

GlobalTcert.com

GLOBALTCERT.COM
Your gateway to success



Demo
STUDY GUIDE

© Copy Right 1998-2005 GlobalTcert LLC. All Rights Reserved.

QUESTION 83

You are a security administrator for GlobalitcerT . The network consists of a single Active Directory domain named GlobalitcerT .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.

GlobalitcerT hosts Web applications for customers. Each customer is a company that has multiple employees who require access to the Web application. Each customer has one Web application. Each Web application is configured as a virtual directory. You configure a user account for each customer. You assign this account permission to read the virtual directory that contains the customer's Web application. You need to ensure that employees can access only their company's Web application. You must accomplish this task without requiring customers to disclose passwords.

What should you do?

- A. Configure anonymous access for each virtual directory.
Configure each virtual directory to use the customer's assigned user account.
Leave the password assigned to the user account blank.
- B. Configure Microsoft .NET Passport authentication for each virtual directory.
Instruct each employee of each customer that requires access to the Web site to enroll for a new .NET Passport.
- C. Configure a certification authority (CA).
Issue certificates to each employee of each customer that requires access to the Web site.
Configure many-to-one certificate mapping.
- D. Acquire a Server Authentication digital certificate from a public certification authority (CA).
Configure the Web server to use this certificate and to require SSL.
Distribute a copy of the Server Authentication certificate to each employee of each customer that requires access to the Web site.

Answer: C

Explanation:

Anonymous would allow access to any of the websites.

Microsoft .NET Passport would have the user use passwords.

11 Deploying, Configuring, and
Managing SSL Certificates

IIS cannot process client certificates unless you have previously installed a server certificate and enabled HTTPS.

There are two ways to improve the security of client certificates. First, you can use client certificate mapping to restrict access to users with specific certificates. (You can also use client certificate mapping to control authorization by mapping the certificates to existing user accounts.) Second, you can configure a certificate trust list (CTL) to reduce the number of root CAs that can issue certificates to your users. One-to-one client certificate mapping

Client certificate mapping has two modes: one-to-one and many-to-one. One-to-one certificate mapping relates a single exported certificate to an Active Directory user account. When Web users present the certificate, they will be authenticated as if they had presented a valid user name and password.

Many-to-one client certificate mapping

Many-to-one certificate mapping uses wildcard matching rules that verify whether a client certificate contains specific information, such as the issuer or subject. This mapping does not identify individual client certificates;

it accepts all client certificates fulfilling the specific criteria. If a client gets another certificate containing all the same user information, the existing mapping will still work. Certificates do not need to be exported for use in many-to-one mappings. To add many-to-one certificate mappings, follow this procedure:

1. View the properties for the Web site, and then click the Directory Security tab.
2. Click the Edit button in the Secure Communications box.
3. Select the Enable Client Certificate Mapping check box, and then click the Edit button.
4. Click the Many-1 tab, and then click the Add button.
5. On the General page, type a name for the rule in the Description box. Click Next.
6. On the Rules page, click New to add a rule. Editing rule properties for many-to-one client certificate mappings
7. In the Edit Rule Element dialog box, click the Certificate Field list to choose either Issuer or Subject. Select Issuer to filter based on the CA that issued the certificate. Choose Subject to filter based on who the certificate was issued to. After completing the rule element, click OK. Security Alert When creating certificate mapping rules, keep in mind how easy it is to create your own root CA
- A. Attackers could easily create their own root CA using your domain names. To prevent this type of impersonation, use certificate mapping along with a certificate trust list.
8. To add an additional rule, return to step 6.
9. Click Next.
10. On the Mapping page, click Refuse Access to reject logons that match the criteria, or click Accept This Certificate For Logon Authentication to map matching certificates to a user account. If you choose to accept the certificate, complete the Account and Password boxes. Click Finish. If prompted, confirm the password and then click OK. Before you can authenticate users with client certificates, you must issue client certificates. If the users are members of an Active Directory domain and you are using an enterprise CA, auto-enrollment is the most efficient way to enroll users. Web servers are often used to communicate with users outside of your organization, however. For these users, you should use Web enrollment. The exercise at the end of this lesson demonstrates the process of enrolling a user certificate by using Web enrollment and then authenticating that user to IIS.

