Vendor:IBM

Exam Code:000-220

Exam Name:IBM Sterling Connect:Direct,
Administration

Version: Demo

QUESTION 1

A Sterling Connect:Direct for UNIX administrator needs to enable the node named CDLOCAL to exchange data with a remote node named CDREMOTE using Secure+ STS protocol. The administrator will use the Secure+ Command Line Interface (SPCLI) to configure the Secure+. The remote node was previously added to the netmap.

The administrator has received the following public keys from CDREMOTE:

```
exporting_node:\
    :name=CDREMOTE:
importing_node:\
    :name=CDLOCAL:\
    :auth.pubkey=0201.69D0.8C97.298C.CODB.E130.2691.C470.A4E1.B5B8.7592:\
    :sig.pubkey=0300.8437.1D18.8FE6.F96B.A445.D43E.2650.34CC.9B2A.BE4F:
```

Considering that the parmfile is already initialized and opened, which sequence of commands will successfully accomplish this task on the CDLOCAL side?

```
C A.  sync netmap path=/ibm/mft/cdunix41/ndm/cfg/CDLOCAL/netmap.cfg name=CDLOCAL;
      update remoterode name=CDREMOTE protocol=sts override=y
          stsauthlocalkey=gen stsauthkeyseedType=dynamic
          stssiglocalkey=gen stssigkeyseedType=dynamic
          STSAuthRemoteKey=0201.69D0.8C97.298C.CODB.E130.2691.C470.A4E1.B5B8.7592
          STSSigRemoteKey=0300.8437.1D18.8FE6.F96B.A445.D43E.2650.34CC.9B2A.BE4F;

C B.  sync netmap path=/ibm/mft/cdunix41/ndm/cfg/CDLOCAL/netmap.cfg name=CDREMOTE;
      update remoterode name=CDREMOTE protocol=sts override=y
          stsauthlocalkey=0201.69D0.0C97.290C.CODD.E130.2691.C470.A4E1.D5D0.7592
          stssiglocalkey=0300.8437.1D18.8FE6.F96B.A445.D43E.2650.34CC.9B2A.BE4F
          STSAuthRemoteKey=gen STSSigRemoteKey=gen;

C C.  update remoterode name=CDREMOTE protocol=sts override=y
          stsauthlocalkey=gen stsauthkeyseedType=dynamic
          stssiglocalkey=gen stssigkeyseedType=dynamic
          STSAuthRemoteKey=0201.69D0.8C97.298C.CUDB.E130.2691.C470.A4E1.B5B8.7592
          STSSigRemoteKey=0300.8437.1D18.8FE6.F96B.A445.D43E.2650.34CC.9B2A.BE4F;
      sync netmap path=/ibm/mft/cdunix41/ndm/cfg/CDLOCAL/netmap.cfg name=CDREMOTE;

C D.  sync netmap path=/ibm/mft/cdunix41/ndm/cfg/CDLOCAL/netmap.cfg name=*;
      update remoterode name=CDREMOTE protocol=sts override=y
          stsauthlocalkey=gen stsauthkeyseedType=dynamic
          stssiglocalkey=gen stssigkeyseedType=dynamic
          STSAuthRemoteKey=0201.69D0.8C97.298C.CODB.E130.2691.C470.A4E1.B5B8.7592
          STSSigRemoteKey=0300.8437.1D18.8FE6.F96B.A445.D43E.2650.34CC.9B2A.BE4F;
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: D

QUESTION 2

What type of key is commonly known as a public-key system because it allows the public key to be freely exchanged, but the private key is never transmitted?

A. Symmetric-key

B. Asymmetric-key

C. Certificate Authority (CA) key

D. Certificate Signing Request (CSR) key

Correct Answer: B

QUESTION 3

A Sterling Connect:Direct for Windows administrator wants to implement Sterling External Authentication Server (SEAS) to improve the security of its environment. Which statement regarding the capability of SEAS is FALSE?

A. Validates the certificate chain.

B. Returns attributes associated with the incoming certificate.

C. Validates certificates against one or more Certificate Revocation Lists (CRLs) that are stored on an LDAP server.

D. Defines an inbound node definition for each trading partner connection from outside the company and an outbound node definition for everycompany server to which SEAS will connect.

Correct Answer: D

QUESTION 4

Review the dump of the Certificate Authority (CA) root certificates: Which certificate will cause the connection to fail if it was used in a Server Authentication process during the SSL/TLS handshake?

