

8

第 8 章 管理域与林信任

两个域之间具备信任关系后，双方的用户便可以访问对方域内的资源并利用对方域的成员计算机登录。

- 域与林信任概述
- 建立快捷方式信任
- 建立林信任
- 建立外部信任
- 管理与删除信任



8.1 域与林信任概述

信任 (trust) 是两个域之间沟通的桥梁，两个域相互信任之后，双方的用户便可以访问对方域内的资源，利用对方域的成员计算机登录。

8.1.1 信任域与受信任域

以图8-1-1来说明，当A域信任B域后：

- ✎ A域被称为**信任域 (trusting domain)**，而B域被称为**受信任域 (trusted domain)**。
- ✎ B域的用户只要具备适当的权限，就可以访问A域内的资源，例如文件、打印机等，因此A域被称为**资源域 (resources domain)**，而B域被称为**账户域 (accounts domain)**。
- ✎ B域的用户可以到A域的成员计算机上登录。

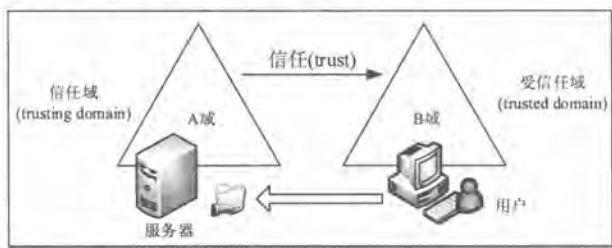


图 8-1-1

注意

A域的用户却不能访问B域内资源、也不能到B域的成员计算机上登录，除非B域也信任A域。

- ✎ 图中的信任关系是**A域信任B域的单向信任 (one-way trust)**，如果B域也同时信任A域的话，则我们将其称为**双向信任 (two-way trust)**，此时双方都可以访问对方的资源，也可以利用对方的成员计算机登录。

8.1.2 跨域访问资源的流程

当用户在某台计算机登录时，系统必须验证用户身份，而在验证身份的过程中，除了需要确认用户名与密码无误外，系统还会为用户建立一个**access token**（访问令牌），其中包含着该用户账户的SID（Security Identifier）、用户所隶属的所有组的SID等数据。用户取得这个access token后，当他要访问本地计算机内的资源时（例如文件），便会出示access



token，而系统会根据access token内的SID数据来决定用户拥有何种权限。

附注

负责验证用户身份的服务是Local Security Authority (LSA)，而验证用户身份的方法分为Kerberos与NTLM两种。

同理当用户连接网络上其他计算机时，这台计算机也会为该用户建立一个access token，而当用户要访问此网络计算机内的资源时（例如共享文件夹），便会出示access token，这台网络计算机便会根据access token内的SID数据，来决定用户拥有何种访问权限。

注意

由于access token是在登录（本地登录或网络登录）时建立的，因此如果在用户登录成功之后，才将用户加入到组的话，此时该access token内并没有包含这个组的SID，因此用户也不会具备该组所拥有的权限。用户必须注销再重新登录，以便重新建立一个包含这个组SID的access token。

图8-1-2为一个域树，图中父域（sayms.local）与两个子域（sh.sayms.local与cn.sayms.local）之间有着双向信任关系。我们利用此图来解释域信任与用户身份验证之间的关系，而且是要通过子域cn.sayms.local信任根域sayms.local、根域sayms.local信任子域sh.sayms.local这条信任路径（trust path），来解释当位于子域sh.sayms.local内的用户George要访问另外一个子域cn.sayms.local内的资源时，系统是如何来验证用户身份与如何来建立access token。

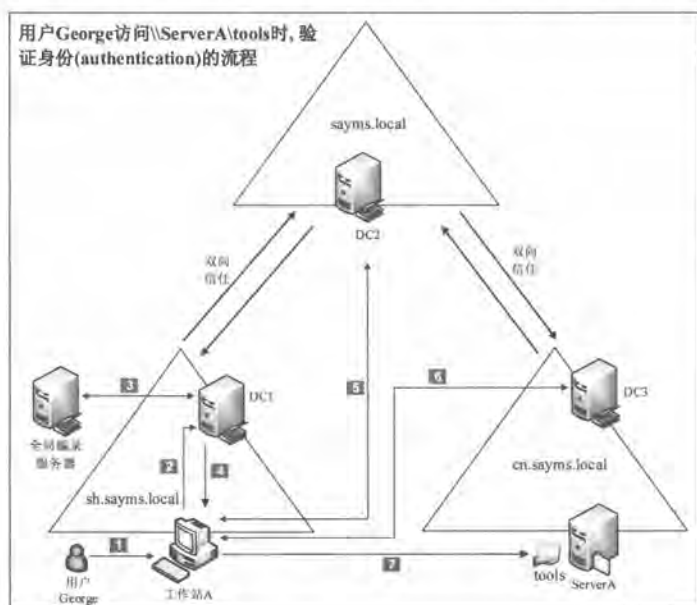


图 8-1-2



图中George是子域sh.sayms.local的用户，而ServerA位于另一个子域cn.sayms.local内，当George要访问共享文件夹\\ServerA\tools时，George的计算机需要先取得一个用来与ServerA通信的**service ticket**（服务票证）。George的计算机取得service ticket并与ServerA通信成功后，ServerA会发放一个**access token**给George，以便让George利用这个access token来访问位于ServerA内的资源。以下详细说明其流程（请参照图8-1-2中的数字）：

（1）George利用所属域sh.sayms.local内的用户账户登录。

当George在工作站A登录时，会由其所属域的域控制器DC1来负责验证George的用户名称与密码，同时发放一个**Ticket-Granting-Ticket**（TGT，索票凭证）给George，以便让George利用TGT来索取一个用来与ServerA通讯的**service ticket**。用户George登录成功后，开始访问共享文件夹\\ServerA\tools的流程。

附注

可以将TGT视为**通行证**，用户必须拥有TGT后，才可以索取**service ticket**。

（2）工作站A会向所属域内扮演**Key Distribution Center**（KDC）角色的域控制器DC1，索取一个用来与服务器ServerA通信的**service ticket**。

（3）域控制器DC1检查其数据库后，发现ServerA并不在它的域内（sh.sayms.local），因此转向全局编录服务器来查询ServerA是位于哪一个域内。

全局编录服务器根据其AD DS数据库的记录，得知服务器ServerA是位于子域cn.sayms.local内，便将此信息通告域控制器DC1。

（4）域控制器DC1得知ServerA是位于域cn.sayms.local后，它会根据信任路径，通知工作站A去找信任域sayms.local的域控制器DC2。

（5）工作站A向域sayms.local的域控制器DC2查询域cn.sayms.local的域控制器。域控制器DC2通知工作站A去找域控制器DC3。

（6）工作站A向域控制器DC3索取一个能够与ServerA通讯的**service ticket**。域控制器DC3发放**service ticket**给工作站A。

（7）工作站A取得**service ticket**后，它会将**service ticket**发送给ServerA。ServerA读取**service ticket**内的用户身份数据后，会根据这些数据来建立**access token**，然后将**access token**发送给用户George。

从上面的流程可知，当用户要访问另外一个域内的资源时，系统会根据信任路径，依序跟每一个域内的域控制器交互后，才能够取得**access token**，并依据**access token**内的SID数据来决定用户拥有何种权限。

8.1.3 信任的种类

总共有6 种类型的信任关系，如表8-1-1所示，其中前面两种是在新建域时，由系统自动建立的，其他4种必须自行手动建立。

表8-1-1

信任类型名称	传递性	单向或双向
父—子（Parent-Child）	是	双向
树状—根目录（Tree-Root）	是	双向
快捷方式（Shortcut）	是（部分）	单向或双向
林（Forest）	是（部分）	单向或双向
外部（External）	否	单向或双向
领域（Realm）	是或否	单向或双向

1. 父—子信任

同一个域树中，父域与子域之间的信任关系称为父—子信任，例如图8-1-3中的sayms.local与sh.sayms.local之间、sayms.local与cn.sayms.local之间、sayiis.local与hk.sayiis.local之间，这个信任关系是自动建立的，也就是说当在域树内新建任何一个AD DS子域后，此子域便会自动信任其上一层的父域，同时父域也会自动信任这个新的子域，而且此信任关系具备双向可传递性（相关说明可参考第1章）。

