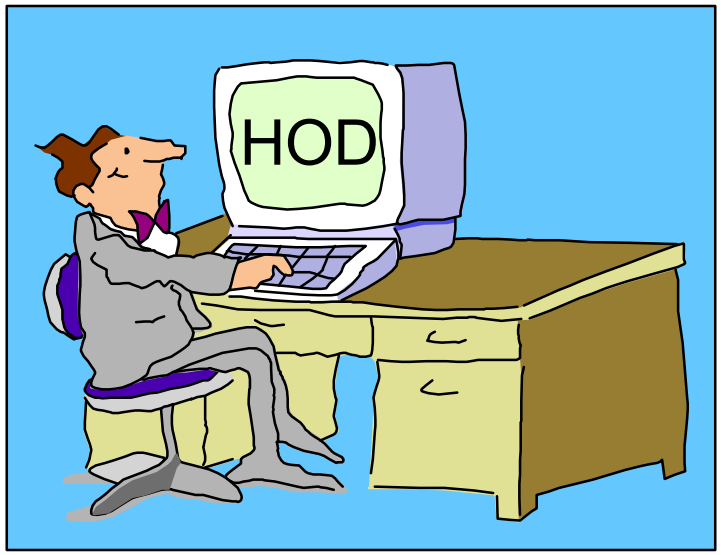
IBM ®

IBM WebSphere Host On-Demand V5 for OS/390



Linda Harrison
lharriso@us.ibm.com

Agenda

- IBM Host On-Demand V5 for OS/390
  - Overview
  - Product Packaging
  - Installation
  - Administration
  - Server
  - Client
  - CS/390 IP Customization and 3270 Host Print
  - TN3270E SSL
  - SSL Client Authentication
  - OS/390 Lightweight Directory Access Protocol HOD Support
  - Host On-Demand Toolkit
  - OS/390 Screen Customizer Support
  - OS/390 Host Publisher Support

Agenda (cont.)

- Appendices
  - Appendix A: Deployment Wizard
  - Appendix B: Edit HTML
  - Appendix C: Configuration Servlet
  - Appendix D: TCP/IP Profile Customization
  - Appendix E: MKKF
  - Appendix F: Migrate MKKF certificate to IKEYMAN
  - Appendix G: GSKKYMAN
  - Appendix H: Make Server certificate available to HOD clients
  - Appendix I: Client SSL
- Bibliography
- Web Sites

Abstract

Title: IBM Host On-Demand V5 for OS/390

Presenter: Linda Harrison supports OS/390 Host On-Demand in IBM Advanced Technical Support.

Audience: OS/390 Host On-Demand Installers

Abstract: Host On-Demand's browser-based access is the simplest way ever for users to reach critical host data because the user is not required to load or configure any software. Host On-Demand is a Java enabled Web based terminal emulation software supporting TN3270(E), TN5250, VT100, and VT220 terminals as well as 3287 and 5250 print emulation. For users, Host On-Demand helps eliminate the confusing host and port names as all of the configuration is easily provided by the Administrator. From a web browser, users just click on a hyperlink that launches a session with the host. In addition to the usual web access, any number of sessions can be launched with multiple hosts at the same time. Since Host On-Demand installs on a server, maintenance, distribution, and upgrades are simplified. In the case of OS/390 Host On-Demand, the server that Host On-Demand installs onto is the OS/390 system, where most of today's enterprise mission-critical information still resides.

IBM ®

OS/390 Host On-Demand V5: Overview

Host On-Demand (Overview)

IBM Host On-Demand V5 is part of the IBM Host Access Client Package.

Announcement Letter 200-324:

- Secure access to your host applications and data, using a simple, Java-enabled Web browser.
- The power of Java to open the doors to your host data, with S/390 (TN3270), AS/400 (TN5250), and DEC/UNIX (VT52/100/220) emulation in a single package.
- Requires no client installation or middle tier server.
- Centralized deployment and administration saves money and enhances control.

Note: Host On-Demand is a client terminal emulator like PComm.

Host On-Demand (Overview)

Steps to establish TN3270 session using Host On-Demand:

1. User connects Web Browser to HTTP Web Server (TCP/IP port 80).
2. User selects Host On-Demand.
3. Userid and password are requested from HOD Server and sent in (TCP/IP port 8999). (Password is encrypted but userid is not.)
4. HOD Applet downloads to the user (TCP/IP port 80).
   (HOD session icons look like PComm session icons.)
5. User selects host session icon.
6. Session is established to TN3270E Server (TCP/IP port 23).

Note: The TN3270E Server does not have to be on the same OS/390 as the Host On-Demand and Web Server; it can be any TN3270E Server on the TCP/IP Network.

Note: HTTP session on port 80 and/or telnet session on port 23 may be SSL encrypted.

IBM ®

OS/390 Host On-Demand V5: Product Packaging

Host On-Demand (Packaging)

- OS/390 Host On-Demand (5648-D70) V5 Features

FMID	Medium	Feature Number
HHOF500	6250 Tape	CU75CNA
HHOF500	3480 cart	CU77QNA
HHOF500	4mm cart	CU7ZXNA

- Host On-Demand Toolkit CD and Host On-Demand Windows CD are delivered with the order.

Software Requirements

- Minimum OS/390 Software Requirements

Program Number	Product Name and Minimum VRM/Service Level	Install Requirement
5647-A01	OS/390 SMP/E Version 2 Release 5 with PTF UR51068	Yes
5655-A46	Java for OS/390 V1.1.8	No
5697-D43	Domino Go Webserver for OS/390 V5R0M0	No

- The OS/390 Communications Server TCP/IP Services and Unix Systems Services, both included with OS/390, are required by IBM Host On-Demand V5 for OS/390 at run time.
- OS/390 V2R10 required APARs (for OS/390 V2R10 only):
  - OW45791 - for LDAP support
  - OW45575 - for Java

Software Requirements (cont.)

- Program Temporary Fix (PTF) = Corrective Service Diskette (CSD)

CSD 1	CSD 2	CSD 3
APAR OW46997 PTF UW75286	APAR OW48084 PTF UW77442	part 1 APAR OW48152 PTF UW77693 part 2 APAR OW48154 PTF UW77707

- HOD V5 Base tape + CSD 1 = HOD V5.0.1
  + CSD 2 = HOD V5.0.2
  + CSD 3 = HOD V5.0.3

IBM ®

OS/390 Host On-Demand V5: Installation

Host On-Demand (Installation)

- SMP/E install with mainframe media provides Reliability, Availability, and Serviceability support.
- Follow directions in Program Directory, GI10-3175-00.
- 700 MB HFS space is required.
- hod50mvs.sh may take a longer than expected time to complete (depending on system resources). TSO timeout and other timers should be customized accordingly to prevent interruption of execution before completion.

HOD Install (cont.)

- The Host On-Demand directories

  /usr/lpp/HOD - default distribution libraries directory

  /usr/lpp/HOD/hostondemand/HOD - the "publish" directory

  /usr/lpp/HOD/hostondemand/private - the private subdirectory

  /usr/lpp/HOD/hostondemand/lib - ServiceManager.sh directory

  /usr/lpp/HOD/hostondemand/HOD/en/doc/samples/html - session1&2 directory

- Optional Step - Add the following to the ServiceManager.sh to make HOD bind to only one TCP/IP stack:

  `export _BPXK_SETIBMOPT_TRANSPORT=`*`stname`

  (where *stname* is the TCP/IP stack name)

Host On-Demand (Installation)

- As per the Program Directory, the following lines should be added to the HTTP Webserver's configuration file (ie. /etc/httpd.conf):

```
pass /hod/*.html /usr/lpp/HOD/hostondemand/HOD/*.html.ascii
pass /hod/*.HTML /usr/lpp/HOD/hostondemand/HOD/*.HTML.ascii
pass /hod/* /usr/lpp/HOD/hostondemand/HOD/*
AddType  .cab  application/octet-steam     binary 1.0
AddType  .jar  multipart/x-zip             binary 1.0
```

  - Note: The HTTP Server must be recycled to pick up the above changes.

