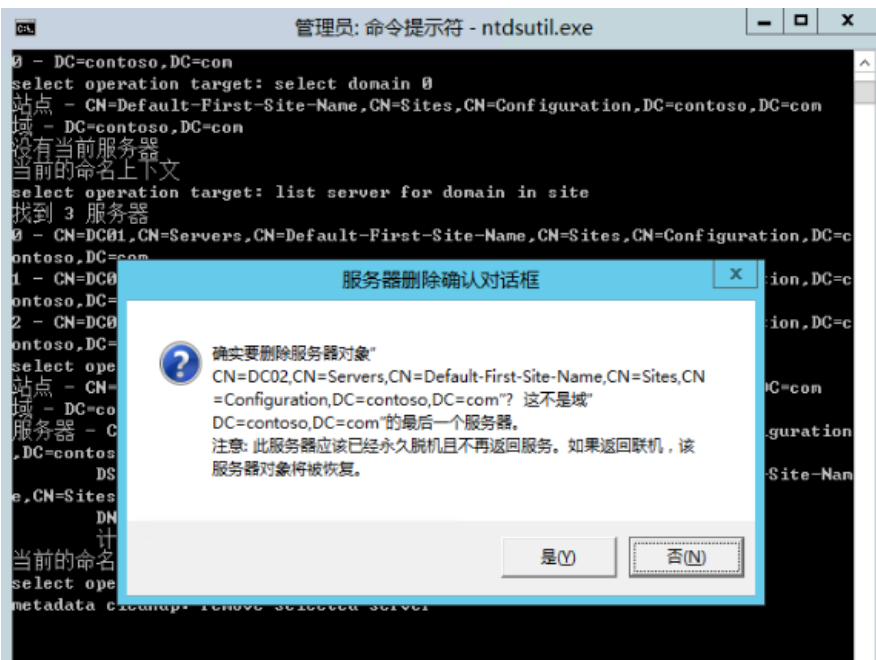
metadata cleanup: _
```

```
server connections: connect to server dc01.contoso.com
绑定到 dc01.contoso.com ...
用本登录的用户的凭证连接 dc01.contoso.com。
```

```
server connections: q
metadata cleanup: select operation target
select operation target: _
```

```
select operation target: list sites
找到 2 站点
0 - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=contoso,DC=com
1 - CN=SH-Site,CN=Sites,CN=Configuration,DC=contoso,DC=com
select operation target: select site 0
站点 - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=contoso,DC=com
没有当前域
没有当前服务器
当前的命名上下文
select operation target: list domain in site
找到 1 域
0 - DC=contoso,DC=com
select operation target: select domain 0
站点 - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=contoso,DC=com
域 - DC=contoso,DC=com
没有当前服务器
当前的命名上下文
select operation target: list server for domain in site
找到 3 服务器
0 - CN=DC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=contoso,DC=com
1 - CN=DC02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=contoso,DC=com
2 - CN=DC05,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=contoso,DC=com
select operation target: _
```

```
select operation target: select server 1
站点 - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=contoso,DC=com
域 - DC=contoso,DC=com
服务器 - CN=DC02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=contoso,DC=com
DSA 对象 - CN=NTDS Settings,CN=DC02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=contoso,DC=com
DNS 主机名称 - dc02.contoso.com
计算机对象 - CN=DC02,OU=Domain Controllers,DC=contoso,DC=com
当前的命名上下文
select operation target: q
metadata cleanup: remove selected server _
```



```
select operation target: q
metadata cleanup: remove selected server
正在从所选服务器传送/获取 FSMO 角色。
正在删除所选服务器中的 FRS 元数据。
正在搜索 "CN=DC02,OU=Domain Controllers,DC=contoso,DC=com" 下的 FRS 成员。
正在删除 "CN=DC02,OU=Domain Controllers,DC=contoso,DC=com" 下的子树。
尝试删除 CN=DC02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=contoso,DC=com 上的 FRS 设置失败, 原因是 "找不到元素。";
继续清除元数据。
"CN=DC02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=contoso,DC=com" 删除了, 从服务器 "dc01.contoso.com"
metadata cleanup: _
```

