



Pro: Windows Server® 2008, Server Administrator

1

Your network contains a Windows Server 2008 server that functions as a file server. All users have laptop computers that run Windows Vista. The network is not connected to the Internet.

Users save files to a shared folder on the server.

You need to design a data provisioning solution that meets the following requirements:

- Users who are not connected to the corporate network must be able to access the files and the folders in the corporate network.
- Unauthorized users must not have access to the cached files and folders.

What should you do?

- A. Implement a certification authority (CA). Configure IPsec domain isolation.
- B. Implement a certification authority (CA). Configure Encrypting File System (EFS) for the drive that hosts the files.
- C. Implement Windows SharePoint Services 3.0. Enable Secure Socket Layer (SSL) encryption.
- D. Configure caching on the shared folder. Configure offline files to use encryption.

2

Your network consists of a single Active Directory domain. All servers run Windows Server 2008. All client computers run Windows Vista Service Pack 1. Some users have laptop computers and work remotely from home.

You need to plan a data provisioning infrastructure to secure sensitive files. Your plan must meet the following requirements:

- Files must be stored in an encrypted format.
- Files must be accessible by remote users over the Internet.
- Files must be encrypted while they are transmitted over the Internet.

What should you include in your plan?

- A. Deploy one Windows SharePoint Services site. Require users to access the SharePoint site by using a Secure Socket Transmission Protocol (SSTP) connection.
- B. Deploy two Windows SharePoint Services sites. Configure one site for internal users. Configure the other site for remote users. Publish the SharePoint sites by using HTTPS.
- C. Configure a Network Policy and Access Server (NPAS) to act as a VPN server. Require remote users to access the files by using an IPsec connection to the VPN server.
- D. Store all sensitive files in folders that are encrypted by using Encrypting File System (EFS). Require remote users to access the files by using Secure Socket Transmission Protocol (SSTP).

3

Your network consists of a single Active Directory domain. Your network contains 10 servers and 500 client computers. All domain controllers run Windows Server 2008.

A Windows Server 2008 server has Terminal Services installed. All client computers run Windows XP Service Pack 2.

You plan to deploy a new line-of-business application. The application requires desktop themes to be enabled.

You need to recommend a deployment strategy that meets the following requirements:

- Only authorized users must be allowed to access the application.
- Authorized users must be able to access the application from any client computer.
- Your strategy must minimize changes to the client computers.
- Your strategy must minimize software costs.

What should you recommend?

- A. Upgrade all client computers to Windows Vista. Deploy the application to all client computers by using a Group Policy object (GPO).
- B. Upgrade all client computers to Windows Vista. Deploy the application to the authorized users by using a Group Policy object (GPO).
- C. Deploy the Remote Desktop Connection (RDC) 6.0 software to the client computers. Install the application on the terminal server. Implement Terminal Services Session Broker (TS Session Broker).
- D. Deploy the Remote Desktop Connection (RDC) 6.0 software to the client computers. Enable the Desktop Experience feature on the terminal server. Install the application on the terminal server.

4

Your network consists of a single Active Directory domain. All domain controllers run Windows Server 2008. There are five servers that run Windows Server 2003. The Windows Server 2003 servers have the Terminal Server component installed. A firewall server runs Microsoft Internet Security and Acceleration (ISA) Server 2006. All client computers run Windows Vista.

You plan to give remote users access to the Terminal Server servers.

You need to create a remote access strategy for the Terminal Server servers that meets the following requirements:

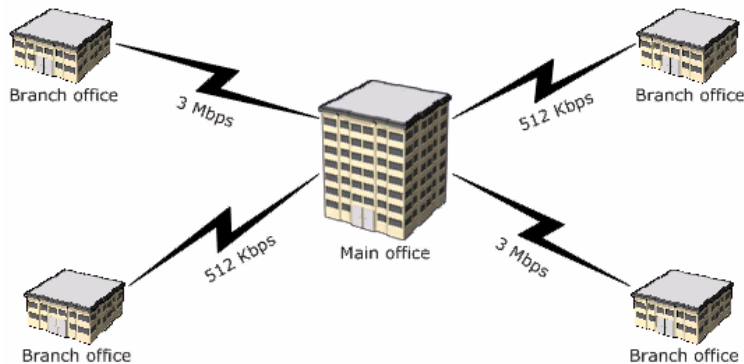
- Minimizes the number of open ports on the firewall server
- Encrypts all remote connections to the Terminal Server servers
- Prevents network access to client computers that have Windows Firewall disabled

What should you do?

