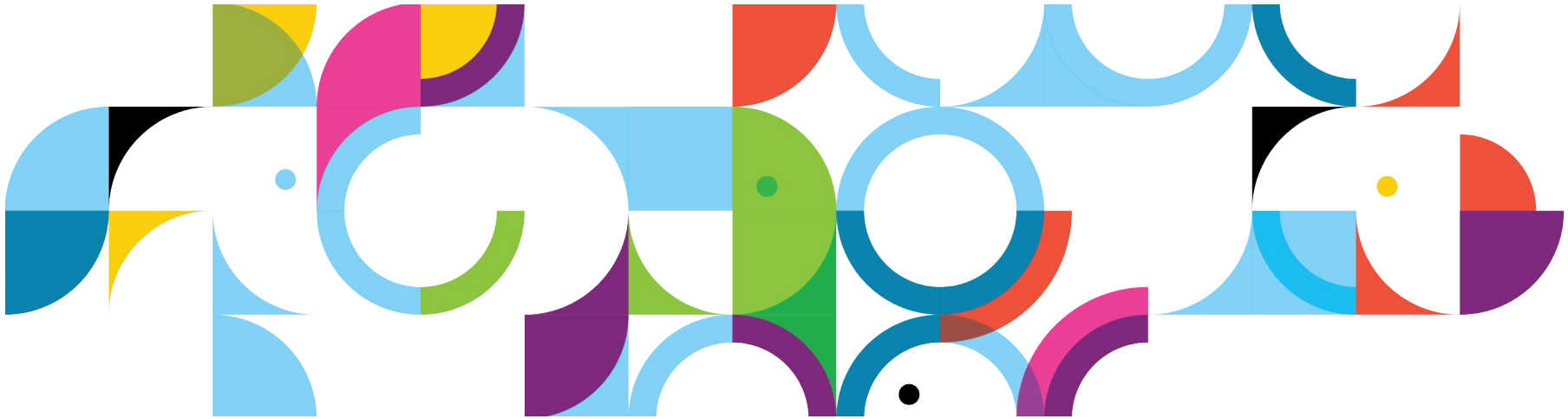
Implementing TLS support with IBM Domino 9.x and IBM HTTP Server (IHS)

19th November 2013

Yvonne Devlin | Software Engineer

IBM Collaboration Solutions



Agenda

- Background
- IBM HTTP Server(IHS) with Domino explained
- Installation of IHS
- Configuration of the Domino HTTP server
- IKEYMAN
- Creating a CSR
- Configuration of IHS
- Loading the IHS module
- Debugging
- Questions

