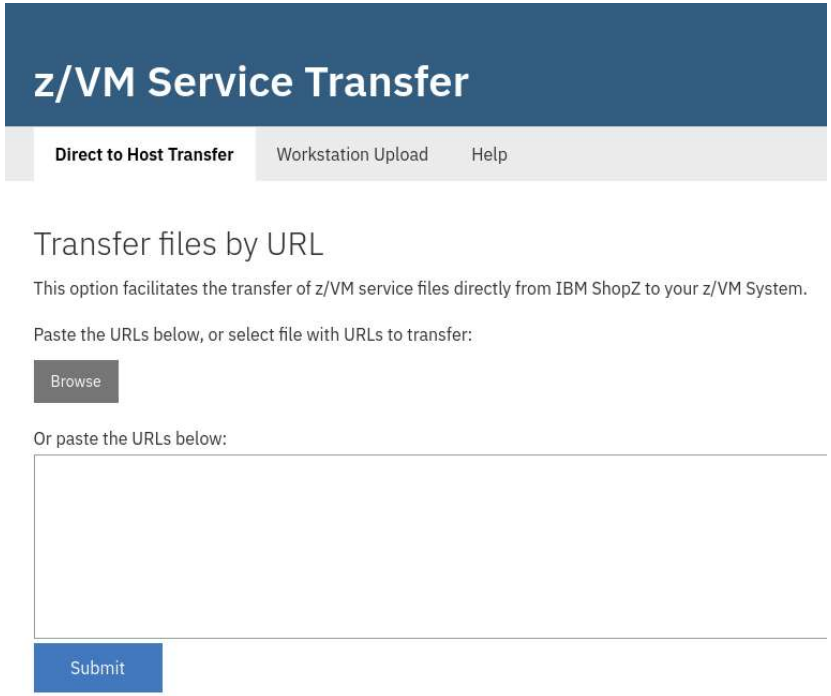
VM66540 - z/VM Direct to Host Service Transfer

Rob van der Heij

robvdheij@nl.ibm.com

z/VM Development - Endicott



Agenda

- z/VM Continuous Delivery Model
- Idea
- Development
- Using the GETSHOPZ Utility
- Status and Plans

z/VM Continuous Delivery Model

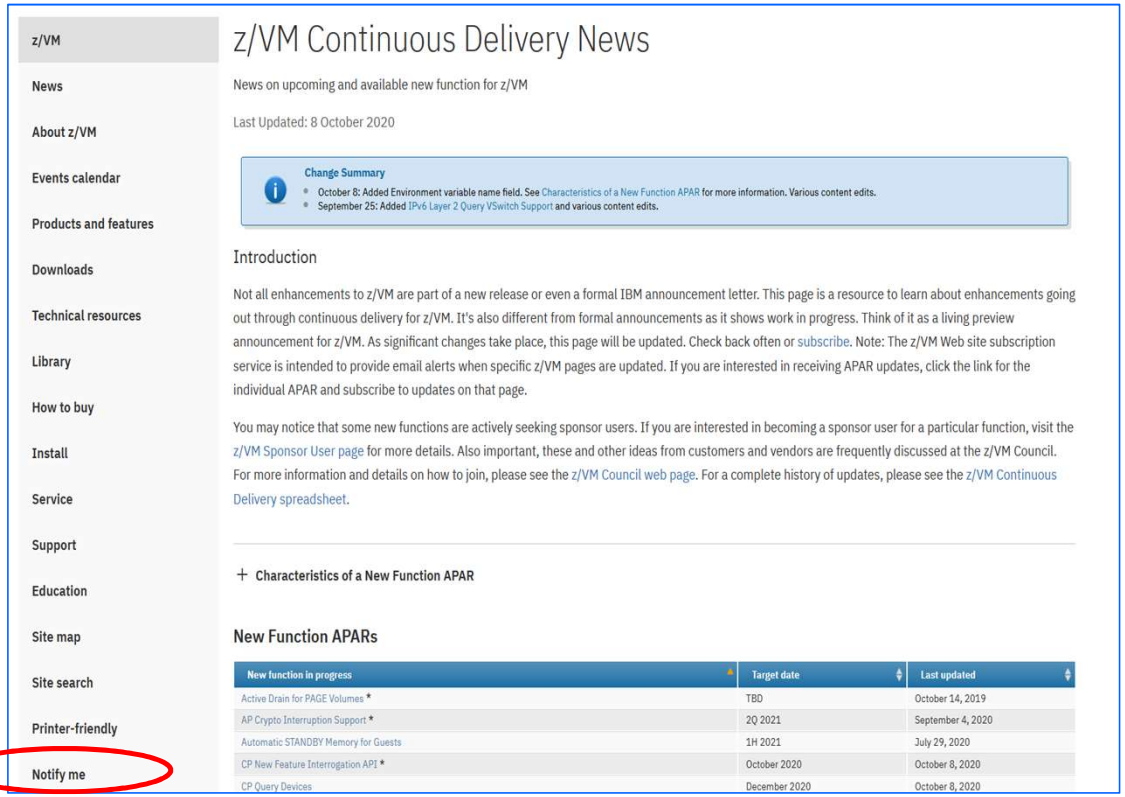
z/VM Continuous Delivery Model

- Based on IBM Design Thinking
- New Function is delivered between releases
- Deliver only the function that is needed
- Co-develop with users to define the scope

