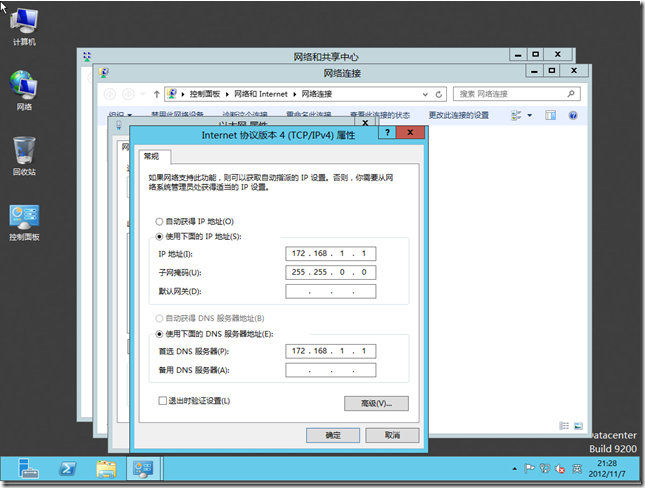
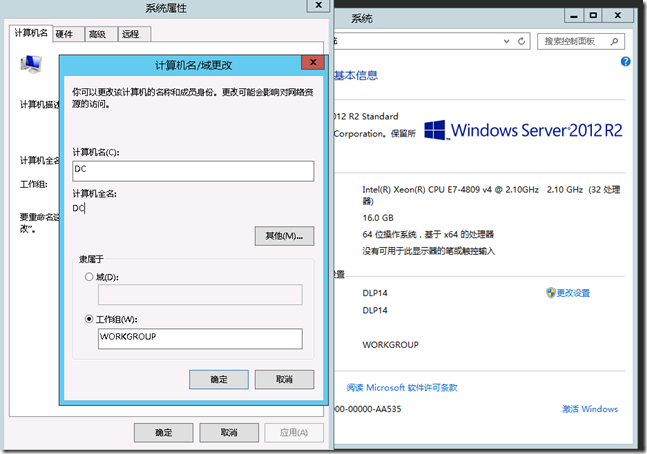
1，我已经安装好了一台windows server 2012服务器，而且已经配置好了IP、DNS（指向本机IP）等信息。如图。

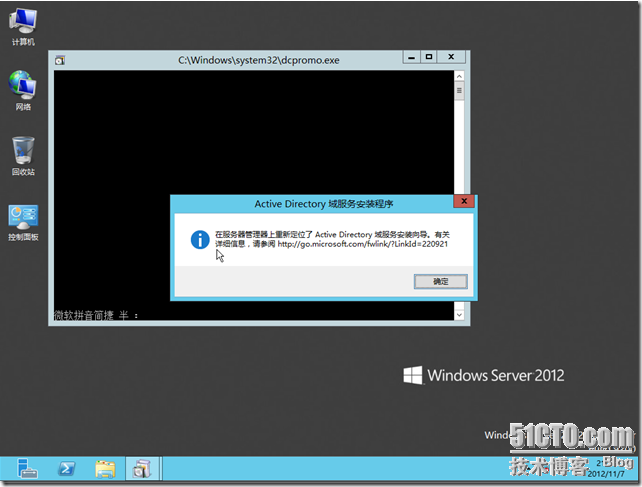
[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108083223997-430052619.png)

2，使用本地管理员账户登录，修改计算机名为“DC”（这个可以随意），升级成域控后，机器名称会自动变成为dc.feel.com，更改完之后重启服务器

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108132843403-1415159018.png)

开始：

下面我要把这台服务器提升为DC，在server 2012中，已经不支持dcpromo进行提升了，如果使用dcpromo /adv，会出现下图的提示，并且会转到服务器管理器的界面。如图。

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108083958419-485900816.png)