```
============================ Certificate #1 ============================
Version: V3
Subject: CN=VeriSign Class 3 Secure Server CA, OU=Terms of use at https://www.verisign.com/rpa (c)05, OU=VeriSign Trust Network,
O="VeriSign, Inc.", C=US
Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5
Validity: [From: Tue Jan 18 18:00:00 CST 2005,
          To: Sun Jan 18 17:59:59 CST 2040]
Issuer: OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
SerialNumber: [    75337d9a b0e1233b ae2d7de4 469162d4]

============================ Certificate #2 ============================
Error: Certificate validity period - NotAfter: Thu Jan 07 17:59:59 CST 2010
Version: V1
Subject: OU=Secure Server Certification Authority, O="RSA Data Security, Inc.", C=US
Signature Algorithm: MD2withRSA, OID = 1.2.840.113549.1.1.2
Validity: [From: Tue Nov 08 18:00:00 CST 1994,
          To: Thu Jan 07 17:59:59 CST 2010]
Issuer: OU=Secure Server Certification Authority, O="RSA Data Security, Inc.", C=US
SerialNumber: [    02ad667e 4e45fe5e 576f3c98 195eddc0]

============================ Certificate #3 ============================
Warning: Certificate Signature Algorithm not FIPS approved - MD2withRSA
Version: V1
Subject: OU=Class 1 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
Signature Algorithm: MD2withRSA, OID = 1.2.840.113549.1.1.2
Validity: [From: Sun Jan 28 18:00:00 CST 1996,
          To: Tue Aug 01 18:59:59 CDT 2028]
Issuer: OU=Class 1 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
SerialNumber: [    cdba7f56 f0dfe4bc 54fe22ac b372aa55]

============================ Certificate #4 ============================
Warning: Certificate Signature Algorithm not FIPS approved - MD2withRSA
Version: V1
Subject: OU=Class 2 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
Signature Algorithm: MD2withRSA, OID = 1.2.840.113549.1.1.2
Validity: [From: Sun Jan 28 18:00:00 CST 1996,
          To: Tue Aug 01 18:59:59 CDT 2028]
Issuer: OU=Class 2 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
SerialNumber: [    2d1bfc4a 178da391 ebe7fff5 8b45be0b]
```

A. Certificate #1A.Certificate #1

B. Certificate #2B.Certificate #2

C. Certificate #3C.Certificate #3

D. Certificate #4D.Certificate #4

Correct Answer: B

QUESTION 5

A company is required to have proof of data origin and data integrity validation. The company would like to accomplish this with the Sterling Connect:Direct Secure+ STS protocol. What will provide strong authentication?

A. Data encryption

B. Digital signature

C. Cipher Block Chaining Mode

D. Certification Revocation List (CRL)

Correct Answer: B

QUESTION 6

A company has Sterling Connect:Direct for UNIX running successfully in their environment for several years. Due to a new company policy, the administrator needs to authenticate local users using LDAP. What configuration file needs to be modified?

A. userfile.cfg

B. ndmapi.cfg

C. netmap.cfg

D. initparm.cfg

Correct Answer: D

QUESTION 7

A Sterling Connect:Direct for UNIX administrator needs to configure Connect:Direct to authenticate remote users. Company policy dictates that these remote users must use snodeid to pass a user id but no password. The administrator will assign a unique user id to each remote user. What needs to be modified in the netmap.cfg that will allow the remote users to authenticate?

A. proxy.attempt

B. netmap.check

C. User proxy record

D. Remote node record

Correct Answer: A

QUESTION 8

Sterling Connect:Direct for Windows or UNIX was just installed in a cluster environment. When testing cluster failover, the Connect:Direct node was successfully restarted on another cluster node, but all previously executing processes were lost. What is the cause of this issue?

A. Connect:Direct was started with tcq.start=W.

B. Connect:Direct was started by the wrong Userid.

C. Connect:Direct was installed on a local file system.

D. Connect:Direct was installed on a shared file system.

Correct Answer: C

QUESTION 9

A Sterling Connect:Direct for z/OS administrator navigated to the Secure+ Admin Tool: Main Screen?shown here:

```
  File   Edit   Key Management   Help
  ------------------------------------------------------------------
                                                        Row 1 of 7
                   Secure+ Admin Tool: Main Screen
  Option ===>                                          Scroll CSR

                   Table Line Commands are:

  E Export pub. key        H View History        D Delete node
  U Update node            I Insert node

