z/OS 3.2 IBM Education Assistant

Solution Name: Hardening Security between z/OS BCPii and HMC/SE

Solution Element(s): 5752SCHWI z/OS BCPii

July 2025

Agenda

- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None.

Objectives

- z/OS BCPii allows authorized applications to query, change, and perform procedures against the systems in the Process Control (HMC) Network

- With the addition of `HWIREST` Callable Service, z/OS BCPii increased the number of capabilities available to the user for managing CPCs

- Hardware Management Consoles (HMCs) require a different authorization scheme to be targeted, causing certain functionality to not be exposed previously through z/OS BCPii

- Adding support for JSON Web Tokens (JWTs) through z/OS BCPii allows for increased functionality and security granularity for our clients

Overview

- Who (Audience)
  - Users of z/OS BCPii desiring additional functionality provided by Hardware Management Consoles (HMCs) and greater user security granularity.

- What (Solution)
  - JWT usage capability can be configured for `HWIREST` and `HWIREST2` Callable Services

- Wow (Benefit / Value, Need Addressed)
  - Automation capabilities of functionality only available through HMCs are now available to z/OS Users through a REST-like API
  - Hardened security through the permissions being mapped from z/OS Users to HMC Users

Usage & Invocation (1 of 5)

```
HWIREST(&request, &response);

REQUEST_REST_PARM_TYPE request;
       request.httpMethod
       request.uri
       request.targetName
       request.requestBody
       request.clientCorrelator
       request.encoding
       request.requestTimeout

RESPONSE_PARM_TYPE response;
       response.responseDate
       response.requestId
       response.location
       response.responseBody
       response.httpStatus
       response.reasonCode
```

`targetName` now supports HMC targets `HMC://hmcname`

Usage & Invocation (2 of 5)

```
HWIREST2(&request, &response);
```

```
REQUEST_REST2_PARM_TYPE request;
      request.httpMethod
      request.uri
      request.targetName
      request.requestBody
      request.clientCorrelator
      request.encoding
      request.requestTimeout
      request.eventExitMode
      request.eventExitAddr
      request.eventExitParm
```

```
RESPONSE_PARM_TYPE response;
      response.responseDate
      response.requestId
      response.location
      response.responseBody
      response.httpStatus
      response.reasonCode
```

`targetName` supports HMC or CPC Targets

note: `HWIREST2` always uses JWTs so JWTs must be configured

Usage & Invocation (3 of 5)

- HMC targets through `HWIREST` will *always* use JWTs
- When targeting CPCs via `HWIREST`, the authentication mode is determined by a FACILITY Class Profile

New FACILITY Class Profile: `HWI.AUTHMODE.HWIREST.<cpcname>.<sysname>`

- APPLDATA Field:
  - `FACILITY` *(or none)*
    - *default* Utilize existing FACILITY Class Profiles for authorization
  - `JWTHYBRID`
    - Utilize JWTs when configured and supported on Local and Remote systems, otherwise fall back to FACILITY Class Profiles
  - `JWT`
    - Exclusively utilize JWTs, fails request when unable to utilize JWT

note: User is always required to have READ access to `HWI.APPLNAME.HWISERV`

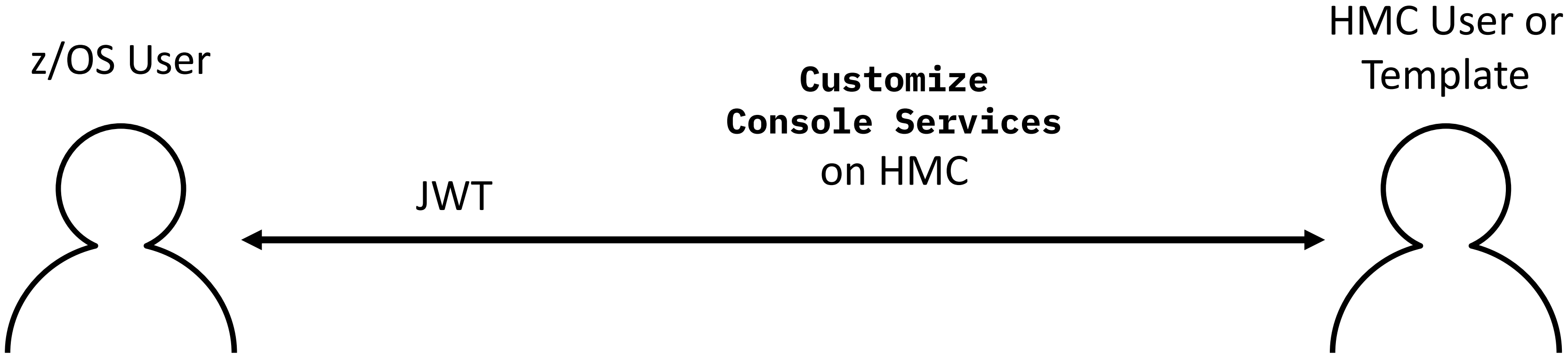
Usage & Invocation (4 of 5)

- `F HWIBCPII,REFRESH,RESTAUTH`
  - Modify Command for changes to authorization mode following BCPii startup

- `D BCPII,RESTAUTH`
  - Display the currently configured authorization mode

Usage & Invocation (5 of 5)

- JWT Mappings are configured by an admin to correlate a z/OS User with an HMC User or Template.



- z/OS BCPii obtains a signed JWT on behalf of the user and sends it along with the `HWIREST` or `HWIREST2` request where the SE / HMC correlates the JWT to a specific HMC User or Template and creates a session
- HMC Users or Templates offer a greater level of permission granularity

Interactions & Dependencies

- Software Dependencies
  - None.
- Hardware Dependencies
  - IBM z17 System is required for JWT Authorizations.
  - IBM Crypto Express Card is required for JWT Authorizations.
- Exploiters
  - None.

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No
- No toleration/coexistence APARs/PTFs.

Installation & Configuration

- Available on z/OS 3.1 with OA65929

- Available in z/OS 3.2 Base

only necessary to use JWT:

- Generate a BCPii Authorization Certificate in a Security Product
- Export and Upload of the BCPii Authorization Certificate to the targeting or managing HMC
- Configuration of a JWT Mapping for the User associated with the BCPii Started Task on the targeting or managing HMC
  - Additionally, any z/OS Users issuing JWT HWIREST or HWIREST2 request will need a mapping defined on the targeting or managing HMC

Summary

- New JWT Mappings allow for more granular permissions checking for z/OS Users targeting both SEs and HMCs

- `HWIREST` and `HWIREST2` along with JWTs can allow for more z/OS BCPii capabilities through HMC Targeting

- `HWI.AUTHMODE.HWIREST.<cpcname>.<sysname>` can be configured to change the authentication mode used for `HWIREST` requests targeting SEs
  - `JWTHYBRID` can be leveraged to enable the added capabilities of JWTs while still utilizing Facility Class Profiles when JWTs aren’t supported or configured
  - `HWI.AUTHMODE.HWIREST.*.*` can be used to cover all systems

Appendix

Publications

- **z/OS MVS Programming: Callable Services for High-Level Languages**
  - Complete z/OS BCPii documentation
- **z/OS MVS System Messages, Volume 6 (GOS – IEA)**
  - z/OS BCPii (HWI) message documentation
- **z/OS MVS System Codes**
  - z/OS BCPii abend ’042’x documentation
- **z/OS MVS System Commands**
  - z/OS BCPii MVS Commands
- **Hardware Management Console Web Services API**
  - Firmware Publication for REST APIs

Additional samples for z/OS BCPii are provided via GitHub

- https://github.com/IBM/zOS-BCPii