我们需要使用服务器管理器的添加功能和角色向导来提升域控制器，首先要安装AD相关的服务，安装完成后再进行后续的配置。

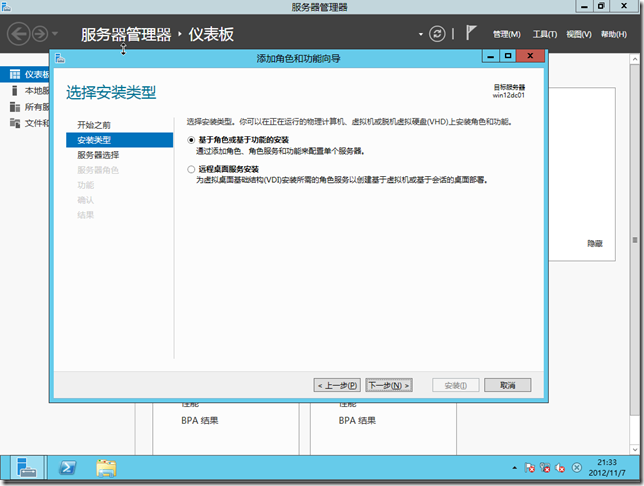
首先打开角色和功能的安装向导，如图。

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108083959263-434604195.png)

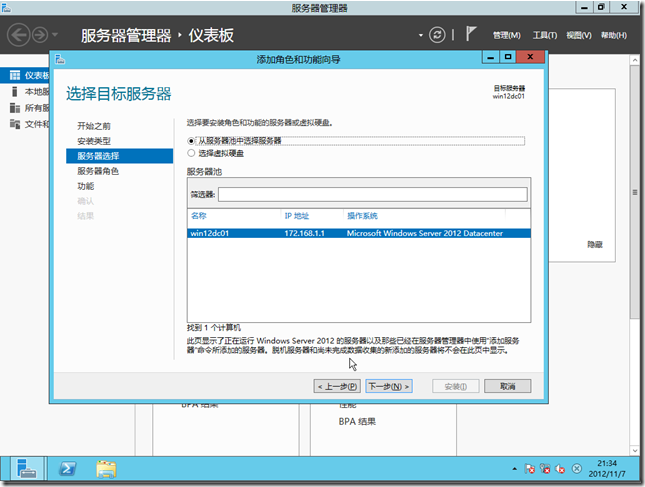
下一步

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108083959903-871115538.png)

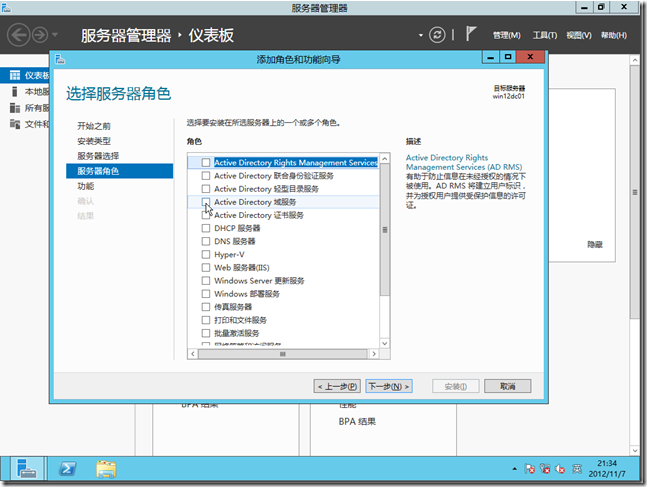
安装类型选择“基于角色或者基于功能的安装”，如图。

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108084000934-586090312.png)

目前我们的服务器池中只有当前这一台机器，保持默认，如图。

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108084001653-1202249231.png)

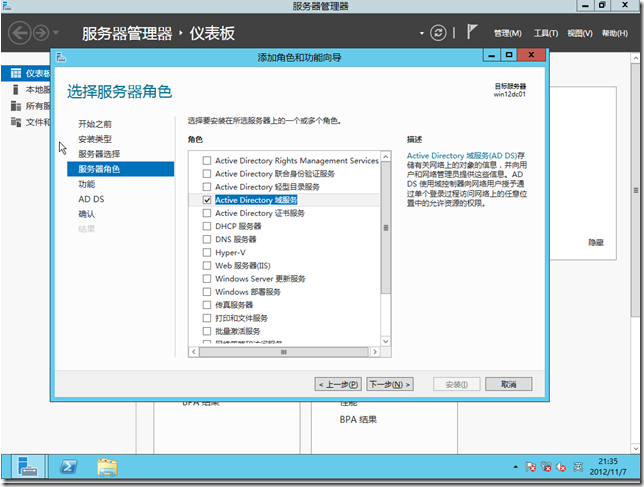
在选择服务器角色界面，勾选“Active Directory服务”，如图。

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108084002403-1116798501.png)

选择添加功能，默认不改动，直接点击添加功能。

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108084003013-1224098380.png)

