



IBM

LOT-841

Lotus Notes Domino 8 Implementing and Administering Security

Answer: A

Question: 103

The Umbrella corporation implemented ID recovery procedures. ID recovery must be performed by more than one person, and they have included the Domino administration team as well as the Chief Security Officer for the company. They wish for Chief Security Officer to be present for all ID recoveries. Where are the names of the people who are allowed to recover IDs stored?

- A. The certifier id file
- B. The server notes.ini file
- C. The user's local notes.ini file
- D. The certifier document in the Domino Directory

Answer: A

Question: 104

Users and Maximum Property Resellers are migrating from Domino 6 to Domino 8 and have deployed Smartcards to all sales agents in the field across the country. One important gain in Smartcard security between the versions is which of the following?

- A. A special password object may now be placed on the Smartcard
- B. X.509 certificates may be used in Domino 8 to secure the notes id
- C. Passphrases may be used in Domino 8 to secure the notes id password
- D. A pin is no longer required entry for servers that start with a Smartcard enabled server.id file

Answer: B

Question: 105

A new corporate security policy has been mandated for all users on Lotus Notes that passwords must be changed every 45 days. You are responsible for forcing the new security policy. After creating the necessary security policy document that applies to the entire Organization, some users are getting locked out of their Notes id files after the first 45 day cycle occurs. Which of the following best explains the reason for users getting locked out of their id files?

- A. The grace period is set to the default for the security policy document and users have passed the default
- B. The users affected have their user id filed placed on Smartcards and a PIN number assigned
- C. The users' new password did not meet the password length criteria assigned by the security policy
- D. The users' Internet password does not match their Notes id password and security policies that enforce password change must also have the Internet and Notes password synchronized

Answer: B

Question: 106

Notes users are able to generate key rollover requests without the use of a security settings policy document. While generating the request, what are the two options the user has in enervating key rollover?

- A. ID recertification and ID recovery
- B. Key enhancement and new key generation
- C. Public key change and private key change 27
- D. Authentication protocol and mail protocol

Answer: D

Question: 107

The trusting of unsigned content has become an issue in the Auto One domain. You, acting as the Domino administrator, must attempt to restrict user from allowing such content to run. You have pushed out an Administration ECL that denies unsigned content to run but users are still allowing it when prompted. Which of the following is your best option at controlling the users in the Auto One domain?

- A. Send the users a button to refresh their ECL with instructions on allowing unsigned content to run
- B. Force another Administration ECL update through a security policy and deselect the users ability to modify
- C. Move unsigned content into another Domino domain that is not trusted and then deny that new domain in the Administration ECL
- D. Update the Administration ECL with the desktop settings policy and deselect the option for allowing unsigned content to run on workstations

Answer: B

Question: 108

A user has entered into their user.id security dialog interface. The user then opens the 'Your Certificates' tab and selects to Create New Public Keys from the Other Actions menu. The user proceeds to initiate this action on their desktop, laptop and home machine in one day with the default settings in the dialog. The user connects to their home server at each request. What is the result of the user initiating this request at each location since they utilize multiple machines?

- A. Each id file will then be synchronized from their home server with the same keys
- B. Each request will generate an email request to the home server administrators to issue new keys
- C. Each id file will receive different password quality restrictions depending on the original type of id issued
- D. Each request will generate a new Adminp document for new keys on their home server waiting for administrator approval

Answer: D

Question: 109

Password verification may not be utilized on which of the following?

- A. ID files that have been cross-certified
- B. ID files that contain multiple passwords
- C. ID files with a password quality of zero
- D. ID files that have password recovery enabled

Answer: B

Question: 110

Kathleen has generated an ECL refresh for user's workstations. Which of the following entries must be entered into the Administration ECL to allow users to export data and allow access to network resources under their own name?

- A. <OSAdmin>
- B. <ECLOwner>

C. <WorkstationManager>
D. <LocalAdministrator>

Answer: B



Download Full Version From <https://www.certkillers.net>



DON'T KNOW
OR NO PREFERENCE

Pass your exam at First Attempt....Guaranteed!