- Uncomment the classpath in the ServiceManager.sh as appropriate. I needed both of the following:

```
export CLASSPATH=/usr/lpp/java/J1.1/lib/classes.zip
export PATH=$PATH:/usr/lpp/java/J1.1/bin
```

IBM ®

OS/390 Host On-Demand: Administration

Host On-Demand (Administration)

- Essentially the same as for all the other Host On-Demand server platforms:
  - Connect to HOD server:

    http://hod_server_name/hod/HODMain.html
  - Select Administration and logon as **admin/password**.
  - Once logged on:

    Create groups

    Create sessions (ie. 3270, 5250, VT100, etc.) for groups

    Create users and assign them to groups

    Create specific sessions for individual users as necessary

HOD Admin (cont.)

- Options when logged on as Administrator:
  - Introduction - Read through the online help
  - Users/Groups
    - Create groups, users, sessions, and multiple session icons
    - Allow users to create accounts
    - Disable User Filter - Filter used to limit userid display
    - Disable Functions - Instead of locking items in session definition
    - Start or Stop Tracing
    - User may be prevented from saving preferences or changing password
    - Enable Native Authentication for user
  - Services
    - Display Status of Services or Start or Stop Services Traces
    - Display Server Log or Send System Properties to Java Console
  - Redirector support (SSL not supported on HOD/390 Redirector)
  - Lightweight Directory Access Protocol (LDAP) support - Configure LDAP support
  - OS/400 Proxy Server - Not supported on HOD/390 server
  - Licenses - Display License-Use Statistics

HOD Admin (cont.)

- A session defines the Emulator Options.
- Sessions can be created for a group or an individual user.
- Users will inherit all sessions associated with all of the groups to which they belong, in addition to any specific sessions created for that individual user.
- Every user must be a member of at least one group.
  - When NOT using LDAP, a user may be a member of multiple groups.
  - When using LDAP, a user may only be a member of ONE group.
- Before creating groups, users, and sessions, the administrator needs to list what users need Host On-Demand access and what sessions they need. Can they be separated into groups? Do they need to be able to modify session options? If they don't need to modify session options they can even share a userid.
- When the administrator creates a session the options can be "locked". Users can only modify options that are not "locked".
- When a user or group session is modified by a user, the changed session is saved as a user session. After a user logs on they are presented with an icon for each session defined for the group they are in and each individual session defined for the user.

HOD Admin (cont.)

- 3270 Display Emulator Options (options can be locked):
  - Connection Options
    - Destination Address - TN3270 server IP address or host name
    - Destination Port - TN3270 server port number
    - Enable SLP - not supported on HOD/390 server
    - TN3270E support, LU or Pool Name, Screen Size, Host Code-Page
    - Associated Printer Session
  - Advanced Options
    - Enable Host Graphics, Character-Cell Size, Session ID
    - Start Automatically, Start in Separate Window, Auto-Connect, Auto-Reconnect
    - Applet/Macro Options
      - Auto-Start, Auto-Start Name
    - SLP Options - Not supported on HOD/390 server
      - Scope, This Scope Only, Maximum Wait-Time

HOD Admin (cont.)

- Security
  - Enable Security (SSL) - SSL Server authentication
  - Telnet-negotiated - Transport Layer Security (TLS) port 23 - CS/390 V2R10 only
  - Server Authentication (SSL) - Server DNS hostname verification
  - If Server Requests Client Certificate (defaults)
    - Send a Certificate, URL or Path and Filename, Prompt Each Time
- Language
  - BIDI Options - Arabic and Hebrew
    - Numeral Shape, Text Type, Text Orientation
  - Thai Options
    - Thai Display Mode
- Screen
  - Screen Customizer
  - Font Name, Font Style, Cursor Style, Show Border
  - Light Pen Mode, Show OIA, Keypad, Toolbar, Toolbar Text, Status Bar, Macro Manager
- Keyboard Remap (cannot be locked)
- File Transfer Options

HOD Admin (cont.)

- One potential issue exists if users are allowed to define their own sessions or modify inherited sessions.
  - A user who modifies a session inherited from a group level definition now has a local "instance" of that session. This may present a help desk problem since neither the help desk nor the user can differentiate the two sessions should the user subsequently have reason to call in for assistance.

IBM ®

OS/390 Host On-Demand V5: Server

Host On-Demand (Server)

- HOD Server is supported on the following platforms:
  - Windows NT 4.0 with SP5
  - Windows 2000 (Professional, Server, and Advanced Server)
  - AIX 4.2.x, 4.3.3, and 4.3.4
  - OS/2 Warp Server 4 and OS/2 Warp Server for e-Business 4.5
  - Novell Netware 4 and 5
  - Sun Solaris 2.6 and 2.7
  - OS/400 V4R3, V4R4, and V4R5
  - HP-UX 10.20
  - Redhat Linux 6.2
  - SUSE Linux 6.4
  - OS/390 2.5, 2.6, 2.7, 2.8, 2.9, and 2.10
  - Caldera OpenLinux 2.3
  - TurboLinux 6.0
  - SCO Unixware 7
  - Windows Terminal Server 4

IBM ®

OS/390 Host On-Demand: Client

Host On-Demand (Client)

- Host On-Demand Client is supported on the following browsers and platforms:
  - Netscape Navigator 4.6 or 4.7.x
    on Windows 95, 98, 2000, NT, and UNIX
  - Netscape Navigator 4.61
    on OS/2
  - Microsoft Internet Explorer 4.01 with SP1, 5.0 or 5.1
    on Windows 95, 98, 2000, and NT
    with JVM level 3165 or higher

Note: Host On-Demand is not supported on Netscape 6 yet. It will be supported when it is feasible.

HOD Client (cont.)

- Types of Host On-Demand Clients

To access a HOD client use a browser to open http://*hod_server*/hod/*htmlpage*, where *hod_server* is the IP address or host name of the HOD server and *htmlpage* is HODMain.html (which lists all the clients) or one of the following to access one of the clients directly:

Function	Client	HTML Page
Administrator	Administrator	HODAdmin.html
	Administrator cached	HODAdminCached.html
	Administrator cached w/ problem determination	HODAdminCachedDebug.html
Emulator Client	Cached	HODCached.html
	Cached w/ problem determination	HODCachedDebug.html
	Download	HOD.html
	Download w/ problem determination	HODDebug.html
	Download w/ Screen Customizer/LE Interface	HODCustom.html
	Function On-Demand	HODThin.html
Database Client	Database	HODDatabase.html
	Database cached	HODDatabaseCached.html
	Database cached w/ problem determination	HODDatabaseCachedDebug.html
Utilities	Remove Cached Client	HODRemove.html
	New user	NewUser.html
	New user cached	NewUserCached.html
	New user cached w/ problem determination	NewUserCachedDebug.html

Host On-Demand (Client)

- The cached client loads faster than the others, and is therefore the recommended client.
- The download client will not run on a workstation with the cached client installed. If the cached client is installed it must be removed before the download client can be used. Remove the cached client with the HODRemove.html page.
- Locally-installed client can be installed from the CD on Windows 95, 98, 2000, NT 4.0 with SP3 or later.
  - To start locally-installed client:

    Click Start, Programs, IBM Host On-Demand, Host On-Demand

Host On-Demand (Client)

- There are some AutoHODxxx.html files, that correspond to some of the HODxxx.html files, that launch the session automatically instead of having to double click the icon. They are located in the "publish" directory (default is /usr/lpp/HOD/hostondemand/HOD).
- There are two more HTML sample files that can be copied to the "publish" directory and customized:
  - Session 1 is like AutoHOD.html with these added capabilities:
    - Save the userid and password in the HTML page.
    - Launch the session automatically instead of having to double click the icon.
    - Run the session embedded in the browser window or in a separate window.
    - Change session icons into buttons.
    - /usr/lpp/HOD/hostondemand/HOD/en/doc/samples/html/session1.html.ascii
  - Session 2 is also like AutoHOD.html with these added capabilities:
    - No userid and password required, which means that settings cannot be saved.
    - /usr/lpp/HOD/hostondemand/HOD/en/doc/samples/html/session2.html.ascii

Host On-Demand (Client)

- The Deployment Wizard on the Host On-Demand for Windows V5 CD may be used to create HTML pages or the HTML may be edited manually.
  - See Appendix A in this presentation for using the Deployment Wizard.
  - The session customization changes done by the client may be saved on their local PC rather than back on the server. To do this, use the Deployment Wizard to create a definition with "Use the Configuration Server"="No" and "Allow users to save session changes?"="Yes". This way one standard session can be created with one shared userid defined. Every user that uses that session may customize it and the changes will be saved locally and only effect them.