- A. Implement port forwarding on the ISA Server. Implement Network Access Quarantine Control on the ISA Server.
- B. Upgrade a Windows Server 2003 server to Windows Server 2008. On the Windows Server 2008 server, implement the Terminal Services Gateway (TS Gateway) role, and implement Network Access Protection (NAP).
- C. Upgrade a Windows Server 2003 server to Windows Server 2008. On the Windows Server 2008 server, implement the Terminal Services Gateway (TS Gateway) role, and configure a Terminal Services connection authorization policy (TS CAP).
- D. Upgrade a Windows Server 2003 server to Windows Server 2008. On the Windows Server 2008 server, implement the Terminal Services Gateway (TS Gateway) role, and configure a Terminal Services resource authorization policy (TS RAP).

5

Your network is configured as shown in the following diagram.



Each office contains a server that has the File Server role installed. The servers have a shared folder named Resources.

You need to plan the data availability of the Resources folder. Your plan must meet the following requirements:

- If a WAN link fails, the files in the Resources folder must be available in all of the offices.
- If a single server fails, the files in the Resources folder must be available in each of the branch offices, and the users must be able to use existing drive mappings.
- Your plan must minimize network traffic over the WAN links.

What should you include in your plan?

- A. a stand-alone DFS namespace that uses DFS Replication in a full mesh topology
- B. a domain-based DFS namespace that uses DFS Replication in a full mesh topology
- C. a stand-alone DFS namespace that uses DFS Replication in a hub and spoke topology
- D. a domain-based DFS namespace that uses DFS Replication in a hub and spoke topology

6

Your network consists of a single Active Directory domain. All domain controllers run Windows Server 2008. All client computers run Windows Vista.

All user accounts are stored in an organizational unit (OU) named Staff. All client computer accounts are stored in an OU named Clients.

You plan to deploy a new application.

You need to ensure that the application deployment meets the following requirements:

- Users must access the application from an icon on the Start menu.
- The application must be available to remote users when they are offline.

What should you do?

- A. Publish the application to users in the Staff OU.
- B. Publish the application to users in the Clients OU.
- C. Assign the application to computers in the Staff OU.
- D. Assign the application to computers in the Clients OU.

7

Your network contains five Windows Server 2008 servers that have Terminal Services installed.

You plan to establish a Terminal Services server farm.

You need to ensure that the server farm meets the following requirements:

- New users automatically connect to the terminal server that has the fewest active sessions.
- Disconnected users are redirected to the server that contains their previous session.

What should you implement?

- A. Network Load Balancing (NLB)
- B. Round-robin DNS
- C. Terminal Services Gateway (TS Gateway)
- D. Terminal Services Session Broker (TS Session Broker)

8

Your network contains a server that runs Windows Server 2008.

You need to design a solution that allows users to collaborate with each other and that meets the following requirements:

- Enables remote access to files by using a Web browser
- Supports the addition of more Web servers based on company growth
- Enables secure access to files by assigning permissions
- Enables full-text indexing of all user content

What should you include in your design?

- A. the Web Server role
- B. the Application Server role
- C. Microsoft Office SharePoint Server 2007
- D. Microsoft System Center Operations Manager (SCOM)

9

Your network contains a single Active Directory domain. All domain controllers run Windows Server 2008. There are 1,000 client computers that run Windows Vista and that are connected to managed switches.

You need to recommend a strategy for network access that meets the following requirements:

- Users are unable to bypass network access restrictions.
- Only client computers that have up-to-date service packs installed can access the network.
- Only client computers that have up-to-date anti-malware software installed can access the network.

What should you recommend?

- A. Implement Network Access Protection (NAP) that uses DHCP enforcement.
- B. Implement Network Access Protection (NAP) that uses 802.1x enforcement.
- C. Implement a Network Policy Server (NPS), and enable IPsec on the domain controllers.
- D. Implement a Network Policy Server (NPS), and enable Remote Authentication Dial-In User Service (RADIUS) authentication on the managed switches.

