看前须知

1. 本栏将以最大程度实现 Windows 智能 DNS 的案例重现。
2. 一名良好的网络工程师会时刻保证自己的计算机处于最安全的状态。
3. 本栏中的 Windows 均采用域环境下来实现效果，域环境与普通工作站大体相同。根据实际情况，可以参考域环境下的配置。
4. 若在图片中出现与环境不符合的参数，请忽略。
5. 文档内的知识是永无止境的，当然也不能完全按照文档中的内容来形成脑海中的刻板印象，请读者需时刻保持清醒的头脑。文档仅提供某一方面的方法，更多视野需要由读者自身开拓。

环境：

镜像信息：

系统	系统版本	发行版本
Windows	WindowsServer2022	21H2

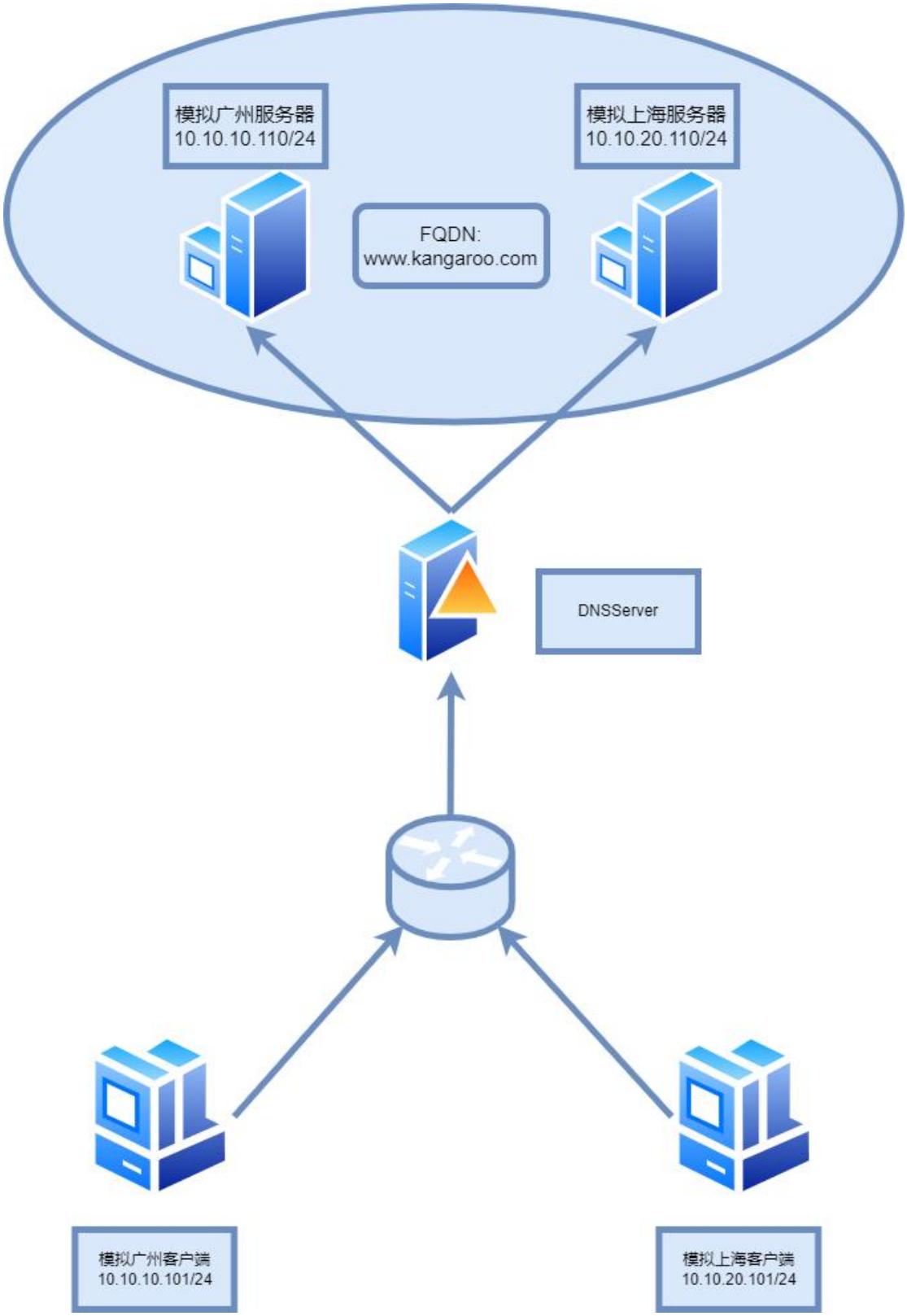
网络信息表

网络名称	VlanID	子网名称	网络地址	网关	IPv4 地址池
Network10	10	Subnet10	10.10.10.0/24	10.10.10.254	10.10.10.100-10.10.10.200
Network20	20	Subnet20	10.10.20.0/24	10.10.20.254	10.10.20.100-10.10.20.200

实例信息表

实例名称	IPv4 地址	完全合格域名
windows1	10.10.10.110 10.10.20.110	dc.kangaroo.com
windows2	10.10.10.101 10.10.10.102(Secondary) 10.10.20.101	client.kangaroo.com

拓扑结构

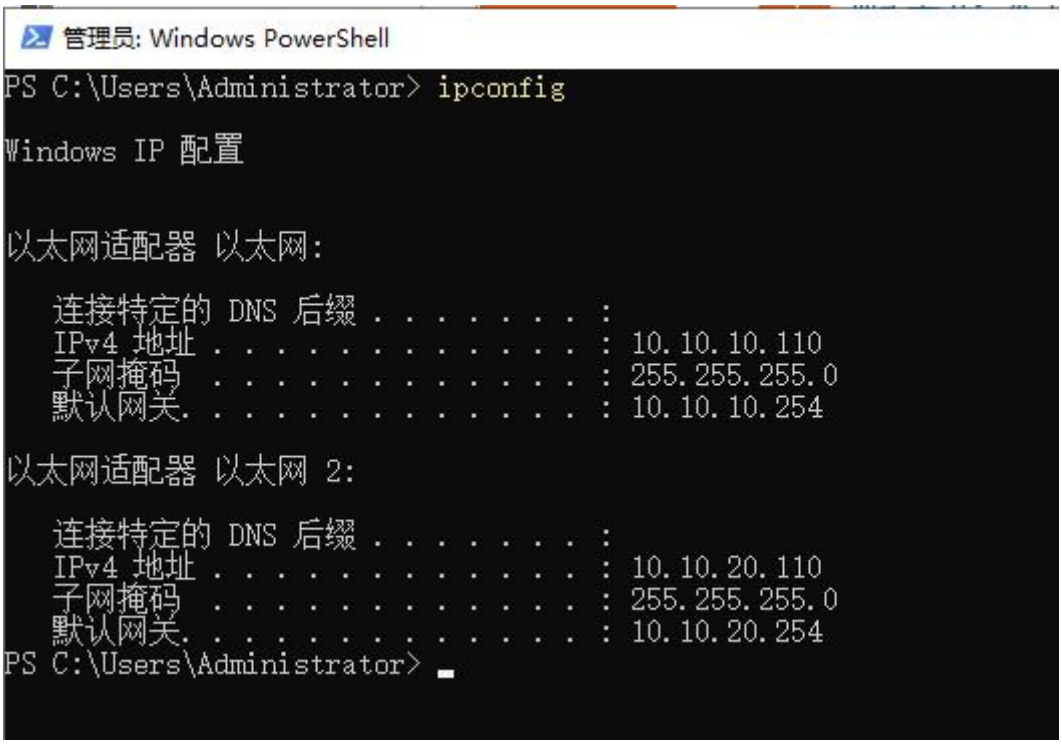

模拟广州服务器
10.10.10.110/24
模拟上海服务器
10.10.20.110/24
FQDN:
www.kangaroo.com
DNSServer
模拟广州客户端
10.10.10.101/24
模拟上海客户端
10.10.20.101/24