    Note: The file permissions must be 666.
- HTML pages must be binary FTPed to the Host On-Demand Publish Directory:

  /usr/lpp/HOD/hostondemand/HOD
- When HTML files are FTPed to the Host On-Demand server for the first time the permission bits setting on the file created in OMVS may not allow the use of the HTML page. You may need to change the permission bits to something usable, like 644.
- HTML pages are in ASCII (even on OS/390). Please see Appendix B in this presentation for editing options.

Host On-Demand (Client)

- To avoid opening up port 8999 on a firewall to access the Host On-Demand server a Configuration Servlet may be used. Please see Appendix C of this presentation.
  - It must be installed on a Web Application Server that supports the Java Servlet 2.0 API. The OS/390 WebSphere Application Server is supported.
  - The Host On-Demand clients connect to the Configuration Servlet using port 80 and the Configuration Servlet connects to the Host On-Demand server using port 8999 (or the configured port if it has been changed).
- Native Authentication allows HOD users to logon with their OS/390 logon password. This requires LDAP.
- If session properties are not locked they can be modified by the user.
  - Session colors can be remapped.
  - Light Pen Mode can be enabled.
  - An Applet can be run.
  - A Macro can be saved or run.

IBM ®

OS/390 Communications Server
IP Customization
and 3270 Host Print

IP Customization

A sample PROC is provided as file "HOMSERVR" in the directory "/usr/lpp/HOD/hostondemand/lib/". This may be copied to your system PROCLIB and used to start the Host On-Demand Server. This requires a userid with **UID 0**. You must use the RACF STARTED class to enable this.

If the userid with **UID 0** is HODSERV in group OMVSGRP and the proc name used to start the Host On-Demand server is HODSRV, enter the following RACF commands:

```
RDEFINE STARTED HODSRV.* STDATA(USER(HODSERV) GROUP(OMVSGRP))
SETROPTS RACLIST(STARTED) REFRESH
```

IP Customization (cont.)

Note: The "/" may be missing from the "STDOUT DD" and "STDERR DD" "PATH" statements in the sample PROC. If the bottom of the PROC looks like this:

```
//STDOUT   DD PATH='tmp/homservr-stdout',
//         PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//         PATHMODE=SIRWXU
//STDERR   DD PATH='tmp/homservr-stderr',
//         PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//         PATHMODE=SIRWXU
//SYSOUT   DD SYSOUT=*
```

It should be changed to this:

```
//STDOUT   DD PATH='/tmp/homservr-stdout',
//         PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//         PATHMODE=SIRWXU
//STDERR   DD PATH='/tmp/homservr-stderr',
//         PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//         PATHMODE=SIRWXU
//SYSOUT   DD SYSOUT=*
```

IP Customization (cont.)

Defining HOD in the PROFILE TCPIP

Host On-Demand can be autologged by TCP/IP and a port can be reserved for the HOD Server. Add the following to the PROFILE TCPIP:

```
AUTOLOG 5
    HOMSERVR
PORT
    8999  TCP  HOMSERVR
```

where HOMSERVR is the name of the proc to start the HOD Service Manager.

IP Customization (cont.)

You may want to rename the HOMSERVR sample job to a started PROC name of less than 8 characters (ie. HOMSRVR). This will help when displaying subprocesses and stopping HOD. You can add the following to the PROFILE TCPIP:

```
AUTOLOG 5
    HODSRVR
PORT
    8999  TCP  OMVS
```

After HOD comes up display the ports and take note of what job is using 8999 with the following command:

```
D TCPIP,procname,NETSTAT,SOCKETS
```

where procname is the name of the proc to start the TCP/IP stack.

Then you can replace OMVS on the PORT statement with the job name using the port. If you do this you may need to do it again when you migrate to new releases.

IP Telnet Customization

PROFILE TCPIP BEGINVTAM STATEMENT

PORT xxxx -define which telnet port the BEGINVTAM effects

HNGROUP -define group of host names (available in OS/390 V2R7 and above)

IPGROUP -define group of ipaddrs

LUGROUP -define group of LUs

LUMAP -map LU or LUGROUP to host name, HNGROUP, ipaddr, or IPGROUP and optionally associate a printer LU or PRTGROUP

PRTGROUP -define group of printer LUs

PRTMAP -map printer LU or PRTGROUP to host name, HNGROUP, ipaddr, or IPGROUP

HOD Session Customization

Destination Port

TN3270E -required for LU or LU Pool specification

LU or LU Pool

Associated Printer Session

3270 Printing

- A Host On-Demand 3270 printer session emulates an IBM 3287 printer in either LU Type 1 (SCS) or LU Type 3 mode.
  - The printer LU must be defined in VTAM and TCP/IP.
  - The mainframe application that the user is printing from must be setup to print to the VTAM LU.
  - Please see the Host On-Demand V4 Host Printing Reference.

- In some applications a printer is associated with a userid. For this type of application TCP/IP has the capability to "associate" or "map" printer LUs "generically" or "specifically" with user terminal LUs.

- Please see Appendix D in this presentation for TCPIP PROFILE example.

IBM ®

OS/390 TN3270E
Secure Sockets Layer (SSL)

TN3270E SSL Requirements

- The optional Level 2 (56-bit Export) or Level 3 (168-bit US) OS/390 V2 IP Security is required if SSL DES support is desired.
- Create a Certificate Request and/or Server Public/Private Keys.
- There have been three Certificate Tools on OS/390. From the oldest to the newest: MKKF, IKEYMAN, and GSKKYMAN.

TN3270E SSL Req (cont.)

OS 390	Product	Optional Feature Name	Function Provided
R5	Domino Go Webserv	DGW Export Security	HTTP SSL 56-bit
R5	Domino Go Webserv	DGW France Secure	HTTP SSL 40-bit
R5	Domino Go Webserv	DGW N America Secure	HTTP SSL 128-bit
R5	Comm Server	IP Security CDMF	IP Sec CDMF
R5	Comm Server	IP Security DES/CDMF	IP Sec DES/CDMF
R5	Comm Server	IP Kerberos DES	Kerberos DES 56-bit
R5	Comm Server	IP Kerberos non-DES	Kerberos non-DES
R6	Domino Go Webserv	DGW Export Security	HTTP SSL 56-bit
R6	Domino Go Webserv	DGW France Secure	HTTP SSL 40-bit
R6	Domino Go Webserv	DGW N America Secure	HTTP SSL 128-bit
R6	Comm Server	IP Security CDMF	IP Sec CDMF, and
			Telnet SSL RC2/RC4 40bit
R6	Comm Server	IP Security DES/CDMF	IP Sec DES/CDMF, and
			Telnet SSL DES 56bit
R6	Comm Server	IP Security TDES	IP Sec TDES, and
			Telnet SSL TDES
R6	Comm Server	IP Kerberos DES	Kerberos DES 56-bit
R6	Comm Server	IP Kerberos non-DES	Kerberos non-DES

TN3270E SSL Req (cont.)

OS 390	Product	Optional Feature Name	Function Provided
R7	IBM HTTP Server	IBM HTTP Export Sec	HTTP SSL 56-bit
R7	IBM HTTP Server	IBM HTTP France Sec	HTTP SSL 40-bit
R7	IBM HTTP Server	IBM HTTP NA Secure	HTTP SSL 128-bit
R7	Comm Server	eNetwork CS Sec Lev 1	IP Sec CDMF, and
			Telnet SSL RC2/RC4 40bit,
			Kerberos non-DES
R7	Comm Server	eNetwork CS Sec Lev 2	IP Sec DES/CDMF,
			Telnet SSL DES 56bit,
			Kerberos DES 56-bit, and
			SNMPV3 CBC DES 56-bit
R7	Comm Server	eNetwork CS Sec Lev 3	IP Sec TDES,
			Telnet SSL TDES,
			Kerberos DES 56-bit, and
			SNMPV3 CBC DES 56-bit

TN3270E SSL Req (cont.)