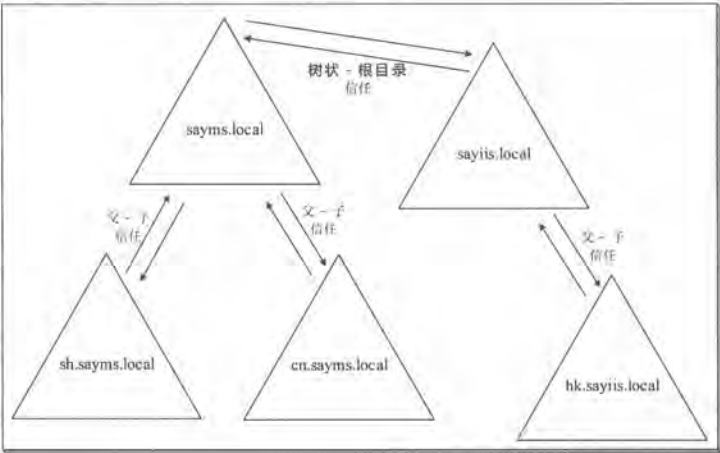


图 8-1-3

2. 树状—根目录信任

同一个林中，林根域（forest root domain，如图8-1-3中的sayms.local）与其他域树的根域（tree root domain，如图中的sayiis.local）之间的信任关系被称为树状—根目录信任。



此信任关系是自动建立的，也就是说当在现有林中新建一个域树后，**林根域**与这个**新域树根域**之间会自动相互信任对方，而且这些信任关系具备**双向可传递性**，因此双方的所有域之间都会自动双向信任。

3. 快捷方式信任

快捷方式信任可以缩短验证用户身份的时间。例如若图8-1-4中域cn.sayms.local内的用户经常需要访问域hk.sayiis.local内的资源，如果按照一般验证用户身份所走的信任路径，就必须浪费时间经过域sayiis.local与sayms.local，然后再传递给cn.sayms.local的域控制器来验证，此时如果我们在域cn.sayms.local与hk.sayiis.local之间建立一个**快捷方式信任**，也就是让域hk.sayiis.local直接信任cn.sayms.local，则域hk.sayiis.local的域控制器在验证域cn.sayms.local的用户身份时，就可以跳过域sayiis.local与sayms.local，也就是直接传递给域cn.sayms.local的域控制器来验证，如此便可以节省时间。

可以自行决定要建立单向或双向快捷方式信任，例如图中的**快捷方式信任**是单向的，也就是**域hk.sayiis.local信任域cn.sayms.local**，它让域cn.sayms.local的用户在访问域hk.sayiis.local内的资源时，可以走**快捷方式信任**的路径来验证用户的身份。由于是单向快捷方式信任，因此反过来域hk.sayiis.local的用户在访问域cn.sayms.local内的资源时，却无法走这个**快捷方式信任**的路径，除非域cn.sayms.local也**快捷方式信任**域hk.sayiis.local。

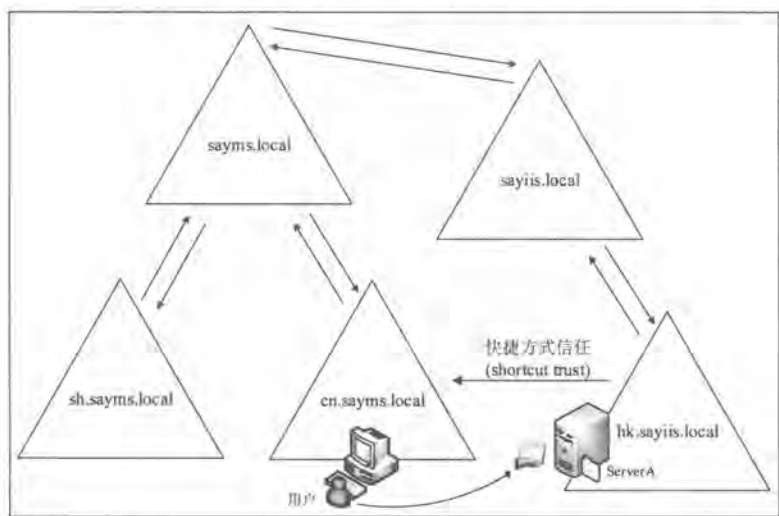


图 8-1-4

注意快捷方式信任仅有部分可传递性，也就是只会向下延伸，不会向上延伸，以图8-1-5来说明，图中在D域建立一个**快捷方式信任**到F域，这个快捷方式信任会自动向下延伸到G域，因此D域的域控制器在验证G域的用户身份时，可以走【D域→F域→G域】的快捷方式路径。然而D域的域控制器在验证E域的用户身份时，仍然需走【D域→A域→E域】的路径，也



就是通过父—子信任【D域→A域】与树状—根目录信任【A域→E域】的路径。

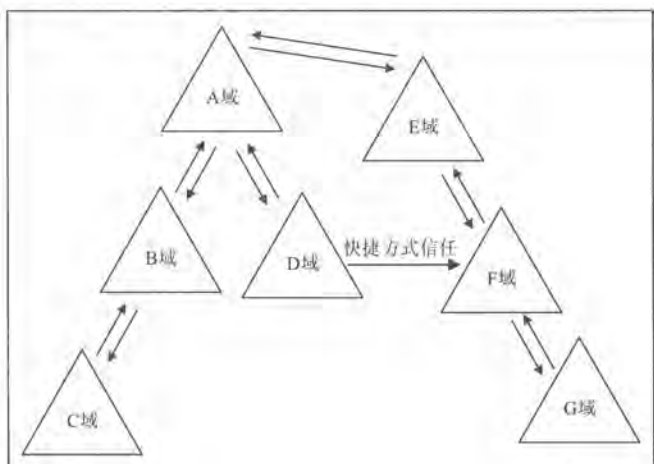


图 8-1-5

4. 林信任

两个林之间可以通过**林信任**来建立信任关系，以便让不同林内的用户可以相互访问对方的资源。可以自行决定要建立单向或双向的信任关系，例如图8-1-6中我们在两个林 sayms.local 与 say365.local 之间建立了双向信任关系，由于**林信任**具备**双向可传递**的特性，因此会让两个林中的所有域之间都相互信任，也就是说所有域内的用户都可以访问其他域内的资源，不论此域是位于哪一个林内。

注意林信任仅有部分可传递性，也就是说两个林之间的**林信任**关系并无法自动的延伸到其他第3个林，例如虽然在林A与林B之间建立了**林信任**，同时也在林B与林C之间建立了**林信任**，但是林A与林C之间并不会自动建立信任关系。

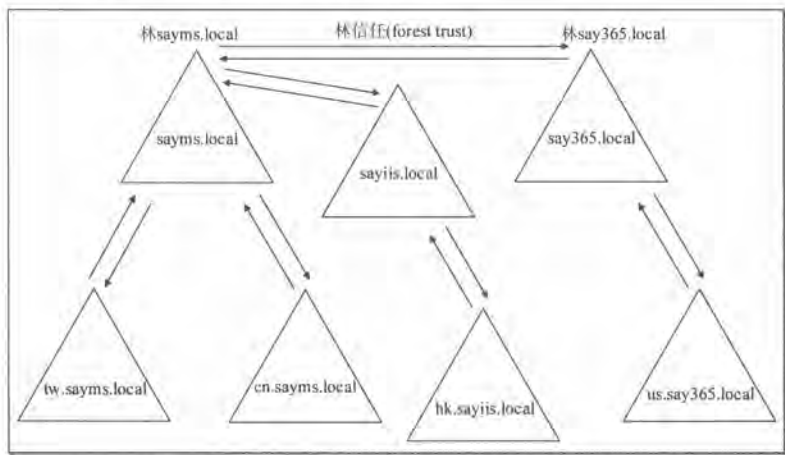


图 8-1-6



5. 外部信任

分别位于两个林内的域之间可以通过**外部信任**来建立信任关系。可以自行决定要建立单向或双向信任关系，例如图8-1-7中两个林sayms.local与sayexg.local之间原本并没有信任关系，但是在域sayiis.local与域sayexg.local之间建立了双向的**外部信任**关系。由于**外部信任**并不具备**传递性**，因此图中除了sayiis.local与sayexg.local之间外，其他例如sayiis.local与uk.sayexg.local、hk.sayiis.local与uk.sayexg.local等之间并不具备信任关系。

