Microsoft

MCSA
Windows Server 2016实现和管理

程尊华

Elink Training

Module 7

实施 DirectAccess

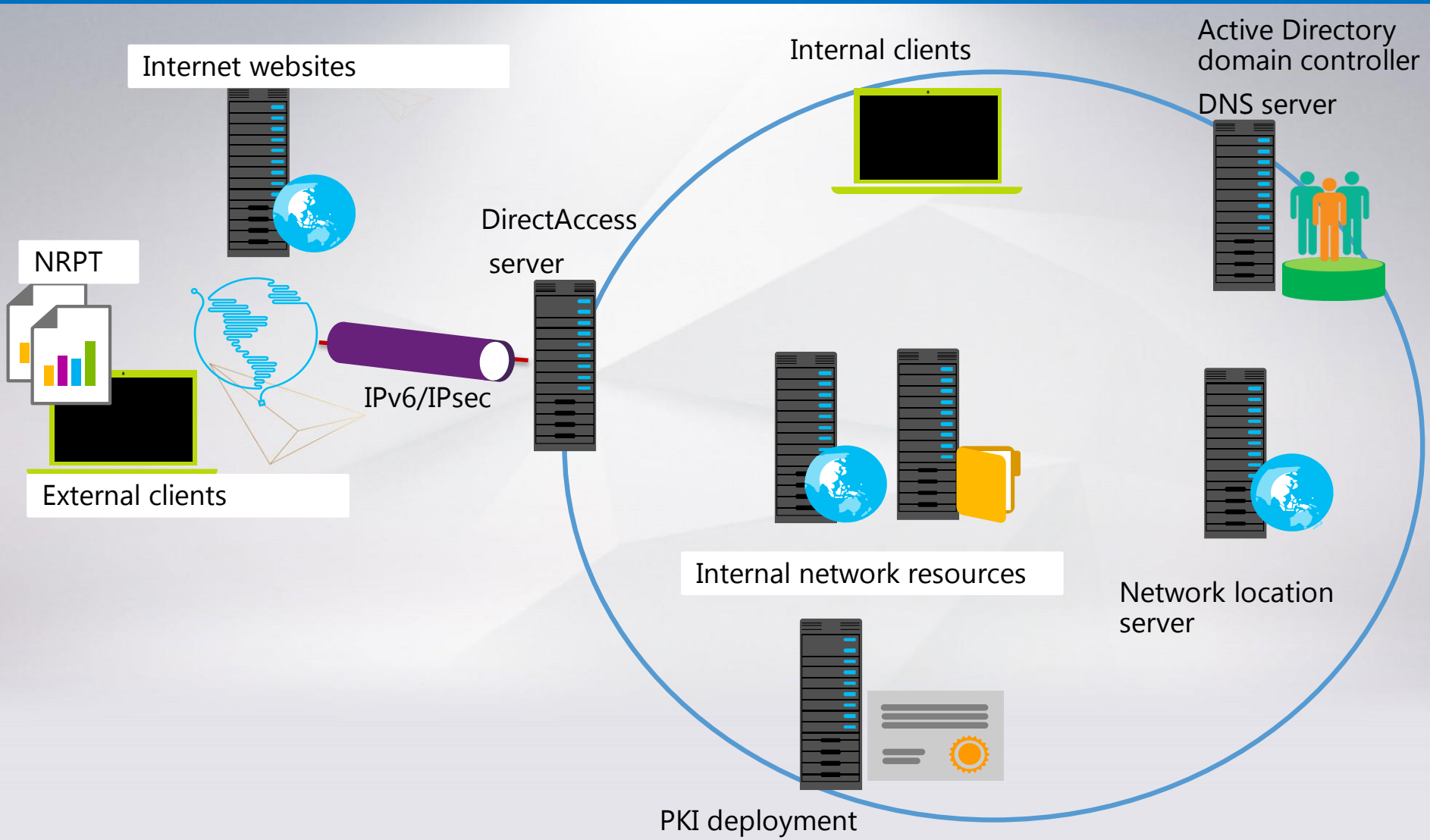
模块概述

- DirectAccess概述
- 使用入门向导实现DirectAccess
- 实施和管理高级DirectAccess基础设施

第1课：DirectAccess概述

- DirectAccess组件
- DirectAccess服务器部署选项
- DirectAccess隧道协议选项
- 在Windows Server 2016中管理远程访问
- DirectAccess如何适用于内部客户端
- DirectAccess如何适用于外部客户端
- 演示：安装远程访问服务器角色