域环境部署：

由于拓扑环境中使用普通工作站来做测试，所以可以将 Client 加入域环境中。

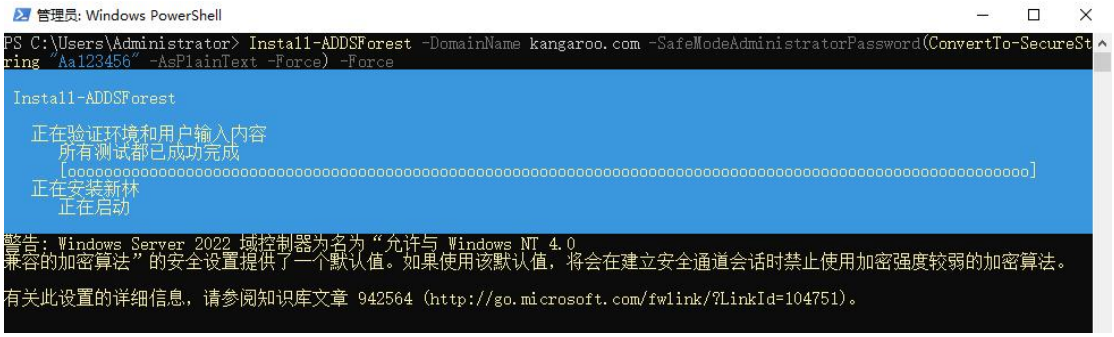
为域控改名：

配置静态 IP 地址：



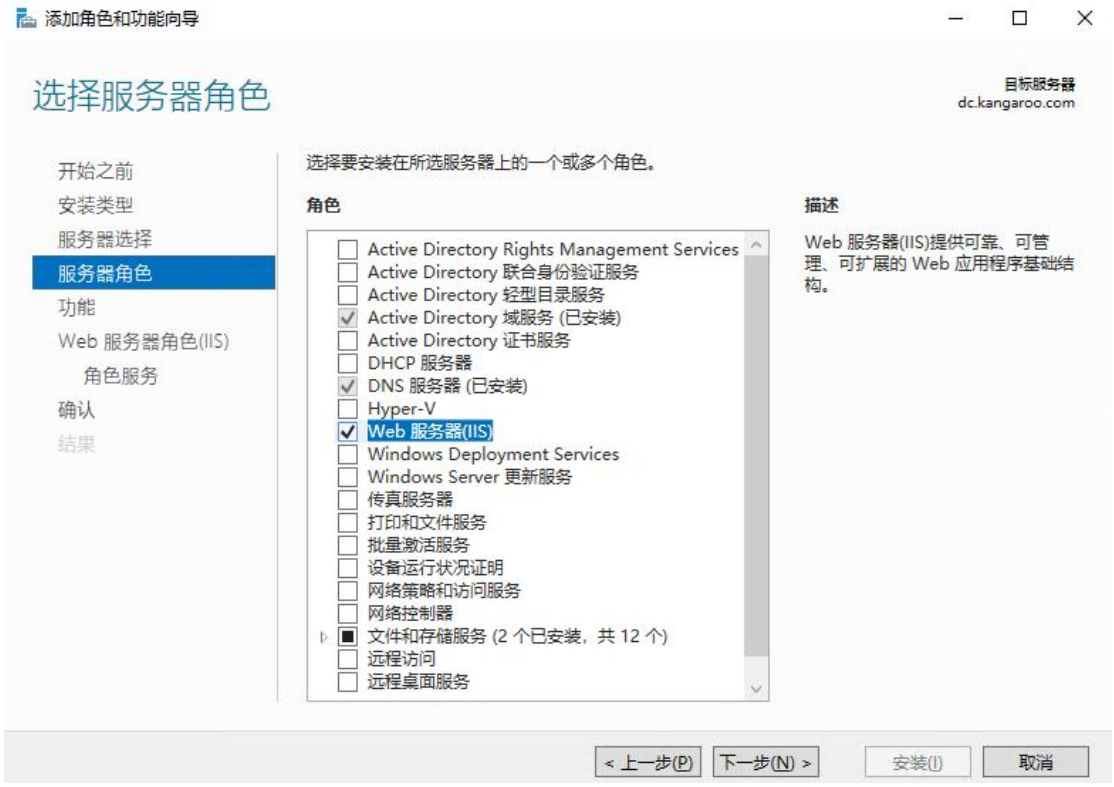
安装域控：

```
Install-ADDSForest -DomainName kangaroo.con
-SafeModeAdministratorPassword(ConvertTo-SecureString "Aa123456"
-AsPlainText -Force) -Force
```



Web 服务器部署

安装 IIS Web 服务



这里使用 dotnet 站点以便更好展示效果。

Web 服务器配置

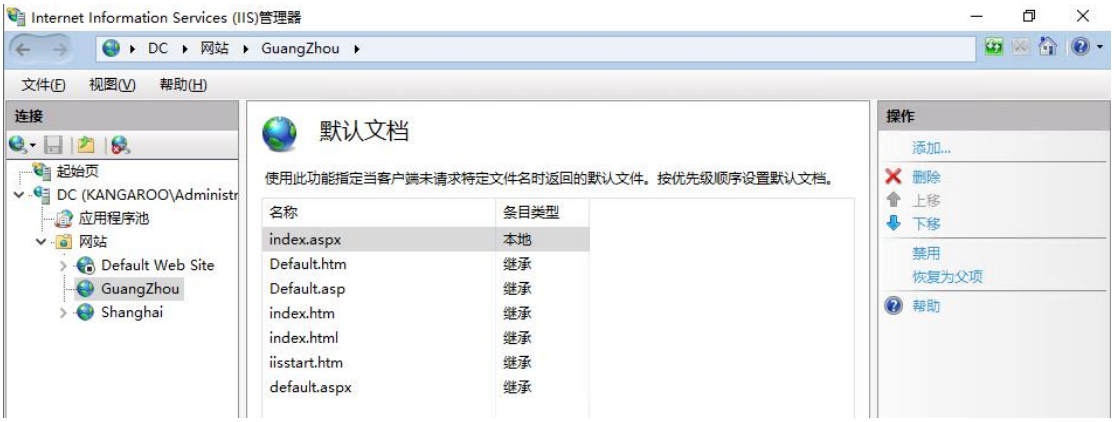
新建两个站点

站点 1 目录为 C:\www\Contents\GuangZhou

站点 2 目录为 C:\www\Contents\Shanghai


添加网站
网站名称(S):
Shanghai
应用程序池(L):
Shanghai
选择(E)...
内容目录
物理路径(P):
C:\www\Contents\Shanghai
...
作为"kangaroo\administrator"连接
连接为(C)...
测试设置(G)...
绑定
类型(T):
http
IP 地址(I):
10.10.20.110
端口(O):
80
主机名(H):
www.kangaroo.com
示例: www.contoso.com 或 marketing.contoso.com
立即启动网站(M)
确定
取消

设置两个站点默认主页



设置两个站点默认主页内容

站点 1 主页文件：

```
<html>
<body bgcolor="yellow">
<center>
<h2>Hello This Is Kangaroo GuangZhou Site !!!</h2>
<p><%Response.Write(now())%></p>
<p>IP: <%Response.Write(Request.ServerVariables("Local_Addr"))%></p>
</center>
</body>
</html>
```

