

70-297: Designing Windows Server 2003 Active Directory & Network

Blue Yonder Airlines

Background

Overview

Blue Yonder Airlines provides air transportation services to locations throughout Australia. Services include executive-class travel and cargo delivery.

Physical Locations

The company's main office is located in Sydney. The company has two branch offices in the following locations:

- Melbourne
- Perth

The main office location consists of the main office in Sydney and two satellite offices located near the Sydney airport. All three locations in Sydney are connected by fiber-optic links.

Planned Changes

The company plans to extend its services internationally. Over the next two years, it will open two European branch offices in the following locations:

- Berlin
- Paris

The Berlin office will serve as the regional office for Europe.

In addition, the company plans to establish a new partnership with an application service provider (ASP) named Contoso, Ltd., which will be used to host the company's air traffic control (ATC) application.

The ATC application is an X.500 directory-enabled application that runs on Windows NT Server 4.0 computers in the Sydney office. The company plans to use a new version of the ATC application that will run on a Windows Server 2003 computer hosted by Contoso, Ltd. Only specified users will have access to this application. Users connect to this application by querying DNS for the application's service record. This record is stored on a UNIX DNS server running the latest version of BIND.

Contoso, Ltd., will create the required users in the domain that hosts the application and will provide this information as a file to Blue Yonder Airlines. No other connections to the Contoso, Ltd., network will be allowed except for access to the application itself.

Existing Environment

Business Processes

Blue Yonder Airlines consists of the following primary departments:

- Finance
- Human resources (HR)
- Information technology (IT)
- Air traffic control (ATC)
- Flight operations

The IT department manages the entire network from the Sydney office or by traveling to the branch offices. All resources are located at the Sydney office and are accessed across the WAN links by users in the branch offices.

Although the ATC department works closely with flight operations, it is still a separate department.

The flight operations department consists of the following groups:

- Flight officers
- Manifest
- Catering

Users in the Manifest group use an application named Manifest. The Manifest application consists of two versions: Passenger Manifest and Cargo Manifest. Passenger information is in Passenger Manifest. Cargo information is in Cargo Manifest.

Users in the Sydney office use only Passenger Manifest. Users in the branch offices use only Cargo Manifest. Currently, access to the Manifest application is limited only by using NTFS permissions.

Passenger Manifest runs on a server in the Sydney office. The information in Passenger Manifest must be current within the hour and must be available at all times to all users in the Manifest group. The information contained in Passenger Manifest must never become publicly available.

Directory Services

The existing domains and trusts are shown in the **Existing Domain Model** exhibit. (Click the **Case Study Exhibits** button.)

The existing Windows NT 4.0 domain is dedicated to the ATC application. A Windows 2000 Active Directory forest named blueyonderairlines.com is used for all other internal resources. The Active Directory forest consists of both Windows 2000 Server and Windows NT Server 4.0 domain controllers.

All user accounts and computer accounts are created in a domain named corp.blueyonderairlines.com. Group Policy objects (GPOs) exist for the control of software distribution, but there are problems with the execution of these GPOs.

A single DNS server that is not Active Directory integrated is running in the Sydney office. A single administrative group controls the entire network from the Sydney office.

Network Infrastructure

The existing network is shown in the **Existing Network Infrastructure** exhibit. (Click the **Case Study Exhibits** button, and then click **Existing Network Infrastructure**.)

The LAN in each office consists of a 100-Mbps Ethernet network. No server computers are located in the branch offices. All IP addresses are statically configured for computers located in the branch offices.

A Microsoft Exchange Server 2000 environment provides Outlook Web Access (OWA) to all users. A single Exchange Server 2000 front-end server computer in the Sydney office is allocated for OWA.

Currently, the company does not have a public Web site. A Microsoft Internet Security and Acceleration (ISA) Server computer in the Sydney office is configured as a firewall and proxy server. The ISA Server computer is also used for publishing OWA to flight officers who connect to the network from outside the firewall.

Flight officers use portable computers to access OWA via an ISP. No other intranet applications are currently available.

Company policy states that client computers should run only Windows 2000 Professional or Windows XP Professional. However, this policy is currently not enforced.

The existing hardware is shown in the following table.