DirectAccess组件



DirectAccess服务器部署选项

- DirectAccess服务器部署选项：
  - 使用入门向导进行简单的部署
  - 通过使用提前配置选项进行复杂部署
- DirectAccess服务器高级部署选项：
  - 部署多个端点
  - 多域支持
  - 在NAT设备后部署服务器
  - 支持OTP和虚拟智能卡
  - 支持NIC分组
  - 外部配置

DirectAccess隧道协议选项

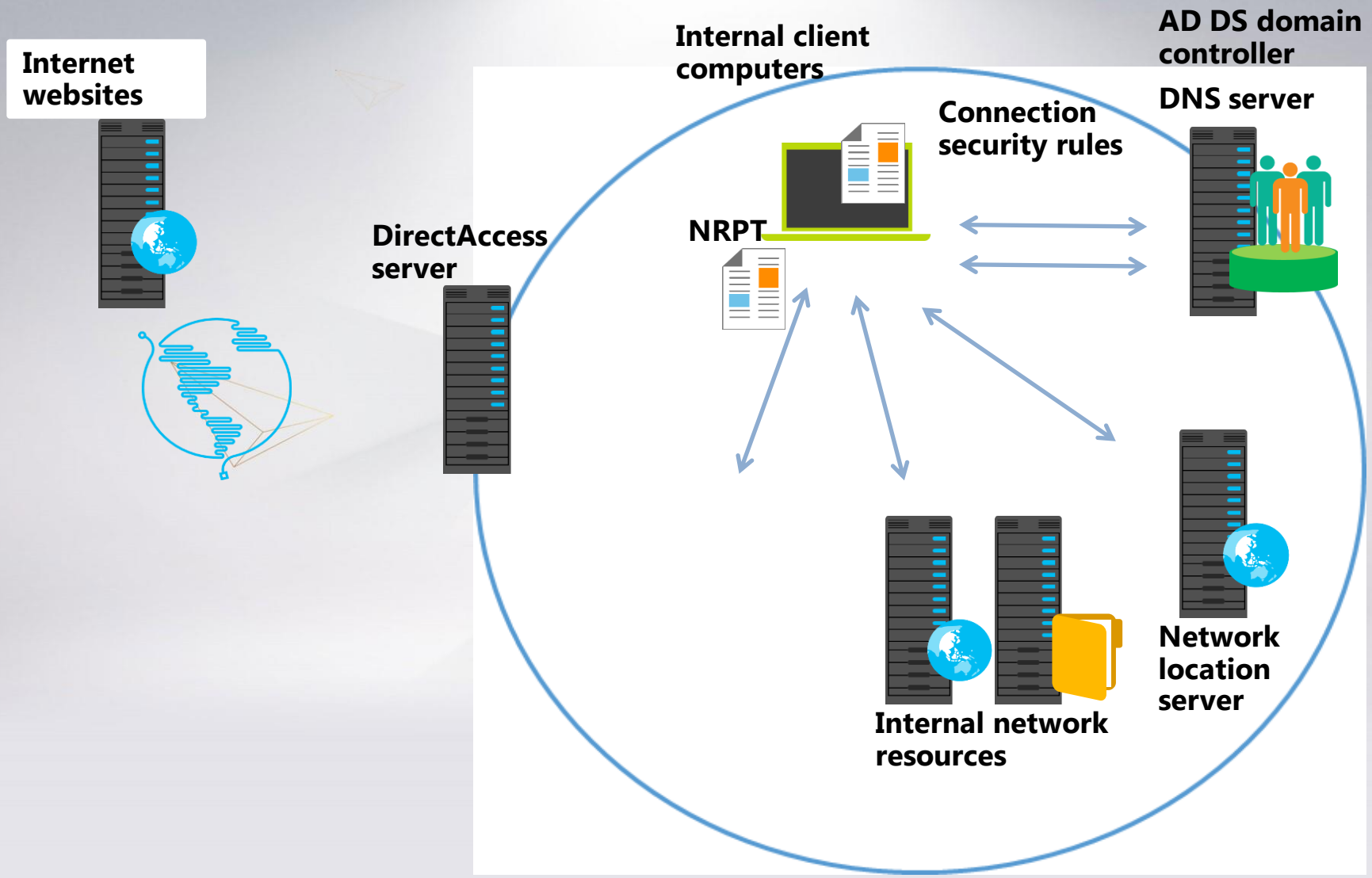
- DirectAccess隧道协议包括：
  - ISATAP, 隧道通过IPv4网络进行内部网通信的IPv6流量
  - 6to4,由DirectAccess客户端使用公共IP地址
  - Teredo,由DirectAccess客户端在NAT设备后面使用私有IP地址
  - IP-HTTPS 由DirectAccess客户端使用，如果不能使用ISATAP，6to4或Teredo