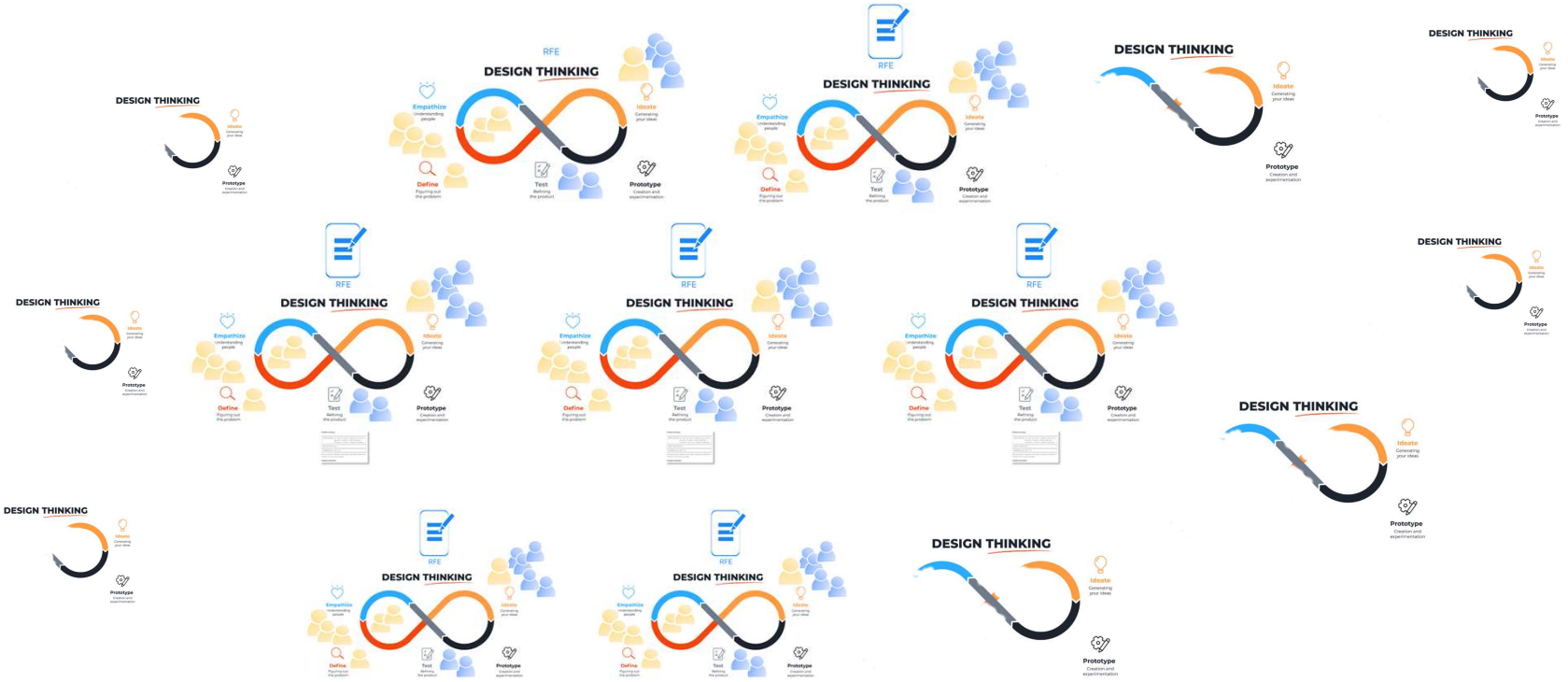
- Shorter development cycle
- Meets user requirements better
- Available for users when code is ready
- Release to wrap up any delivered new function

z/VM Continuous Delivery Page

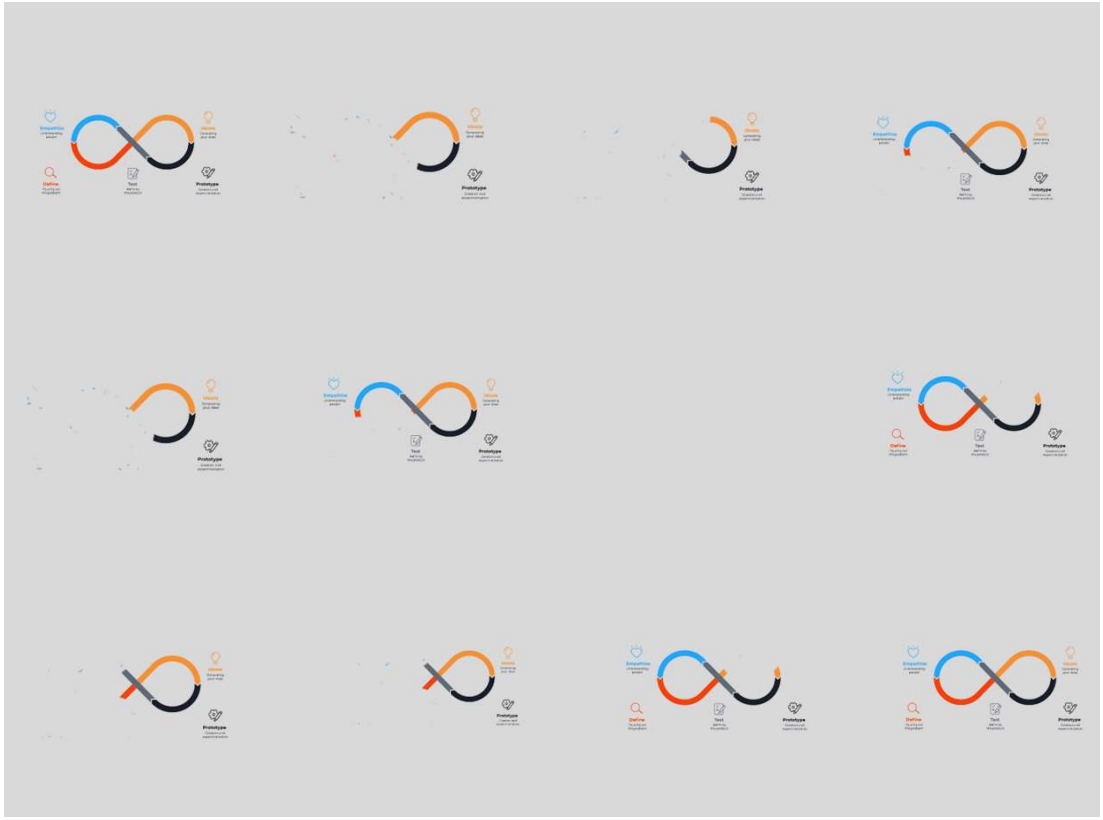
- Gives an overview of new function that is under consideration. Allows clients to:
  - Express interest in being a sponsor user for an item.
  - Plan for new support coming out in the future.
  - Understand the value, benefit, and impact of new enhancements.
- https://www.vm.ibm.com/newfunction/
- Subscribe for updates via “Notify me” link on left navigation bar.