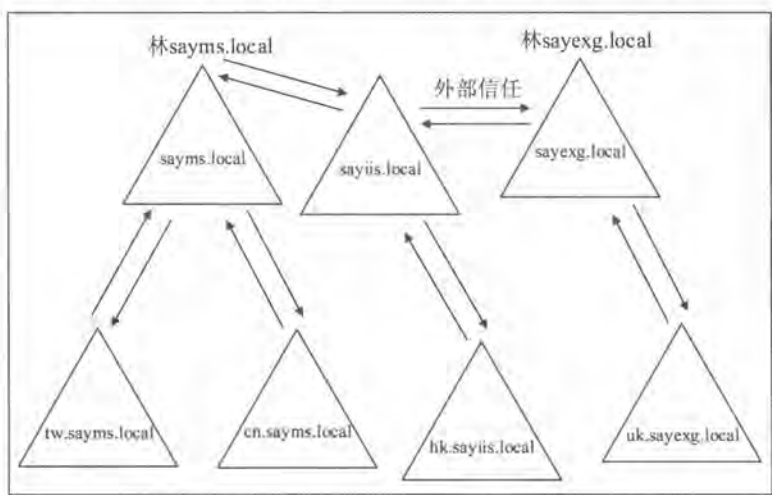


图 8-1-7

6. 领域信任

AD DS域可以与**非Windows系统**（例如UNIX）的Kerberos领域之间建立信任关系，这个信任关系称为**领域信任**。这种跨平台的信任关系，让AD DS域能够与其他Kerberos系统相互通信。**领域信任**可以是单向或双向，而且可以从**可传递性**切换到**不可传递性**，也可以从**不可传递性**切换到**可传递性**。

8.1.4 建立信任前的注意事项

前面6种信任关系中，**父-子信任**是在新建子域时自动建立的，而**树状一根目录信任**则是在新建域树时自动建立的，其他的4种信任关系必须手动建立。请先了解以下事项，以减少在建立信任关系时的困扰：

- 建立信任就是在建立两个不同域之间的沟通桥梁，从域管理的角度来看，两个域各需要有一个拥有适当权限的用户，在各自域中分别做一些设置，以完成双方域之间信任关系的建立工作。其中**信任域**一方的系统管理员，需要为此信任关系建立一个**传出信任**（outgoing trust）；而**受信任域**一方的系统管理员，则需要为此信任关系建立一



- 个传入信任（incoming trust）。传出信任与传入信任可视为此信任关系的两个端点。
- 以建立图8-1-8中A域信任B域的单向信任进行说明，我们需在A域建立一个传出信任，相对也需要在B域建立一个传入信任。也就是说在A域建立一个传出到B域的信任，同时相对也需要在B域建立一个让A域传入的信任。

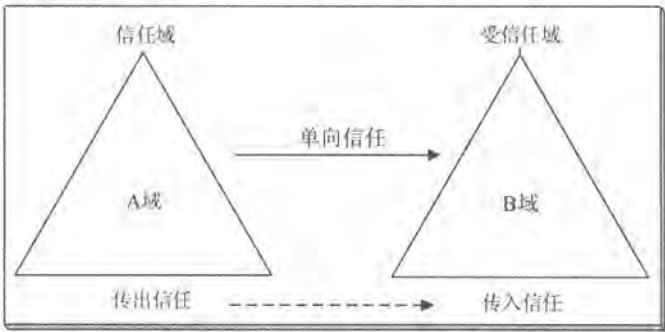


图 8-1-8

- 在利用新建信任向导来建立图中的单向信任关系时，可以选择先单独建立A域的传出信任，然后再另外单独建立B域的传入信任；或是选择同时建立A域的传出信任与B域的传入信任：
- 如果是分别单独建立这两个信任的话，则需要在A域的传出信任与B域的传入信任设置相同的信任密码。
 - 如果是同时建立这两个信任的话，则在信任过程中并不需要设置信任密码，但需要在这两个域都拥有适当权限，默认是Domain Admins或Enterprise Admins组的成员拥有此权限。
- 以建立图8-1-9的A域信任B域，同时B域也信任A域的双向信任来说，我们必须在A域同时建立传出信任与传入信任，其中的传出信任是用来信任B域，而传入信任是要让B域可以信任A域。相对也必须在B域建立传入信任与传出信任。

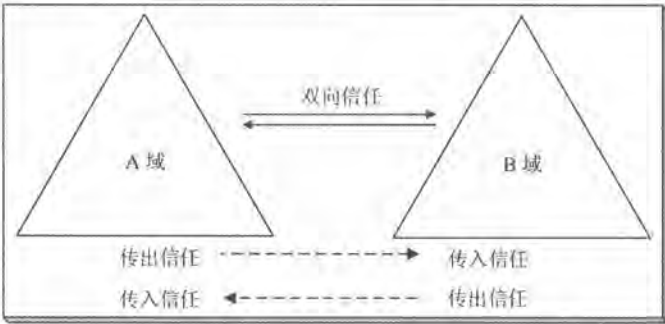


图 8-1-9

在利用新建信任向导来建立图中的双向信任关系时，可以单独先建立A域的传出信任与传入信任，然后再另外单独建立B域的传入信任与传出信任；或选择同时建立A域与B域的传入信任、传出信任：



- 如果是分别单独建立A域与B域的传出信任、传入信任的话，则需要要在A域与B域设置相同的信任密码。
- 如果是同时建立A域与B域的传出信任、传入信任的话，则在信任过程中并不需要设置信任密码，但需要在这两个域都拥有适当的权限，默认是Domain Admins或Enterprise Admins组的成员拥有此权限。
- 两个域之间在建立信任关系时，相互之间可以利用DNS名称或NetBIOS名称来指定对方的域名：
 - 如果是利用DNS域名，则相互之间需通过DNS服务器来查询对方的域控制器。
 - 如果是利用NetBIOS域名，则可以通过广播或WINS服务器来查询。但是广播消息无法跨越到另外一个网络，因此如果通过广播来查询的话，则两个域的域控制器必须位于同一个网络内。如果是通过WINS服务器（可参考Windows Server 2016网络与网站建置实务这本书的电子书）来查询的话，则两个域的域控制器可以不需要在同一个网络内。
- 除了利用新建信任向导来建立两个域或林之间的信任外，也可以利用netdom trust命令来新建、删除或管理信任关系。

8.2 建立快捷方式信任

以下利用建立图8-2-1中域hk.sayiis.local信任域cn.sayms.local的单向快捷方式信任来说明。请务必先参考8-1节中建立信任前的注意事项的说明后，再继续以下的步骤。

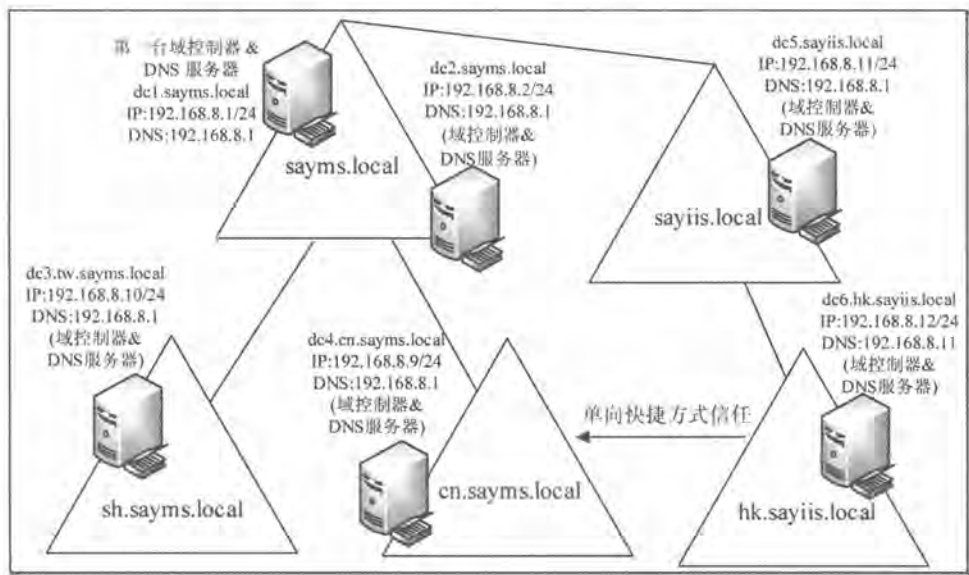


图 8-2-1



我们将图重新简化为图8-2-2，图中必须在域hk.sayiis.local建立一个传出信任，相对也必须在域cn.sayms.local建立一个传入信任。我们以同时建立域hk.sayiis.local的传出信任与域cn.sayms.local的传入信任为例来说明。