站点 2 主页文件：

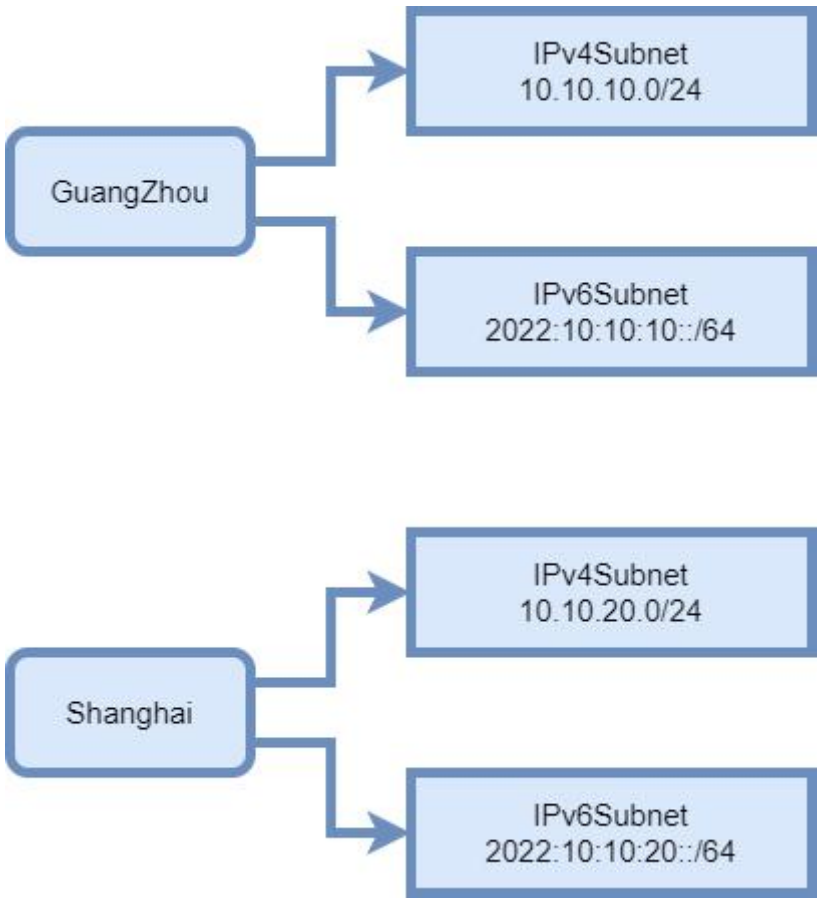
```
<html>
<body bgcolor="yellow">
<center>
<h2>Hello This Is Kangaroo Shanghai Site !!!</h2>
<p><%Response.Write(now())%></p>
```

```
<p>IP: <%Response.Write(Request.ServerVariables("Local_Addr"))%></p>
</center>
</body>
</html>
```

SmartDNS 服务器配置

创建 DNS 区域子网

在配置的过程中，我们会需要使用 Poweshell 进行配置。为了实现地理隔离，首先我们需要创建 DNSClientSubnet。换句话说，就是告诉 DNS 服务器，哪一个子网属于广州的客户端，哪一个属于上海的客户端。当我将这两个客户端的子网特征告诉 DNS 后，DNS 才知道如何判断转发请求。



创建广州与上海的子网：

```
Add-DnsServerClientSubnet -Name "GuangZhouSubnet" -IPv4Subnet
"10.10.10.0/24"
```

```
Add-DnsServerClientSubnet -Name "ShanghaiSubnet" -IPv4Subnet
"10.10.20.0/24"
```

创建完毕后，我们可以查询一下：

```
PS C:\Users\Administrator> Get-DnsServerClientSubnet

Name            IPV4Subnet      IPV6Subnet
----            ----------      ----------
GuangZhouSubnet {10.10.10.0/24}
ShanghaiSubnet  {10.10.20.0/24}


PS C:\Users\Administrator>
```

当然也可以配置 IPv6 子网：

```
Add-DnsServerClientSubnet -Name "GuangZhouSubnet" -IPv4Subnet
"10.10.10.0/24" -IPv6Subnet "2022:10:10:10::/64"
```

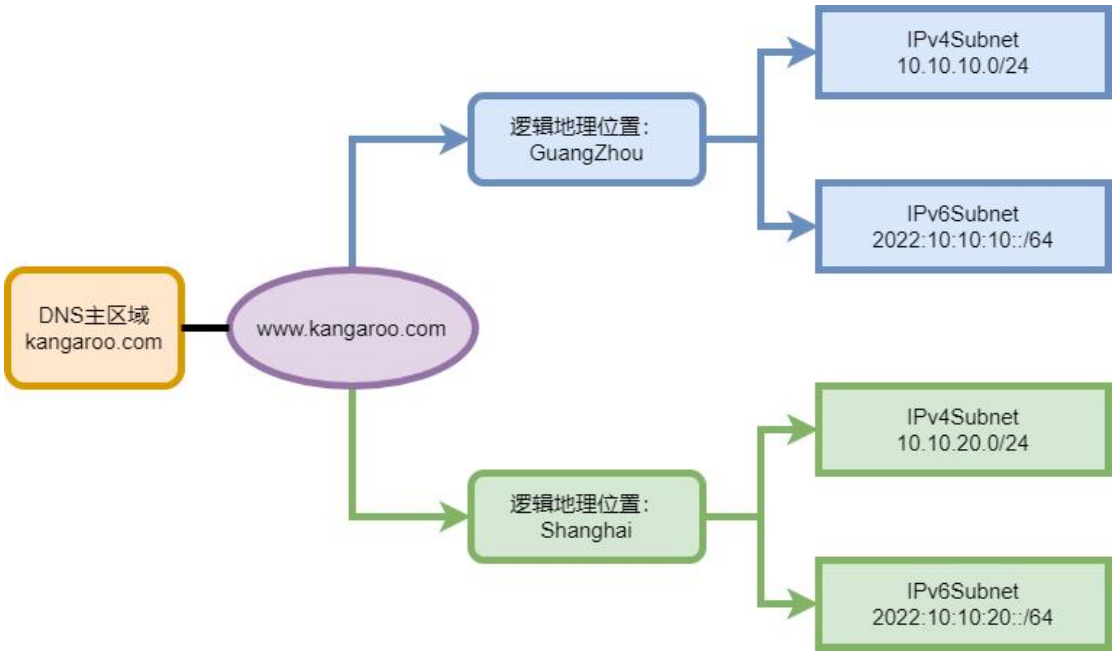
```
Add-DnsServerClientSubnet -Name "ShanghaiSubnet" -IPv4Subnet
"10.10.20.0/24" -IPv6Subnet "2022:10:10:20::/64"
```

```
PS C:\Users\Administrator> Get-DnsServerClientSubnet

Name            IPV4Subnet      IPV6Subnet
----            ----------      ----------
GuangZhouSubnet {10.10.10.0/24} {2022:10:10:10::/64}
ShanghaiSubnet  {10.10.20.0/24} {2022:10:10:20::/64}
```

创建 DNS 作用域

创建完子网后，下一步需要创建 DNSServerZoneScope，这一步极为重要！

我们需要在一个 DNS 区域中划分多个逻辑地理区域。我们需要理解这一个概念，举个例子，现在我们有一个名为 kangaroo.com 的 DNS 主区域，我们就要从 kangaroo.com 中再划分两个逻辑地理范围。例如，我们需要创建一个广州区域，一个上海区域。操作完毕后，我们就在同一个 DNS 主区域下面，包括了多个地理区域。




```
Add-DnsServerZoneScope -ZoneName "kangaroo.com" -Name "GuangZhou"
```

```
Add-DnsServerZoneScope -ZoneName "kangaroo.com" -Name "Shanghai"
```