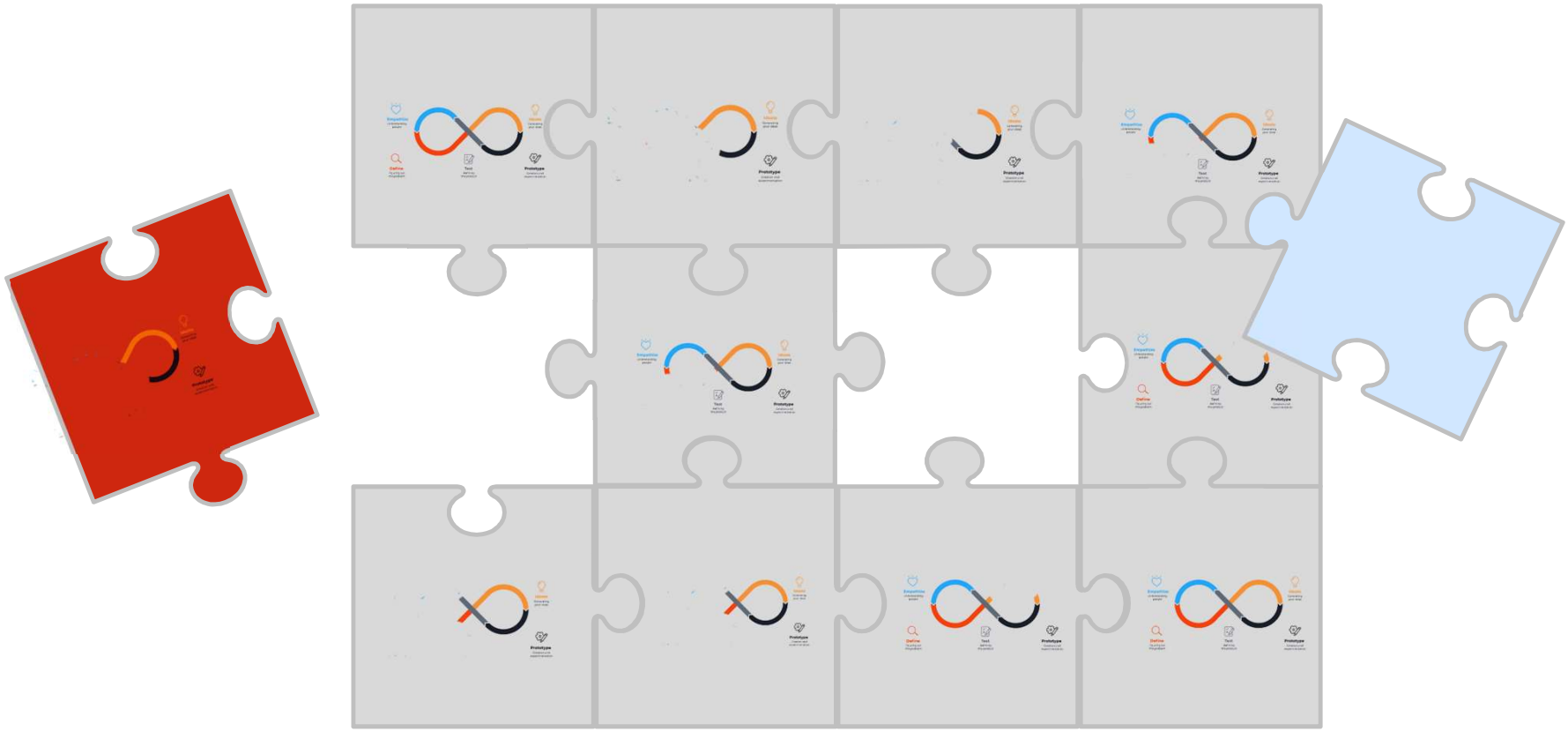
z/VM Development



Plumber's Head

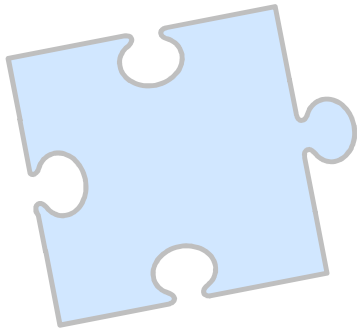


Plumber's Head



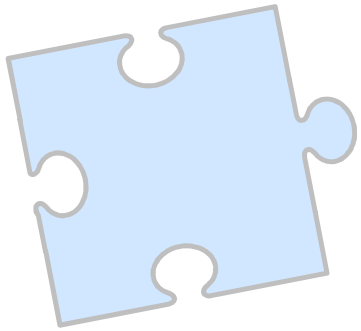
Idea – Where did this come from?

CMS Pipelines TCP/IP Support



- Pipe-think alternative for REXX Sockets
  - **tcpclient** enables a CMS application to connect to a (remote) server via TCP/IP
- Fairly easy to create an HTTP client for CMS
  - Very effective for specific applications dealing with specific (REST) servers
  - Generic web client is still more work (following links, rendering HTML pages, etc)
  - Some customers used parts of the Charlotte browser for downloading z/VM service
- Plain text HTTP traffic has been frowned upon for some time
  - Does not comply with corporate security policies
  - Some services simply stopped tolerating plain text connections

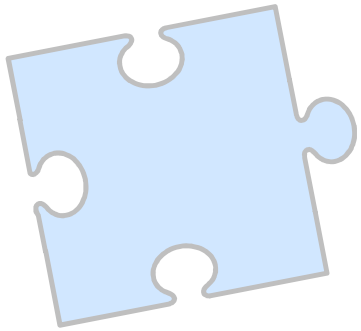
z/VM TCP/IP Support for SSL/TLS



- Initial Secure Socket Layer support in TCP/IP was decades ago
  - Application Transparent SSL for server applications through secure port
- Dynamic SSL (2005) only supported the Pascal API
  - Effectively limited to client and server applications provided with z/VM, like TELNET and FTP
- Additional SSL/TLS support through new IOCTL commands (2016)
  - Motivated by the need to secure TCPNJE connections in RSCS
  - Secure connections established through C and IUCV Socket API
- CMS Pipelines TCP/IP support uses the IUCV Socket API

"This is so easy, probably just an afternoon of work"

Prototype - CMS Pipelines SSL Support



- Prototype for CMS Pipelines SSL Support
  - Leverages the existing SSL/TLS configuration to implement security policy
  - Minimal change to add SSL support to an existing application
  - Experimental stages for HTTP and HTTPS (like curl and wget)
  - Prototype limited to implicit SSL like for HTTPS

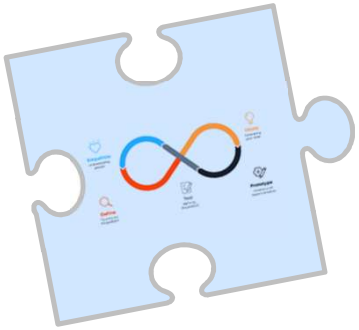
- Representational State Transfer (REST)
  - Protocol layer on top of HTTPS used for most modern web services
  - Covers data transfer in both directions with POST and GET commands

- Many opportunities and interesting use cases
  - Exchange data between CMS and IBM Cloudant NoSQL Database
  - Post a message on Slack using a CMS client
  - Exchange CMS data with GitHub for version management
  - Upload data from CMS to ECuRep

```
PIPE reader 4kblock file 383 | pack f
  | rexx toecurep TS002528918 prb00001.vmdump
```

- Missing jigsaw pieces
  - Authentication for remote services (no credentials in the code)
  - JavaScript Object Notation (JSON)