Background

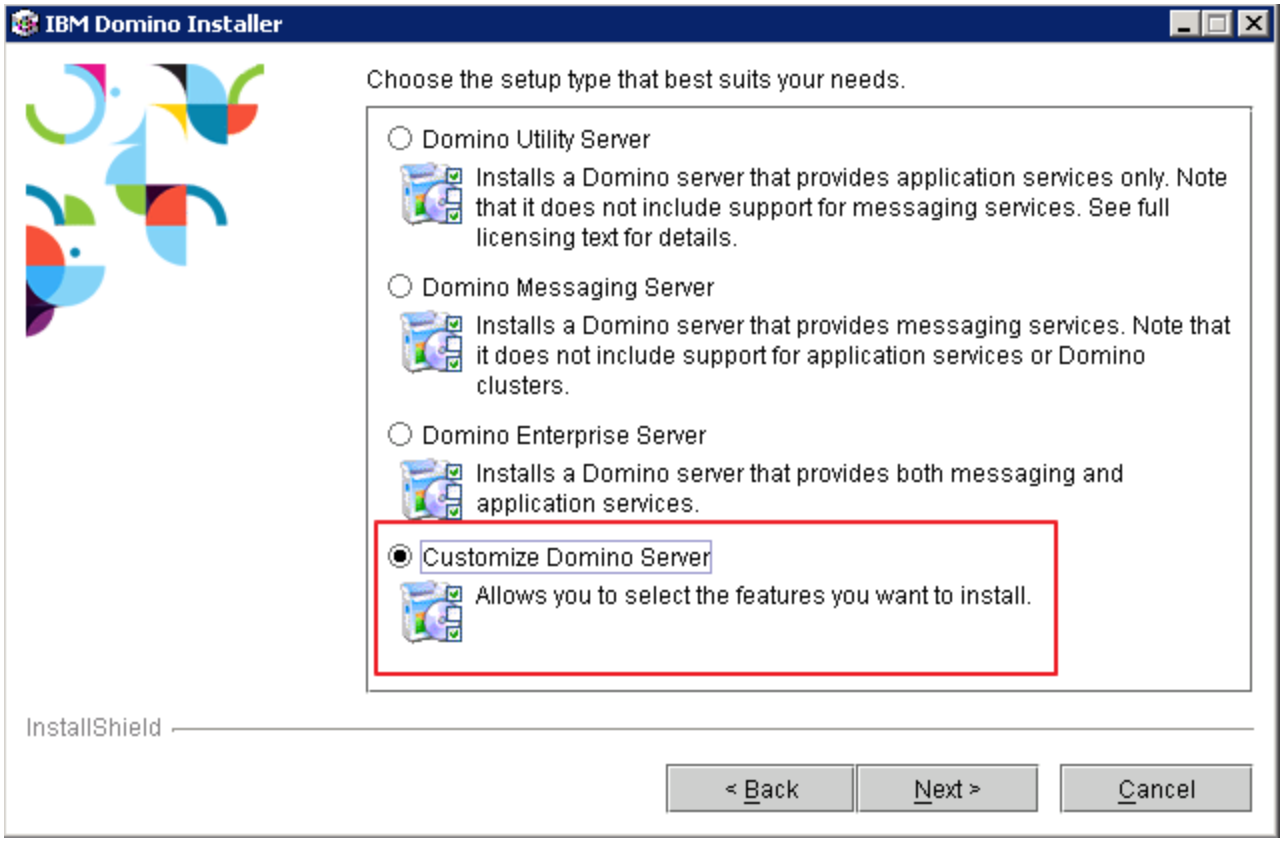
- In previous versions of Domino only SSL 3.0 was supported for secure connections. Later versions such as SSL 3.1 or TLS 1.0,1.1, 1.2 were not supported
- Applications and servers could make the initial connection to Domino using TLS but then Domino would negotiate down to SSL 3.0
- If they did not support negotiated handshakes or SSL 3.0 then the connection was dropped

IBM HTTP Server with Domino explained

- With the release of R9 Administrators now have the option of running the IBM HTTP Server on the same computer as a Domino HTTP server;
- The purpose of this enhancement is to support the Transport Layer Security (TLS) protocol
- A pass-through reverse proxy module named mod_domino is provided to forward HTTP requests to the Domino HTTP server.
- The module creates the context necessary to allow Domino interpret data received from other servers and applications using TLS.
- The IHS server is able to run "in front of" the Domino server.
- Once IHS has been enabled on the Domino server, it stops listening for requests on port 80 and port 443 and only accepts connections that originate from the same computer
- The Domino HTTP server listens on port 9288 for loop back connections from mod_domino/IBM HTTP Server.
- By default, mod_domino uses the local loop back address of 127.0.0.1 to connect to the Domino HTTP server.
- The Domino HTTP server connection settings are overridden with settings that maximize the re-use of connections between mod_domino/IBM HTTP Server and the Domino HTTP server.