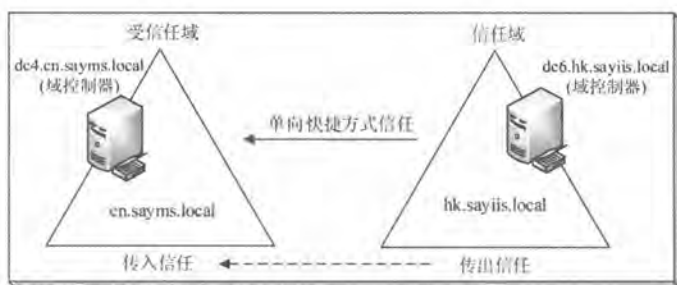


图 8-2-2

- STEP 1 以下假设是要在左边受信任域cn.sayms.local的域控制器dc4.cn.sayms.local上，利用Domain Admins (cn.sayms.local) 或Enterprise Admins (sayms.local) 组内的用户登录与建立信任。
- STEP 2 单击左下角开始图标Windows 管理工具Active Directory域和信任关系。
- STEP 3 如图8-2-3所示【单击域cn.sayms.local单击上方属性图标】。

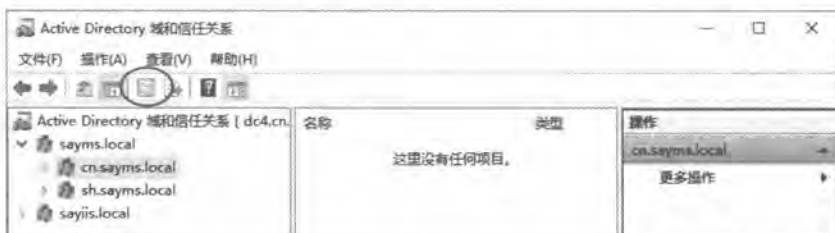


图 8-2-3

- STEP 4 点选图8-2-4中的信任选项卡，单击新建信任按钮。



图 8-2-4



附注

由图中的上半段可看出域cn.sayms.local已经信任其父域sayms.local；同时从下半段可看出，域cn.sayms.local也已经被其父域sayms.local所信任。也就是说，域cn.sayms.local与其父域sayms.local之间已经自动有双向信任关系，它就是父-子信任。

STEP 5 出现欢迎使用新建信任向导界面时单击 **下一步** 按钮。

STEP 6 在图8-2-5中输入对方域的DNS域名hk.sayiis.local（或NetBIOS域名HK）。完成后单击 **下一步** 按钮。



图 8-2-5

STEP 7 在图8-2-6中选择**单向：内传**，表示我们要建立前面图8-2-2的单向快捷方式信任中左侧域cn.sayms.local的传入信任。完成后单击 **下一步** 按钮。

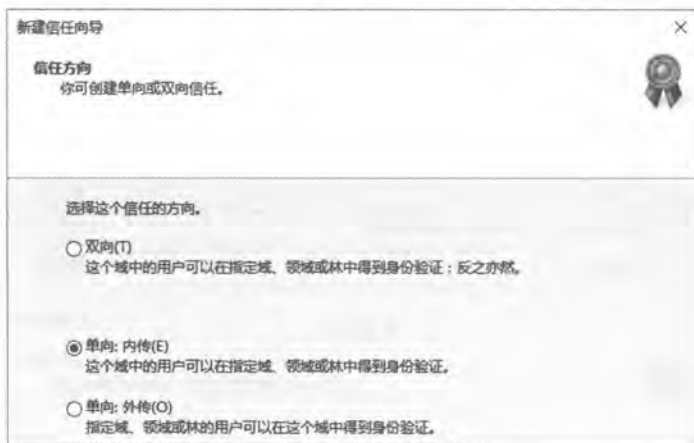


图 8-2-6

STEP 8 在图8-2-7中选择**此域和指定的域**，也就是除了要建立图8-2-2中左侧域cn.sayms.local的传入信任之外，同时也要建立右侧域hk.sayiis.local的传出信任。完成后单击 **下一步** 按钮。

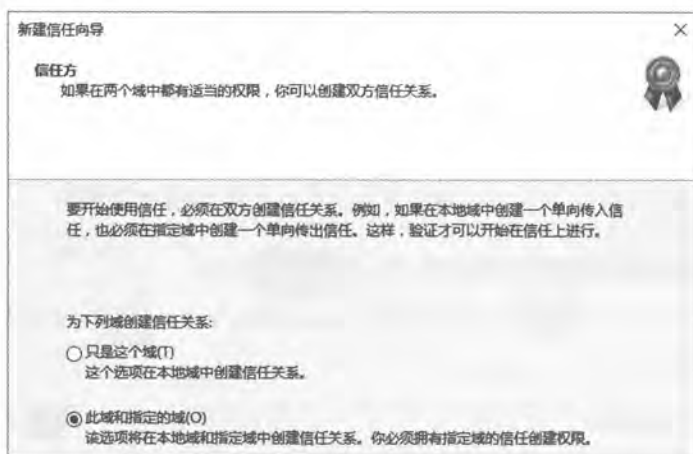


图 8-2-7

注意

如果选择只是这个域的话，则必须事后另外再针对域hk.sayiis.local建立一个传出到域cn.sayms.local的传出信任。

STEP 9 在图8-2-8中输入对方域（hk.sayiis.local）的Domain Admins组内的用户名称与密码（图中使用hk\Administrator），或sayms.local内Enterprise Admins组内的用户名称与密码。完成后单击 **下一步** 按钮。



图 8-2-8

附注

若要输入Enterprise Admins组内的用户账户的话，请在用户名称之前输入林根域的域名，例如 sayms\administrator 或 sayms.local\administrator，其中的 sayms 为林根域的 NetBIOS 域名，而 sayms.local 为其 DNS 域名。

STEP 10 在图8-2-9中单击 **下一步** 按钮。



图 8-2-9

STEP 11 在图8-2-10中单击 **下一步** 按钮。



图 8-2-10

STEP 12 可以在图8-2-11中选择是，确认传入信任，以便确认cn.sayms.local的传入信任与hk.sayiis.local的传出信任两者是否都已经建立成功，也就是要确认此单向快捷方式信任是否已经建立成功。

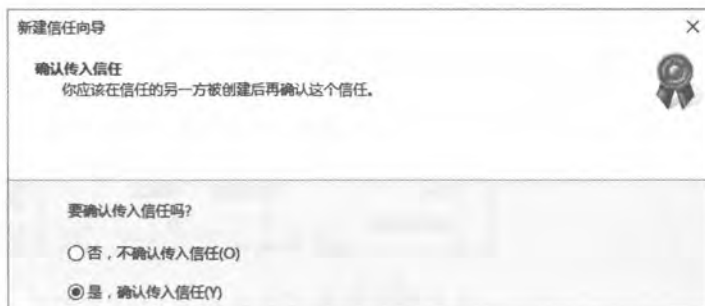


图 8-2-11

**附注**

如果是分别单独建立域cn.sayms.local的传入信任与域hk.sayiis.local的传出信任的话，请确认这两个信任关系都已建立完成后，再选择是，确认传入信任。

STEP 13 出现正在完成新建信任向导界面时单击**完成**按钮。

图8-2-12为完成建立单向快捷方式信任后的界面，表示在域cn.sayms.local中有一个从域hk.sayiis.local来的**传入信任**，也就是说域cn.sayms.local是被域hk.sayiis.local信任的**受信任域**。



图 8-2-12

同时在域hk.sayiis.local中也会有一个连到域cn.sayms.local的**传出信任**，也就是说域hk.sayiis.local是域cn.sayms.local的**信任域**，可以通过【如图8-2-13所示单击sayiis.local之下的域hk.sayiis.local 单击上方**属性**图标 单击**信任**选项卡】的方法来查看此设置。