在Windows Server 2016中管理远程访问

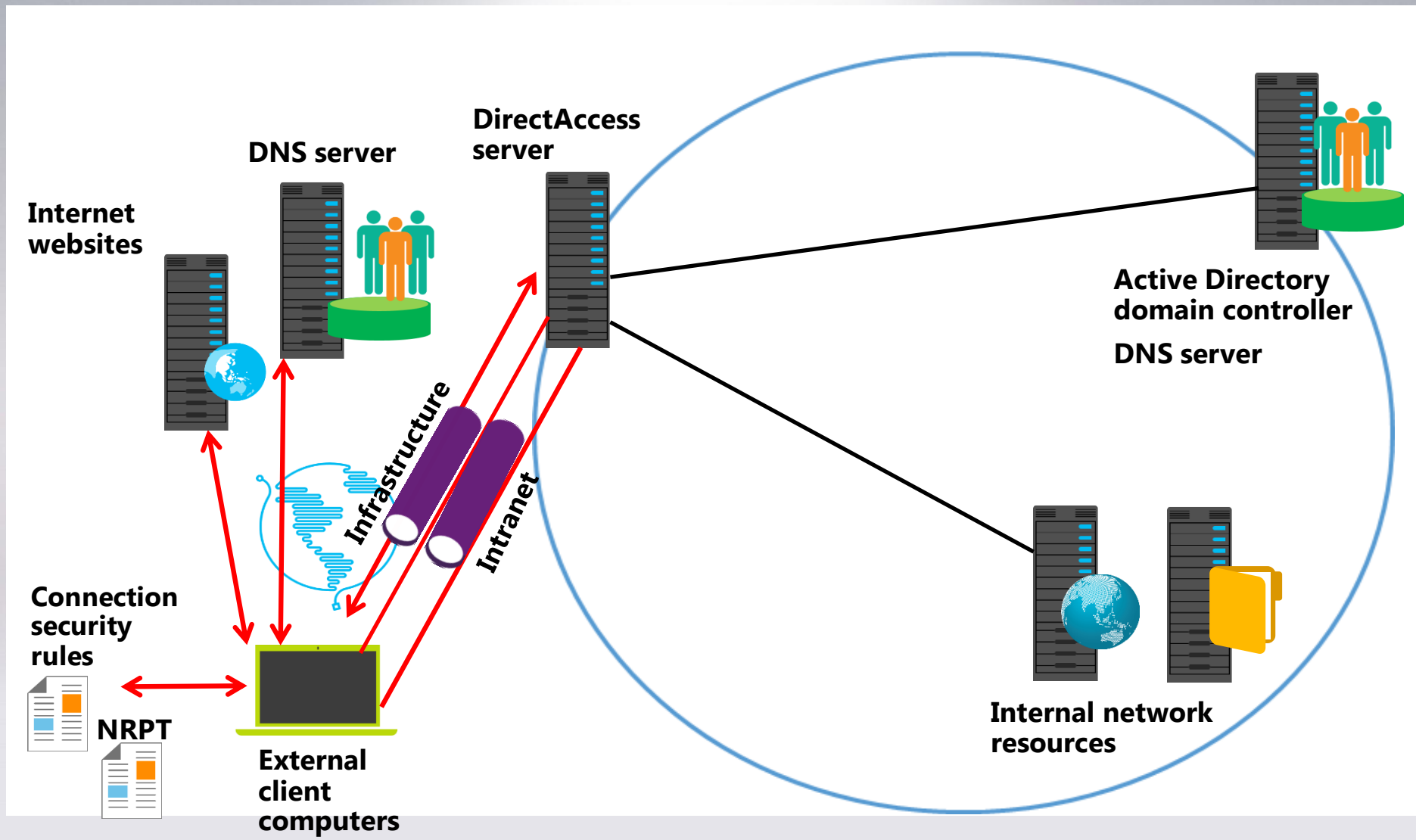
使用以下命令管理远程访问服务器角色：

- 远程访问管理控制台
- 路由和远程访问控制台
- Windows PowerShell：
- **Set-DAServer**
- **Get-DAServer**
- **Set-RemoteAccess**
- **Get-RemoteAccess**