10

Your network consists of a single Active Directory domain. All domain controllers run Windows Server 2008.

Your company and an external partner plan to collaborate on a project. The external partner has an Active Directory domain that contains Windows Server 2008 domain controllers.

You need to design a collaboration solution that meets the following requirements:

- Allows users to prevent sensitive documents from being forwarded to untrusted recipients or from being printed.
- Allows users in the external partner organization to access the protected content to which they have been granted rights.
- Sends all inter-organizational traffic over port 443.
- Minimizes the administrative effort required to manage the external users.

What should you include in your design?

- A. Establish a federated trust between your company and the external partner. Deploy a Windows Server 2008 server that has the Windows SharePoint Services role installed.
- B. Establish a federated trust between your company and the external partner. Deploy a Windows Server 2008 server that runs Microsoft Office SharePoint Server 2007 and that has the Active Directory Rights Management Services (AD RMS) role installed.
- C. Establish an external forest trust between your company and the external partner. Deploy a Windows Server 2008 server that has the Active Directory Certificate Services role installed. Implement Encrypting File System (EFS).
- D. Establish an external forest trust between your company and the external partner. Deploy a Windows Server 2008 server that has the Active Directory Rights Management Service (AD RMS) role installed and the Windows SharePoint Services role installed.

11

Your network consists of a single Active Directory forest. The sales department in your company has 600 Windows Server 2008 servers.

You need to recommend a solution to monitor the performance of the 600 servers. Your solution must meet the following requirements:

- Generate alerts when the average processor usage is higher than 90 percent for 20 minutes.
- Automatically adjust the processor monitoring threshold to allow for temporary changes in the workload.

What should you recommend?

- A. Install Windows System Resource Manager (WSRM) on each server.
- B. Deploy Microsoft System Center Operations Manager (SCOM).
- C. Deploy Microsoft System Center Configuration Manager (SCCM).
- D. Configure Microsoft Windows Reliability and Performance Monitor on each server.

12

You install an application on a Windows Server 2008 failover cluster. The cluster contains a node named Server1.

You have a service level agreement (SLA) that requires 50 percent of the processor utilization and the memory utilization to be reserved for the application.

You need to recommend a solution that guarantees the level of performance specified in the SLA.

What should you recommend?

- A. Implement File Server Resource Manager (FSRM) and configure quotas.
- B. Implement Storage Manager for SANs (SMfS) and configure the LUN Management settings.
- C. Implement Windows System Resource Manager (WSRM) and configure a resource-allocation policy for user-based management.
- D. Implement Windows System Resource Manager (WSRM) and configure a resource-allocation policy for process-based management.

13

Your network consists of a single Active Directory domain. All domain controllers run Windows Server 2008. All client computers run Windows Vista and Microsoft Office Outlook 2007.

Users access the following resources on the network:

- Windows Server 2008 file servers
- A database server on TCP port 47182
- Microsoft Exchange Server 2007 servers by using Outlook 2007

You plan to provide users with remote access to the network. The remote users work from locations that only support access to the Internet by using HTTP and HTTPS.

You need to recommend a remote access strategy that meets the following requirements:

- Remote users must have access to the database server.
- Remote users must be able to establish secure connections to the network.
- Remote users must have access to e-mail and file resources on the network.

What should you recommend?

- A. Upgrade all client computers to Windows Vista Service Pack 1. Implement Outlook Anywhere for Exchange Server 2007.
- B. Upgrade all client computers to Windows Vista Service Pack 1. Implement a VPN solution that uses Secure Socket Tunneling Protocol (SSTP).
- C. Implement a VPN solution that uses Point-to-Point Tunneling Protocol (PPTP). Deploy Connection Manager Administration Kit (CMAK) profiles to the client computers.
- D. Implement a VPN solution that uses Layer Two Tunneling Protocol (L2TP). Deploy Connection Manager Administration Kit (CMAK) profiles to the client computers.

14

Your network consists of a single Active Directory domain. The network contains two Windows Server 2008 computers named Server1 and Server2. The company has two identical print devices.

You plan to deploy print services.

You need to plan a print services infrastructure to meet the following requirements:

- Manage the print queue from a central location.
- Make the print services available, even if one of the print devices fails.