默认选项，下一步

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108084003763-191084495.png)

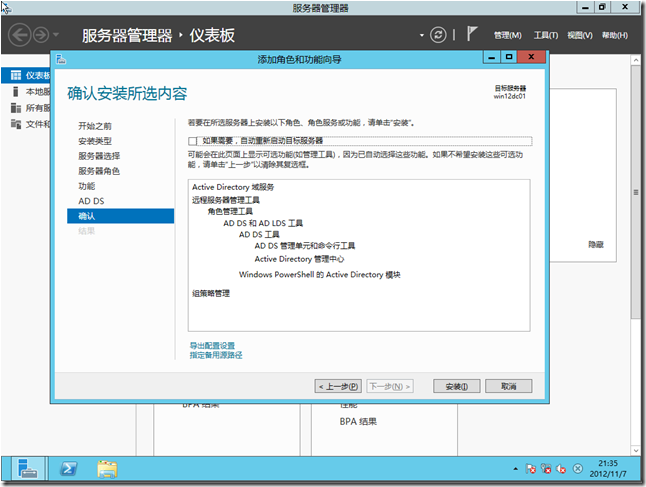
在选择功能界面，不需要选择任何功能，直接单击下一步，如图。

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108084005419-1725305536.png)

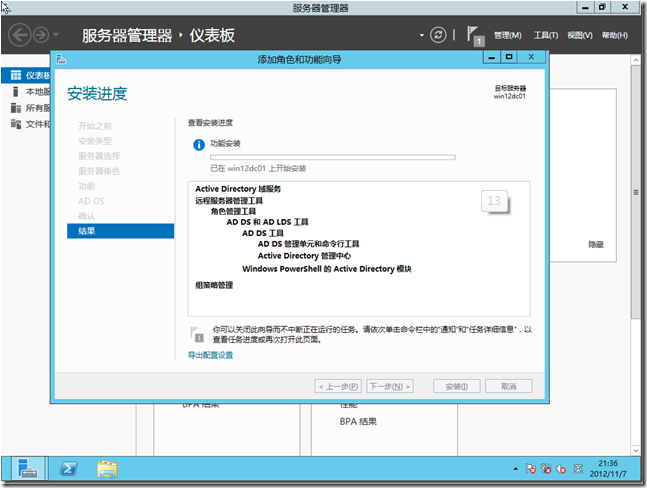
进入AD域服务的安装向导，如图。

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108084007747-42862378.png)

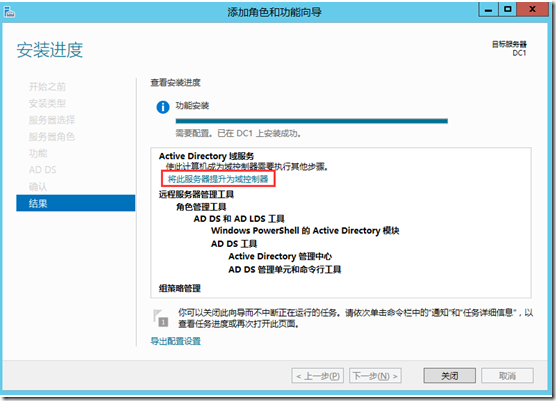
确认需要安装的组建后，勾选“如果需要，自动重新启动目标服务器”单击“安装”，如图。

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108084008341-695226145.png)

正在安装。如图。

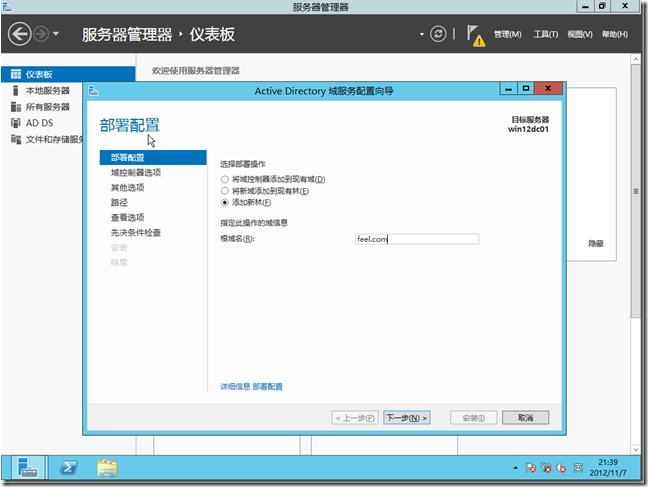
[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108084009169-1564320425.png)