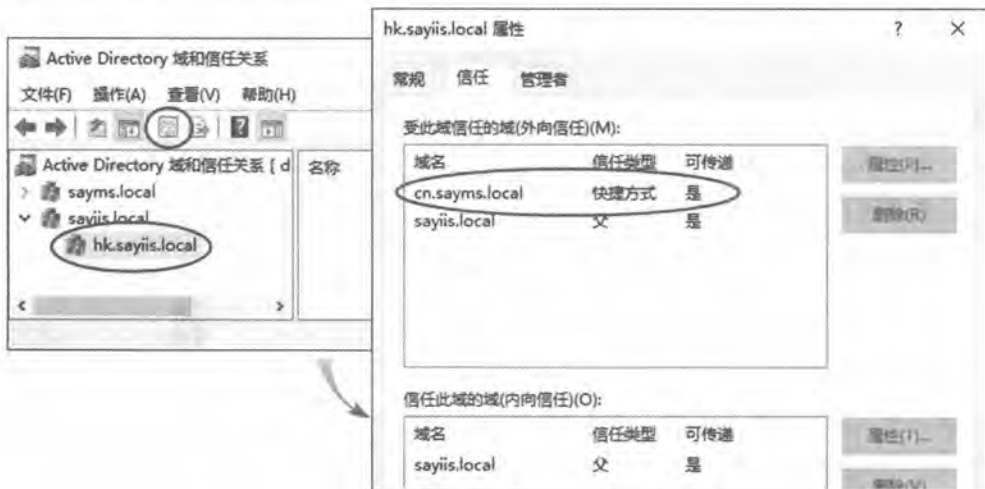


图 8-2-13



8.3 建立林信任

以下利用建立图8-3-1中林sayms.local与林say365.local之间的双向林信任进行说明。

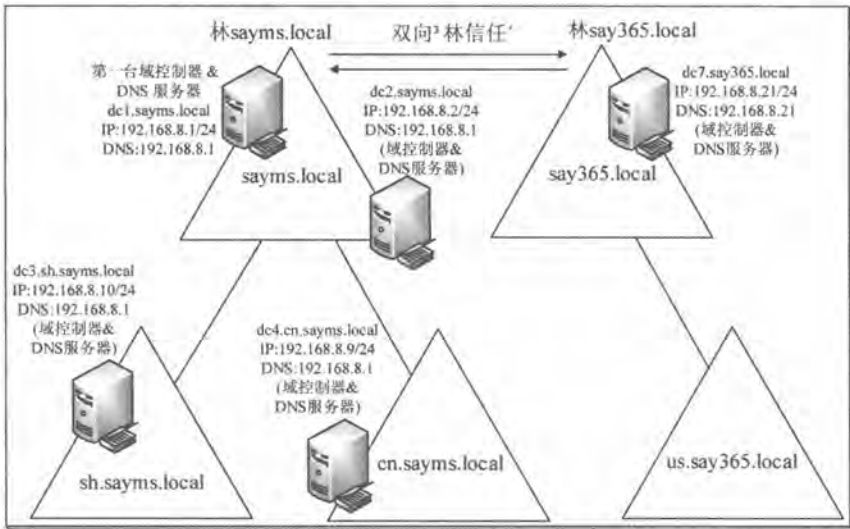


图 8-3-1

我们将图重新简化为图8-3-2，图中需要在林根域sayms.local建立传出信任与传入信任，相对的也需要在林根域say365.local建立传入信任与传出信任。



图 8-3-2

8.3.1 建立林信任前的注意事项

在建立林信任之前，请先注意以下事项：

- 请务必先了解章节8-1节建立信任前的注意事项的内容。
- 两个林之间需要通过DNS服务器来找到对方林根域的域控制器。以图8-3-2来说，必



须确定在域sayms.local中可以通过DNS服务器找到域say365.local的域控制器，同时在域say365.local中也可以通过DNS服务器找到域sayms.local的域控制器：

- 如果两个林根域使用同一台DNS服务器，也就是此DNS服务器内同时有sayms.local与say365.local区域，则双方都可以通过此DNS服务器来找到对方的域控制器。
- 如果两个林根域不是使用同一台DNS服务器，则可以通过**条件转发器**（conditional forwarder）来达到目的，例如在sayms.local的DNS服务器中指定将say365.local的查询请求，转发给say365.local的DNS服务器（参见图8-3-3。图中假设域say365.local的DNS服务器的IP地址为192.168.8.21），同时也请在say365.local的DNS服务器中指定将sayms.local的查询请求，转发给sayms.local的DNS服务器（192.168.8.1）。



图 8-3-3

附注

以下练习采用这种方式，因此请先完成**条件转发器**的配置，再分别到sayms.local与say365.local的域控制器上，利用ping对方区域内主机名的方式来测试**条件转发器**的功能是否正常。

- ✎ 如果两个林根域不是使用同一台DNS服务器的话，则还可以通过**辅助区域**来实现DNS查找，例如在sayms.local的DNS服务器建立一个名称为say365.local的辅助区域，其数据是从say365.local的DNS服务器通过**区域传送**复制过来；同时也在say365.local的DNS服务器建立一个名称为sayms.local的辅助区域，其数据是从sayms.local的DNS服务器通过**区域传送**复制过来。

8.3.2 开始建立林信任

我们将在林sayms.local与say365.local之间建立一个双向的**林信任**，也就是说我们将为林sayms.local建立**传出信任**与**传入信任**，同时也为林say365.local建立相应的**传入信任**与**传出信任**。请先确认前述DNS服务器的设置已经完成。



- STEP 1** 以下假设是要在图8-3-2中左侧林根域sayms.local的域控制器上dc1.sayms.local，利用Domain Admins或Enterprise Admins组内的用户登录与建立信任。
- STEP 2** 单击左下角开始图标Windows 管理工具Active Directory域和信任关系。
- STEP 3** 如图8-3-4所示【单击域sayms.local单击上方属性图标】。



图 8-3-4

- STEP 4** 点选图8-3-5中的信任选项卡，单击新建信任按钮。

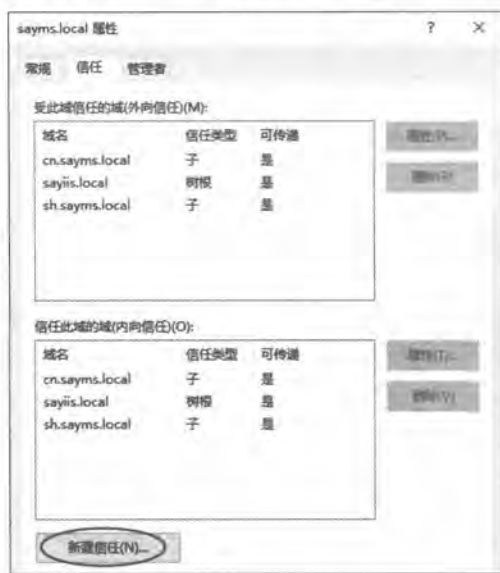


图 8-3-5

附注

从图8-3-5的中上半段可看出，域sayms.local已经信任其子域cn.sayms.local与sh.sayms.local，同时也信任了另一个域树的根域sayiis.local；从图中的下半段可看出，域sayms.local已经被其子域cn.sayms.local与sh.sayms.local所信任，同时也被另外一个域树的根域sayiis.local所信任。也就是说，域sayms.local与其子域之间已经自动有双向父子信任关系。还有域sayms.local与域树sayiis.local之间也已经自动有双向树状-根目录信任关系。

STEP 5 在图8-3-6中单击 **下一步** 按钮。图中支持的信任关系包含了我们需要的林信任（图中的另一个林）。



图 8-3-6

STEP 6 在如图8-3-7所示中输入对方域的DNS域名say365.local（或NetBIOS域名SAY365）后单击 **下一步** 按钮。



图 8-3-7

STEP 7 在图8-3-8中选择林信任后单击 **下一步** 按钮。

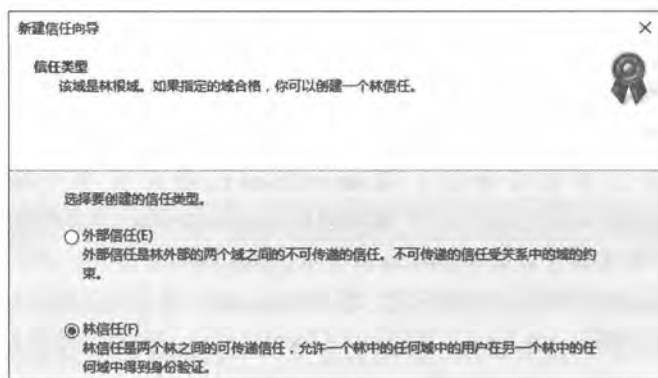


图 8-3-8



附注

如果图中选择**外部信任**的话，也可以让sayms.local与say365.local之间建立信任关系，不过它不具备**传递性**，然而本练习的林信任有**传递性**。

STEP 8 在图8-3-9中选择**双向**后单击**下一步**按钮，表示我们要同时建立图8-3-2中左方域sayms.local的**传出信任**与**传入信任**。



图 8-3-9

STEP 9 在图8-3-10中选择**此域和指定的域**，也就是除了要建立图8-3-2左侧域sayms.local的**传出信任**与**传入信任**之外，同时也要建立右侧域say365.local的**传入信任**与**传出信任**。

