IBM z17 News / Overview

Advanced AI where it matters most

zExpertenforum Oktober z17 News

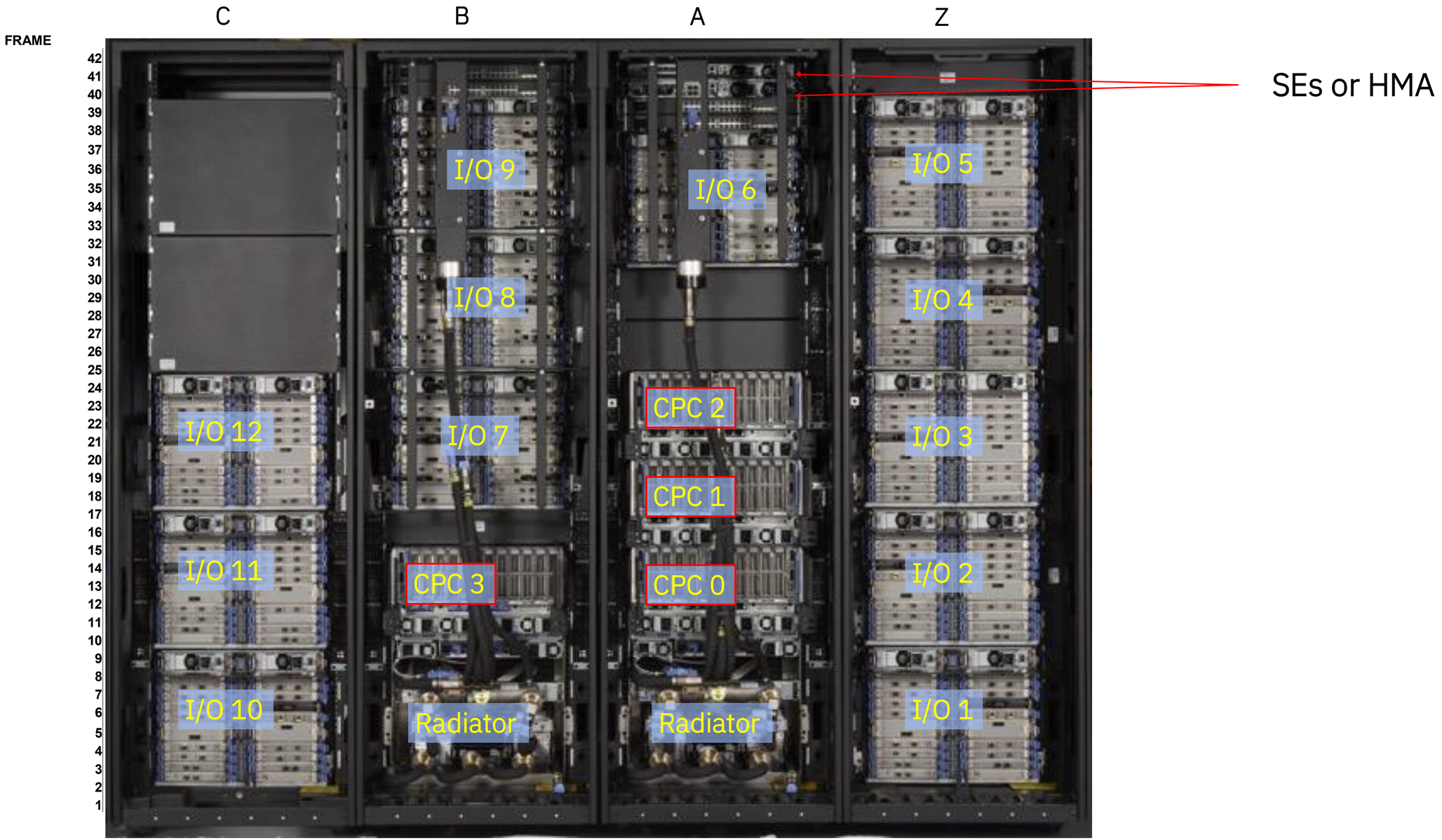
André Spahni
IBM Z Brand Technical Specialist
aspa@ch.ibm.com