VM66365 - CMS Pipelines SSL Support



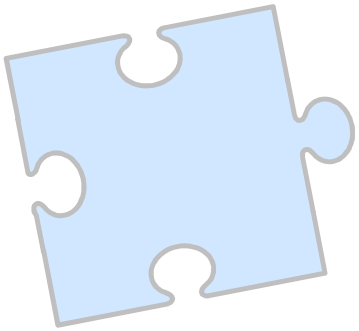
- Presented to the z/VM Council to look for sponsor users
  - Satisfied two or three open user group requirements
  - Minimal change to enable SSL in existing pipeline applications
  - Limited to “Implicit SSL” (recognized by the different port for secure connections)

tcpclient www.vm.ibm.com 80 ⇨ tcpclient www.vm.ibm.com 443 secure

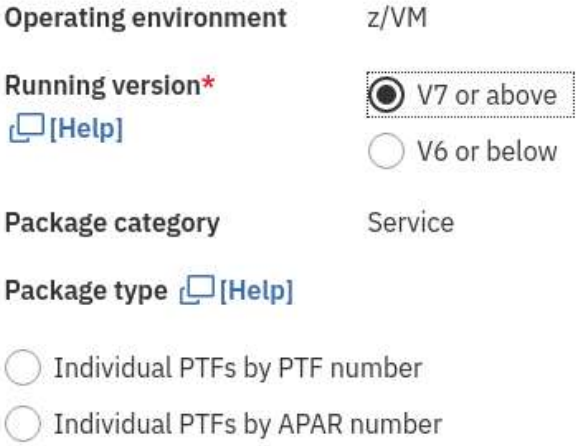
- Sponsor user response on first alpha release of the code to try
  - Nice, but we want to use FTP with SSL to exchange data with z/OS
  - Customers had expected the unsupported FTP REXX would work with SSL
  - FTP with SSL requires “explicit SSL” where FTP client negotiates SSL with the FTP server
  - Transparent SSL is nice, but I want to see that a secure connection was established
  - Designed a still-minimal compatible interface to allow the application to start the SSL handshake
    - Deliver a new built-in FTP stage in CMS Pipelines so users don’t have to write their own
    - Many mini-loop iterations with a sponsor user to fit most requirements
- Beta release of the code appeared to meet the requirements
  - Pending enhancements in VM SSL support to enable hostname validation
- Some options for improvement, but apparently not very important to have right now

UM35658 for z/VM 7.1
Shipped May 2020

Revised Packaging Format for z/VM Service



- Align with z/OS SMP/E service format
  - GIMZIP uses compressed UNIX tar file
  - Include a SHA1 hash to verify data integrity
  - Retire the older DETERSE format
- Rushed into z/VM 7.1
  - REXX wrapper around the DETERSE MODULE
- Provided additional jigsaw pieces
  - Ability to compress and decompress in UNIX compress style
  - Logic to decode the GIMZIP tar files



Challenges to Receive z/VM Service

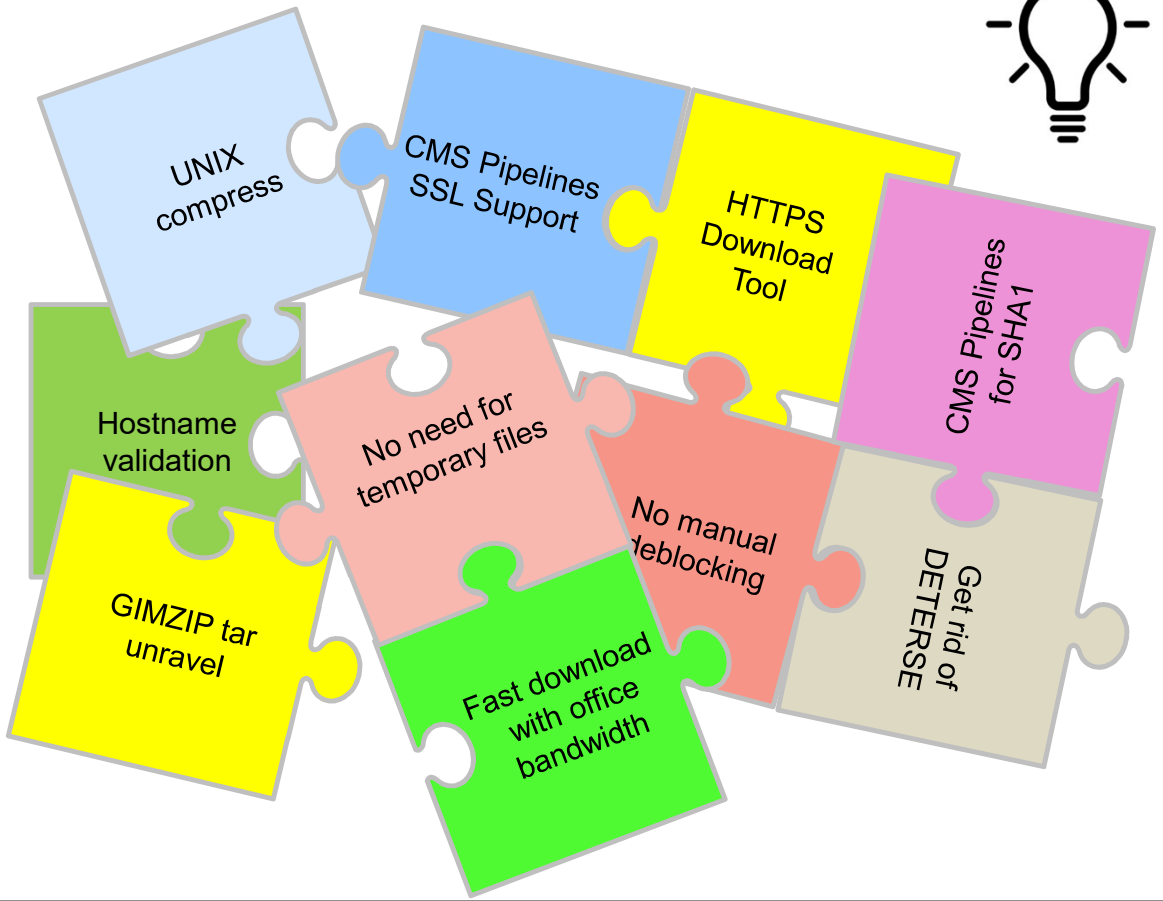
- IBM download servers disabled non-secure connections
  - Previously some customers were using portions of Charlotte browser to download service
  - FTP-SSL downloads only available for customers with ServiceLink contract
  - Most customers have to download to the workstation and then upload to VM
- Many systems staff working from home
  - Service downloaded to workstation at home, uploaded to z/VM via VPN is often very slow
  - Some customers postponed upgrade to a new release - Recommended Service Update (RSU) gets larger
- Applying service is rare enough that few people have developed “muscle memory”
  - Process didn’t get easier with the additional options for packaging service
  - Less easy access to colleagues and documentation to get the details right
- Sometimes takes days to get the RSU ready to use on the maintenance user’s disk
  - “Thought I needed to upload with LRECL 1028 but that failed”
  - “Decided to order again, since it didn’t work first time”
  - “I have this EXEC that fixes a VMARC file after upload, why didn’t that work?”
  - “Uploading 550 MB with 80 KB/s VPN took 2 hours – to fill up the disk”
  - “Thought I would better try V6 packaging, just in case, but that gave errors during DETERSE”
  - “Used COPYFILE to correct the record format, but that didn’t work”