Processor	Hard disk drive	Memory	Roles
Pentium III-800 MHz dual	Two 9-GB SCSI	256 MB	Two domain controllers for Windows 2000 corporate domain; one domain controller for Windows 2000 root domain
Pentium III-800 MHz single	Two 9-GB SCSI	256 MB	PDC for Windows NT 4.0 domain
Pentium III-750 MHz single	Two 9-GB SCSI	256 MB	Exchange Server 2000 computer as member of Windows 2000 corporate domain

Problem Statements

The following business problems must be considered:

- The ATC application uses the inetOrgPerson class when authenticating to the X.500 directory-enabled database the application uses for authentication.
- The existing GPOs result in extremely lengthy logon times for users in the branch offices. Members of the Administrators group are currently excluded from the GPO that forces password changes.
- The current dial-up solution results in expensive long-distance calls and only supports OWA. Currently, an on-site user must send the information to flight officers via an e-mail message because the Manifest application requires that users map to drive T to operate.
- Existing airline security requirements specify that only smart card authentication should be used for the administration of servers by network administrators.

Interviews

Chief Executive Officer

Blue Yonder Airlines has experienced consistent growth since its startup in 1997. However, this year the market has leveled off and we need to expand our services to Europe. We anticipate substantial growth over the next two years.

Our current offices are located near the major airports in Australia. Each office provides all airline-related administrative features for its respective location. The only exception is network administration, which is provided by the Sydney office. If network administrators are needed in one of the branch offices, they are provided air transportation by our company.

Chief Information Officer

Our company plans to establish a Web site named www.blueyonderairlines.com that will include an online booking system for our customers. blueyonderairlines.com is already registered to the company and is used for e-mail addresses. This must not change.

I am concerned about the security risks of the new Web site. Our DNS information must remain secure. The Manifest group must still remain a separate group for security purposes.

All servers must be upgraded to Windows Server 2003 to meet new airline security requirements and to ease the management concerns we are currently facing. We are planning a hardware refresh within the next year to upgrade all computers to a minimum of 1 GB of RAM and seven SCSI hard disk drives per server.

I anticipate that 300 new devices will be added to the network in the Sydney office over the next two years.

Network Administrator

The WAN links are unreliable and can fail for hours at a time. We cannot copy large files because of this, and there are bandwidth problems related to slow links and unreliability.

Fault tolerance for the domains will be required for instances when the WAN links are down or when a single server fails.

We have adequate hardware, but performance of our existing Windows 2000 Server computers is inadequate.

The Exchange 2000 Server computer has excessively high processor utilization once a day. The high utilization lasts for almost an hour and users report that processing is very slow during this time. There cannot be servers in branch offices because of the smart card authentication requirement.

A separate network administrator will be appointed to manage the Manifest application. The NetBIOS name of the corp.blueyonderairlines.com domain is Airlines. Some applications still rely on this NetBIOS name to operate.

Currently, if service packs or new applications need to be installed on computers in the branch offices, a network administrator has to fly to that location. We do this because users do not have permissions to install software on their computers.

Flight Officer

Our network is generally performing adequately. However, I frequently have to make long-distance calls to the office to establish a dial-up connection. Often I do not get a connection because of a busy tone, and when I do get a connection I frequently get disconnected.

Business Requirements

Office Worker

It takes more than five minutes to log on to the network. When I finally log on to the network, my computer tries to automatically install software, but eventually fails. However, I have noticed that my computer seems to respond better after this occurs.

I have to remember too many passwords. Currently, there are three: one for the domain, one for access to the ATC application, and one for access to the Manifest application.

Business Drivers

The following business requirements must be considered:

- Blue Yonder Airlines wants to establish a public Web site that is available 24 hours a day, seven days a week. New customers must be able to access this Web site by using a single URL.
- Internal users must be able to access resources by providing their respective user names and passwords once per session.
- Managers in the finance department are dissatisfied with the high number of expense claims they receive from flight officers for dial-up connections to the ISP.

Organizational Goals

The following organizational requirements must be considered:

- Two new branch offices will be established in Berlin and Paris.
- The new offices will connect to each other by means of a permanent WAN link.
- The new offices will share a new WAN link to the Sydney office.
- The expected number of new users in these offices is 100.
- A new European administrative group will be established to manage these users and their resources.

Security

The following security requirements must be considered:

- Flight officers must be able to access secure data from any company office or from any remote location.
- Flight officers and users of the Manifest application must be able to access Manifest data.

Customer Requirements

The following customer requirements must be considered:

- User accounts must be created correctly in Active Directory and must be able to use all features of Active Directory and the ATC application simultaneously.
- Faster name resolution is required when connecting to internal servers and external Web sites.

Technical Requirements

Active Directory

The following Active Directory requirements must be considered:

- The Manifest application requires separate administration to meet European legal requirements.
- Software deployment and security settings are different for users in each department. As users travel between locations, their user information must always be available locally.
- Each branch office needs to resolve all NetBIOS names even if a WAN link goes down.
- The browser settings must be distributed to computers by using GPOs.
- The company's administrative model will change to a decentralized model with the addition of a second administrative group in Europe. Both administrative groups require smart card authentication for server administration.
- VPN access is required for flight officers only.