DirectAccess如何适用于内部客户端



DirectAccess如何适用于外部客户端



Elink Training

演示：安装远程访问服务器角色

在此演示中，您将学习如何安装远程访问服务器角色

第2课：使用入门向导实现DirectAccess

- 演示：运行入门向导
- 入门向导配置更改
- 演示：识别入门向导设置
- 使用入门向导部署DirectAccess的限制

演示：运行入门向导

在此演示中，您将学习如何通过运行入门向导来配置DirectAccess

入门向导配置更改

入门向导所做的更改包括：

- GPO设置：
  - DirectAccess服务器设置GPO
  - DirectAccess客户端设置GPO
  - 不支持手动编辑GPO
- DNS服务器设置
- 远程客户端
- 远程访问服务器
- 基础设施服务器

演示：识别入门向导设置

在此演示中，您将学习如何识别DirectAccess入门向导所做的更改

使用入门向导部署DirectAccess的限制

- 证书：
  - 创建无法在多站点部署或双因素身份验证中使用的自签名证书
  - 需要确保两个证书的CRL分发点在外部可用
- 网络定位服务器设计：
  - 在与DirectAccess服务器相同的服务器上部署网络位置服务器
- Windows客户端操作系统支持：
  - 入门向导配置适用于运行Windows 10，Windows 8.1或Windows 8或Windows Server 2016，Windows Server 2012 R2或Windows Server 2016的客户端
  - Windows 7客户端需要客户端证书进行IPsec认证

实验A：使用入门向导实现DirectAccess

- 练习1：验证DirectAccess部署的准备情况
- 练习2：配置DirectAccess
- 练习3：验证DirectAccess部署

登录信息

虚拟机:	**20741B-LON-DC1** **20741B-LON-SVR1** **20741B-EU-RTR** **20741B-LON-CL1**
用户名:	**Adatum\Administrator**
密码:	**Pa55w.rd**
虚拟机:	**20741B-INET1**
用户名:	**Administrator**
密码:	**Pa55w.rd**

预计时间: 45 minutes

实验场景

A. Datum Corporation的许多用户从组织外部工作。 这包括移动用户和在家工作的人。 这些用户当前通过使用非Microsoft VPN解决方案连接到内部网络。 安全部门关心外部连接的安全性，并希望确保连接尽可能安全。 支持团队希望最大限度地减少与远程访问相关的支持呼叫数量，并希望有更多选项来管理远程计算机。

A. Datum的IT管理正在考虑将DirectAccess部署为组织的远程访问解决方案。 作为概念部署的初始证明，管理要求您配置一个简单的DirectAccess环境，即运行Windows 10的客户端计算机可以使用。

实验回顾

- 为什么要创建DirectAccessClients组？
- 您将如何配置IPv6地址
- 运行Windows 10的客户端计算机使用DirectAccess？

第3课：实施和管理高级DirectAccess基础设施

- 高级DirectAccess选项概述
- 负载平衡和高可用性选项
- 支持多个位置
- 将PKI与DirectAccess集成
- 为DirectAccess实施客户端证书
- 内部网络配置选项
- 配置高级DNS设置
- 实现网络位置服务器
- 实施管理服务器
- 演示：修改DirectAccess基础架构
- 如何监控DirectAccess连接
- 如何解决DirectAccess连接问题
- 演示：监控和故障排除DirectAccess连接
- 实现DirectAccess离线域连接

高级DirectAccess选项概述

- 高级DirectAccess配置选项包括：
  - 可扩展和定制的PKI基础设施
  - 自定义网络配置选项
  - 可扩展且高可用性的服务器部署
  - 定制监控和故障排除

负载平衡和高可用性选项

- DirectAccess可以使用以下方式进行高可用性：
  - 网络负载平衡（NLB）
  - 第三方解决方案，如Citrix NetScaler，F5等
- 如果DirectAccess服务器在Hyper-V虚拟机中运行，则必须启用MAC欺骗
- 负载平衡集群中的所有DirectAccess服务器必须具有相同的配置
- 您应该考虑使网络位置服务器高度可用

支持多个位置

- 通过多站点部署，两个或多个DirectAccess服务器放置在多个位置
- 多站点部署具有以下优点：
  - 您的DirectAccess客户端连接到最接近和最快的DirectAccess服务器
  - 如果一个站点中的DirectAccess服务器脱机，客户端可以连接到另一个站点中的DirectAccess服务器
- 多站点部署需要：
  - PKI
  - 已部署高级设置的单个DirectAccess服务器
  - 内部网络必须启用IPv6
  - Windows 7客户端必须手动分配到一个站点