OS 390	Product	Optional Feature Name	Function Provided
R8&9	IBM HTTP Server	IBM HTTP Export Sec	HTTP SSL 56-bit
R8&9	IBM HTTP Server	IBM HTTP France Sec	HTTP SSL 40-bit
R8&9	IBM HTTP Server	IBM HTTP NA Secure	HTTP SSL 128-bit
R8&9	Comm Server	SecureWay CS Sec Lev 1	IP Sec CDMF, and
			Telnet SSL RC2/RC4 40bit,
			Kerberos non-DES
R8&9	Comm Server	SecureWay CS Sec Lev 2	IP Sec DES/CDMF,
			Telnet SSL DES 56bit,
			Kerberos DES 56-bit, and
			SNMPV3 CBC DES 56-bit
R8&9	Comm Server	SecureWay CS Sec Lev 3	IP Sec TDES,
			Telnet SSL TDES,
			Kerberos DES 56-bit, and
			SNMPV3 CBC DES 56-bit

TN3270E SSL Req (cont.)

OS 390	Product	Optional Feature Name	Function Provided
R10	IBM HTTP Server	IBM HTTP NA Secure	HTTP SSL 128-bit
R10	Comm Server	IBM CS base	IP Sec CDMF,
			IP Sec DES/CDMF, and
			SNMPV3 CBC DES 56-bit
R10	Comm Server	SecureWay CS Sec Lev 1	Kerberos non-DES
R10	Comm Server	SecureWay CS Sec Lev 2	Kerberos DES 56-bit
R10	Comm Server	SecureWay CS Sec Lev 3	IP Sec TDES
R10	Crypto Services	Crypto Services base	HTTP SSL 56-bit,
			HTTP SSL 40-bit, and
			Telnet SSL RC2/RC4 40bit,
			Telnet SSL DES 56-bit
R10	System SSL Sec	Sys SSL Security Lev 3	Telnet SSL TDES

(System SSL Sec does not need to be enabled unless Firewall is used)

TN3270E SSL Req (cont.)

- The OS/390 V2R6 and V2R7 TCP/IP telnet servers require an MKKF format certificate.
  - The MKKF utility that ships as part of the OS/390 V2R6 and V2R7 LDAP server supports a 512-bit key size.
  - For OS/390 V2R6 and R7, how to create a private key and server certificate in the server's key ring file and a password stash file using MKKF is documented in "OS/390 Communications Server, IP Configuration, SC31-8513", Appendix D. Please see Appendix E in this presentation.
  - To use MKKF with certificate authority (CA) VeriSign, APAR OW39793 is required and a password for the keyringfile has to be 6 to 8 characters.

SSL Server Authentication

- Some releases of the HTTP Web Server require an IKEYMAN format certificate. A certificate created with MKKF can be migrated to an IKEYMAN format. Please see Appendix F in this presentation.
- The OS/390 V2R8+ telnet server requires a certificate in the format of the GSKKYMAN utility or RACF's Certificate Management Support.
  - GSKKYMAN utility is part of OS/390 V2R8+ System Secure Sockets Layer.
  - For OS/390 V2R8+, how to create the server key database using GSKKYMAN is documented in "OS/390 Communications Server, IP Configuration, SC31-8513", Appendix C, and the Redbook "IBM Host On-Demand 4.0: Enterprise Communications in the Era of Network Computing, SG24-2149-01". Please see Appendix G in this presentation.

SSL Server Authentication

- A certificate created with MKKF can be migrated to GSKKYMAN. Please see "OS/390 System SSL Programming Guide and Reference, SC24-5877-03", chapter 6, section "Using the gskkyman Command-line Options".
- A certificate created with IKEYMAN can be exported using IKEYMAN and then a GSKKYMAN key database file can be created and the certificate can be imported into it.
- To start a TN3270 SSL port on an OS/390 telnet server the Cryptograhy library must be defined to LINKLST. I added the line
  `LNKLST ADD NAME(WSC.LINKLST) DSNAME(SYS1.CRYPTO.SGSKLOAD)`
  to my SYS1.PARMLIB(PROGF2) member. Without this I received an IEA995I SYMPTOM DUMP with CODE=0C4. The dataset must also be program controlled. In RACF I changed the CLASS=PROGRAM with PROFILE=*. I added 'SYS1.CRYPTO.SGSKLOAD' to the member list.

SSL Server Authentication

- On OS/390 V2R6+ TCP/IP uses the TELNETPARMS SECUREPORT statement to enable SSL Server Authentication.
- On OS/390 V2R10 TCP/IP you can specify SECUREPORT in the TELNETGLOBALS block instead of the TELNETPARMS block.
- On OS/390 V2R7+ the TELNETPARMS ENCRYPTION statement specifies a subset of the supported encryption algorithms to use for a port.
- After the certificate has been created it can be made available to all clients. So even self signed certificates or ones created by non-well-known CA's can be used without distributing the CA's public key to each client individually. Please see Appendix H of this presentation.

Optional SSL Client Authentication

- Client certificate validation requires the root certificate for the Certificate Authority (CA) who issued the client certificate.
- On OS/390 V2R8+ use the TELNETPARMS CLIENTAUTH statement to enable SSL Client Authentication.
  - SSLCERT enables SSL Client Authentication only
  - SAFCERT enables SSL Client Authentication and checks that the user has a valid RACF userid assigned. The certificate must be defined to RACF with the RACDCERT command.
- RACF class SERVAUTH may be used to limit access on a port basis.
- Express Logon is available to logon to an SNA host application without entering userid and password. Requires CS/AIX, CS/NT, or CS/2 TN3270 server between client and OS/390 V2R10 application host. See White Paper on Host On-Demand web site.

IBM ®

HOD SSL Client Authentication

SSL Client Authentication

- Create Client Certificate
  - Host On-Demand Locally Installed Client has a key-management utility that can be used to create a Client Certificate. This is detailed in the Redbook "SecureWay Communications Server for OS/390 V2R8 TCP/IP: Guide to Enhancements, SG24-5631-00", section "3.2.3.6 Working with the client certificate".
    http://www.redbooks.ibm.com
  - A Client Certificate can be obtained from a Well Known CA and exported in pkcs12 format from the browser thru which it was received. The certificate can be stored on the local disk, network drive, or web server, from which the client can get it.
  - A Self Signed Client Certificate created on OS/390 using GSKKYMAN is only a V1 P12 file. HOD needs a V3 PKCS12 file so a browser can be used to convert the file. See Appendix I in this presentation for converting the file using a browser.

IBM ®

OS/390 Lightweight Directory Access Protocol (LDAP) Server HOD Support

OS/390 LDAP

- Host On-Demand V5 supports LDAP Directory Servers:
  - Netscape Directory Server V3.1 and V4.0 on NT or AIX
  - IBM SecureWay LDAP Server V2.1 on NT or AIX
  - OS/390 LDAP Server on OS/390 V2R5, V2R6, or V2R7
  - IBM LDAP Directory Server V3.1.1
    - IBM schema pre-installed
- See the Program Directory and Planning and Installation Guide for LDAP configuration.

IBM ®

OS/390 Host On-Demand: Toolkit

HOD HACL

- Host On-Demand Toolkit CD
  - Host Access Class Libraries (HACL) for Java
    - Allows the development of platform-independent applications that can access host information without the need for a graphical display.
  - Host Access Beans for Java
    - Beans that use HACL libraries.
  - ActiveX support the same as PComm

IBM ®

OS/390 Screen Customizer Support

Screen Customizer Overview

- Screen Customizer is a thin Java client that automatically converts host screens into a graphical presentation.
- A Limited Edition version of Screen Customizer (Screen Customizer/LE), also referred to as the default GUI, is included in all the Host On-Demand clients and can be turned on in the session configuration panels but cannot be customized. The separate Screen Customizer product is required for customization.

Screen Customizer

- There are three components of Screen Customizer:
  - Administrator
    - Capture host screens for customization.
    - Identify screens and save as maps.
    - Set global defaults and save in profile.
  - Customization Studio
    - Customize screens captured by Administrator.
  - Client
    - Default or customized graphical interface for host sessions.
- Only the Screen Customizer "Client" is supported on OS/390.

Screen Customizer (cont.)