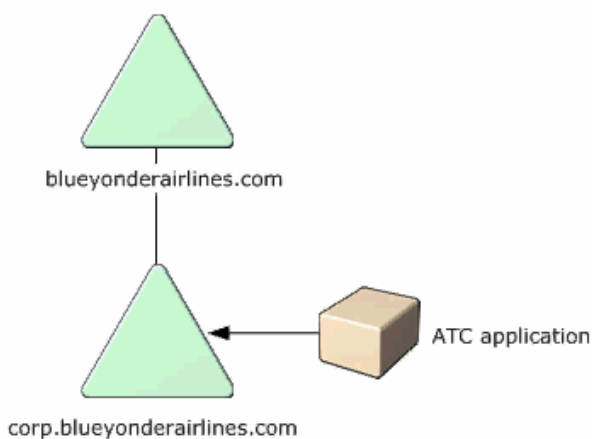
Network Infrastructure

The following infrastructure requirements must be considered:

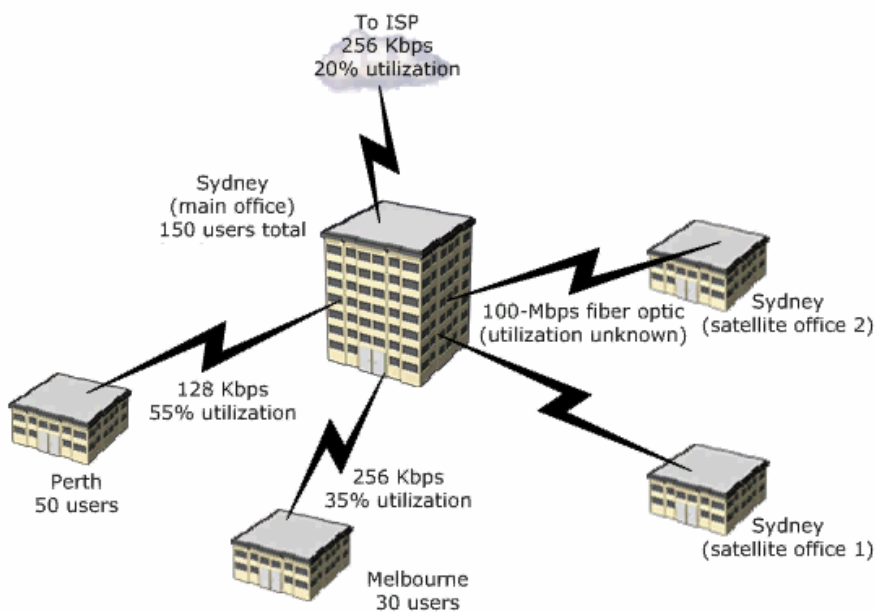
- The planned network is shown in the **Planned Network Infrastructure** exhibit. (Click the **Case Study Exhibits** button, and then click **Planned Network Infrastructure**.)
- Redundancy for any service must be provided if a single server fails.
- A WAN link from the new Berlin office will connect to the Sydney office. Another WAN link will connect the Paris office to the Berlin office.
- User reports of lengthy logon times must be resolved.
- Daily updates of antivirus software must be executed for all desktop computers.