等待安装完毕，点击“将此服务器提升为域控制器”

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108152324716-1555268204.png)

AD域服务安装完成，下面我们进入提升域控制器的向导。如图。

因为是搭建全新的域，所以没有已有的DC，所以我这里选择“添加新林”，安装新林中的第一个域，根域名为“feel.com”

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108084013028-1840473654.png)

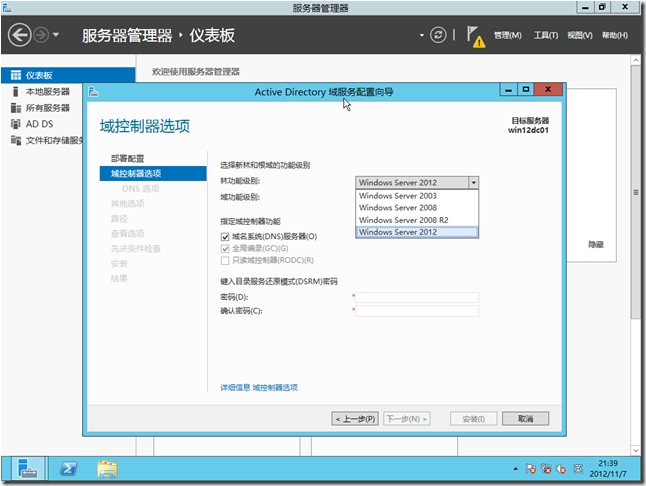
选择林功能级别、域功能级别。

此处我们选择的为windows server 2012

默认会直接在此服务器上安装DNS服务器

第一台域控制器必须是全局编录服务器的角色

第一台域控制器不可以是只读域控制器（RODC）

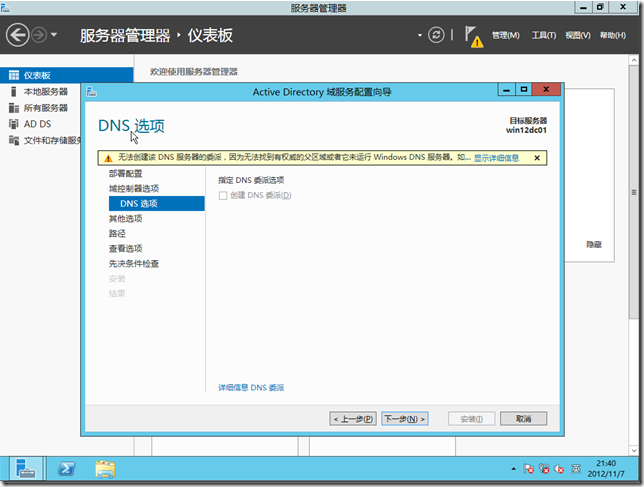
[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108084013559-636140841.png)

勾选“域名系统DNS服务器”，并输入目录服务还原模式密码

目录还原模式是一个安全模式，可以开机进入安全模式时修复AD数据库，使用此密码

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108084014184-1575243099.png)

出现关于DNS的警告，因为目前还没有安装DNS，所以不用理会，直接选择下一步，如图。

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108084014716-766408677.png)

在netbios域名(不支持DNS域名的旧系统，如win98 winnt需要通过netbios名来进行通信 )界面，保持默认，选择下一步

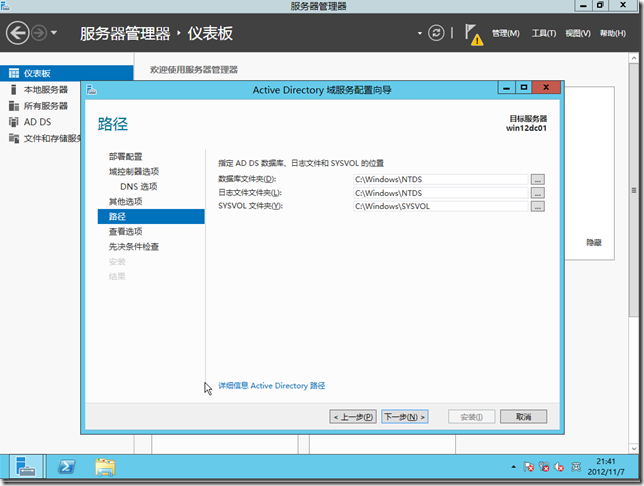
[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108084016138-1777305571.png)

指定数据库、日志、sysvol的存放位置.