- Screen Customizer Administrator is supported on:
  - Host On-Demand V4.01 or later Client
  - Personal Communications V4.3 with CSD 2 or later
- Screen Customizer Client is supported on:
  - Host On-Demand V4.01 or later Server
  - Host On-Demand V4.01 or later Client
  - Personal Communications V4.3 with CSD 2 or later
- Screen Customizer Studio is supported on:
  - Windows 95 or 98
  - Windows NT 4.0 with SP5
  - Windows 2000

Screen Customizer (cont.)

- ResQ!Net was renamed to IBM Screen Customizer.
- Screen Customizer V2 is part of the IBM Host Access Client Package.
  - Announcement Letter 200-324
- HOD V5.0 supports IBM Screen Customizer (CS) 2.0.

Program Temporary Fix (PTF) = Corrective Service Diskette (CSD)

CSD 1	CSD 2	CSD 3
APAR OW47000 PTF UW75551	APAR OW48085 PTF UW77452	APAR OW48153 PTF UW77685

- SC V2 Base tape + CSD 1 = SC V2.0.1 (supported by HOD V5.01)
  + CSD 2 = SC V2.0.2 (supported by HOD V5.02)
  + CSD 3 = SC V2.0.3 (supported by HOD V5.03)

Copy Custom Files

- After installing Screen Customizer Client, copy customized files from a Windows Screen Customizer Administrator to OS/390.

Copy Custom Files Steps

FTP the files of each subdirectory in C:\hostondemand\HOD\custom on the Windows Administrator to the OS/390 host in the /usr/lpp/customizer/customizer/custom directory. Files must be transferred in BINARY.

Note: In order to FTP the files you will need to create the subdirectories on OS/390 in the /usr/lpp/customizer/customizer/custom directory, ie.:

/usr/lpp/customizer/customizer/custom/lst

/usr/lpp/customizer/customizer/custom/map

/usr/lpp/customizer/customizer/custom/ps

/usr/lpp/customizer/customizer/custom/ref

/usr/lpp/customizer/customizer/custom/wsp

/usr/lpp/customizer/customizer/custom/img

/usr/lpp/customizer/customizer/custom/(lang)/help

Note: Set the permission bits to (7,5,5) for the subdirectories.

Copy Custom Files (cont.)

- If separate sets of customizations for different users/groups have been stored in replicas of the custom directory, these directories must also be copied to OS/390.

IBM ®

OS/390 Host Publisher Support

Host Publisher Overview

- Host Publisher takes 3270, 5250, VT, JDBC, and Java host applications, and turns them into HTML Web pages for web access from even non-Java browsers.

Host Publisher

- There are two components of Host Publisher:
  - Studio - Development Environment
    - Generates Integration Object (JavaBean).
    - Contains JavaBean Factories.
    - Creates Applications.
    - Generates Java Server Pages (JSP).
  - Server - Run Time Environment
    - Integrates multi-platform Web servers.
    - Provides JSP parsing.
    - Provides Servlet API support.
    - Contains Java classes for connection management.
    - Provides an administration capability.
- Only the Host Publisher "Server" is supported on OS/390.

Host Publisher (cont.)

- Host Publisher Studio is only supported on:
  - Windows 95, 98, and NT
- Host Publisher Server is supported on:
  - AIX
  - Windows NT
  - Solaris
  - OS/390
- OS/390 Host Publisher V2.2:

  Announcement Letter 200-262

Host Publisher (cont.)

- There are three parts of Host Publisher Studio:
  - Host Publisher Studio
    - Creates Applications using JSP's to invoke Integration Objects.
  - Host Access Wizard
    - Create 3270, 5250, and VT Integration Objects.
  - Database Access Wizard
    - Create JDBC Integration Objects.

IBM ®

Appendix A:
Deployment Wizard

Deployment Wizard

- If the Deployment Wizard is used to create an HTML page, two HTML files and a subdirectory structure with multiple files in it are created in one zip file. This zip file must be binary FTPed to the Host On-Demand Server and unzipped, or all the files, preserving the subdirectory structure, must be binary FTPed to the Host On-Demand Server. The files must be put in the publish directory (the default is /usr/lpp/HOD/hostondemand/HOD) on the Host On-Demand Server and the HTML files and (if there are any) .txt files must have the .ascii extension added. There is no .ascii extension required on .cf and .obj files. As an example, if the Deployment Wizard created file HODTest1.html, you might end up with the following files on OS/390:
  - /usr/lpp/HOD/hostondemand/HOD/HODTest1.html.ascii
  - /usr/lpp/HOD/hostondemand/HOD/AutoHODTest1.html.ascii
  - /usr/lpp/HOD/hostondemand/HOD/HODData/HODTest1/params.txt.ascii
  - /usr/lpp/HOD/hostondemand/HOD/HODData/HODTest1/wInfo.txt.ascii
  - /usr/lpp/HOD/hostondemand/HOD/HODData/HODTest1/cfg0.cf
  - /usr/lpp/HOD/hostondemand/HOD/HODData/HODTest1/policy.obj
  - /usr/lpp/HOD/hostondemand/HOD/HODData/HODTest1/preloads.obj

Deployment Wizard (cont.)

- Deployment Wizard Pages:
  1. "Welcome to Host On-Demand Deployment Wizard"
     - "Do you want to create or edit an HTML file?"

       Select "Create a new HTML file" or "Edit an existing HTML file"
     - And then Click "Next"
  2. "Connection Options"
     - "Use the Configuration Server"

       Select "Yes" or "No"
       - If "Yes" then "Do you want to use the Configuration Servlet?"

         Select "Yes" or "No"
         - If "Yes" then enter "Configuration Servlet URL"

           For example /iphost/servlet/hodconfig/hod (where "iphost" is either the IP address or hostname of the Configuration Server)
         - If "No" then enter "Configuration Server Port"

           For example 8999
     - And then Click "Next"
     - If "Use the Configuration Server" = "No" then skip to 4

Deployment Wizard (cont.)

- Deployment Wizard Pages (cont.):
  3. "Logon Options"
     - "Require users to logon?"

       Select "Yes" or "No"
       - If "No" then enter "User ID to automatically logon as" and "Password for this user ID"
     - And then Click "Next"
  4. "Additional Options"
     - "Allow users to save session changes?"

       Select "Yes" or "No"
     - "Cache Host On-Demand applet?"

       Select "Yes" or "No"
     - "Include problem determination components?"

       Select "Yes" or "No"
     - And then Click "Next"
     - If "Cache Host On-Demand applet" = "No" then skip to 7

Deployment Wizard (cont.)

- Deployment Wizard Pages (cont.):
  5. "Cache Client Options"
     - "Debug cached client installation process?"

       Select "Yes" or "No"
     - "Where will the components be installed from?"

       Select "Web server" or "CD/Network Drive"
     - "Enter the size of the progress indicator frame"

       Enter "Width" (default 550) (options 300, 350, 400, 450...800)

       Enter "Height (default 250) (options 150, 200, 250, 300, 350, 400)
     - And then Click "Next"

Deployment Wizard (cont.)

- Deployment Wizard Pages (cont.):
  6. "Cache Client Upgrade Options"
     - "When an upgrade version of cached client is available"

       Select "Allow all users to upgrade", "Don't allow any users to upgrade", or "Control user upgrades"
       - If "Control user upgrades" then select "Percent of users who can upgrade at a time" or "Only allow upgrade if specified file contains the word upgrade"
         - If "Percent of users who can upgrade at a time" then enter the percentage (default 100) (options 10, 20, 30...100)
         - If "Only allow upgrade if specified file contains the word upgrade" then enter "URL to file"
     - Select "Upgrade in foreground", "Upgrade in background", or "Prompt user"
     - And then Click "Next"

Deployment Wizard (cont.)

- Deployment Wizard Pages (cont.):
  7. "Display Options"
     - Select "Standard Host On-Demand Client" or "Grid of Buttons"
     - Enter "Applet size" (default Large) (options Autosize, Small, Medium, Large)
     - Enter "Maximum number of concurrent sessions per user" (default 26) (options 1 to 26)
     - And then Click "Next"
  8. "Preload Configuration"
     - Select the components to include in the initial download
     - And then Click "Next"
  9. "Page Title and Summary"
     - Enter Bookmark page title
     - And then Click "Next"
  10. "Create HTML"
     - Select Path for file to be saved
     - Enter "File Name"
     - And then Click "Create"

Deployment Wizard (cont.)