创建完 DNS 作用域后，我们可以查看一下：

```
PS C:\Users\Administrator> Get-DnsServerZoneScope -ZoneName "kangaroo.com"

ZoneScope            FileName
---------            --------
kangaroo.com
GuangZhou
Shanghai
```

添加 DNS 记录

创建完逻辑地理区域后，我们必须将 Web 服务器的主机记录添加到两个作用域中。逻辑地理区域主要用来包含主机记录，串起来用以 DNS Policy 判断使用。

例如我们创建了逻辑区域 GuangZhou，那么我们就需要创建 GuangZhou 的 Web 服务器记录，创建主机记录的过程中，最主要的一步就是指定-ZoneScope。

指定参数之后创建出来的主机记录就会绑定在指定的地理区域内，之后创建策略，且只有策略中指定的子网范围客户端或特定客户端可以访问对应的“地理区域主机记录”。

就比如在作用域 GuangZhou，添加了 IP 地址为 10.10.10.110 www.kangaroo.com Web 服务器主机记录，那么这个主机记录就位于广州的数据中心；在上海的作用域范围中，

我们同样需要为上海的数据中心添加 IP 地址 10.10.20.110 www.kangaroo.com 的 Web 服务器主机记录。

在使用 Powershell 配置前，我们需要注意：我们定义的 A 记录名称为 www，所以我们的用户最终是以 www.kangaroo.com 来访问服务器的。

```
Add-DnsServerResourceRecord -ZoneName "kangaroo.com" -A -Name
"www" -IPv4Address "10.10.10.110" -ZoneScope "GuangZhou"
```

```
Add-DnsServerResourceRecord -ZoneName "kangaroo.com" -A -Name
"www" -IPv4Address "10.10.20.110" -ZoneScope "Shanghai"
```

创建完 DNS 记录后，我们可以查看一下：

```
PS C:\Users\Administrator> Get-DnsServerResourceRecord -ZoneName "kangaroo.com"

HostName                  RecordType Type     Timestamp           TimeToLive      RecordData
--------                  ---------- ----     ---------           ----------      ----------
@                         A          1        2022/11/21 0:00:00  00:10:00        10.10.10.110
@                         A          1        2022/11/21 0:00:00  00:10:00        10.10.20.110
@                         NS         2        0                   01:00:00        dc.kangaroo.com.
@                         SOA        6        0                   01:00:00        [61][dc.kangaroo.com.][hostmaster.kangaroo.com.]
_msdcs                    NS         2        0                   01:00:00        dc.kangaroo.com.
_gc._tcp.Default-First... SRV        33       2022/11/21 0:00:00  00:10:00        [0][100][3268][dc.kangaroo.com.]
_kerberos._tcp.Default... SRV        33       2022/11/21 0:00:00  00:10:00        [0][100][88][dc.kangaroo.com.]
_ldap._tcp.Default-Fir... SRV        33       2022/11/21 0:00:00  00:10:00        [0][100][389][dc.kangaroo.com.]
_gc._tcp                  SRV        33       2022/11/21 0:00:00  00:10:00        [0][100][3268][dc.kangaroo.com.]
_kerberos._tcp            SRV        33       2022/11/21 0:00:00  00:10:00        [0][100][88][dc.kangaroo.com.]
_kpasswd._tcp             SRV        33       2022/11/21 0:00:00  00:10:00        [0][100][464][dc.kangaroo.com.]
_ldap._tcp                SRV        33       2022/11/21 0:00:00  00:10:00        [0][100][389][dc.kangaroo.com.]
_kerberos._udp            SRV        33       2022/11/21 0:00:00  00:10:00        [0][100][88][dc.kangaroo.com.]
_kpasswd._udp             SRV        33       2022/11/21 0:00:00  00:10:00        [0][100][464][dc.kangaroo.com.]
dc                        A          1        0                   01:00:00        10.10.20.110
dc                        A          1        0                   01:00:00        10.10.10.110
DomainDnsZones            A          1        2022/11/21 0:00:00  00:10:00        10.10.20.110
DomainDnsZones            A          1        2022/11/21 0:00:00  00:10:00        10.10.10.110
_ldap._tcp.Default-Fir... SRV        33       2022/11/21 0:00:00  00:10:00        [0][100][389][dc.kangaroo.com.]
_ldap._tcp.DomainDnsZones SRV        33       2022/11/21 0:00:00  00:10:00        [0][100][389][dc.kangaroo.com.]
ForestDnsZones            A          1        2022/11/21 0:00:00  00:10:00        10.10.20.110
ForestDnsZones            A          1        2022/11/21 0:00:00  00:10:00        10.10.10.110
_ldap._tcp.Default-Fir... SRV        33       2022/11/21 0:00:00  00:10:00        [0][100][389][dc.kangaroo.com.]
_ldap._tcp.ForestDnsZones SRV        33       2022/11/21 0:00:00  00:10:00        [0][100][389][dc.kangaroo.com.]
gz                        A          1        2022/11/21 2:00:00  00:20:00        10.10.10.101
sh                        A          1        2022/11/21 0:00:00  00:20:00        10.10.20.101
```

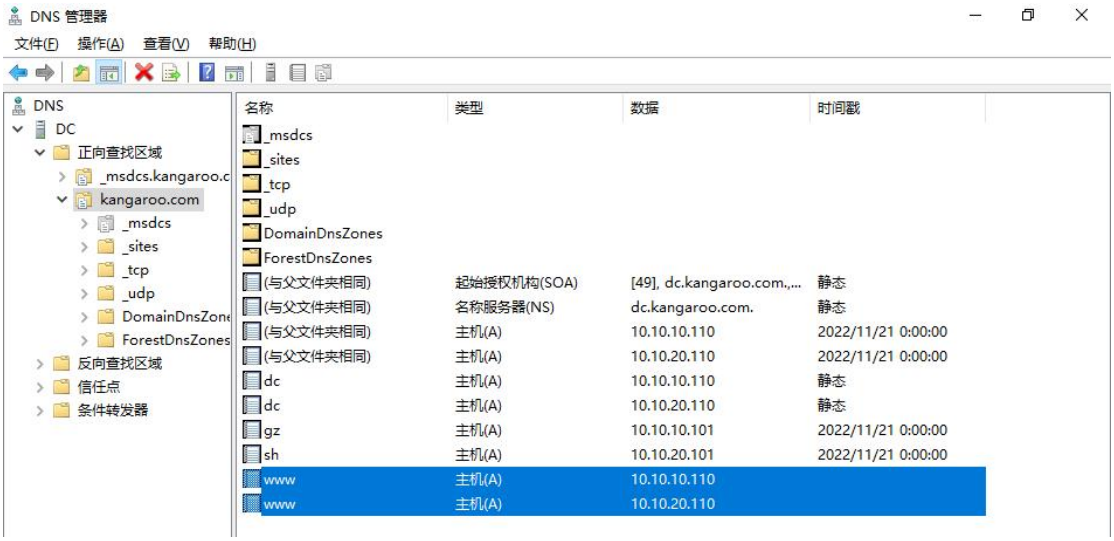
在上述操作中，我们创建的是基于 ZoneScope 的解析记录，但是我们需要注意的是。如果只给 ZoneScope 区域中添加记录，ZoneScope 以外没有记录的话。则除了自定义的子网用户外的访问都会出现无法解析的情况。于是，我们还需要在 ZoneScope 中增加解析记录。