                      Secure
  LC Node Name         Type  123C  Override Encryption Signature ExtAuth Autoupd
  -- ------------      ----  ----  -------- ---------- --------- ------- -------
     SECURE.LOCAL01    L     NNNN     Y         N          N        N       N
     SECURE.REMOTE01   R     NNYY     N         N          N        N       N
     SECURE.REMOTE02   R     YNNN     Y         Y          Y        N       N
     SECURE.REMOTE03   R     NYNN     N         N          N        N       N
     SECURE.REMOTE04   R     NNYY     Y         N          N        N       N
     SECURE.REMOTE05   R     NYNY     Y         N          N        N       N
  ************************** BOTTOM OF DATA **************************
```

Which Connect:Direct Secure+ remote node supports the STS encryption protocol?

A. SECURE.REMOTE01

B. SECURE.REMOTE02

C. SECURE.REMOTE03

D. SECURE.REMOTE04

Correct Answer: B

QUESTION 10

Which SYSOPTS uses the correct RUN TASK syntax for a Sterling Connect:Direct for UNIX process?

A. sysopts = "unix command;unix command;unix command"

B. sysopts = ":unix command:unix command:unix command:"

C. sysopts = "\\'unix command\\',\\'unix command\\',"unix command""

D. sysopts = "cmd(unix command,unix command,unix command)"

Correct Answer: A

QUESTION 11

A Sterling Connect:Direct for Windows user1 has submitted process number 4711. User1 asks user2 for assistance with determining process completion. User2 issues a Select Statistics command, which returns information on some other processes, but nothing for process number 4711. What has happened here?

A. The process has failed to submit.

B. The process has not completed yet.

C. User1 is configured with Statistics=N.

D. User2 is configured with Statistics=Y.

Correct Answer: D

QUESTION 12

A Sterling Connect:Direct for UNIX administrator needs to enable the node named CDLOCAL to exchange data with a remote node named CDREMOTE using Secure+ with SSL protocol. Both nodes will use server authentication level, and external authentication must not be enabled. The administrator will use the Secure+ Command Line Interface (SPCLI) to configure the Secure+. The administrator has saved the trusted root certificate with filename:

/ibm/mft/cdunix41/ndm/secure+/certificates/CDREMOTE_trusted.txt

The Key Certificate file is: /ibm/mft/cdunix41/ndm/secure+/certificates/keycert.txt

Which sequence of commands will accomplish this task on the CDLOCAL side?

A. sync netmap path=/ibm/mft/cdunix41/ndm/cfg/CDLOCAL/netmap.cfg name=CDREMOTE; update remotenode name=CDREMOTE protocol=ssl override=n
SSLTLSTRUSTEDROOTCERTFILE=/ibm/mft/cdunix41/ndm/secure+/certificates/ CDREMOTE_tru sted.txt
SSLTLSCERTFILE=/ibm/mft/cdunix41/ndm/secure+/certificates/keycert.txt
SSLTLSCERTPASSPHRASE=myprivkeypassword SslTlsEnableClientAuth=n SslTlsSeaEnable=y
SeaCertValDef=CDREMOTESEA SSLTLSENABLECIPHER=all;

B. sync netmap path=/ibm/mft/cdunix41/ndm/cfg/CDLOCAL/netmap.cfg name=CDLOCAL; update remotenode name=CDREMOTE protocol=ssl override=n
SSLTLSTRUSTEDROOTCERTFILE=/ibm/mft/cdunix41/ndm/secure+/certificates/CDREMOTE_tru sted.txt
SSLTLSCERTFILE=/ibm/mft/cdunix41/ndm/secure+/certificates/keycert.txt
SSLTLSCERTPASSPHRASE=myprivkeypassword SslTlsEnableClientAuth=n SslTlsSeaEnable=n
SSLTLSENABLECIPHER=all;

C. sync netmap path=/ibm/mft/cdunix41/ndm/cfg/CDLOCAL/netmap.cfg name=*; update remotenode name=CDREMOTE protocol=ssl override=n
SSLTLSTRUSTEDROOTCERTFILE=/ibm/mft/cdunix41/ndm/secure+/certificates/CDREMOTE_tru sted.txt
SSLTLSCERTFILE=/ibm/mft/cdunix41/ndm/secure+/certificates/keycert.txt
SSLTLSCERTPASSPHRASE=myprivkeypassword SslTlsEnableClientAuth=n SslTlsSeaEnable=n
SSLTLSENABLECIPHER=all;

D. sync netmap path=/ibm/mft/cdunix41/ndm/cfg/CDLOCAL/netmap.cfg name=*; update remotenode name=CDREMOTE protocol=ssl override=n
SSLTLSTRUSTEDROOTCERTFILE=/ibm/mft/cdunix41/ndm/secure+/certificates/keycert.txt

SSLTLSCERTFILE=/ibm/mft/cdunix41/ndm/secure+/certificates/CDREMOTE_trusted.txt
SSLTLSCERTPASSPHRASE=myprivkeypassword SslTlsEnableClientAuth=n SslTlsSeaEnable=n
SSLTLSENABLECIPHER=all;

Correct Answer: C

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:

One Year Free Update
Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee
To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy
We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.