QUESTION 84

You are a security administrator for GlobalitcerT .com. The network consists of a single Active Directory domain named GlobalitcerT .com. The domain contains Windows Server 2003 computers. You manage a Windows Server 2003 computer named GlobalitcerT 6 that is a domain member server. You use IIS on GlobalitcerT 6 to host an Internet Web site. This web site published information to employees of a partner company.

The partner company network consists of a single Active Directory domain. Approximately 500 partner company employees connect over the Internet to access company confidential data on GlobalitcerT 6. All partner company employees need access to the same data.

The partner company IT department maintains a certificate authority (CA). They use this CA to issue Authentication Session certificates to all employees in their company. Copies of these certificates are stored with employee user accounts in the partner company's Active Directory domain.

You need to authenticate users to GlobalitcerT 6 based on possession of their company-issued certificate. You want to achieve this goal by using the minimum amount of administrative effort. You enable SSL and the certificate-based authentication option on GlobalitcerT 6. You add the partner root CA certificate to the Trusted Root Certification Authorities store on GlobalitcerT 6.

Which three additional actions you perform? (Each correct answer presents part of the solution. Choose

three.)

- A. Create a security group named PartnerEmployees and a user account named PartnerUser in your Active Directory domain. Add this account to the PartnerEmployees group.
- B. Create a security group named PartnerEmployees and a user account for every partner company employee in your Active Directory domain. Add these accounts to the PartnerEmployees group.
- C. Assign the PartnerEmployees group access to the appropriate data on GlobalitcerT 6.
- D. Add a many-to-one certificate mapping in ISS on GlobalitcerT 6. Create a mapping rule to accept certificates issued by the partner company's internal CA.
- E. Add one-to-one certificate mappings for every partner employee in IIS on GlobalitcerT 6.

Answer: A, C, D

Note: Many-to-one certificate mapping uses wildcard matching rules that verify whether a client certificate contains specific information, such as the issuer or subject.

QUESTION 85

You are a security administrator for GlobalitcerT . The network consists of a single Active Directory domain named GlobalitcerT .com. All domain controllers run Windows Server 2003. All client computers run Windows XP Professional.

Users store files on a server named GlobalitcerT 1. These files are confidential and must be encrypted at all times while on GlobalitcerT 1.

You configure a new certification authority (CA) and issue certificate that support Encrypting File System (EFS) to all users. Users report that they cannot encrypt files that are stored on GlobalitcerT 1. They report that they can encrypt files that are stored locally on their client computers.

You need to ensure that users can encrypt files that are stored on GlobalitcerT

1. What should you do?

- A. Enroll GlobalitcerT 1 for a Computer certificate that supports file encryption.
- B. Configure a new EFS recovery agent. Deploy the EFS recovery agent by using Active Directory.
- C. Configure the GlobalitcerT 1 computer account to be trusted for delegation.
- D. Enroll each client computer for a Computer certificate that supports file encryption.

Answer: C

Explanation:

Unable to Encrypt Files

If you find that you are unable to encrypt files or folders, one of the following might be the cause:

The file is not an NTFS volume.

You do not have Write access to the file.

If you are having trouble encrypting a remote file, check to see that your user profile is available for EFS to use on that computer (this typically means having a roaming user profile), make sure the remote computer is trusted for delegation, and make sure your account is configured to enable delegation. Sensitive accounts are not enabled for delegation by default, so users like Enterprise Administrator might not be able to encrypt or decrypt files remotely.

Note: Sometimes users think that a file is not encrypted because they can open it and read the file. You can