这一步可以使用 GUI 创建，也可以使用 Powershell 创建：

```
Add-DnsServerResourceRecord -ZoneName "kangaroo.com" -A -Name
"www" -IPv4Address "10.10.10.110"
```

```
Add-DnsServerResourceRecord -ZoneName "kangaroo.com" -A -Name
"www" -IPv4Address "10.10.20.110"
```

两条 DNS 记录分别指向不同的 IP 地址



配置 DNS Policy

在子网，作用域，记录，以上条件配置好后，我们接下来就要创建 DNS 查询策略，这一步同样很重要。

在这里，我们来指定客户端的子网范围，eq 为 Equal，代表等于的意思。一旦客户端子网刚好成功与预定义的子网范围相匹配，则会有对应区域内的主机记录给予响应。

ZoneScope 中的参数后跟随一个 1，这个值会在后续多次用到。在本次案例中，我们所实现的是一个完全分流的场景，如果不完全分流，则会有一定比例的广州用户访问到上海的服务器。

反过来，则会由一定比例的上海用户访问到广州的服务器，更有甚者会走 DNS 流负载均衡。

当然，身为运维人员肯定是不希望这种事情的发生。我们为 ZoneScope 定义为 1，则表示广州/上海客户端百分百由广州/上海区域的主机记录给予响应。

在这里，我们仍然使用 Powershell 创建 DNS Policy：

```
Add-DnsServerQueryResolutionPolicy -Name "GuangZhouPolicy"
-Action ALLOW -ClientSubnet "eq,GuangZhouSubnet" -ZoneScope
"GuangZhou,1" -ZoneName "kangaroo.com"
```

```
Add-DnsServerQueryResolutionPolicy -Name "ShanghaiPolicy"
-Action ALLOW -ClientSubnet "eq,ShanghaiSubnet" -ZoneScope
"Shanghai,1" -ZoneName "kangaroo.com"
```

创建完 DNS Policy 后，我们可以查看一下：

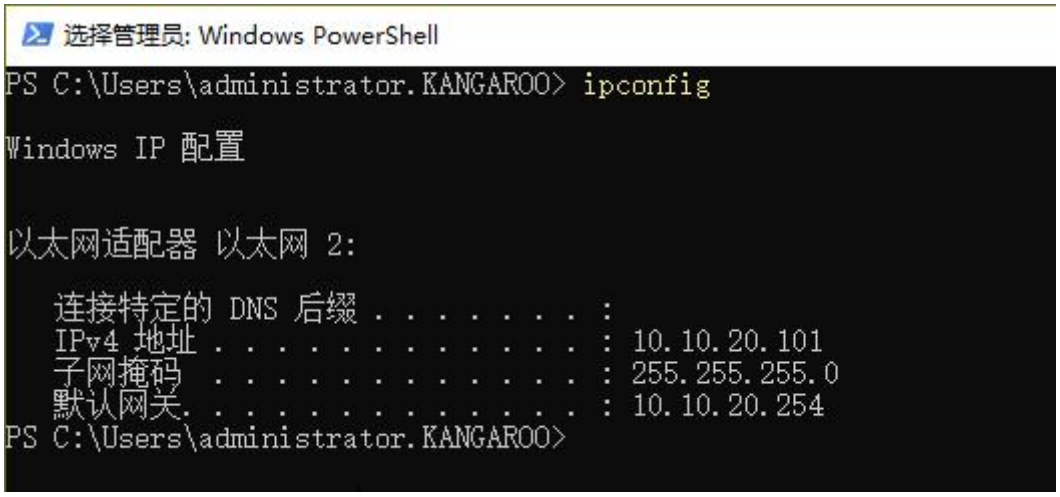
```
PS C:\Users\Administrator> Get-DnsServerQueryResolutionPolicy -ZoneName "kangaroo.com"

Name            ProcessingOrder IsEnabled Action
----            --------------- --------- ------
GuangZhouPolicy 1               True      Allow
ShanghaiPolicy  2               True      Allow
```

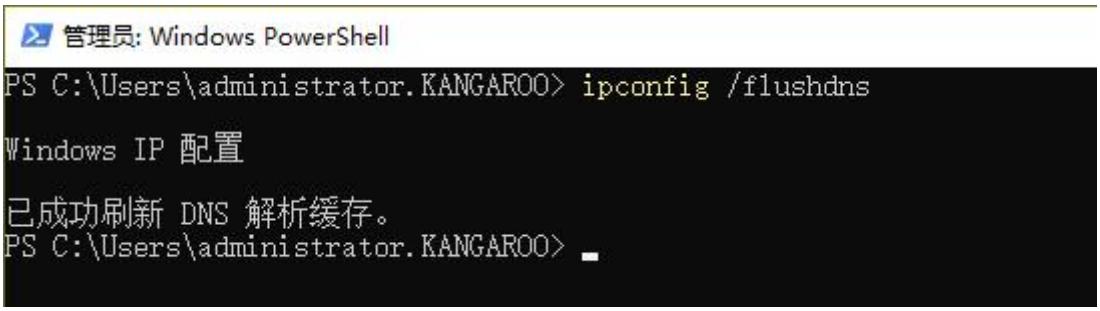
模拟测试:

模拟广州测试

模拟上海测试

由于这里我是用一台计算机来实现的,所以在模拟测试广州后我们需要重新刷新 DNS 缓存。





特殊案例:

指定客户端流量重定向

如果上述方式的测试结果不是很满意，这里使用特定客户端用作测试：

```
Add-DnsServerClientSubnet -Name "ClientGuangZhou-1" -IPv4Subnet
"10.10.10.101"
```

```
Add-DnsServerClientSubnet -Name "ClientGuangZhou-2" -IPv4Subnet
"10.10.10.102"
```

```
Add-DnsServerZoneScope -ZoneName "kangaroo.com" -Name
"ClientGuangZhou-1"
```

```
Add-DnsServerZoneScope -ZoneName "kangaroo.com" -Name
"ClientGuangZhou-2"
```

```
Add-DnsServerResourceRecord -ZoneName "kangaroo.com" -A -Name
"www" -IPv4Address "10.10.10.110" -ZoneScope "ClientGuangZhou-1"
```

```
Add-DnsServerResourceRecord -ZoneName "kangaroo.com" -A -Name
"www" -IPv4Address "10.10.20.110" -ZoneScope "ClientGuangZhou-2"
```

```
Add-DnsServerResourceRecord -ZoneName "kangaroo.com" -A -Name
"www" -IPv4Address "10.10.10.110"
```

```
Add-DnsServerResourceRecord -ZoneName "kangaroo.com" -A -Name
"www" -IPv4Address "10.10.20.110"
```