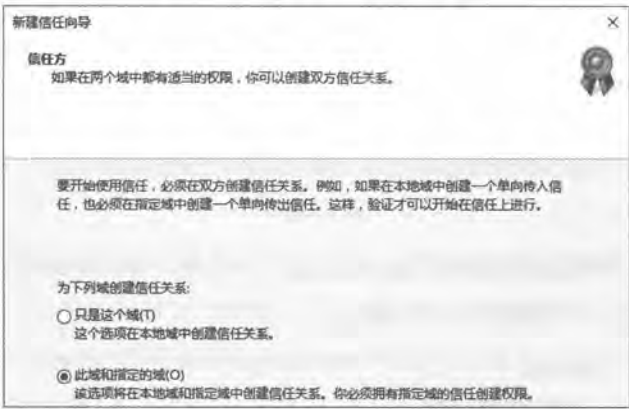


图 8-3-10

注意

如果选择**只是这个域**的话，则必须事后再针对域say365.local来建立与域sayms.local之间的**传入信任**与**传出信任**。

STEP 10 在图8-3-11中输入对方林根域（say365.local）内Domain Admins或Enterprise Admins组的用户名与密码后单击**下一步**按钮。



图 8-3-11

STEP 11 图8-3-12选择如何验证另一个林（say365.local）的用户身份：

- **全林性身份验证：**表示要验证另一个林内（say365.local）所有用户的身份。用户只要经过验证成功，就可以在本林内（sayms.local）访问他们拥有权限的资源。
- **选择性身份验证：**此时另一个林内只有被选择的用户（或组）才会被验证身份，其他用户会被拒绝。被选择的用户只要经过验证成功，就可以在本林内访问他们拥有权限的资源。选择用户的方法后述。

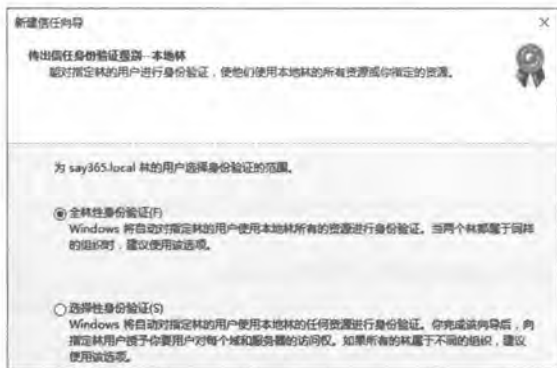


图 8-3-12

STEP 12 图8-3-13是用来设置当本林（sayms.local）中的用户要访问另外一个林（say365.local）内的资源时，如何来验证用户身份。

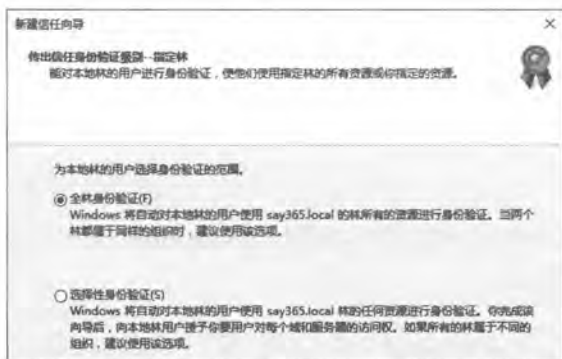


图 8-3-13



STEP 13 在图8-3-14中单击 **下一步** 按钮。

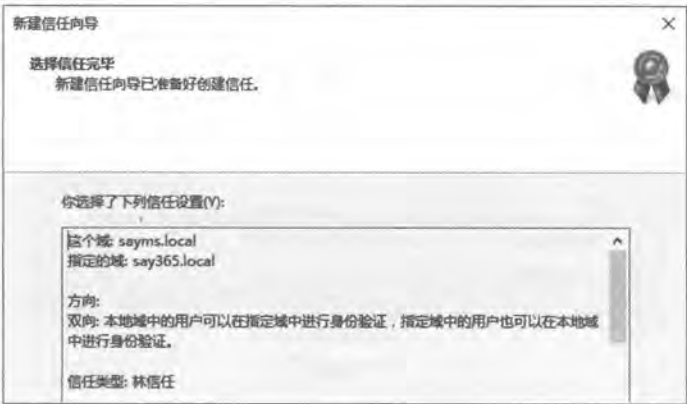


图 8-3-14

STEP 14 在图8-3-15中单击 **下一步** 按钮。

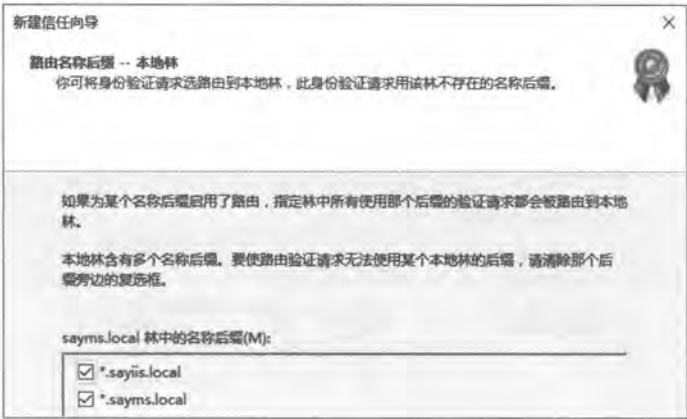


图 8-3-15

路由名称后缀 (routing name suffixes) 是什么呢? 图中显示本林会负责验证的后缀为 sayms.local 与 sayiis.local , 因此当本林中的用户利用 UPN 名称 (例如 george@sayms.local , 其后缀为 sayms.local) 在对方林中登录或访问资源时, 对方就会将验证用户身份的工作转到本林来执行, 也就是根据后缀来将验证用户身份转到 (路由到) 本林。

图 8-3-15 表示本林支持 *.sayiis.local 与 *.sayms.local 后缀 , 也就是 sayms.local 、 sh.sayms.local、cn.sayms.local、sayiis.local、hk.sayiis.local等都是本林所支持的后缀, 用户的UPN后缀只要是上述之一, 则验证工作就会转给本林来执行。如果不想让对方林将特定后缀的验证转到本林的话, 可在图中取消勾选该后缀。

STEP 15 在图8-3-16中单击 **下一步** 按钮。



图 8-3-16

STEP 16 可以在图8-3-17中选择是, 确认传出信任, 以便确认在图8-3-2中sayms.local的传出信任与say365.local的传入信任这一组单向的信任是否建立成功。

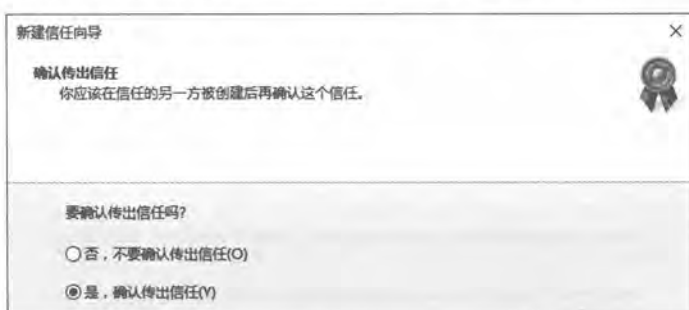


图 8-3-17

附注

如果是分别单独建立域sayms.local的传出信任与域say365.local的传入信任的话, 请确认这两个信任关系都已经建立完成后, 再选择是, 确认传出信任。

STEP 17 可以在图8-3-18中选择是, 确认传入信任, 以便确认在图8-3-2中sayms.local的传入信任与say365.local的传出信任这一组单向的信任是否建立成功。

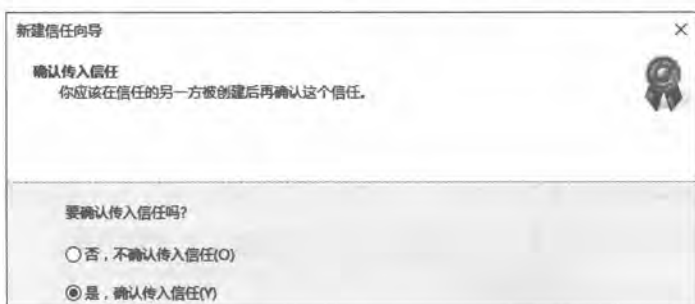


图 8-3-18



STEP 18 在图8-3-19中单击**完成**按钮。



图 8-3-19

图8-3-20为完成建立双向**林信任**后的界面，图上方表示在域sayms.local中有一个传出到域say365.local的传出信任，也就是说域sayms.local信任域say365.local；图下方表示在域sayms.local中有一个从域say365.local来的传入信任，也就是说域sayms.local被域say365.local所信任。