IBM Z – Naming for IBM z17

Brand Name:	IBM
Product Class:	IBM mainframe
Family Name:	IBM Z®
Model and Processor Capacity Features:	ME1, Features: Max43, Max90, Max136, Max183, Max208
Machine Type:	9175

IBM z17 4-frame

IBM z17 ME1, rear view



IBM z17 system highlights

- 1-4 , 19” frames
- 208 customer cores
- IBM Telum II processor
- Improved I/O subsystem
- Less weight & floor space

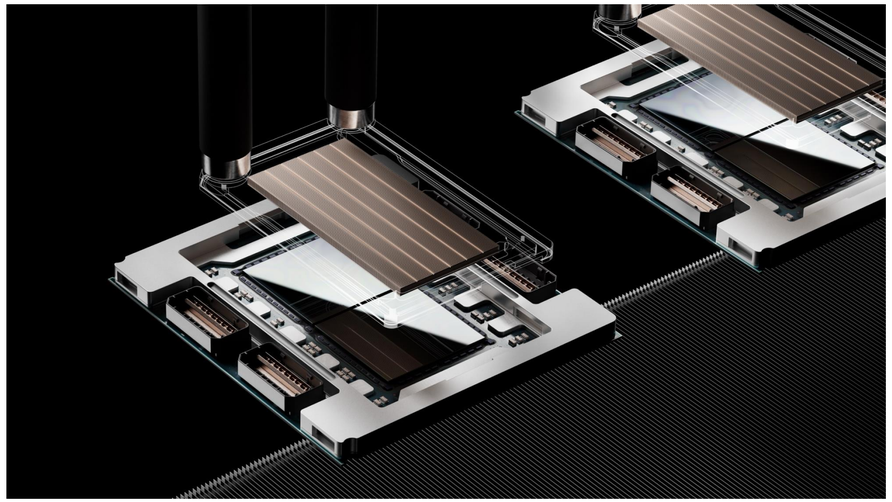
11% more performance — Single thread performance vs IBM z16