数据库文件夹：用了存储AD数据库  
日志文件文件夹：用了存储AD的更改记录，此记录可以用来修复AD数据库  
SYSVOL文件夹：用了存储域共享文件（例如组策略）

建议最好不要跟系统盘放在一起

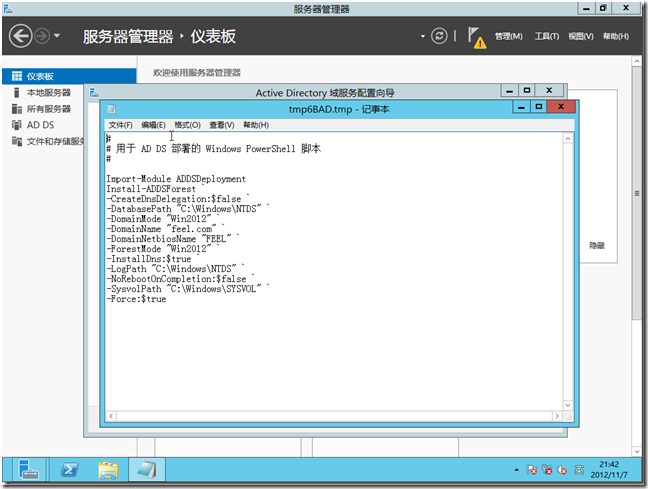
如果计算机内有多个硬盘，建议将数据库与日志文件夹分别设置到不同的硬盘内，分两个硬盘可以提供运行效率，而且分开存储可以避免两份数据同时出现问题，以提高修复AD的能力。（不过我认为现在都是RAID模式了没必要分开，和操作系统分区分开就可以了）

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108084016638-1328006620.png)

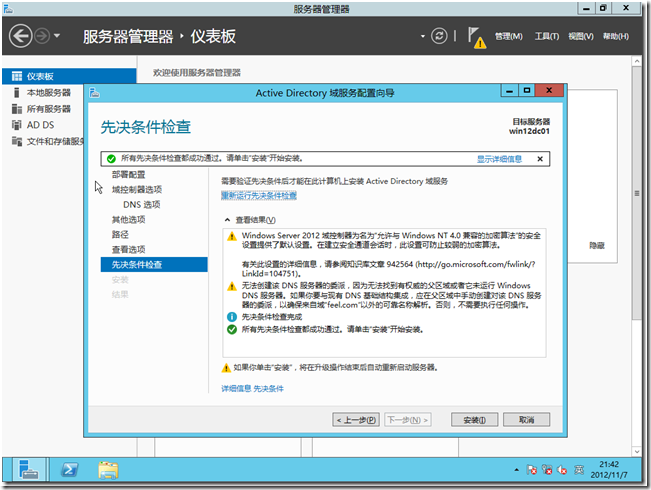
在摘要界面，如果没有问题，我们可以选择下一步，如果有问题，则可以返回修改，如图。

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108084017419-1036994102.png)

我们可以点击“查看脚本”，将配置信息导出为powershell脚本文件，如图。

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108084017903-1358470668.png)

顺利通过检查，直接安装

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108084019106-24473450.png)

正在启动安装，如图。

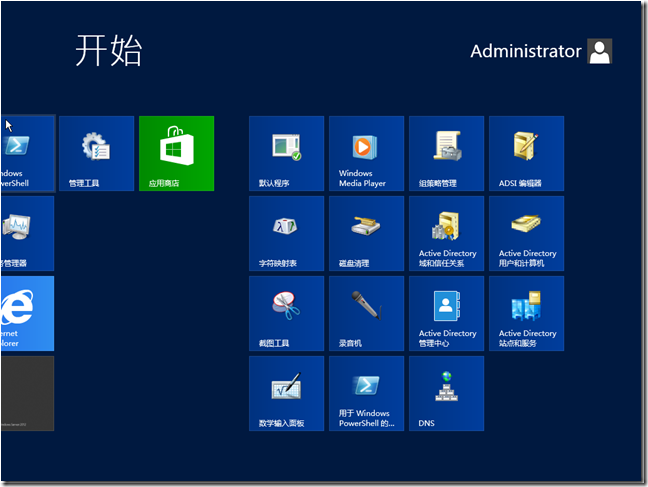
[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108084019763-1510802705.png)