- Deployment Wizard Pages (cont.):
  11. "Congratulations!"
      - Click "Restart Wizard" to create or edit more HTML files, or click "Close" to exit the Deployment Wizard

IBM ®

Appendix B:
Edit HTML Files

Edit HTML

- To be able to edit the OS/390 file it must be converted to EBCDIC or sent to another platform like Windows 95:
  - To edit on OS/390:
    1. In OMVS issue the following command, all on one line:
       ```
       iconv -f IBM-932 -t IBM-1047
       /usr/lpp/HOD/hostondemand/HOD/en/doc/samples/html/session1.html.ascii >
       /u/user1/session1.html
       ```
    2. Edit /u/user1/session1.html from the OS/390 ISHELL.
    3. In OMVS use the iconv command again to "publish" the html page, all on one line:
       ```
       iconv -f IBM-1047 -t IBM-932 /u/user1/session1.html >
       /usr/lpp/HOD/hostondemand/HOD/session1.html.ascii
       ```
  - To edit on Windows 95:
    1. FTP the file in binary to a Windows 95 workstation.
    2. Edit the file with Windows Notepad or WordPad.
    3. FTP the file in binary to the "publish" directory (default is /usr/lpp/HOD/hostondemand/HOD).

Edit HTML (cont.)

- The following parameter must be changed:

  <PARAM NAME="Host" VALUE="">

  to add the IP Address or Hostname of the TN3270 Server, ie.:

  <PARAM NAME="Host" VALUE="9.82.1.100">

  to be able to use the following HTML files properly:

  AutoHOD.html.ascii

  AutoHODCached.html.ascii

  AutoHODCachedDebug.html.ascii

  AutoHODCustom.html.ascii

  AutoHODDebug.html.ascii

  AutoHODThin.html.ascii

  session2.html.ascii

Edit HTML (cont.)

- The following parameters must be changed:

  <PARAM NAME="User" VALUE="">

  <PARAM NAME="Password" VALUE="">

  to add the userid and password of the Host On-Demand user, ie.:

  <PARAM NAME="User" VALUE="huser1">

  <PARAM NAME="Password" VALUE="u1pass">

  to be able to use the following HTML file properly:

  session1.html.ascii

Edit HTML (cont.)

- The following parameters may be changed:

  <PARAM NAME="User" VALUE="">

  <PARAM NAME="Password" VALUE="">

  to add the userid and password of the Host On-Demand user, ie.:

  <PARAM NAME="User" VALUE="huser1">

  <PARAM NAME="Password" VALUE="u1pass">

  to skip the logon prompt when using the following HTML files:

  HOD.html.ascii

  HODDebug.html.ascii

  HODThin.html.ascii

- Please see "applet tag parameters" and "cached client" in the online help for more HTML parameters.

IBM ®

Appendix C: Configuration Servlet

Configuration Servlet

- I did the following on my system which has WebSphere Application Server V1.2:
  1. I added the following to my was.config file "ncf.jvm.classpath=" statement:

     /usr/lpp/HOD/hostondemand/lib/cfgsrvlt.jar
  2. I also added the following statement to my was.config file:
     servlet.hodconfig.code=com.ibm.eNetwork.HODUtil.services.remote.HODCfgServlet
  3. I did not add the following to my httpd.conf file because it was already there:

     Service /servlet/* /usr/lpp/WebSphere/AppServer/lib/libadpter.so:AdapterService
  4. I copied HOD.html.ascii to HODCServ.html.ascii.
  5. I added the following to HODCServ.html.ascii:

     <PARM NAME=ConfigServerURL VALUE=9.82.1.100/servlet/hodconfig/hod>

     Where 9.82.1.100 is the IP address or hostname of the Configuration Server.

Configuration Servlet

- I did the following on my system which has WebSphere Application Server V3.02:

1. I added the following to my was.config file:

```
deployedwebapp.HOD.host=default_host
# rooturi must match pathname on Service statement in httpd.conf:
deployedwebapp.HOD.rooturi=/servlet
# The following two lines are all on one line with no spaces:
deployedwebapp.HOD.classpath=/usr/lpp/servlets:/usr/HOD/hostondemand/lib/cfgsrvl
   t.jar:/usr/lpp/HOD/hostondemand/HOD:/usr/lpp/java/J1.1/lib/classes.zip
deployedwebapp.HOD.documentroot=/usr/lpp/HOD/hostondemand/lib
webapp.HOD.jspmapping=*.jsp
webapp.HOD.jspmapping=*.jhtml
webapp.HOD.jsplevel=1.0
webapp.HOD.filemapping=/
# URL to servlet by code name or servletmapping alias listed below:
# The following two lines are all on one line with no spaces:
webapp.HOD.servlet.HODConfigServlet.code=com.ibm.eNetwork.HODUtil.services.remot
   e.HODCfgServlet
webapp.HOD.servlet.HODConfigServlet.servletmapping=/hodconfig
# The following two lines are all on one line with no spaces:
webapp.HOD.servlet.HODConfigServlet.initargs=ConfigServer=127.0.0.1,ConfigPort=8
   999,ShowStats=true,Trace=true
webapp.HOD.servlet.HODConfigServlet.autostart=true
```

2. I added the following to my httpd.conf file:

```
Service /servlet/* /usr/lpp/WebSphere/AppServer/bin/was302plugin.so:service_exit
Service /*.jsp /usr/lpp/WebSphere/AppServer/bin/was302plugin.so:service_exit
EnableFRCA off
```

Configuration Servlet (cont.)

3. I copied HOD.html.ascii to HODCServ.html.ascii.
4. I added the following to HODCServ.html.ascii:

```
<PARM NAME=ConfigServerURL VALUE=servlet/hodconfig/hod>
```

Where 9.82.1.100 is the IP address or hostname of the Configuration Server.

IBM ®

Appendix D:
OS/390 TCPIP PROFILE Customization

IP PROFILE

PROFILE TCPIP BEGINVTAM STATEMENT

```
PORT 223
HNGROUP HNAMES1 andyh.washington.ibm.com patb.washington.ibm.com
ENDHNGROUP
HNGROUP HNAMES2 **.bet.ibm.com ENDHNGROUP
IPGROUP IPNAMES1 255.255.240.0:9.82.0.0 ENDIPGROUP
IPGROUP IPNAMES2 9.82.130.4 9.82.1.161 ENDIPGROUP
IPGROUP IPNAMES3 255.255.224.0:9.82.128.0 ENDIPGROUP
IPGROUP IPNAMES4 9.82.1.2 9.82.1.10 ENDIPGROUP
LUGROUP NONHOD1 TCP20001..TCP20010 ENDLUGROUP
LUGROUP NONHOD2 TCP20011..TCP20020 ENDLUGROUP
LUGROUP HODLUG2 TCP20H01..TCP20H02 ENDLUGROUP
LUGROUP HODLUG3 TCP20H11..TCP20H20 ENDLUGROUP
LUGROUP HODLUG4 TCP20H21..TCP20H22 ENDLUGROUP
PRTGROUP PRTLUS1 TCP20P01..TCP20P10 ENDPRTGROUP
PRTGROUP PRTLUS2 TCP20P11..TCP20P12 ENDPRTGROUP
PRTGROUP PRTLUS4 TCP20P21..TCP20P22 ENDPRTGROUP
```

IP PROFILE (cont.)

PRTMAP PRTLUS1 IPNAMES1 ===> see section 1 below

LUMAP NONHOD1 HNAMES1 ===> see section 2 below

LUMAP NONHOD2 HNAMES2 ===> see section 3 below

LUMAP HODLUG2 IPNAMES2 SPECIFIC PRTLUS2 ===> see section 4 below

LUMAP HODLUG3 IPNAMES3 ===> see section 5 below

LUMAP HODLUG4 IPNAMES4 GENERIC PRTLUS4 ===> see section 6 below

1. If a printer session is initiated to port 223 from any IP address in the 9.82.0.0 subnet (mask 255.255.240.0), the first available LU will be assigned between TCP20P01 and TCP20P10.
2. If andyh or patb from domain washington.ibm.com telnets into port 223, the first available LU will be assigned between TCP20H01 and TCP20H10.
3. If any host from domain bet.ibm.com or any sub-domain (including tomv.bet.ibm.com and suej.rustbuck.bet.ibm.com) telnets into port 223, the first available LU will be assigned between TCP20H11 and TCP20H20.