What should you include in your plan?

- A. Install and share a printer on Server1. Enable printer pooling.
- B. Install the Terminal Services server role on both servers. Configure Terminal Services Session Broker (TS Session Broker).
- C. Install and share a printer on Server1. Install and share a printer on Server2. Use Print Manager to install the printers on the client computers.
- D. Add Server1 and Server2 to a Network Load Balancing cluster. Install a printer on each node of the cluster.

15

Your company has 10,000 computers.

You need to design a storage architecture for Windows Server Update Services (WSUS) updates. You also need to ensure that the WSUS updates are highly available.

What should you include in your design?

- A. Store the WSUS updates on a remote file share.
- B. Store the WSUS updates on a Distributed File System (DFS) link that uses multiple replicating targets.
- C. Store the WSUS updates on each WSUS server. Configure each WSUS server to use a RAID 0 hardware controller.
- D. Store the WSUS updates on a multihomed network file server. Create two host (A) resource records for the WSUS servers.

16

Your network consists of a single Active Directory domain. All domain controllers run Windows Server 2008. All servers run Windows Server 2008. All client computers run Windows Vista.

You need to generate a monthly report on the status of software updates for the client computers. Your solution must meet the following requirements:

- Display all of the operating system updates that installed successfully
- Display all of the Microsoft application updates that installed successfully
- Display all of the operating system updates that failed to install
- Display all of the Microsoft application updates that failed to install
- Minimize administrative effort
- Minimize costs

What should you do?

- A. Install Microsoft System Center Essentials (Essentials) 2007. Deploy management agents on all client computers.
- B. Install Microsoft System Center Configuration Manager (SCCM) 2007. Deploy management agents on all client computers.
- C. Install Windows Software Update Services (WSUS) 3.0. Configure Windows Update by using a Group Policy object (GPO).
- D. Deploy Microsoft Baseline Security Analyzer (MBSA) 2.1 on the client computers. Run MBSA on each client computer, and save the report to a shared folder on the network.

17

Your network contains several Windows Server 2008 servers that run Windows Server Update Services (WSUS). The WSUS servers distribute updates to all computers on the internal network.

Remote users connect from their personal computers to the internal network by using a split-tunnel VPN connection.

You need to plan a strategy for patch management that deploys updates on the remote users' computers. Your strategy must meet the following requirements:

- Minimize bandwidth use over the VPN connections
- Require updates to be approved on the WSUS servers before they are installed on the client computers

What should you include in your plan?

- A. Create a Group Policy object (GPO) to perform client-side targeting.
- B. Create a computer group for the remote users' computers. Configure the remote users' computers to use the internal WSUS server.
- C. Create a custom connection by using the Connection Manager Administration Kit (CMAK). Deploy the custom connection to all of the remote users' computers.
- D. Deploy an additional WSUS server. Configure the remote users' computers to use the additional WSUS server. Configure the additional WSUS server to leave the updates on the Microsoft Update Web site.

18

Your network contains two DHCP servers. The DHCP servers are named DHCP1 and DHCP2. The internal network contains 1,000 DHCP client computers that are located on a single subnet. A router separates the internal network from the Internet. The router has a single IP address on the internal interface.

DHCP1 has the following scope information.

- Starting IP address: 172.16.0.1
- Ending IP address: 172.16.7.255
- Subnet mask: 255.255.240.0

You need to provide a fault-tolerant DHCP infrastructure that supports the client computers on the internal network. In the event that a DHCP server fails, all client computers must be able to obtain a valid IP address.

How should you configure DHCP2?

- A. Create a scope for the subnet 172.16.0.0/20. Configure the scope to use a starting IP address of 172.16.8.1 and an ending IP address of 172.16.15.254.
- B. Create a scope for the subnet 172.16.0.0/21. Configure the scope to use a starting IP address of 172.16.0.1 and an ending IP address of 172.16.15.254.
- C. Create a scope for the subnet 172.16.8.0/21. Configure the scope to use a starting IP address of 172.16.8.1 and an ending IP address of 172.16.10.254.
- D. Create a scope for the subnet 172.17.0.0/16. Configure the scope to use a starting IP address of 172.17.0.1 and an ending IP address of 172.17.255.254.