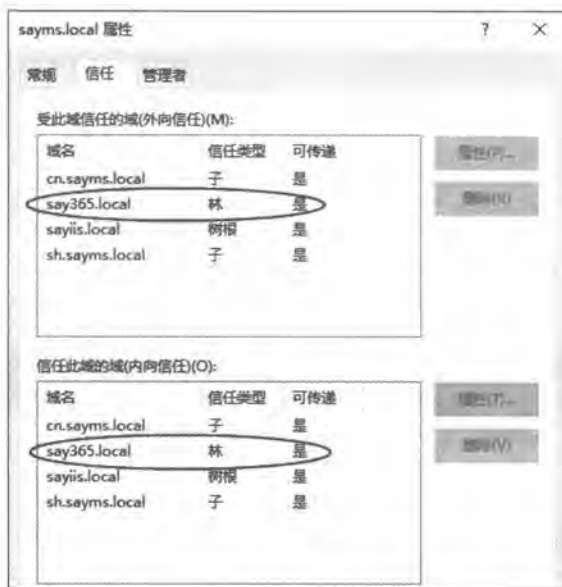


图 8-3-20

也可以到林say365.local的域控制器上【单击左下角**开始**图标→**Windows管理工具**→**Active Directory域和信任关系**→如图8-3-21所示单击**say365.local**→单击上方的**属性**图标→**信任**选项卡】来查看这个双向信任。图上方表示在域say365.local中有一个传出到域sayms.local的传出信任，也就是说域say365.local信任域sayms.local；图下方表示在域say365.local中有一个从域sayms.local来的传入信任，也就是说域say365.local被域sayms.local所信任。

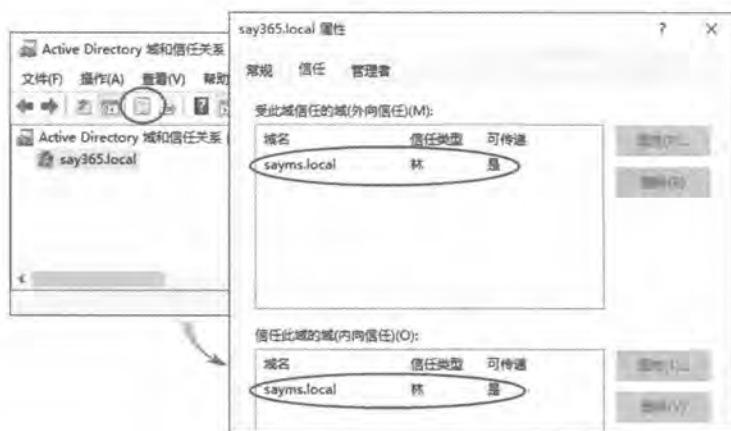


图 8-3-21

8.3.3 选择性身份验证设置

如果在图8-3-12是选择**选择性身份验证**的话，则需要在本林内的计算机上，将**允许身份验证**（Allowed to Authenticate）权限授予另外一个林内的用户（或组），只有拥有**允许身份验证**权限的用户来连接此计算机时才会被验证身份，而在经过验证成功后，该用户便有权来访问此计算机内的资源。以下假设**信任林**（trusting forest）为sayms.local，而**受信任林**为say365.local。

STEP 1 请到**信任林**（sayms.local）内的域控制器dc1.sayms.local上【单击左下角**开始**图标田Windows 管理工具Active Directory管理中心如图8-3-22所示双击要设置的计算机账户（假设是Win10PC1）】。



图 8-3-22

STEP 2 如图8-3-23所示单击**安全**选项卡下的**添加**按钮。



图 8-3-23

STEP 3 在图8-3-24中单击 **位置** 按钮，选择对方林say365.local后单击 **确定** 按钮。



图 8-3-24

STEP 4 在图8-3-25中的 **查找位置** 已被改为 say365.local，接着请通过单击 **高级** 按钮来选择 say365.local 内的用户或组，图中是已经完成选择后的界面，而所选的用户为 Robert。单击 **确定** 按钮。



图 8-3-25

STEP 5 如图8-3-26所示在允许身份验证右侧勾选允许后单击**确定**按钮。



图 8-3-26

8.4 建立外部信任

以下利用建立图8-4-1中林sayms.local与林sayexg.local之间的双向外部信任来说明。

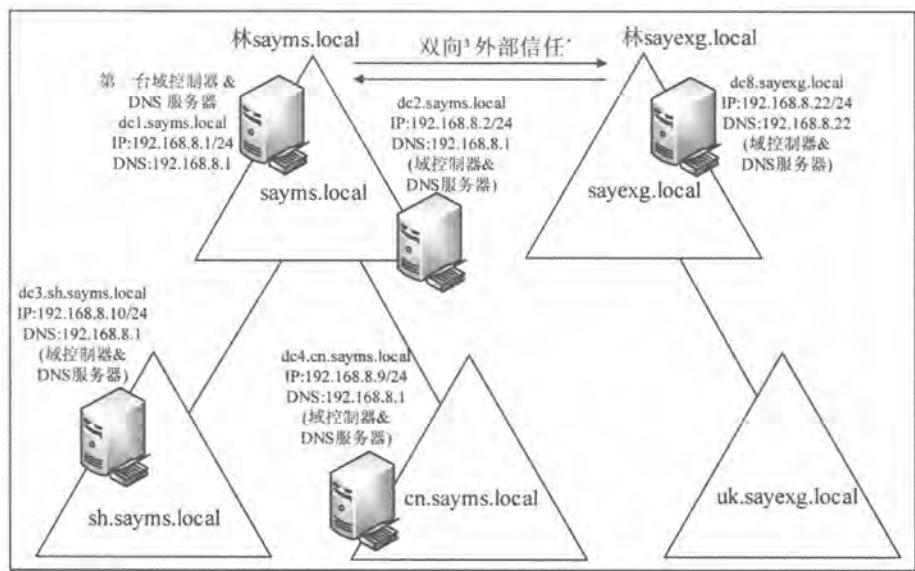


图 8-4-1

我们将图重新简化为图8-4-2，图中要在林根域sayms.local建立传出信任与传入信任，相对也要在林根域sayexg.local建立传入信任与传出信任。

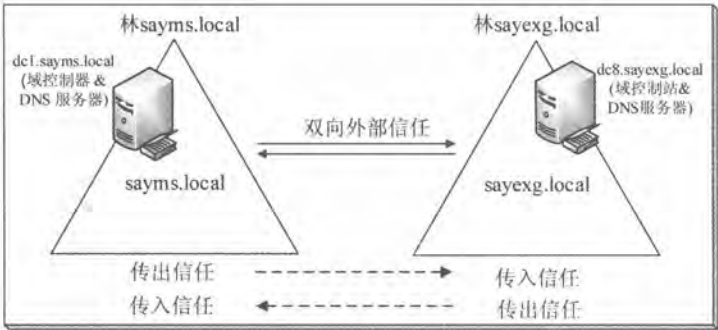


图 8-4-2

外部信任的注意事项、DNS服务器设置、建立步骤等与林信任相同，此处不再赘述，不过在建立外部信任时需要改为如图8-4-3所示选择外部信任。



图 8-4-3

还有会在步骤的最后另外显示图8-4-4的界面，表示系统默认会自动启用**SID筛选隔离**（SID Filter Quarantining）功能，它可以增加安全性，避免入侵者通过**SID历史**（SID history）取得信任域内不该拥有的权限。