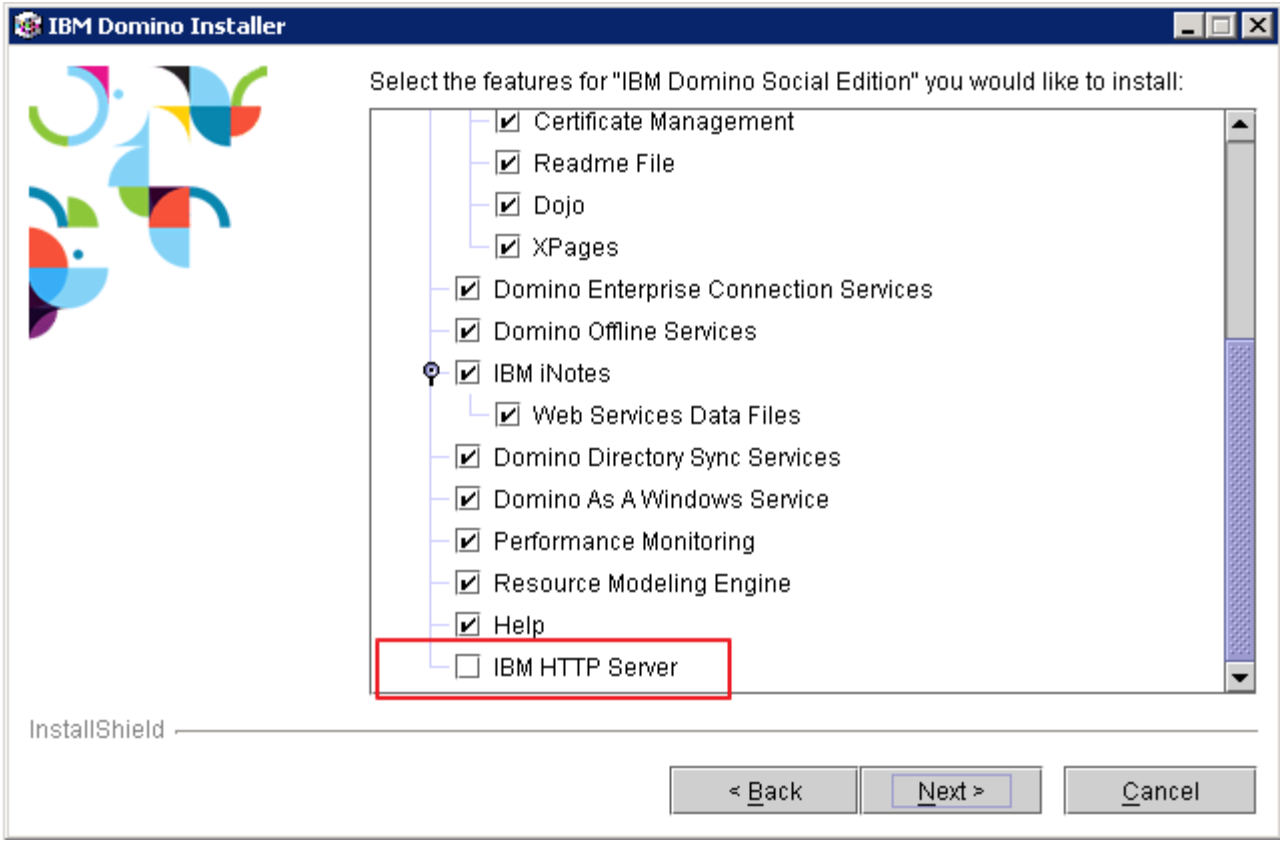
Installing IHS with Domino

- The version of IBM HTTP server required for running on the same machine as Domino is shipped with the R9 installer
- The IHS is not installed by default so select the “Customise Domino Server”



Installing IHS with Domino (cont.)

- Under Select the features for "IBM Domino Social Edition" you would like to install, enable IBM HTTP server.
- Complete the rest of the installation as normal



Configuring Domino

- Add the following parameter to the notes.ini
  - HTTPIHSEnabled=1
- Some environment variables are set prior to Domino HTTP starting the IBM HTTP server (IHS).
- You should not need to modify any of these settings.
- These environment variables are specified in the ihs\conf\domino.conf file
  - DOMINO_IHS_ROOT
  - DOMINO_SERVER_NAME
  - DOMINO_DOCUMENT_ROOT
  - DOMINO_DOCUMENT_DIRECTORY
  - DOMINO_PORT
  - DOMINO_MAX_REQUESTLINE
  - DOMINO_RESPONSE_TIMEOUT
  - DOMINO_THREADS