IP PROFILE (cont.)

4. If 9.82.130.4 telnets to port 223 and requests LU TCP20H01, it will be assigned and a printer session with LU TCP20P11 will be initiated and associated with the host session. Likewise if 9.82.1.161 telnets to port 223 and requests LU TCP20H02, it will be assigned and a printer session with LU TCP20P12 will be initiated and associated with the host session.
5. If any IP address in the 9.82.128.0 subnet (mask 255.255.224.0) telnets into port 223, the first available LU will be assigned between TCP20H11 and TCP20H20.
6. If 9.82.1.2 telnets to port 223, the first available LU will be assigned between TCP20H21 and TCP20H22, and a printer session will be initiated and associated with the host session. Likewise if 9.82.1.10 telnets to port 223, the first available LU will be assigned between TCP20H21 and TCP20H22, and a printer session will be initiated and associated with the host session. Where TCP20P21 is the printer LU if the host LU is TCP20H21, and TCP20P22 is the printer LU if the host LU is TCP20H22.

IBM ®

Appendix E:
OS/390 V2R6 and R7
MKKF Server Certificate

MKKF Server Certificate

Create Certificate with MKKF

1. Go to OMVS on OS/390, change the directory to the directory that you want the key ring to be in, and start MKKF:

   mkkf

2. Create and name the Server Keyring file (n for new):

   n

3. Input the key ring filename or press Enter for the default keyfile.kyr filename.

   This is the key ring filename to be used in the TCPIP PROFILE.

4. 'Work with keys and certificates':

   w

5. 'Create a key pair and request a certificate':

   c

6. Input the key ring password.
7. Input the password again for verification.

MKKF Server Certificate (cont.)

8. Select if the password will expire.

   To have the password expire, enter y and the number of days until it expires.

   To have the password not expire, enter n.

9. Request a server certificate or a CA certificate:

   s

10. Modify the key and certificate fields:

    m

11. Enter the Key Name label.
12. Select the Key Size.
13. Enter the Server Name; fully-qualified host name of the TN3270E server.

    If you select "Server Authentication" on your HOD session this Server Name must match the host name in the DNS for the IP address of the TN3270E server.

14. Enter the Organization Name.
15. Enter the Organization Unit Name.
16. Enter the Locality/City.
17. Enter the State/Province.

MKKF Server Certificate (cont.)

18. Enter the Postal Code.
19. Enter the two digit Country Code:

    US

20. Create the key pair and certificate request:

    r

21. Enter the certificate request filename.
22. Exit the Key menu:

    x

23. Create a stash file:

    c

24. Exit the Key Ring menu

    x

25. Save the key ring file and exit MKKF:

    y

26. If you are going to purchase a signed certificate from a Well Known Certificate Authority (CA), like VeriSign or Thawte, e-mail the certificate request to the CA and they will return it signed.

MKKF Server Certificate (cont.)

27. Start MKKF:

    mkkf

28. Open the key ring file:

    o

29. Enter the key ring filename from step 3.

30. Enter the password from step 6.

31. Receive the certificate into the key ring:

    r

32. Enter the certificate filename from step 21.

33. If you are receiving a self-signed certificate, confirm that you want to add the certificate to the key ring:

    y

34. If prompted, enter the certificate label for the signed certificate.

35. Exit the Key Ring Menu:

    x

36. Save the key ring file and exit MKKF:

    y

MKKF Server Certificate (cont.)

37. Start MKKF:

    mkkf

38. Open the key ring file:

    o

39. Enter the key ring filename from step 3.

40. Enter the password from step 6.

41. Work with keys and certificates:

    w

42. List the keys:

    l

43. Either select the key you want to make the default key:

    s

    Or display the next key:

    n

44. Make the key the default key in the key ring:

    f

MKKF Server Certificate (cont.)

45. Confirm the default key:

    y

46. Exit the Key Menu:

    x

47. Exit the Key Ring Menu:

    x

48. Save the key ring file and exit MKKF:

    y

IBM ®

Appendix F:
Migrate MKKF Certificate to IKEYMAN

Migrate MKKF Certificate to IKEYMAN

Migrate the certificate from MKKF to IKEYMAN

1. Go to OMVS on OS/390, change the directory to the directory that has the certificate in it.
2. Set up the environment for IKEYMAN:

   export PATH=/usr/lpp/internet/bin:$PATH
   export LIBPATH=/usr/lpp/internet/bin:$LIBPATH
   export NLSPATH=/usr/lpp/internet/%L/%N:$NLSPATH
3. Convert kyr file to kdb format:

   ikeyman -m -r keyfile.kyr

   where keyfile is the name of the mkkf key ring file.
4. Enter password.

   File keyfile.kdb is created.
5. Start IKEYMAN:

   ikeyman
6. 'Open key database':

   2
7. Enter the key database name:

   keyfile.kdb

Migrate MKKF Certificate (cont.)

8. Enter password.
9. 'List/Manage keys and certificates':

   1
10. Select the number of the certificate you want to make available to HOD clients.
11. 'Copy the certificate of this key to a file':

    5
12. Select binary file type:

    2
13. Input filename:

    cert.der

    This is the certificate to be made available to the HOD clients.
14. Exit IKEYMAN:

    1

IBM ®

Appendix G:
OS/390 V2R8
GSKKYMAN Server Certificate

GSKKYMAN Server Certificate

Create Certificate with GSKKYMAN

1. Go to OMVS on OS/390, change the directory to the directory that you want the key ring to be in.

   My directory on my system is /u/harrisl.

2. You can display your environment settings, including STEPLIB:

   env

   I needed to add the C and Crypto library to my STEPLIB:

   export STEPLIB=$STEPLIB:SYS1.CRYPTO.SGSKLOAD:SYS1.CPP.SCLBDLL

3. Start GSKKYMAN:

   gskkyman

4. 'Create new key database':

   1

5. Input a database filename or press Enter for the default key.kdb filename.

   I input nm512.kdb and file ***/u/harrisl/nm512.kdb*** was created.

6. Input a password.

   I input *one0ssl* on my system.

GSKKYMAN Server Certificate (cont.)

7. Input password again for verification.
8. Select if the password will expire.

   I selected *1* so that the password would expire.

   Then I pressed *Enter* to default to a 60 day expiration.
9. Select to work with the database now:

   1
10. If you are going to purchase a signed certificate from a Well Known Certificate Authority (CA), like VeriSign or Thawte, select 3 'Create new key pair and certificate request'. If you are going to create a self-signed certificate, select 5 'Create a self-signed certificate'.

    I created a self-signed certificate:

    5
11. Select a version 3 Certificate:

    3
12. Input a certificate label name:

    I input *nmlow* for a certificate label name on my system.

GSKKYMAN Server Certificate (cont.)

13. Select key size.

    I selected *1* for 512 key size.

14. Input 'Common Name'; the fully-qualified host name of the TN3270E server.

    I input *mvsnm2*.

    If you select "Server Authentication" on your HOD session this 'Common Name' must match the hostname in the DNS for the IP address of the TN3270E server.

15. Input the 'Organization'.

    I input *IBM*.

16. Input the 'Organization Unit'.

    I input *nsc*.

17. Input the 'City'.

    I input *GBURG*.

18. Input 'State'.

    I input *MD*.

GSKKYMAN Server Certificate (cont.)

19. Input two digit 'Country'.

    I input *US*.

    Note: If you use USA then you get the following error when you try to save:

    Error: An asn.1 encoding/decoding error occurred.

20. Input number of days for certificate.

    I pressed *ENTER* to default to 365 days.

21. If you are purchasing a signed certificate, send the request to CA and after the request is returned select 4 'Receive a certificate issued for your request'.

22. Set key as the default key in the database:

    1

23. Save the certificate to a file:

    1

24. Save as a binary file:

    2

25. Input a filename or press Enter for the default name of cert.crt.

    I input *nmlow.crt* and file ***/u/harrisl/nmlow.crt*** was created.

GSKKYMAN Server Certificate (cont.)

26. Do not exit yet:

    0

27. 'Store encrypted database password':

    11

    I received a message back that password had been stored in

    /u/harrisl/nm512.sth.