安装完成后，需要重启服务器，如图。

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108153907341-655622030.png)

重启完成后，需要使用域管理员账户登录   （FEEL.COM/Administrator）

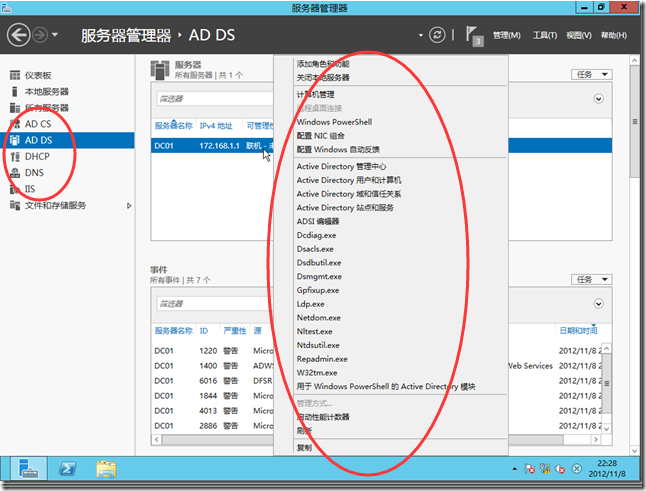
我们可以看到在开始菜单中已经有了AD相关的管理工具，如图。

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108084023700-1872180951.png)

======================================================================

在服务器管理器中，如果我们右击AD服务器，会发现windows server 2012提供了很多AD的常用管理命令

不管是ADDS服务，还是DNS服务，还是其他的服务，都可以通过服务器管理器进行管理

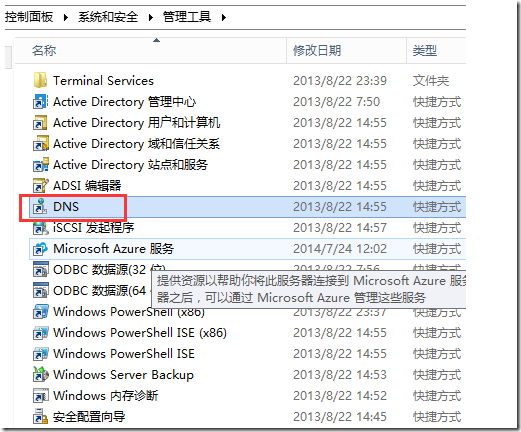
[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108141934981-1111719286.png)

**检查DNS服务器内的记录是否完备 (以下内容为参考)**

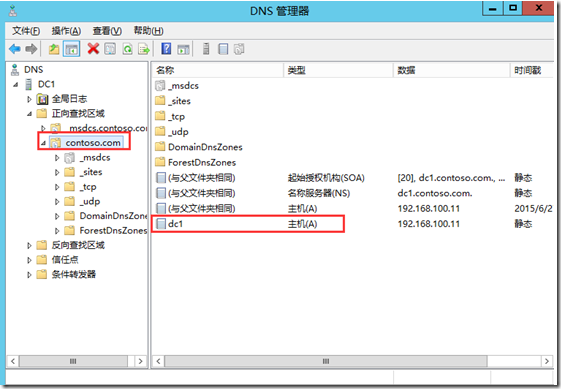
域控会将自己扮演的角色注册到DNS服务器内，以便让其他计算机能够通过DNS服务器来找到域控。因此先检查DNS服务器内是否已经存在这些记录。

**检查主机记录**

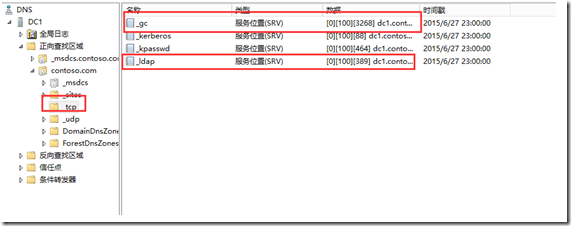
选择管理工具-dns

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108155152388-1657805018.png)

默认会有一个contoso.com的区域，主机记录表示域控dc.contoso.com已经正确的将其主机名与IP地址注册到DNS服务器内。

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108155153044-686720019.png)