Idea: CMS Client to Download Service from IBM

- Pass URL to a CMS tool to download via HTTPS
- SSL/TLS hostname validation for authenticity
- Compute the SHA1 hash during download
- Decompress the file during download
- Unravel the GIMZIP tar format during download
- Only store the decompressed SERVLINK file
- Exploit office bandwidth

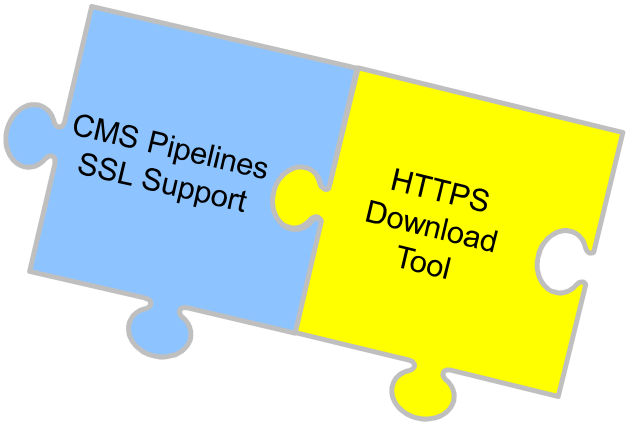
- Explained idea to the packaging team
  - Most of the pieces are there already
  - It's probably not very hard to do

"Customers wanted this for years, but who's going to build it?"



Development – How hard can it be?

Pipeline Stage to Retrieve via HTTP



- Earlier attempts were utilities as REXX EXEC writing the output to a file

- Created a WGET REXX pipeline stage
  - Reads the URL through primary input
  - Writes the contents of the downloaded file to the primary output

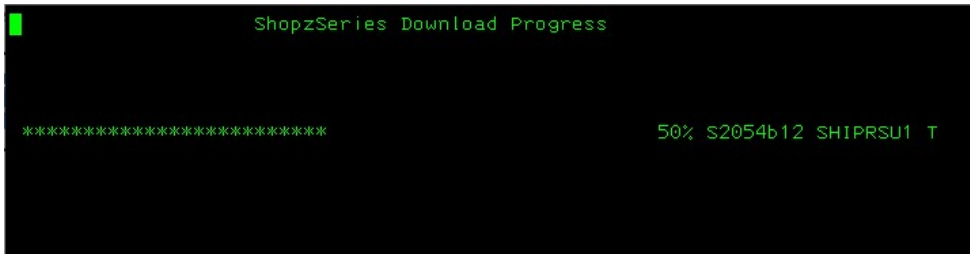
- Pretty easy with TCPCLIENT stage

```
PIPE < url txt | rexx wget | > temp data a
```

- Secure download with TLS/SSL needs VM System SSL
  - Proper root certificate (DigiCert) needs to be stored in VM System SSL with GSKKYMAN

https://www.vm.ibm.com/related/tcpip/ecudigic.html

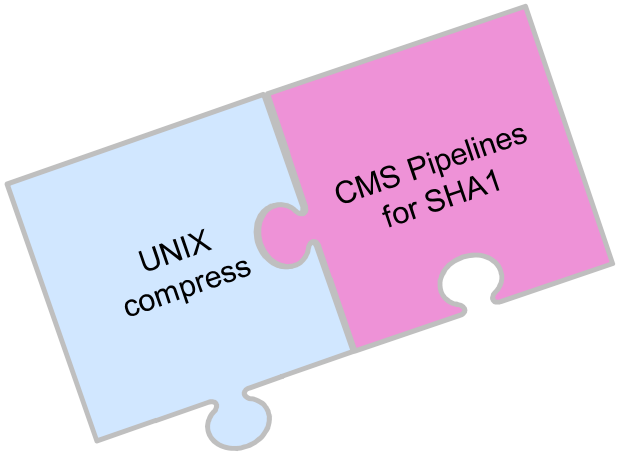
- Downloading a 550 MB RSU takes time, even at 5 MB/s
  - Using FULLSCR stage we can animate the progress



Decompress Downloaded Data

- Re-purpose the GIMZIP decompression code

```
PIPE < url txt | rexx wget | rexx gimzip | > temp data a
```



- Unable to predict whether decompressed file will fit
- GIMPAF XML is not very helpful
  - Quoted size is much more than needed

```
<ARCHDEF
name="S0002.SHOPZ.S0016005.SHIPRSU1.pax.Z"
archid="SHIPRSU1"
originalsize="898410375"
size="303561216"
hash="8A32E62F733329836CA3F4EAFCCE1D5FBBDFE317">
</ARCHDEF>
```

- Computed SHA1 hash could be useful as integrity check

```
PIPE (end \) < url txt | rexx wget | sha: digest sha1 | rexx gimzip | > temp data a
          \ sha: | spec 1-* c2x | cons
```

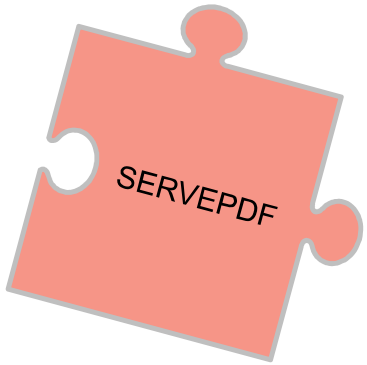
Dealing With the Download URL

- Download URL must be copied from the Shopz web page to CMS
  - The URL is almost 300 characters long
  - Not possible to type it into a CMS program
  - Copy and paste into 3270 session may not work
  - Field wrap varies by type of 3270 emulator

```
https://deliverycb-bld.dhe.ibm.com/sdfdl/v2/
edeliver/S015186371/S8h02866/2021081064190/PROD/
Xa.2/Xb.2M6bqbhMRw4PQHzSAAwJlKU/Xc.S015186371/S8
h02866/2021081064190/PROD/S7064190.SHIPTFSS/Xd./
Xf.LpR.F1AZ/Xg.11367199/Xi./XY.shopz/XZ.Ve1Z_LFZ
3B3OFhdcdz0OiqecmWR_0OQA/S7064190.SHIPTFSS
```