Case Study Exhibit

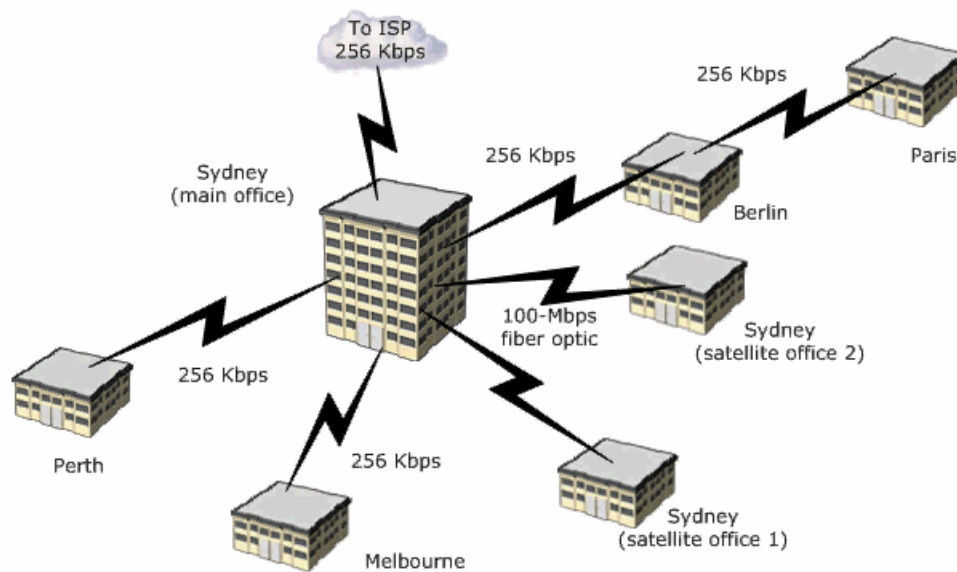
Existing Domain Model



Existing Network Infrastructure



Planned Network Infrastructure



Question

1

You are designing an authentication solution to meet the security needs of the network administrators. You install an enterprise root certification authority (CA). Which three additional actions should you perform? (Each correct answer presents part of the solution. Choose three.)

- A. Enroll each administrative account for a smart card authentication certificate.
- B. Configure autoenrollment for computer authentication certificates.
- C. Install a smart card reader on each server computer.
- D. Install a smart card reader on each network administrator's computer.
- E. Configure each administrative account to require a smart card for interactive logon.
- F. Configure the Default Domain Policy Group Policy object (GPO) to require smart cards for interactive logon.

2

You are designing a domain naming strategy for the new environment. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. Register airlines.com as a new domain.
- B. Register manifest.airlines.com as a new domain.
- C. Register manifest.blueyonderairlines.com as a new domain name.
- D. Maintain the existing blueyonderairlines.com registered domain name.
- E. Use the UPN suffix of airlines.com for all new users.
- F. Use the UPN suffix of blueyonderairlines.com for all new users.

3

You are designing a DNS implementation strategy to meet the business and technical requirements. What should you do?

- A. Configure a domain controller in each branch office to contain a secondary zone of the contoso.com domain.
- B. Configure the DNS Server service on a domain controller in each office. Configure an Active Directory-integrated zone to replicate to all DNS servers.
- C. Configure an Active Directory-integrated zone on a domain controller in Sydney. Configure this zone to replicate to all domain controllers.
- D. Configure a primary zone for blueyonderairlines.com on a domain controller in Sydney. Configure a secondary zone on another DNS server in Sydney.

4

You are designing an IP address management strategy to address the anticipated growth of the company and to meet the business and technical requirements. What should you do?

- A. Install one DHCP server in each branch office and in Sydney. On each server, create duplicate scopes that contain the necessary scope options. Configure the scopes to assign all of the available IP addresses to each office.
- B. Install one DHCP server in each branch office and in Sydney. On each server, create duplicate scopes that contain the necessary scope options. Configure the scopes to assign half of the available IP addresses to each office.
- C. Install two DHCP servers in each branch office and in Sydney. Authorize one server in each office. On each server, create duplicate scopes that contain the necessary scope options. Configure the scopes to assign half of the available IP addresses to each office.
- D. Install two DHCP servers in each branch office and in Sydney. Authorize both servers in each office. On each server, create duplicate scopes that contain the necessary scope options. Configure the scopes to assign half of the available IP addresses to each office.

5

You are designing a site topology for the new Active Directory environment. What should you do?

- A. Create one site for all offices. Place the subnets for the four branch offices and the Sydney main office in this site.
- B. Create two sites: one site for the four branch offices and one site for the Sydney main office. Place the subnets for the branch offices in one site. Place the subnet for the Sydney main office in the other site.
- C. Create three sites: one site for the four branch offices, one site for the Sydney main office, and one site for the Sydney satellite offices.
- D. Create four sites: one site for the Melbourne and Perth branch offices, one site for the Berlin and Paris branch offices, one site for the Sydney main office, and one site for the Sydney satellite offices.
- E. Create five sites: one site for the Melbourne branch office, one site for the Perth branch office, one site for the Berlin branch office, one site for the Paris branch office, and one site for the Sydney main office. Place the subnets for each branch office and the Sydney main office in their respective sites.

6

You are designing a strategy for the placement of servers to meet the business and technical requirements. What should you do?

To answer, drag the appropriate server or servers to the correct location or locations in the work area.

Servers	Work Area
<div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">Domain controller</div> <div style="border: 1px solid black; padding: 5px;">Domain controller with global catalog</div>	<p>The diagram shows a central Sydney office (represented by a large building icon) connected to four other offices: Perth, Melbourne, Berlin, and Paris (represented by smaller building icons). Each office location has a grey box next to it with the text "Drag server here".</p>