如果域控制器已经正确的将家里注册到dns服务器，应该还会有\_tcp \_udp等文件夹。单击\_tcp文件夹后可以看到数据类型为服务位置(SRV)的\_ldap记录，表示dc1.contoso.com已经正确的注册为域控制器。还能看到\_gc记录全局编录也是由dc1.contoso.com所扮演。

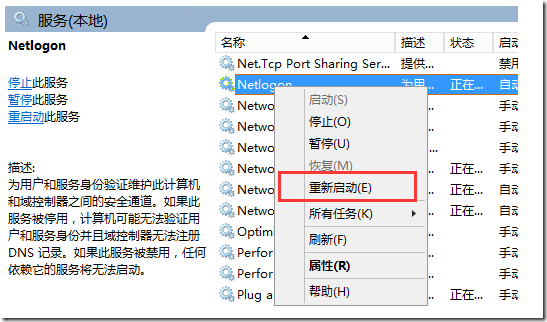
[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108155153653-1167324472.png)

**排除注册失败的问题**

如果域成员本身的设置或者网络问题，会造成无法将数据注册到DNS服务器。

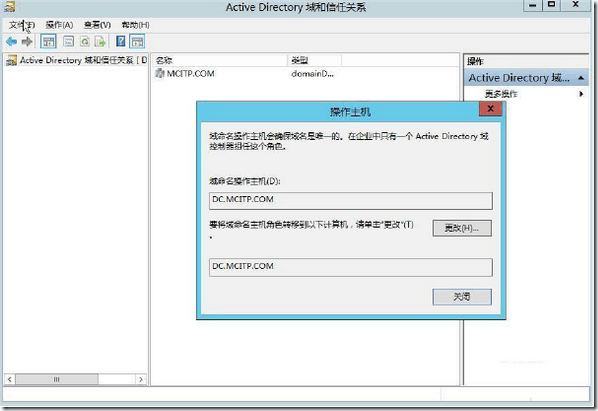
如果有成员计算机的主机与ip美元正确注册到DNS服务器，可以到此机器上运行ipconfig /registerdns来手动注册。完成后，到DNS服务器检查是否已有正确记录，例如server1.contoso.com，ip地址192.168.100.13则坚持区域contoso.com是否有对应的a记录和ip。

如果发现域控制器没有将其扮演的角色注册到dns服务器，也就是没有\_tcp文件夹与记录，到服务器中重启netlogon服务

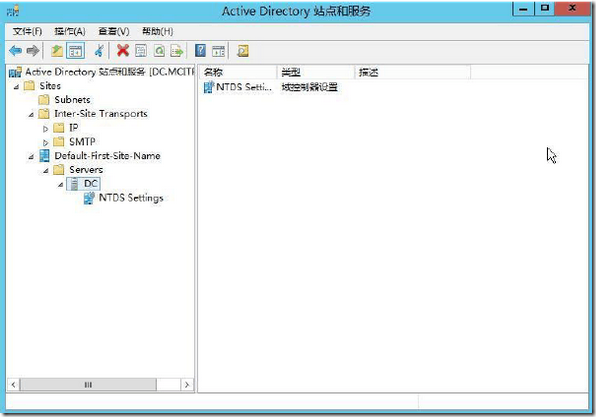
[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108155154169-1698684384.png)

**再查看其他相关管理工具能否正常打开。**

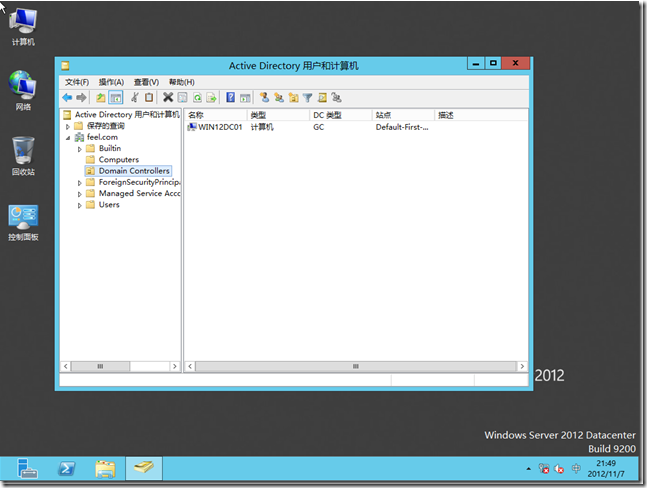
1，通过Active Directory域和信任关系，查看操作主机信息。

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108141935809-1529739227.png)