IKEYMAN

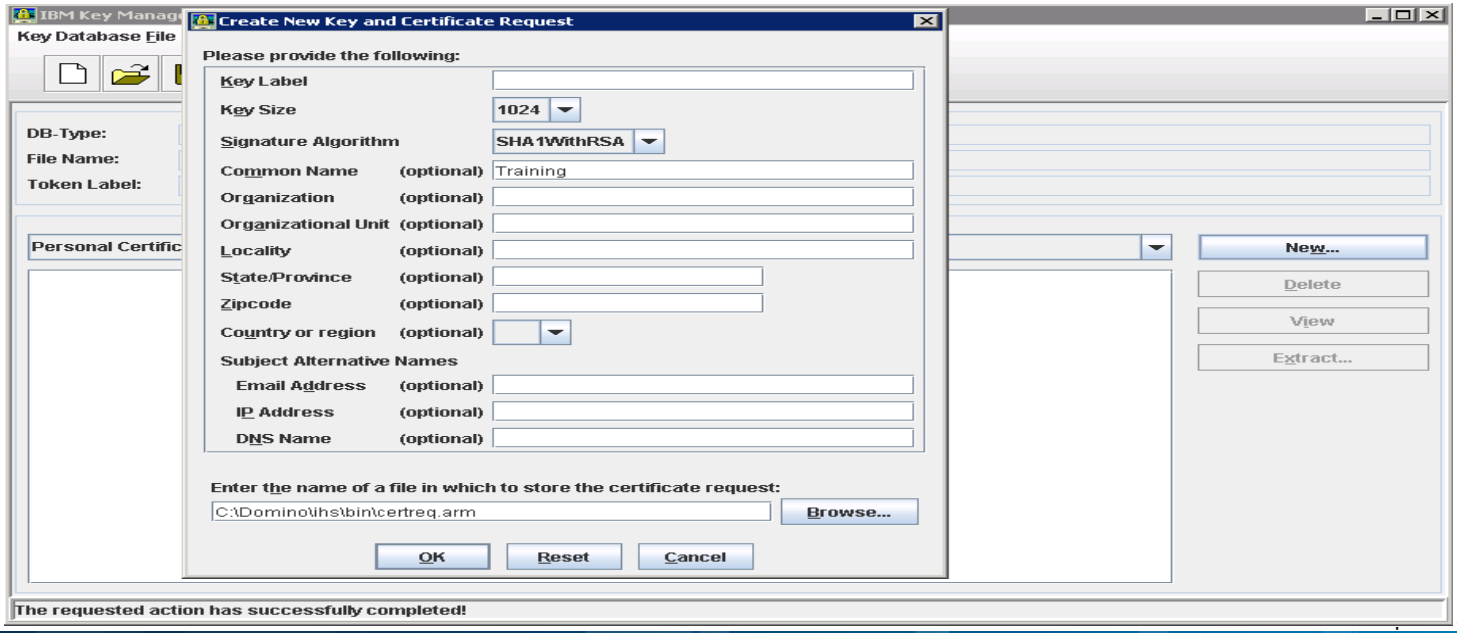
- The IBM HTTP Server uses key database files as keystores to store the certificates used in setting up TLS
- The iKeyman (IBM Key Management) tool is used to manage SSL keys and Trusted Roots.
- IKEYMAN shipped with Domino can be used to create the keystore used by IHS. ikeyman.bat can be found in the following directory \ihs\bin
- It can be launched by double-clicking it or running it from the command line
- You can either generate a new certificate request using the IKEYMAN utility

Creating a Certificate Signing Request (CSR) with IKEYMAN

- From the Menu Bar select Key Database File > New.
- Enter a file name for the new key database file you are creating.
- Enter a location for your key database file(KDB)
- Click OK.
- You are then prompted to enter a password. This is the password that will be used to open the key database file in iKeyman in the future.
- Select the checkbox “Stash the password to a file?” This encrypts the password and saves the file as a .sth file in the same directory as the kdb file

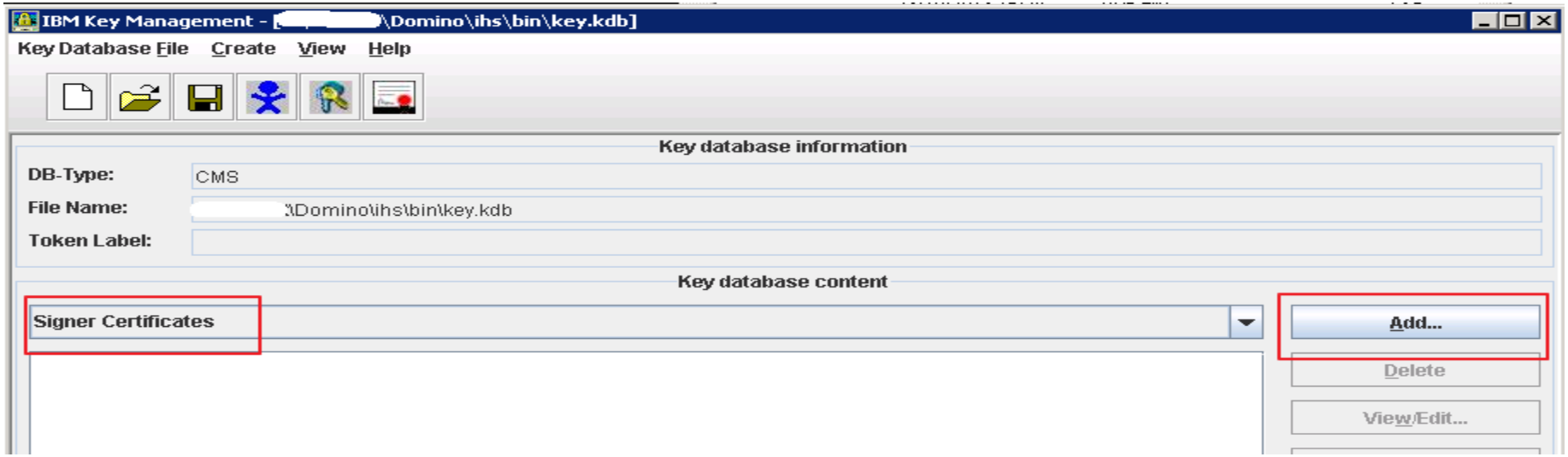
Creating a Certificate Signing Request (CSR) with IKEYMAN