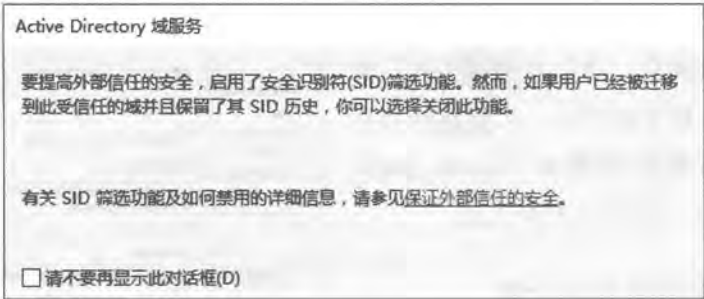


图 8-4-4

图8-4-5为完成外部信任建立后，在信任域sayms.local所看到的界面；而图8-4-6为在受信域sayexg.local所看到的界面。

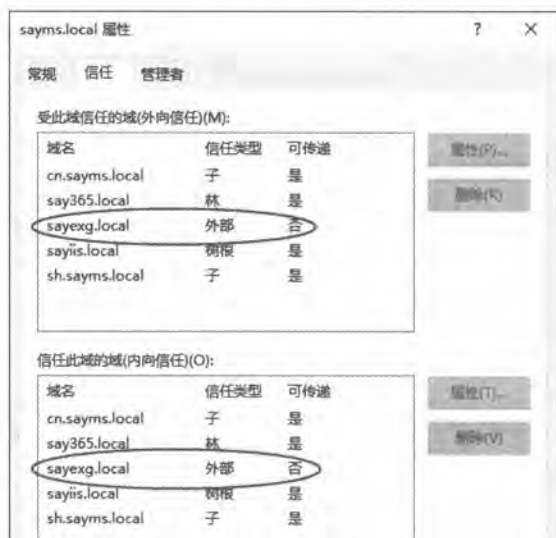


图 8-4-5

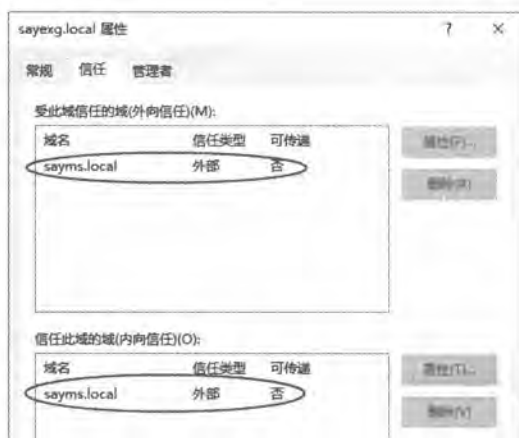


图 8-4-6

8.5 管理与删除信任

8.5.1 信任的管理

如果要更改信任设置的话：【如图8-5-1所示选择要管理的传出或传入信任➡单击**属性**按钮】，然后通过前景图的选项卡来管理信任关系。

1. 验证信任关系

如果对方域支持Kerberos AES加密的话，则可勾选图8-5-1中的**其他域支持Kerberos AES加密**。如果要重新确认与对方域或林之间的信任关系是否仍然有效的话，请单击**验证**按钮。如果对方域或林内有新子域的话，此**验证**按钮也可以同时更新名称后缀路由（name prefix routing，详见图8-3-15的说明）的信息。

2. 更改名称后缀路由设置

当用户的UPN（例如george@say365.local）后缀是隶属于此指定林时，则用户身份的验证



图 8-5-1



工作会转给此林的域控制器。图8-5-2中的**名称后缀路由**选项卡用来更改所选林的名称后缀路由状态，例如要停止将后缀为say365.local的验证转发给林say365.local的话，请在图8-5-2中单击该林后缀后单击**禁用**按钮。

如果该林内包含多个后缀，例如say365.local、us.say365.local，而只是要禁用将其中部分后缀验证工作转发给该林的话：【单击前面图8-5-2中的**编辑**按钮 ➡ 在图8-5-3中选择要禁用的名称后缀（图中假设有us.say365.local存在） ➡ 单击**禁用**按钮】。

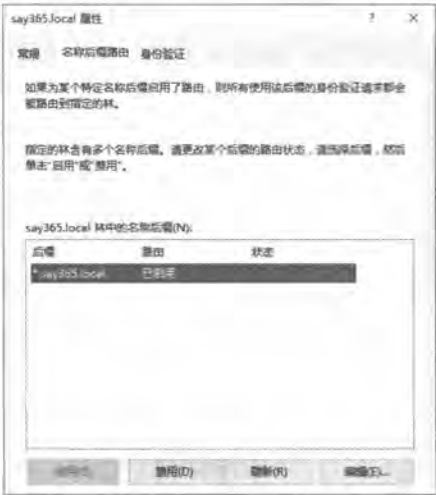


图 8-5-2



图 8-5-3

另外，为了避免**后缀名称冲突**现象的发生，此时可以通过图8-5-3上方的**添加**按钮来将后缀排除。何谓**后缀名称冲突**现象？举例来说，图8-5-4中林sayms.local与林say365.local之间建立了双向林信任、林say365.local与林jp.say365.local（注意是林！不是子域！）之间也建立了双向林信任、林sayms.local与林jp.say365.local之间建立了单向林信任。

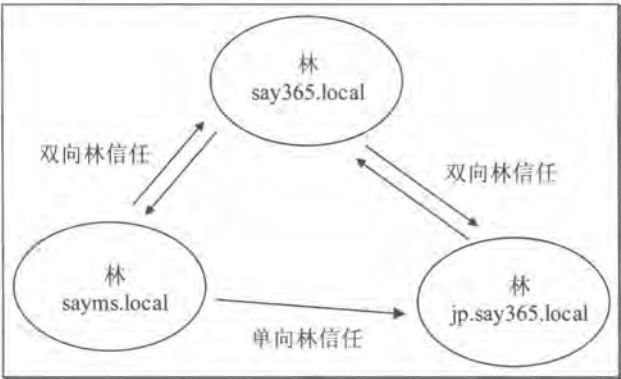


图 8-5-4

图中林sayms.local默认会将后缀为*.say365.local的身份验证工作转发给林say365.local来执行，包含后缀say365.local与jp.say365.local，可是因为两个林之间的**林信任**关系并无法自动的



扩展到其他第3个林，因此当林say365.local收到后缀为jp.say365.local的身份验证请求时，并不会将其转发给林jp.say365.local。



解决上述问题的方法是在林sayms.local中将后缀jp.say365.local排除，也就是编辑信任关系say365.local：【在图8-5-5中单击**添加**按钮输入后缀jp.say365.local单击**确定**按钮】，如此林sayms.local就不会将后缀是jp.say365.local的身份验证请求转发给林say365.local，而是直接转发给林jp.say365.local（因为图8-5-4中林sayms.local与林jp.say365.local之间有单向林信任）。



图 8-5-5

3. 更改身份验证方法

如果要更改身份验证方法的话，请通过图8-5-6的身份验证选项卡来设置，图中两个验证方法的说明请参考前面图8-3-12的相关说明。

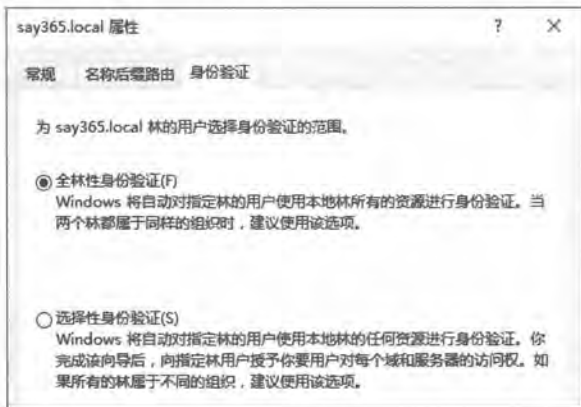


图 8-5-6

8.5.2 信任的删除

你可以将快捷方式信任、林信任、外部信任、领域信任等手动建立的信任删除，然而系



统自动建立的父—子信任与树状—根目录信任不能删除。

我们以图 8-5-7 为例来说明如何删除信任，而且是要删除图中林 sayms.local 信任 say365.local 这个单方向的信任，但是保留林 say365.local 信任 sayms.local。

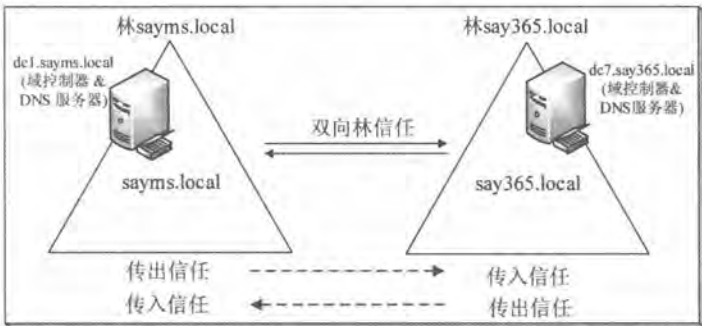


图 8-5-7

STEP 1 如图8-5-8所示【单击域sayms.local 单击上方属性图标】。



图 8-5-8

STEP 2 在图8-5-9中【单击信任选项卡 选择受此域信任的域（外向信任）之下的域 say365.local】，也就是选择图8-5-7左侧域sayms.local的传出信任，然后单击删除按钮。



图 8-5-9



STEP 3 在图8-5-10中可以选择:

- ✎ 不, 只从本地域删除信任: 也就是只删除图8-5-7左侧域sayms.local的传出信任。
- ✎ 是, 从本地域和另一个域中删除信任: 也就是同时删除图8-5-7左侧域sayms.local的传出信任与右侧域say365.local的传入信任。如果选择此选项的话, 则需要输入对方域say365.local的Domain Admins或林根域sayms.local内Enterprise Admins组内的用户名与密码。

Active Directory 域服务

要从本地域和另一个域删除信任吗? 要从另一个域删除信任, 你必须有 say365.local 域的系统管理权限。

☒ 不, 只从本地域删除信任(O)

☐ 是, 从本地域和另一个域中删除信任(Y)

请键入在另一个域中有系统管理权限的帐户的用户名和密码。

用户名(U):

密码(P):

图 8-5-10