z/OS ISPF
Secure HTTP access of the ISPF Gateway
V2R4

Contents

List of Tables

Chapter 1

IBM Health Checker for z/OS User's Guide

Topics:

ISPF checks (IBMISPF)

ISPF_GW_HTTPS

Description:

Checks whether the ISPF Gateway has been accessed on this system using non-secured HTTP.

If this check determines that the ISPF Gateway has been accessed on this system using non-secured HTTP, it will continue to be reported for the duration of this IPL, or as long as this Health Check is active. When this exception condition is detected, message ISTH040E is issued and is followed by message ISTH900I, which indicates the date and time that the ISPF Gateway was last accessed using non-secured HTTP. You can use message ISTH900I to determine whether a new non-secured HTTP access of the ISPF Gateway has been detected or the exception condition is related to an earlier access.

Reason for check:

The communication between a client and the ISPF Gateway is not secure when non-secured HTTP is used.

z/OS® releases the check applies to:

z/OS V2R4, with the PTFs for APARs OA58151 and OA58450 applied, and later.

User override of IBM values:

The following sample shows the defaults for customizable values for this check. Use this sample to make permanent check customizations in an HZSPRMxx parmlib member used at IBM Health Checker for z/OS startup. If you just want a one-time only update to the check defaults, omit the first line (ADDREPLACE POLICY) and use the UPDATE statement on a `MODIFY hzsproc` command. Note that using non-POLICY UPDATEs in HZSPRMxx can lead to unexpected results and is therefore not recommended.

```
ADDREPLACE POLICY[(policyname)] [STATEMENT(name)]
UPDATE
CHECK(IBMISPF,ISPF_GW_HTTPS)
DATE('date of the change')
REASON('Your reason for making the update')
ACTIVE
SEVERITY(LOW)
INTERVAL(24:00)
```

Debug support:

No

Verbose support:

No

Parameters accepted:

No

Reference:

See *Update the configuration to enable SSL for your TSO/ISPF Gateway traffic* in *ISPF Planning and Customizing* for information on modifying your HTTP Server configuration so that the ISPF Gateway is accessed using Hypertext Transfer Protocol Secure (HTTPS).

Messages:

This check issues the following messages:

- *ISTH039I*
- *ISTH040E*
- *ISTH900I*

See *SNA Messages*.

SECLABEL recommended for multilevel security users:

SYSLOW - see *z/OS Planning for Multilevel Security and the Common Criteria* for information on using SECLABELs.

Chapter 2

z/OS Upgrade Workflow

Topics:

ISPF upgrade actions

This topic describes upgrade actions for base element ISPF.

ISPF actions to perform before installing z/OS V2R4

This topic describes ISPF upgrade actions that you can perform on your current (old) system. You do not need the z/OS V2R4 level of code to make these changes, and the changes do not require the z/OS V2R4 level of code to run after they are made.

ISPF: Use SSL to secure HTTP access of the ISPF Gateway

Description

Beginning in z/OS V2R4, the ISPF Gateway requires, by default, that it is accessed using Hypertext Transfer Protocol Secure (HTTPS).

The communication between a client and the ISPF Gateway is not secure when non-secured HTTP is used.

Table 1: Information about this upgrade action

This table provides more details about the upgrade action. Use this information to plan your changes to the system.

Element or feature:	ISPF
When change was introduced:	z/OS V2R4.
Applies to upgrade from:	z/OS V2R3 and z/OS V2R2.
Timing:	Before installing z/OS V2R4.
Is the upgrade action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM® Health Checker for z/OS check:	To determine whether the ISPF Gateway is being accessed on your system using non-secure HTTP, use health check IBMISPF, ZOSMIGV2R3_Next_ISPF_GW_HTTPS. This health check is added by ISPF APAR OA58151, which is applicable to z/OS V2R2 and later.

Steps to take

Determine whether the ISPF Gateway is being accessed on your system using non-secured HTTP.

If the ISPF Gateway is being accessed using non-secured HTTP, update the HTTP configuration on your system to enable SSL for your ISPF Gateway traffic.

Reference information

For more information, see the topic *Update the configuration to enable SSL for your TSO/ISPF gateway traffic* in *ISPF Planning and Customizing*.

Chapter 3

ISPF Planning and Customizing

Topics:

Customizing IBM HTTP server powered by Apache

If you plan to use IBM HTTP server powered by Apache to invoke the gateway, changes must be made to the HTTP configuration and environment files.

To invoke the gateway as installed, make these changes to the HTTP configuration file, httpd.conf:

- Include Alias and ScriptAlias directives to map the gateway URLs to their file system locations. The path specified in these directives must be the path where the gateway was installed. For example:

```
Alias        /ISPZIVP.html  /usr/lpp/ispf/bin/ISPZIVP.html
ScriptAlias  /ISPZIVP.cgi   /usr/lpp/ispf/bin/ISPZIVP.cgi
ScriptAlias  /ISPZXML       /usr/lpp/ispf/bin/ISPZXML
```

- If the gateway modules are not in the LINKLIST, include a STEPLIB directive to indicate the load library data sets that contain these modules. For example, if the libraries were DEV.USER.LOAD, DEV.STG.LOAD, and DEV.BASE.LOAD:

```
setenv STEPLIB DEV.USER.LOAD:DEV.STG.LOAD:DEV.BASE.LOAD
```

- Include LoadModule directives and a Directory directive to:
  - cause IBM HTTP server powered by Apache to prompt users to enter their user ID and password
  - invoke the gateway under the user's user ID
  - allow the gateway directory to serve content only to users who are authenticated using the System Authorization Facility (SAF) security product

  The path specified in the Directory directive must be the path where the gateway was installed. For example:

```
LoadModule auth_basic_module modules/mod_auth_basic.so
LoadModule authnz_saf_module modules/mod_authnz_saf.so
<Directory /usr/lpp/ispf/bin>
  AuthName "SAF auth ISPF Gateway"
  AuthType Basic
  AuthBasicProvider saf
  Require valid-user
  SAFRunAs %%CLIENT%%
</Directory>
```

- Update the configuration to enable SSL for your TSO/ISPF gateway traffic.