- In the middle of the iKeyman GUI you will see a section called Key database content.
- Click on the "down arrow" to the right, to display a list of three choices.
- Select “Personal Certificate Requests”
- From the Personal Certificate Requests section, click New.
- Enter the relevant details for your certificate request



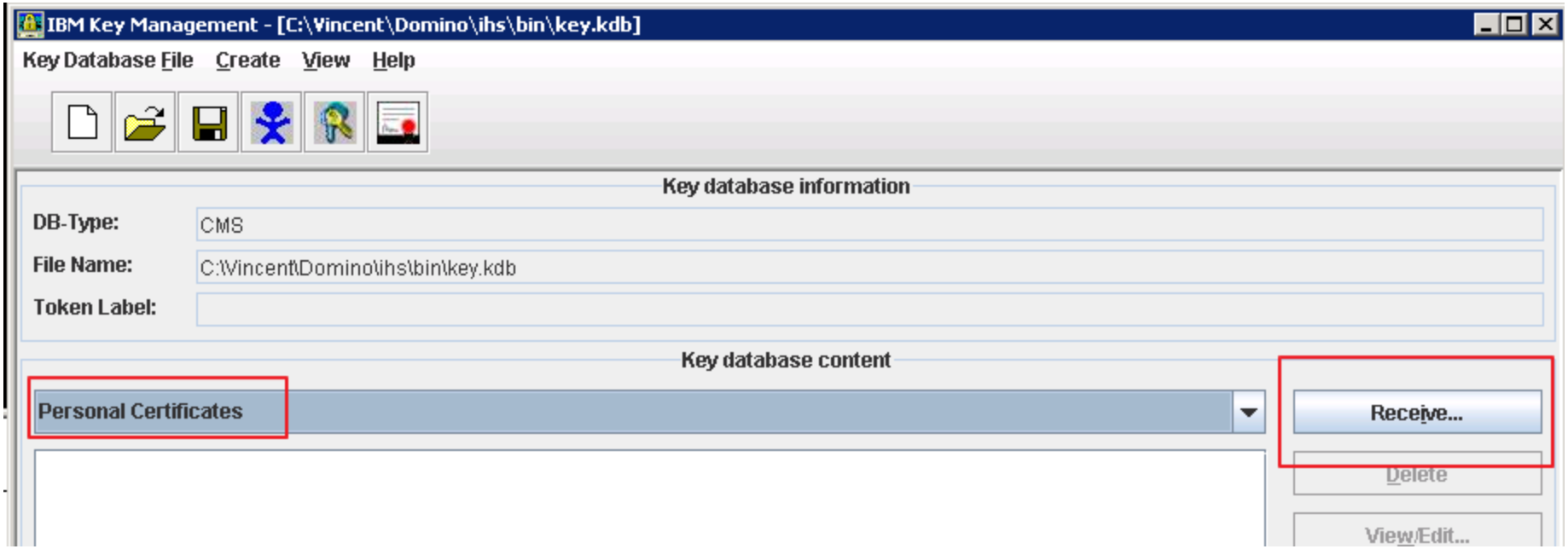
Creating a Certificate Signing Request (CSR) with IKEYMAN

- Once the CSR has been created you are able to submit the request to a 3rd party Certificate Authority or your own CA
- Once you receive your certificate from the CA you will need to import the root certificate and any intermediate certificates first
- To import the root certificate to your KDB file then select 'Signer Certificates' from the Key database content section and click add
- Browse to where you have the root stored and click OK



Creating a Certificate Signing Request (CSR) with IKEYMAN

- To import your server certificate select 'Personal Certificates' from Key database content section and then Receive
- Browse to where you have the personal certificate stored and complete the import
- Your Key database file is now ready to be used in your IHS environment