- Idea: Use a web server on VM
  - Bring up a web page with an input field to paste the URL
  - Server-side process can capture URL to initiate the download
  - Web page could also show transfer progress
- Not a very practical solution
  - Many customers will not have a z/VM web server
  - Requirement to license a web server would be a show-stopper
  - Introduces extra complexity with passwords and authentication

Disposable Web Server

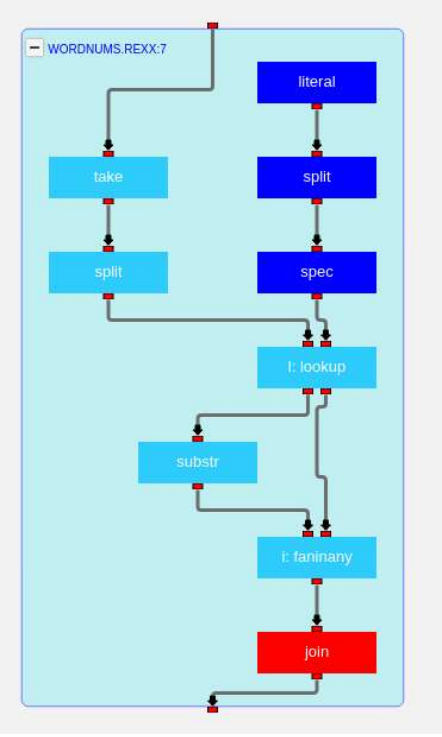


- Inspired by SERVEPDF
  - Runs a disposable web server for the duration of a single web transaction
  - Started on your own CMS userid with SERVEPDF specifying the PDF file as argument
  - Picks a random free port to connect the web server to
  - SERVEPDF presents the URL to use in the web browser
  - Browser downloads the PDF from CMS and saves the file on the workstation
  - Authentication through browser IP address avoids the need for password
  - Inherits all privileges of the user virtual machine
  - Available on the VM Download Packages pages

- Exploit CMS Pipelines SSL Support to allow for secure web server with TLS/SSL
  - Suitable server certificate for the VM system must be stored in VM System SSL certificate database
  - Browsers have stronger requirements than the average TN3270 client

- User dialogue in the browser to avoid switching between CMS and browser several times
  - Download URL is pasted into an input field in the web page
  - CMS program downloads the file and reports status back to the browser
  - Progress of the download must be shown on the web page – harder than simply return an HTML page as response

JavaScript with Chunked Transfer



https://www.rvdheij.nl/pdweb/

- Special response header to announce incremental output
  - Transfer-Encoding: chunked
  - Web server sends response in small pieces

- JavaScript application in the browser to initiate transactions
  - Uses XMLHttpRequest() function in JavaScript
  - Asynchronous requests
  - Typically uses data in JavaScript Object Notation (JSON)
  - JavaScript code reads JSON document to apply changes to web page being displayed

```
{ "id": "file2", "done": 5731730, "bw": "47.55 kB/s", "size": 7419102, "transfer": "77.2%", "eta": "0:34" }
{ "id": "file2", "done": 7418880, "bw": "61.26 kB/s", "size": 7419102, "transfer": "99.9%", "eta": "0:00" }
{ "id": "file2", "cmsfile": "0684PTFS SERVLINK T", "blocks": 4971 }
{ "id": "file2",  "transfer": "Completed" }
```

Filename	Size	CMS File	Blocks	Transfer	Transfer Rate
S0001.SHOPZ.S6960684.SHIPDOCS.pax.Z	189.2 kB	0684DOCS SERVLINK T	182	Completed	581.30 kB/s
S0002.SHOPZ.S6960684.SHIPTFSS.pax.Z	7.1 MB			36%	2.6 MB

Workstation Upload

- Some customers have a strict security policy

  "Nothing for us, our VM systems can't connect to the Internet"

- Sometimes possible to get an exception through firewall rules for specific web sites like the IBM download site
  - *"But it's also done for z/OS…"*

- Additional Requirement: Allow for service packages to be uploaded from the workstation with the same user interface
  - Does not avoid the need to download to the workstation and upload to VM again
  - Ensure data is uploaded correctly the first time
  - Decompress the data being uploaded, no need for extra space on disk
  - Verify integrity of the data during upload
  - Reduced number of manual steps to get service applied

It's About the People

- About a dozen excited sponsor users signed up to participate
  - Provided additional requirements to make it work in a customer configuration
  - Kicked the tires of several versions of the code
  - Encouraged developers to complete the project

- Glenda Ford
- Les Geer
- Kerry Wilson
- Jeff Gertner
- John Hollenbeck
- Jim Sculley
- Tom Kovach

and many more

Live Demo Ahead

Using the GETSHOPZ Utility

Invoking the CMS Program

- GETSHOPZ is installed on the MAINT 193 Systems Programmer Tools Disk
- Intended to be used on the MAINT720 userid

GETSHOPZ [RUN [(options]]

```
id
RVDHEIJ  AT GDLVM7   VIA RSCS     10/14/21 03:04:03 EDT     THURSD
Ready; T=0.01/0.01 03:04:03
getshopz run
GETSHOPZ v1.0

Web Interface:
 http://GDLVM7.POK.IBM.COM:27012/

Use PF3 to stop the web interface
```

http:// Workstation-to-VM connection not using TLS/SSL

This does not affect the connection to the IBM download site

DMSRXS1408W File TCPIP DATA * not found
Create TCPIP DATA with DNS address.
Specify hostname and domain when not properly resolved by DNS.

Enable TLS/SSL Connections

Options:

- **SECURE** – Use default certificate as defined with GSKKYMAN
- **TLSLABEL <label>** - Use the certificate with the specified label

getshopz run (secure
GETSHOPZ v1.0

Web Interface:
https://GDLVM7.POK.IBM.COM:27012/

Use PF3 to stop the web interface

https:// Uses TLS/SSL

URL based on DNS reverse lookup, use HOSTNAME option to override

- **HOSTNAME <hostname>** - Specify host and domain to connect to your VM system
- Update TCPIP DATA with proper DNS server address

TCP/IP Error 10006 KeyLabelNotFound
Specified (or default) label not defined in certificate database (message is issued when the browser tries to connect)