28. Exit GSKKYMAN:

    1

IBM ®

Appendix H:
Make SSL Server Certificate Available to HOD Clients

HOD SSL Server Certificate

Make the Certificate Available to the HOD Clients

1. Change to the root directory:

   cd /

2. Locate the HOD web-published directory:

   find . -name WellKnown TrustedCAs.class*

   The published directory on my system is the default /usr/lpp/HOD/hostondemand/HOD.

3. Copy the binary certificate into the published directory:

   cp /u/harrisl/nmlow.crt /usr/lpp/HOD/hostondemand/HOD/nmlow.crt

   Note: Copy as a binary file and no character conversion.

4. Locate the Host On-Demand server directory:

   find . -name sm.zip*

   The server directory contains the file archives used to run the Service Manager.

   The server directory on my system is /usr/lpp/HOD/hostondemand/lib.

5. Change to the HOD published directory:

   cd /usr/lpp/HOD/hostondemand/HOD

HOD SSL Server Certificate (cont.)

6. Add the certificate to the CustomizedCAs.class file, using the keyrng Java Utility.

   For HOD V3 type the following, all on one line:

   `java -classpath .:HOD_SERVER_DIR/sm.zip:$CLASSPATH com.ibm.sslight.tools.keyrng CustomizedCAs add --certificatetype cert.der`

   For HOD V4 or V5 type the following, all on one line:

   `java -classpath .:HOD_SERVER_DIR/sm.zip:$CLASSPATH com.ibm.hodsslight.tools.keyrng CustomizedCAs add --certificatetype cert.der`

   where **`HOD_SERVER_DIR`** is the HOD server directory,

   `certificatetype` is **`ca`** if you are adding a CA root certificate

   or **`site`** if you are adding a site or self-signed certificate,

   and **`cert.der`** is the name of the file containing the binary certificate.

(continued on next page)

HOD SSL Server Certificate (cont.)

6. (cont.)

Note: **CustomizedCAs** must be capitalized exactly as shown, there is a single hyphen before the classpath parameter, and a double hyphen before the certificate parameter. If the java command is typed in with incorrect syntax you will get the following error:

Unable to initialize Threads: Cannot find class /java/lang/Thread

If no CustomizedCAs.class file exists, keyrng prompts you for a password with which to encrypt the new class-file. However, CustomizedCAs.class must NOT be encrypted, so just ENTER at the password prompt.

I found I needed the following path to the java code:

```
export PATH=$PATH:/usr/lpp/java/J1.1/bin
```

I found this in the ServiceManager.sh script in /usr/lpp/HOD/hostondemand/lib.

I issued the following on my system:

```
java -classpath .:/usr/lpp/HOD/hostondemand/lib/sm.zip:\
/usr/lpp/java/J1.1/lib/classes.zip \
com.ibm.hodsslight.tools.keyrng CustomizedCAs add --site nmlow.crt
```

HOD SSL Server Certificate (cont.)

7. Check to see if the certificate was added.

   For HOD V3 type the following, all on one line:

   java -classpath .:HOD_SERVER_DIR/sm.zip:$CLASSPATH

   com.ibm.sslight.tools.keyrng CustomizedCAs verify

   For HOD V4 or V5 type the following, all on one line:

   java -classpath .:HOD_SERVER_DIR/sm.zip:$CLASSPATH

   com.ibm.hodsslight.tools.keyrng CustomizedCAs verify

   This should be followed by something similar to the following:

   ```
   --------Key ring entry:  1 -------------------
   Entry type:  Site Certificate
   Key:  RSA/512 bits
   Subject:  aix-f26.raleigh.ibm.com,ibm,US
   Issuer:  aix-f26.raleigh.ibm.com,ibm,US
   Valid from:  Fri Aug 13 2:21:29 EDT 1999
   Valid to:  Sun Aug 13 12:21:29 EDT 2000

   Finger print:  D7:2D:E9:6B:66:00:54:04:44:DE:02:E4:4E:1C:80:85
   ```

   The last certificate shown should be the one just added.

(continued on the next page)

HOD SSL Server Certificate (cont.)

7. (cont.)

   I issued the following on my system:

   ```
   java -classpath .:/usr/lpp/HOD/hostondemand/lib/sm.zip:\
   /usr/lpp/java/J1.1/lib/classes.zip \
   com.ibm.hodsslight.tools.keyrng CustomizedCAs verify
   ```

   Note: The CustomizedCAs.class file does not remove any previous information but instead adds the new certificate information so the file may be corrupted if an error occurs when trying to use SSL like the following:

   ```
   keyrng: Cannot retrieve key ring data: com.ibm.hodsslight.SSLException
   ```

   If this happens try deleting the CustomizedCAs.class file from the publish directory and issuing the above java command again.

8. Exit OMVS.
9. Create HOD session with "Enable Security (SSL)" selected.

   Note: If you select "Server Authentication (SSL)" on your HOD session the 'Common Name' input when creating the certificate must match the host name in the DNS for the IP address of the TN3270E server.

HOD SSL Server Certificate (cont.)

10. On OS/390 TN3270E server create TELNET SECUREPORT statement and BEGINVTAM PORT statement in TCPIP PROFILE:

```
TELNETPARMS
   SECUREPORT 723 KEYRING HFS /u/harrisl/nm412.kdb
   ...
ENDTELNETPARMS
BEGINVTAM
   PORT 723
   ...
ENDVTAM
```

11. Recycle HOD and TCP/IP servers and you're done!

IBM ®

Appendix I:
Client Certificate and Browser

Client Certificate

Create Client Certificate with GSKKYMAN

1. Create a new key database and self-signed certificate with GSKKYMAN, just like the server certificate. This is the client key database and public key.
2. Add this client certificate (public key) to the Server key database.
3. Use GSKKYMAN to export the key by using option "9 Export keys" to create a p12 file.
4. FTP p12 file (in binary) to the client workstation.
5. Use the workstation browser to upgrade the p12 certificate.

Client Certificate

Create Client Certificate with GSKKYMAN

- Add Client Public key to Server Key Database:
  1. Start GSKKYMAN:

     gskkyman
  2. Open Server key database:

     nm512.kdb
  3. Enter password:

     one0ssl
  4. Store a CA certificate:

     6
  5. Enter certificate file name:

     lin512.crt
  6. Enter label:

     lin512
  7. Exit GSKKYMAN:

     1

Client Certificate

Client Certificate and Netscape Browser

- Netscape Communicator 4.72 - On the Netscape Communicator window:
  1. Select Communicator, Tools, Security Info
  2. Select Yours under Certificates
  3. Select Import a Certificate
  4. Enter the password of the file to import it
  5. Select file that you FTPed from OS/390
  6. Enter password
  7. Select the P12 file that just appeared under "These are your certificates"
  8. Select Export
  9. Enter new password for the new file
  10. Enter the location to save the new file (to be used by HOD)

Client Certificate (cont.)

Client Certificate and Internet Explorer Browser

- Internet Explorer V5 - On the Internet Explorer window:
  1. Select Tools, Internet Options
  2. Select the Content tab
  3. Select Certificates
  4. Select Import
  5. Enter filename to import it
  6. Enter the password of the file
  7. Select the P12 file that just appeared under "Issued To"
  8. Select Export
  9. Enter new password for the new file
  10. Enter the location to save the new file (to be used by HOD)

IBM ®

Bibliography

Bibliography

- Program Directory for IBM Host On-Demand for System/390:
  - GI10-3175-00 Version 5.0
- The following three documents are available after installation (where 9.82.1.100 is the IP address of the OS/390 system where HOD is installed) and they are also available on the HOD Library page off of the Host On-Demand Home page:
  - Host On-Demand Readme

    http://9.82.1.100/hod/en/doc/readme/readme.html
  - Planning and Installation Guide (also available in pdf as install.pdf)

    http://9.82.1.100/hod/en/doc/install/install.html
  - Host Printing Reference

    http://9.82.1.100/hod/en/doc/hostprint/hostprintref.html

IBM ®

Web Sites

Web Sites

- Host On-Demand Product Information site:

  http://www-4.ibm.com/software/webservers/hostondemand

  Select Support from the above Home Page to get to the Support Page.

  Select Library from the above Home Page to get to the Library page.

- This presentation is available as presentation PRS162 on web site:

  http://www.ibm.com/support/techdocs