Configuring your IBM HTTP server

- The IBM HTTP server configuration file that is used to start the IBM HTTP server is named domino.conf and is located in the Domino Program directory under the ihs\conf subdirectory
- By default all listen ports are disabled so you need to modify this file to enable any listen ports you want the server to use
- To enable port 80
  - Remove the comment character (#) from the following line
    - # IPv4 support:
    - Listen 0.0.0.0:80
    - # Uncomment the following line for IPv6 support on Windows XP or Windows
    - # 2003 or later. Windows IPv6 networking must be configured first.
    - # Listen [::]:80

Configuring your IBM HTTP server

- To allow the IBM HTTP Server to accept HTTP SSL connections, enable the SSL/TLS port 443, and remove the comment character (#) for the following lines
  - Listen 0.0.0.0:443
  - ## IPv6 support:
  - #Listen [::]:443
  - <VirtualHost *:443>
  - SSLEnable
  - #SSLProtocolDisable SSLv2
  - #SSLProtocolDisable SSLv3
  - </VirtualHost>

  - KeyFile d:/keys/myserver.kdb
  - SSLDisable
  - #

Configuring your IBM HTTP server

- If you have internet sites enabled with one internet site document with a hostname different from the FQHM
  - Listen 0.0.0.0:80
  - ServerName "${DOMINO_SERVER_NAME}"
  - <VirtualHost 192.168.1.103:80>
  - ServerName www.mycompany2.com
  - </VirtualHost>

  - Listen 0.0.0.0:443
  - <VirtualHost 192.168.1.103:443>
  - ServerName www.mycompany2.com
  - SSLEnable
  - </VirtualHost>
  - SSLDisable
  - KeyFile "c:/program files/ibm http server/key.kdb"

Configuring your IBM HTTP server

- If you have internet sites enabled with multiple internet site documents
  - Listen 0.0.0.0:80
  - ServerName "${DOMINO_SERVER_NAME}"
  - <VirtualHost 192.168.1.103:80>
  - ServerName www.mycompany.com
  - </VirtualHost>
  - <VirtualHost 192.168.1.104:80>
  - ServerName www.mycompany2.com
  - </VirtualHost>

Configuring your IBM HTTP server

- If you have internet sites enabled with multiple internet site documents
  - Listen 0.0.0.0:443
  - <VirtualHost 192.168.1.103:443>
  - ServerName www.mycompany.com
  - SSLServerCert mycompany
  - SSLEnable
  - </VirtualHost>
  - <VirtualHost 192.168.1.104:443>
  - ServerName www.mycompany2.com
  - SSLServerCert mycompany2
  - SSLEnable
  - </VirtualHost>
  - SSLDisable
  - KeyFile "c:/program files/ibm http server/key.kdb"

Loading the IHS server

- Once you have updated the Domino.conf file with the correct settings you are ready to launch Domino and your IHS server
- With the parameter HTTPIHSEnabled=1 enabled the HTTP task loads the IHS server

Debugging

- **HTTPIHSDebugStartup=1**
  - This will display environment variables that are used in the domino.conf configuration file
  - Good to make sure that all settings are being honoured.
- Enable the mod_net_trace in the domino.conf
  - #LoadModule net_trace_module modules/debug/mod_net_trace.so
  - #<IfModule mod_net_trace.c>
  - #NetTraceFile logs/nettrace.log
  - #NetTrace client * dest file event senddata=65535 event recvdata=65535
  - #</IfModule>
- **Enable HTTP thread logs**
  - Tell http debug thread on
- **Collect the following logs**
  - error.log
  - nettrace.log
  - Htthr log files

Issues to be aware of

- DMEA96CMVX
  - infinite redirection issue when HTTPEnableConnectorHeaders is enabled (set to 1) in the notes.ini and when a browser connects directly over SSL to a Domino Server to a resource that requires SSL
  - Fixed in 9.0.1 and also 9.0IF1
- MKEN966HFR
  - IHS sends back a 500 status code if mod_domino receives a 449 status code, causes traveler to fail
  - Fixed in 9.0.1 and also 9.0IF2

Press *1 on your telephone to ask a question.

Visit our Support Technical Exchange page or our Facebook page for details on future events.

To help shape the future of IBM software, take this quality survey and share your opinion of IBM software used within your organization: https://ibm.biz/BdxqB2

Find us on Facebook

IBM Collaboration Solutions Support page
http://www.facebook.com/IBMLotusSupport

follow us on twitter

IBM Collaboration Solutions Support
http://twitter.com/IBM_ICSSupport