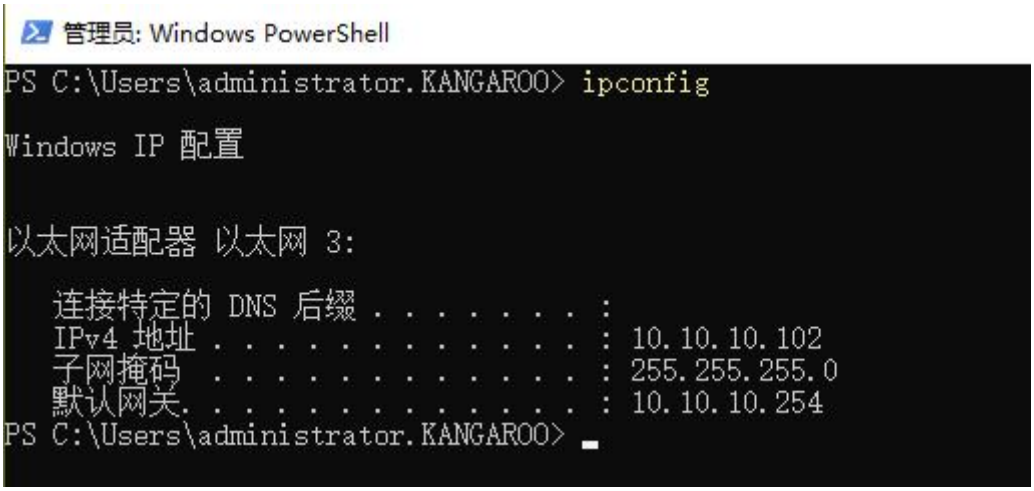
```
Add-DnsServerQueryResolutionPolicy -Name "ClientGuangZhou-1"
-Action ALLOW -ClientSubnet "eq,ClientGuangZhou-1" -ZoneScope
"ClientGuangZhou-1,1" -ZoneName "kangaroo.com"
```

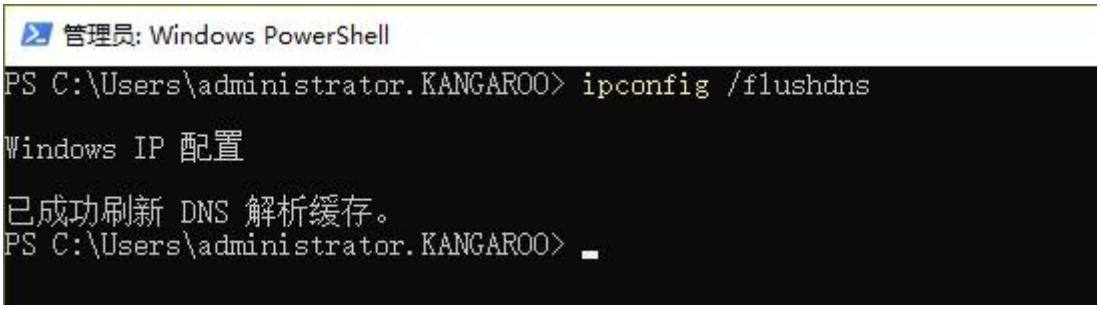
```
Add-DnsServerQueryResolutionPolicy -Name "ClientGuangZhou-2"
-Action ALLOW -ClientSubnet "eq,ClientGuangZhou-2" -ZoneScope
"ClientGuangZhou-2,1" -ZoneName "kangaroo.com"
```

模拟广州测试

模拟上海测试

由于这里我是用一台计算机来实现的，所以在模拟测试广州后我们需要重新刷新 DNS 缓存。





至此，Windows 的智能 DNS 就配置完成了，后续还有更多 DNS 相关的案例展示。敬请期待。

文档参照：

Use DNS Policy for Geo-Location Based Traffic Management with Primary Servers | Microsoft Learn

SmartDNS 主辅服务器配置

在 Internet 的基础架构中，DNS 服务器广泛部署于主-辅模型中，其中可写的区域副本存储在更为安全的主 DNS 中，只读副本保存在多个 DNS 辅助服务器中。

辅助服务器使用区域传输协议权威传输 （AXFR） 和增量区域传输 （IXFR） 来请求和接收区域更新，其中包括对主 DNS 服务器上区域的新更改。

环境:

镜像信息：

系统	系统版本	发行版本
Windows	WindowsServer2022	21H2

网络信息表

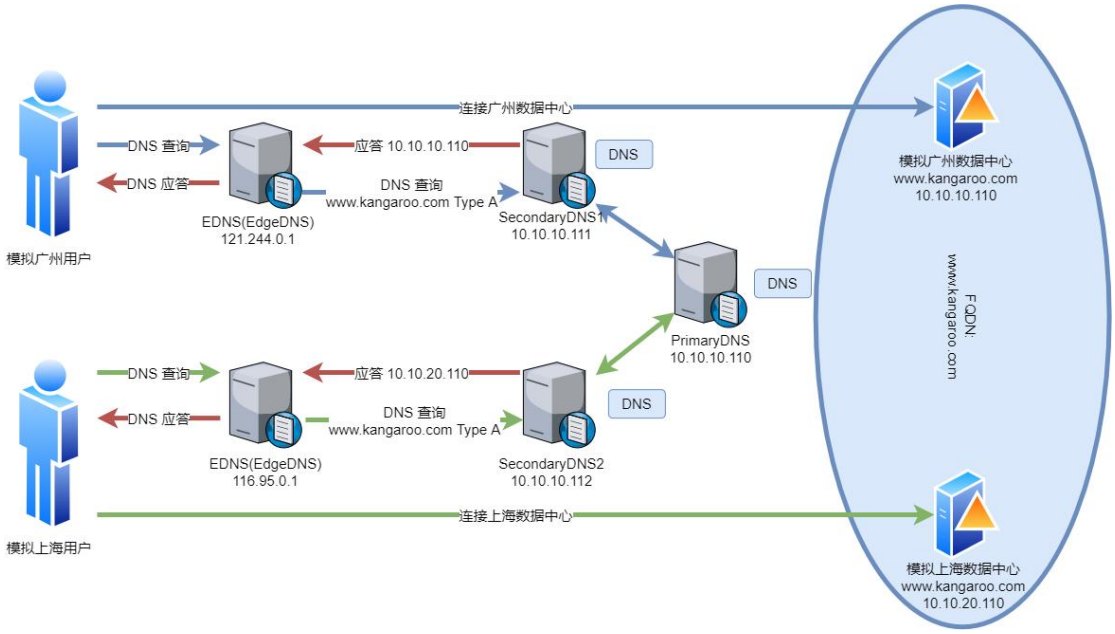
网络名称	VlanID	子网名称	网络地址	网关	IPv4 地址池

Network10	10	Subnet10	10.10.10.0/24	10.10.10.254	10.10.10.100-10.10.10.200
Network20	20	Subnet20	10.10.20.0/24	10.10.20.254	10.10.20.100-10.10.20.200

实例信息表

实例名称	IPv4 地址	完全合格域名
windows1	10.10.10.110 10.10.20.110	dc.kangaroo.com
windows2	10.10.10.111 10.10.10.112	bdc.kangaroo.com
windows3	10.10.10.101 10.10.10.102(Secondary) 10.10.20.101	client.kangaroo.com

拓扑结构



拓扑思路来源：
Use DNS Policy for Geo-Location Based Traffic Management with Primary-Secondary Deployments | Microsoft Learn

需求分析:

您做为一名云服务商，为各地区用户提供 Web 服务解析方案，在全国范围内拥有一个名为 www.kangaroo.com 的网站。

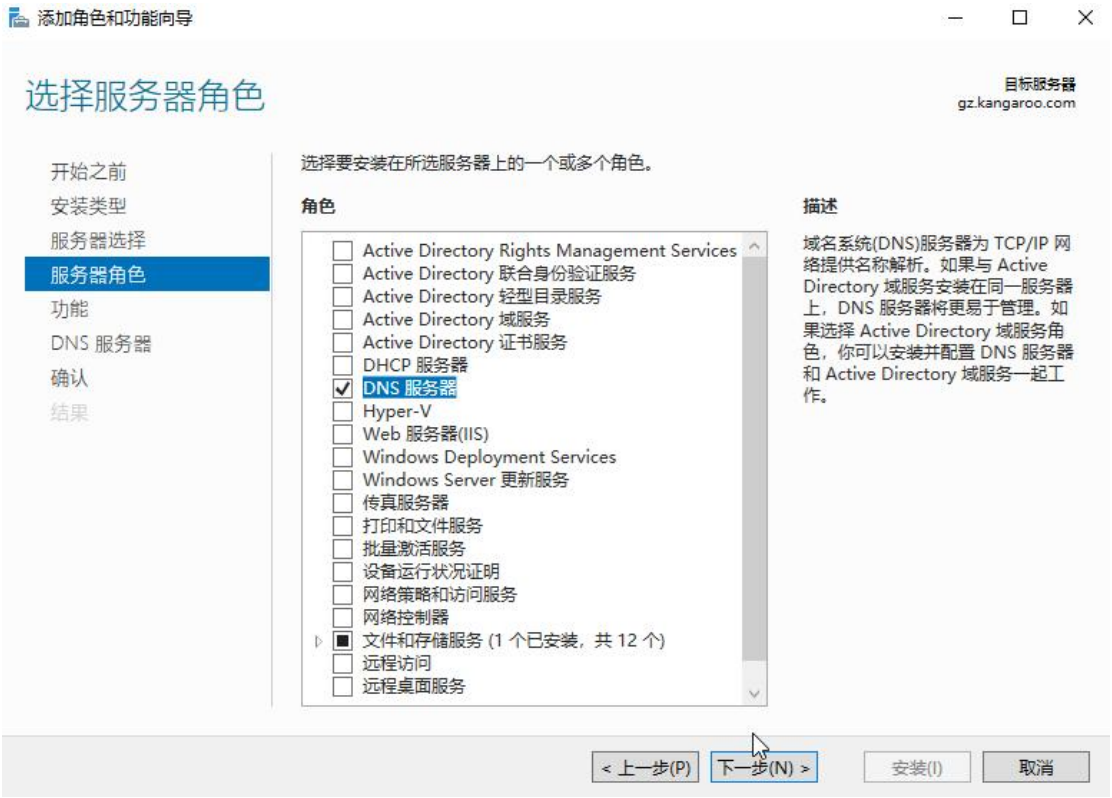
为减少国内不同地区用户的访问响应，您在广州，上海分别部署了数据中心。Kangaroo 希望广州用户的流量重定向到广州的数据中心，上海用户的流量重定向到上海的数据中心。

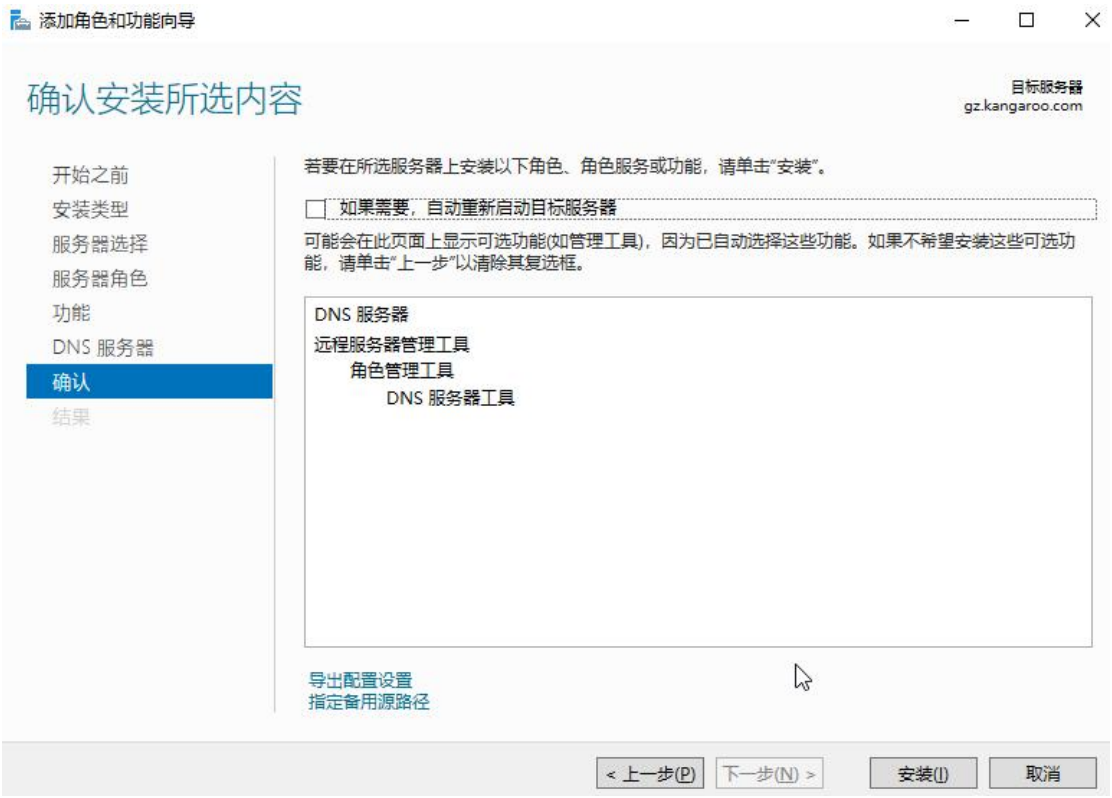
随着用户日益增长的海量请求需要和高时延，高并发的不同需求之间的矛盾。您在广州与上海这两座城市分别新部署了两台 DNS 服务器：辅助服务器 1，IP 地址为 10.10.10.111；辅助服务器 2，IP 地址为 10.10.10.112。这两个辅助服务器在不同地区中充当 DNS 使用。

主服务器上存在一个可写的副本(IP 地址为 10.10.10.110)，假定管理员对区域进行了更改。DNS 会使用 AXFR 和 IXFR 协议定期将区域传输到辅助服务器，辅助服务器始终会即使同步主服务器中的更改，这还有一个专业术语——动态更新(Dynamic Upate)。