将PKI与DirectAccess集成

- 为DirectAccess配置PKI包括以下步骤：
  1. 添加和配置CA服务器角色（如果尚未存在）
  2. 创建证书模板
  3. 创建CRL分发点并发布CRL列表
  4. 分发计算机证书

为DirectAccess实施客户端证书

- 需要运行Windows 7 DirectAccess客户端进行IPSec身份验证计算机证书
- 部署客户端计算机证书的步骤：
  1. 创建一个GPO并将其链接到包含DirectAccess客户端的组织单位
  2. 配置GPO用于为计算机帐户自动证书请求
  3. 应用GPO
  4. 验证证书颁发
- DirectAccess的可以被配置为使用OTP
- 通常需要第三方软件或硬件来提供密码

内部网络配置选项

规划内部网络配置包括：

- 对于DirectAccess服务器的位置（边缘，外围网络和内部网络）计划
- 计划中的IP地址分配
- 计划中的防火墙配置
- 为AD DS计划
- 客户端部署计划

配置高级DNS设置

- DirectAccess使用DNS来解决：
  - 网络位置服务器
  - IP-HTTPS
  - CRL分发点
  - ISATAP
  - 连接验证
- 您可以通过使用组策略具有以下设置配置NRPT：
  - DNS后缀
  - CRL分发点
  - 拆分式DNS

实现网络位置服务器

- 您可以找到网络位置服务器上：
  - 一个DirectAccess服务器
  - 安装与IIS的另一台服务器
- 对于网络位置服务器配置的要求包括：
  - 配置网络位置服务器证书的网站
  - 确保DirectAccess客户端信任CA
  - 确保网络位置服务器网站服务器证书是针对CRL检查
  - 网络位置服务器应该是内部客户端访问
  - 网络位置服务器不应该是由Internet客户端访问
  - 网络位置服务器应是高度可用

实施管理服务器

- 在DirectAccess管理服务器：
  - 域控制器
  - 系统中心配置管理服务器
- 管理服务器通过DirectAccess的检测：
  - 自动
  - 如果手动修改
- 管理服务器的要求：
  - 应为基础设施隧道访问
  - 必须全面支持IPv6

演示：修改DirectAccess的基础设施

- 在此演示中，您将学习如何：
  - 修改您使用入门向导部署在DirectAccess基础设施
  - 应用高级的配置设置

如何监控DirectAccess连接

- 远程访问管理控制台监视组件：
  - 仪表板
  - 操作状态
  - 远程访问客户端状态
  - 远程访问报告

如何排错DirectAccess连接

- 您可以通过使用解决DirectAccess连接：
  - 故障排除方法
  - 命令行工具
  - GUI工具

演示：监控和故障诊断DirectAccess连接

在本演示中，您将学习如何监视和解决DirectAccess连接

实现的DirectAccess脱机加入域

配置DirectAccess的脱机加入域：

1. 远程客户端计算机创建一个新的计算机帐户和运行djoin.exe命令生成一个配置包
2. 在客户端计算机帐户添加到安全DirectAccessClients组
3. 供应包复制到将要加入域的远程客户计算机
4. 应用供应包到远程客户计算机
5. 重新启动远程客户计算机

实验B：部署一个高级的DirectAccess解决方案

- 练习1：为DirectAccess准备环境
- 练习2：实施高级DirectAccess基础设施
- 练习3：验证DirectAccess部署

登录信息

虚拟机:	**20741B-LON-DC1** **20741B-LON-SVR1** **20741B-EU-RTR** **20741B-LON-CL1** **20741B-LON-CL2**
用户名:	**Adatum\Administrator**
密码:	**Pa55w.rd**
虚拟机:	**20741B-INET1**
用户名:	**Administrator**
密码:	**Pa55w.rd**

预计时间: 75 minutes

实验场景

概念部署DirectAccess的证明是成功的，因此IT管理部门已决定启用DirectAccess的所有移动客户端，其中包括运行Windows 7的IT管理还希望确保DirectAccess部署具有可扩展性，并提供冗余的计算机。

您需要修改的理念部署的证明，以满足新的要求。

实验回顾

- 你为什么让边缘服务器上可用的CRL？
- 你为什么要安装客户端计算机上的证书？

模块回顾和作业

- 复习题
- 工具
- 最佳实践
- 常见问题和故障排除技巧

- 感谢大家！
- 也欢迎大家加入我们的技术交流群，我会定时将课程资料下发到群里，供大家下载学习。
- 也请大家持续关注我们的公众号！
- 最后祝大家学习顺利！再次感谢！