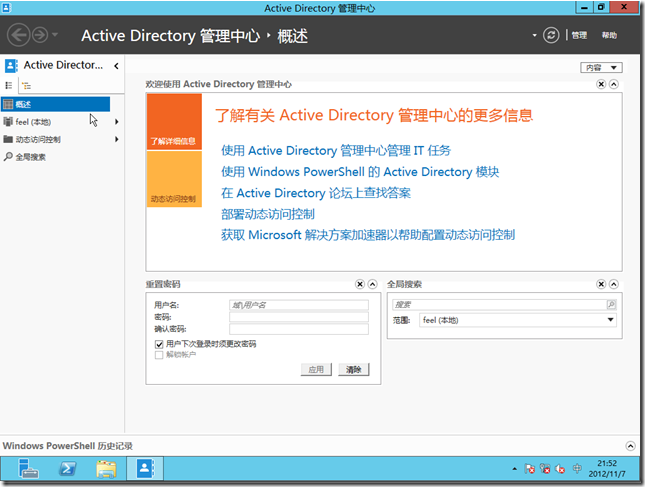
现默认站点只有一台域控服务器

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108141936388-1061299852.png)

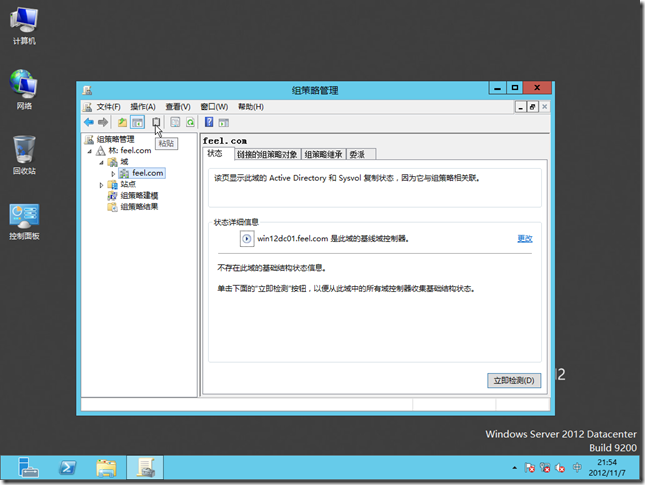
2，查看AD用户和计算机，如图。

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108141937294-1327630239.png)

3，AD管理中心，如图。

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108141938294-806681097.png)

4，组策略管理，如图。

[](http://images2017.cnblogs.com/blog/581253/201711/581253-20171108141939841-279024991.png)

小结：

将网络元素组织为分层结构可带来以下好处：

　　林可以充当组织的安全边界并定义管理员的授权范围。默认情况下，一个林包含一个域（称为林根域）。在林中还可以创建其他域，以提供 AD DS 数据分区，从而使组织仅在需要时复制数据。因此，在可用带宽有限的网络上，AD DS 可以进行全局缩放。Active Directory 域还支持与管理相关的许多其他核心功能，包括网络范围的用户标识、身份验证和信任关系。OU 简化了授权的委派以方便管理大量对象。所有者可以通过委派将对象的全部或有限授权转移给其他用户或组。委派十分重要，因为它有助于将大量对象的管理分发到多个被信任执行管理任务的人。

安全性方面：

　　安全性能过登录身份验证以及到目录中资源的访问控制与 AD DS 集成。借助单点网络登录，管理员可以管理其整个网络中的目录数据和组织。授权网络用户还可以使用单点网络登录访问网络中任意位置的资源。基于策略的管理简化了即使最复杂的网络的管理。

其他 AD DS 功能包括下列各项：

　　一组规则，即架构，它定义包含在目录中的对象和属性的类别、这些对象的实例的约束和限制及其名称的格式。包含有关目录中每个对象的信息的全局编 录。无论目录中的哪个域实际包含目录信息，用户和管理员都可以使用全局编录查找这些数据。一种查询和索引机制，以便对象及其属性可由网络用户或应用程序发 布和发现。一种复制服务，可在整个网络中分发目录数据。域中所有可写域控制器均参与复制，并包含其域的所有目录信息的完整副本。对目录数据的任何更改均复 制到域中的所有域控制器。操作主机角色（也称为灵活单主机操作或 FSMO）。包含操作主机角色的域控制器被指定为执行特定任务，以确保一致性以及消除目录中有冲突的条目。