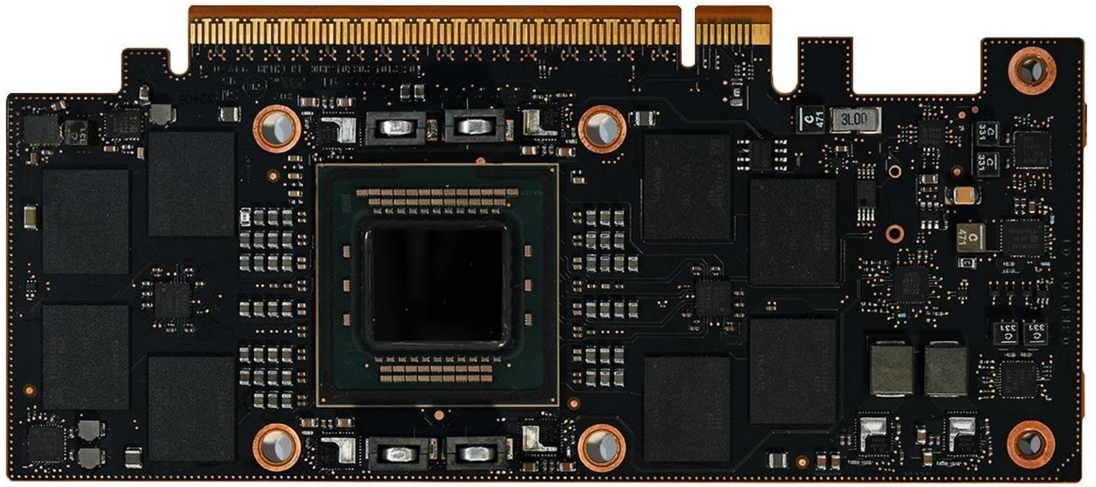
15-20% capacity growth — vs IBM z16

60% more memory — Up to 64 TB memory

19% less power — than IBM z16

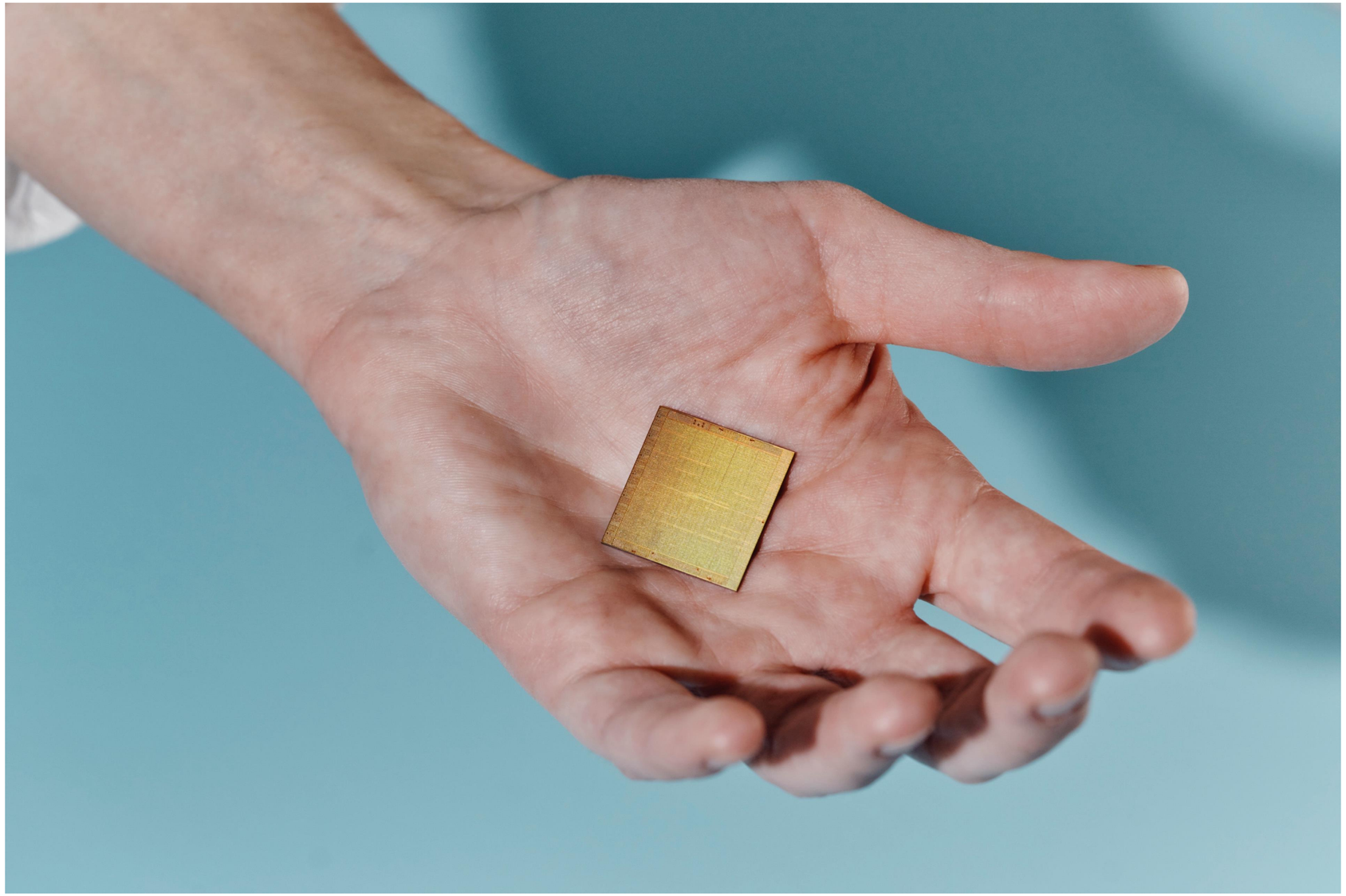
IBM Telum II Processor and Spyre Accelerator