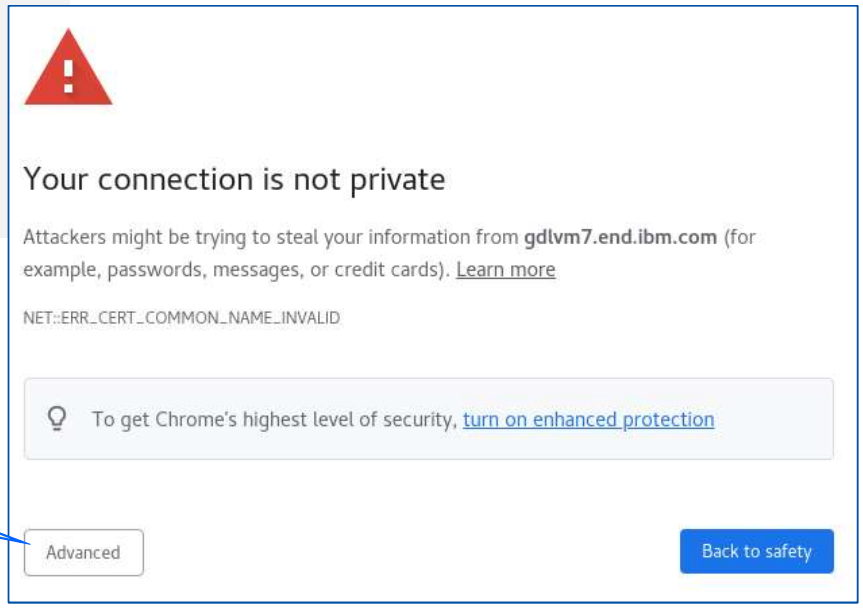
TLS Hostname Validation

- Ensures the certificate is valid for the host you connect to

```
rvdheij:~$ ping -c 1 gdlvm7.end.ibm.com
PING gdlvm7.end.ibm.com (9.56.214.105) 56(84) bytes of data.
64 bytes from gdlvm7.end.ibm.com (9.56.214.105): icmp_seq=1 ttl=52 time=155 ms
```

```
getshopz run ( hostname gdlvm7.end.ibm.com secure tls gdlvm7
GETSHOPZ v1.0

Web Interface:
 https://gdlvm7.end.ibm.com:27012/

Use PF3 to stop the web interface
```

Shows “common name” from the certificate and can be used to connect and review the certificate



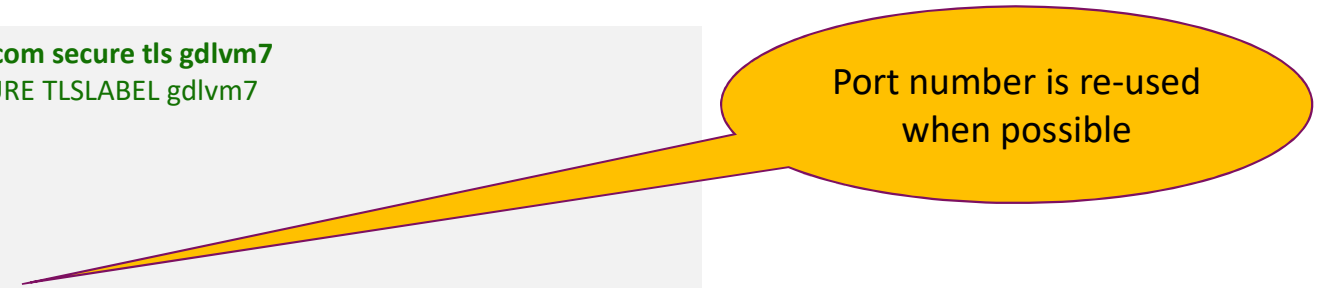
TCP/IP Error 10414
Certificate is not valid

GETSHOPZ Default Options

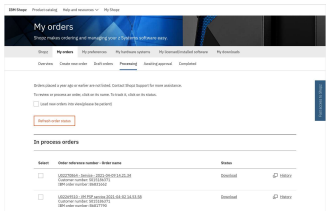
- Use the DEFAULT sub-command to set your default options

GETSHOPZ DEFAULT (options

```
getshopz default ( hostname gdlvm7.endicott.ibm.com secure tls gdlvm7
parms: ( HOSTNAME gdlvm7.endicott.ibm.com SECURE TLSLABEL gdlvm7
Ready; T=0.01/0.01 05:16:13
getshopz
GETSHOPZ v1.0

Web Interface:
 https://gdlvm7.endicott.ibm.com:27012/

Use PF3 to stop the web interface
```



