z/OS ISPF

Secure HTTP access of the ISPF Gateway

V2R2, V2R3

Contents

Chapter 1

IBM Health Checker for z/OS User's Guide

Topics:

ISPF checks (IBMISPF)

ZOSMIGV2R3_Next_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 Migration Health Check is active. When this exception condition is detected, message ISTM040E is issued and is followed by message ISTM900I, which indicates the date and time that the ISPF Gateway was last accessed using non-secured HTTP. You can use message ISTM900I 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. Beginning in z/OS V2R4, the ISPF Gateway will require, by default, that it is accessed using Hypertext Transfer Protocol Secure (HTTPS).

z/OS® releases the check applies to:

z/OS V2R2 and V2R3 with the PTFs for APARs OA58151 and OA58450 applied.

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,ZOSMIGV2R3_Next_ISPF_GW_HTTPS)
DATE(’date of the change’)
REASON(’Your reason for making the update’)
INACTIVE
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:

- *ISTM039I*
- *ISTM040E*

- *ISTM900I*

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

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:

  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 directives that identify the work area and configuration directories for the gateway. The CGI_ISPWORK directive defines the path for the WORKAREA directory used by the gateway. The CGI_ISPCONF directive defines the path for the CONFIG directory where the ISPF configuration file ISPF.conf is stored. These examples of the CGI_ISPWORK and CGI_ISPCONF directives specify the default paths for the WORKAREA and CONFIG directories:

  ```
  setenv CGI_ISPWORK /var/ispf
  setenv CGI_ISPCONF /etc/ispf
  ```

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 in the IBM Knowledge Center.

Chapter 3

SNA Messages

Topics:

ISTM039I

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

Explanation

The check ZOSMIGV2R3_Next_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. In z/OS V2R4, the ISPF Gateway will require, by default, that it is accessed using Hypertext Transfer Protocol Secure (HTTPS).

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

```
ISTM039I The ISPF Gateway is not being accessed using non-secured HTTP
```

ISTM040E

The ISPF Gateway is being accessed using non-secured HTTP

Explanation

The check ZOSMIGV2R3_Next_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. In z/OS V2R4, the ISPF Gateway will require, by default, that it is accessed using Hypertext Transfer Protocol Secure (HTTPS).

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 ZOSMIGV2R3_Next_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 Migration Health Check is active. Message ISTM040E is followed by message ISTM900I, which indicates the date and time that the ISPF Gateway was last accessed using non-secured HTTP. You can use message ISTM900I 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

```
ISTM040E The ISPF Gateway is being accessed using non-secured HTTP
```