安装 DNS 功能

新部署的 DNS 服务器可以按需加入到域环境中，加入至域环境中，下一步就要为这两台计算机安装 DNS 功能。





创建 DNS 辅助区域

由于两台 DNS 服务器均以加入至域环境中，在这里我们可以直接指定 ComputerName 通过 WMI 远程操作服务器。

下面的操作都会使用 Powershell 命令进行创建，GUI 点下鼠标就可以了，这里不多演示。

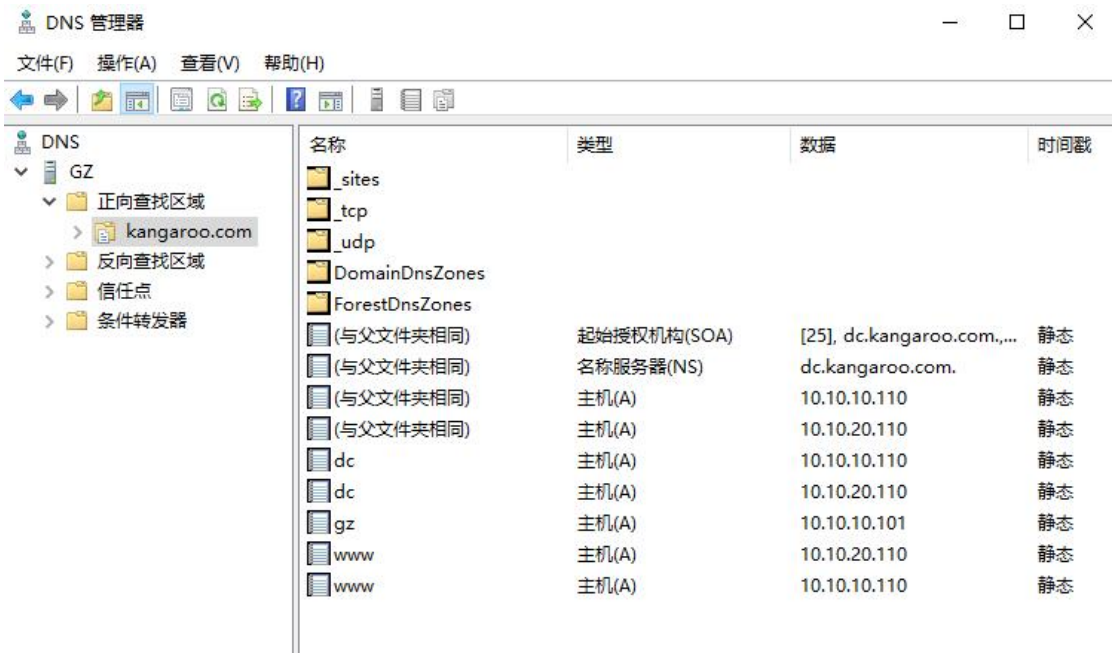
```
Add-DnsServerSecondaryZone -Name "kangaroo.com" -ZoneFile
"kangaroo.com.dns" -MasterServers 10.10.10.110 -ComputerName
SecondaryServer1
```

```
Add-DnsServerSecondaryZone -Name "kangaroo.com" -ZoneFile
"kangaroo.com.dns" -MasterServers 10.10.10.110 -ComputerName
SecondaryServer2
```

设置 DNS 主区域传输

这一步如果不配置，辅助 DNS 则不会被运行加载主要区域。

```
Set-DnsServerPrimaryZone -Name "kangaroo.com" -Notify Notify
-SecondaryServers "10.10.10.111,10.10.10.112" -SecureSecondaries
TransferToSecureServers -ComputerName dc
```



设置 DNS 区域子网

将客户端子网从主服务器复制到辅助服务器中。此处仍然使用 Powershell 来进行操作：

```
Get-DnsServerClientSubnet -ComputerName dc|
Add-DnsServerClientSubnet -ComputerName SecondaryServer1
```

```
Get-DnsServerClientSubnet -ComputerName dc |
Add-DnsServerClientSubnet -ComputerName SecondaryServer2
```

创建辅助 DNS 作用域

在 DNS 中，区域作用域也开始从主服务器发送 XFR 请求。管理员对主服务器上的区域作用域进行更改时，将向辅助服务器发送包含区域作用域信息的通知。随后，辅助服务器可以使用增量或更改更新其区域作用域。

```
Get-DnsServerZoneScope -ZoneName "kangaroo.com" -ComputerName dc |
Add-DnsServerZoneScope -ZoneName "kangaroo.com" -ComputerName
SecondaryServer1 -ErrorAction Ignore
```

```
Get-DnsServerZoneScope -ZoneName "kangaroo.com" -ComputerName dc
| Add-DnsServerZoneScope -ZoneName "kangaroo.com" -ComputerName
SecondaryServer2 -ErrorAction Ignore
```

配置 DNS Policy

在子网，作用域，记录，以上条件配置好后，我们接下来就要创建 DNS 查询策略。一旦客户端子网刚好成功与预定义的子网范围相匹配，则会有对应区域内的主机记录给予响应。在前面章节中我们配置完毕的 DNS Policy 能被直接引用：

```
$policy = Get-DnsServerQueryResolutionPolicy -ZoneName
"kangaroo.com" -ComputerName dc
```

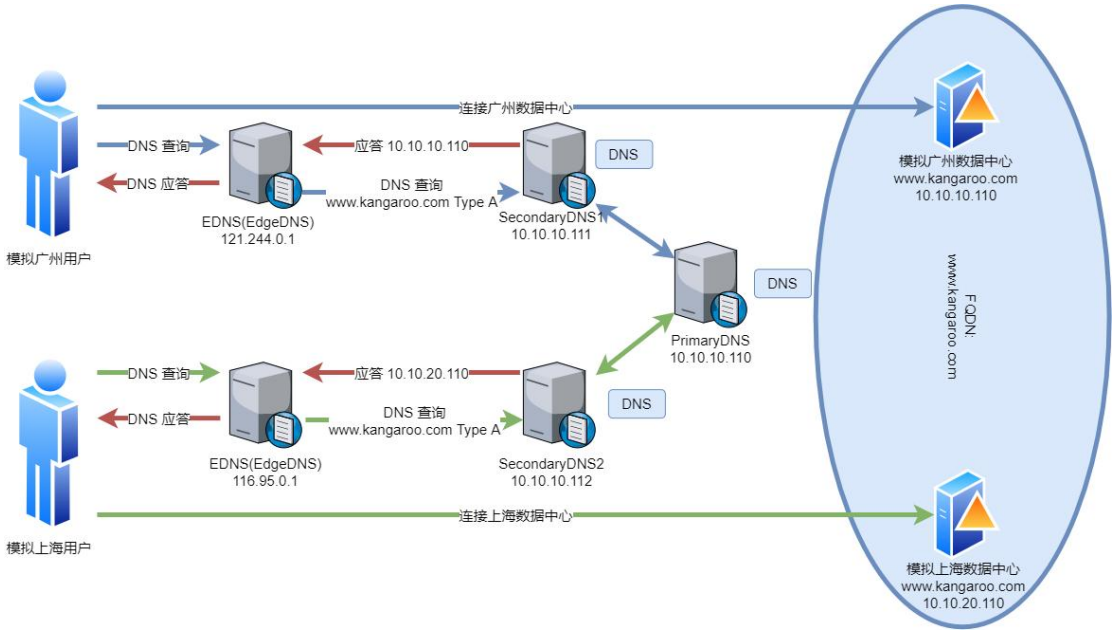
```
$policy | Add-DnsServerQueryResolutionPolicy -ZoneName
"kangaroo.com" -ComputerName SecondaryServer1
```

```
$policy | Add-DnsServerQueryResolutionPolicy -ZoneName
"kangaroo.com" -ComputerName SecondaryServer2
```

现在，我们在辅助 DNS 服务器配置了 DNS 策略，那这些 DNS 辅助服务器将会以定义好的逻辑地理位置重定向流量。

当用户向边缘 DNS 服务器发送查询请求时，边缘 DNS 就会将请求发送至上级 DNS。上级 DNS 服务器收到域名解析查询时，DNS 服务器会根据配置的 DNS 策略判断 DNS 请求中的字段。如果名称解析请求中的源 IP 地址与策略相匹配，则关联的区域范围将会用于响应查询，并将用户流量重定向到地理位置上最接近他们的数据中心。

在实际的生产环境中，大多数情况会和下述拓扑一致：


连接广州数据中心
DNS 查询
DNS 应答
EDNS(EdgeDNS)
121.244.0.1
应答 10.10.10.110
DNS 查询
www.kangaroo.com Type A
SecondaryDNS1
10.10.10.111
DNS
模拟广州用户
模拟广州数据中心
www.kangaroo.com
10.10.10.110
PrimaryDNS
10.10.10.110
DNS
FQDN:
www.kangaroo.com
DNS 查询
DNS 应答
EDNS(EdgeDNS)
116.95.0.1
应答 10.10.20.110
DNS 查询
www.kangaroo.com Type A
SecondaryDNS2
10.10.10.112
DNS
模拟上海用户
连接上海数据中心
模拟上海数据中心
www.kangaroo.com
10.10.20.110