Direct-to-Host – With z/VM Internet Connectivity



Shopz

1

IBM Download Site

4

proxy

Optional Customer Proxy Server

IBM Network

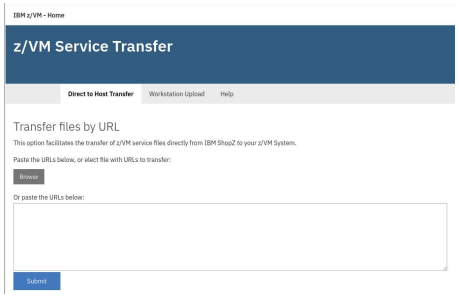
Customer Network

Customer VM System

2
Copy URLs from Shopz

Web Browser

3
Paste URLs into GETSHOPZ Web Application



GETSHOPZ on CMS

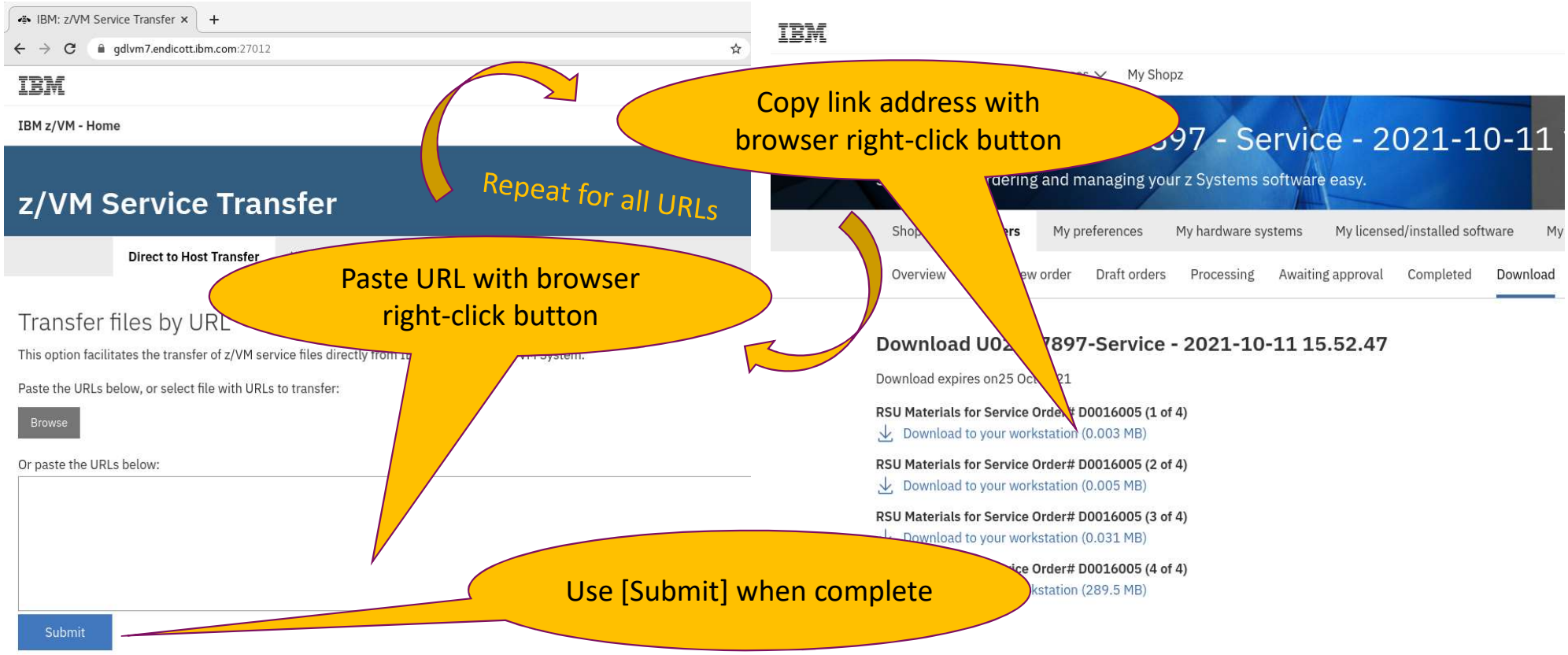
Checksum Verification

Data Decompression

5

CMS Minidisk MAINT720 500

Demo: Copying Links from Shopz into GETSHOPZ



Demo: Progress Displayed in Web Browser

File being downloaded

Size of download

SHA1 matched

Filename	Size	CMS File	Blocks	Transfer	Transfer Rate	Status
GIMPAF.XML	2.7 kB	28032285 GIMPAF T	1	Completed	1087.01 kB/s	From deliverycb-mul.dhe.ibm.com authenticated by SHA1
GIMPAF.XSL	4.9 kB	28021981 GIMXSL T	2	Completed	567.44 kB/s	From deliverycb-mul.dhe.ibm.com authenticated by SHA1
S0001.SHOPZ.S0016005.SHIPDOC.pax.Z	31.5 kB	6005DOC TXT T	5	Completed	376.12 kB/s	From deliverycb-mul.dhe.ibm.com authenticated by SHA1
S0002.SHOPZ.S0016005.SHIPRSU1.pax.Z	289.5 MB	6005RSU1 SERVLINK T	184836	Completed	2720.33 kB/s	From deliverycb-mul.dhe.ibm.com authenticated by SHA1

CMS file

Number of blocks on disk

Downloaded directly from the IBM site

FPLTCR1142E Unable to resolve deliverycb-mul.dhe.ibm.com
(RXSOCKET error 2016 EHOSTNOTFOUND Host not found in SITEINFO file)

Ensure the correct DNS server is specified in TCPIP DATA with nsinteraddr parameter

Review TCPIP, TCPIPEXT, and PROXY options on GETSHOPZ for very complex network configuration

Demo: Verify the SHA1 of GIMPAF

- Download confirmation e-mail contains SHA1 hash for the package

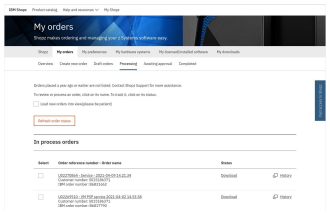
```
ORDER REFERENCE INFORMATION

   IBM customer number:                        S015186371

   SERVICE: IBM order number:                  D0016005

            ShopzSeries reference number:      U02307897

   Hash Value : 5F006884A337EF9CBB2818D657F13517753648C5
```

From the “ready for download” mail

- View the downloaded GIMPAF file and check the last line
- The hash value was used to verify package consistency
- Matching SHA1 hash confirms this is the same order

```
 28032285 GIMPAF    T1   V 80  Trunc=80 Size=34 Line=34 Col=1 Alt=0
00031 hash="91210A8FDC8C4155576EFDB71E76F999B72957F6">
00032 </ARCHDEF>
00033 </PKGDEF>
00034 <?PKGHASH hash="5F006884A337EF9CBB2818D657F13517753648C5" ?>
00035 * * * End of File * * *
```

Workstation Upload – Without z/VM Internet Connectivity



Shopz

1

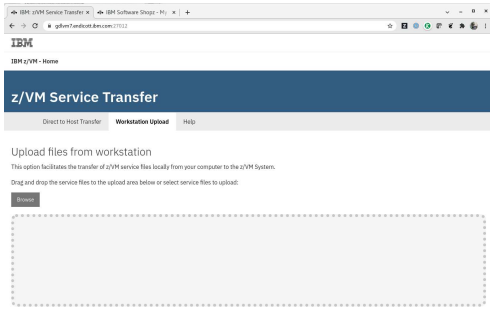
IBM Download Site

3
Download Files
from Shopz

2
Use URLs
from Shopz

Web Browser

4
Upload Files to
GETSHOPZ
Web Application



GETSHOPZ on CMS

Checksum Verification

Data Decompression

5

CMS Minidisk
MAINT720 500

Browser Authentication

- Default is to authenticate by browser IP address being the same as TN3270 client address
  - Convenient because it just works
  - Secure because no credentials can be captured
- May not comply with your security policy
- Fails in more complicated network configurations

Option:

- **TOKEN** – Generate one-time token to authenticate web session

```
getshopz run ( token
GETSHOPZ v1.0

Web Interface:
 https://gdlvm7.endicott.ibm.com:27012/?token=WlsYJVeQwU9kR5lESJunfw

Use PF3 to stop the web interface
```

Specify Output Disk for Download

- Make sure to ACCESS the output disk before starting GETSHOPZ
- Use the DISK option to point GETSHOPZ to where you want the SERVLINK files

- Default: Use the file mode with most available space

Option:

- **DISK <fm>** – Specify file mode of disk where output files are stored

Direct to Host Service Download – Status and Plans

VM66540 Status and Plans

- PTF is available for z/VM 7.2
- Included in the 7203RSU of Sept 30, 2021
- Works with recent versions of most browsers
  - Google Chrome
  - Mozilla Firefox
  - Microsoft Edge
- Partially working with Safari on iOS

APAR **VM66540** Direct to Host Service Download
PTF **UM35899** for z/VM 7.2 shipped Aug 31, 2021

Possible Future Improvements

- Support for ServiceLink orders
- Include support for digital signatures
  - Especially important when using the upload from workstation
- Fixing some known issues with the code
- Customer-reported defects and feature requests

Use your communication channels with z/VM Development to make sure we understand what is most important for you