  By default, an HTTPS connection is required to access the TSO/ISPF Gateway and unencrypted HTTP connections are rejected with an error message:

```
***ERROR: Connection is NOT using HTTPS. HTTPS is required.
```

  Although not recommended, you can override this default by adding the environment variable CGI_SECURECONN to your HTTP configuration and setting it to "FALSE".

  1. Use the gskkyman utility to create a key database and password stash file. See *z/OS Cryptographic Services System Secure Sockets Layer Programming* for information on the gskkyman utility.
  2. Store the key database file and password stash file in your HTTP ServerRoot directory.
  3. Include directives to enable SSL support:

```
# Replace @@ServerRoot@@ with your ServerRoot directory name
# Replace ihsserverkey.kdb with your database file name
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 443
```

```
<VirtualHost *:443>
SSLEnable
</VirtualHost>
KeyFile @@ServerRoot@@/ihsserverkey.kdb
SSLDisable
```

4. Include the LoadModule directive and rewrite rules to redirect your TSO/ISPF gateway traffic to use HTTPS:

```
LoadModule rewrite_module modules/mod_rewrite.so
RewriteEngine on
RewriteCond %{SERVER_PORT} =80
RewriteRule ^(.*) https://%{SERVER_NAME}%{REQUEST_URI} [R,L]
```

- To use the Interactive ISPF Gateway, include the following directives:
  - Set the CGI_CEATSO directive to the value TRUE:

```
setenv CGI_CEATSO  TRUE
```

    When the CGI_CEATSO directive is not included or is set to a value other than TRUE, the Legacy ISPF Gateway is invoked.
  - Set the LIBPATH directive to include the directory where the CEA TSO/E address space services programs are located (/usr/lib). For example:

```
setenv LIBPATH     /usr/lib
```

- To use the Legacy ISPF Gateway, include the following directives:
  - Set the CGI_ISPWORK directive to the path for the WORKAREA directory used by the gateway. For example, this directive specifies the default path for the WORKAREA directory:

```
setenv CGI_ISPWORK /var/ispf
```

  - Set the CGI_ISPCONF directive to the path for the CONFIG directory where the ISPF configuration file ISPF.conf is stored. For example, this directive specifies the default path for the CONFIG directory:

```
setenv CGI_ISPCONF /etc/ispf
```

  - Set the CGI_ISPLOGLEVEL directive to the level of logging requested from the gateway. See *Customizing other environments* for information on the available log levels. For example, this directive requests default logging:

```
setenv CGI_ISPLOGLEVEL 0
```

To invoke the gateway as installed, make this change to the HTTP environment file, envvars:

- Update the path statement to include the path where the gateway was installed. If dot(.), indicating the current directory, is already specified then no update is required. In this example, the gateway path /usr/lpp/ispf/bin is added to the existing path statement:

```
export PATH=$PATH:/etc/ihs9_rw/bin:/usr/lpp/ispf/bin
```

For additional information about configuring IBM HTTP server powered by Apache, review the manuals at http://www-01.ibm.com/support/knowledgecenter/SSEQTJ/welcome?lang=en.

Chapter 4

SNA Messages

Topics:

ISTH039I

The ISPF Gateway is not being accessed using non-secured HTTP

Explanation

The check ISPF_GW_HTTPS ran successfully and found no exceptions. The check determined that the ISPF Gateway has not been accessed on this system using non-secured Hypertext Transfer Protocol (HTTP) during this IPL.

The communication between the client and the ISPF Gateway is not secure when non-secured HTTP is used.

System action

The system continues processing.

Operator response

Not applicable.

System programmer response

Not applicable.

User response

Not applicable.

Problem determination

Not applicable.

Source

z/OS Communications Server Health Checker

Module

ISTHCCK2

Routing code

Not applicable.

Descriptor code

Not applicable.

Automation

Not applicable for automation.

Example

```
ISTH039I The ISPF Gateway is not being accessed using non-secured HTTP
```

ISTH040E

The ISPF Gateway is being accessed using non-secured HTTP

Explanation

The check ISPF_GW_HTTPS determined that the ISPF Gateway has been accessed on this system using non-secured Hypertext Transfer Protocol (HTTP) during this IPL.

The communication between the client and the ISPF Gateway is not secure when non-secured HTTP is used.

System action

The system continues processing.

Operator response

Not applicable.

System programmer response

See *Update the configuration to enable SSL for your TSO/ISPF Gateway traffic* in *ISPF Planning and Customizing* for information on modifying your HTTP Server configuration so that the ISPF Gateway is accessed using Hypertext Transfer Protocol Secure (HTTPS).

When the check ISPF_GW_HTTPS determines that the ISPF Gateway has been accessed on this system using non-secured HTTP, it will continue to be reported for the duration of this IPL, or as long as this Health Check is active. Message ISTH040E is followed by message ISTH900I, which indicates the date and time that the ISPF Gateway was last accessed using non-secured HTTP. You can use message ISTH900I to determine whether a new non-secured HTTP access of the ISPF Gateway has been detected or this report is related to an earlier access.

User response

Not applicable.

Problem determination

Not applicable.

Source

z/OS Communications Server Health Checker

Module

ISTHCCK2

Routing code

Not applicable.

Descriptor code

Not applicable.

Automation

Not applicable for automation.

Example

```
ISTH040E The ISPF Gateway is being accessed using non-secured HTTP
```