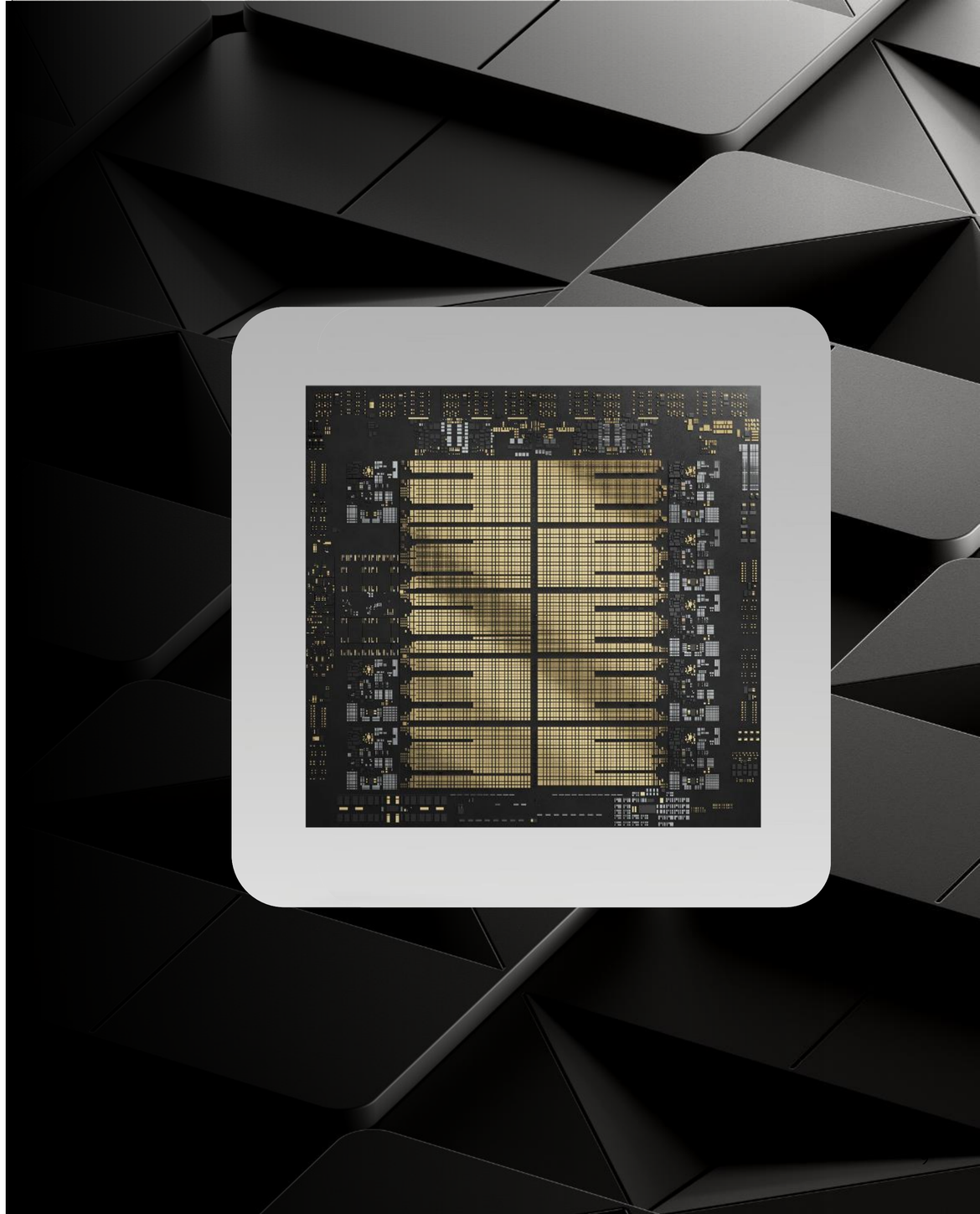
IBM Telum II Dual Chip Module (DMC)

Telum II Chip in hand



IBM Telum II Processor

- 5nm technology, 5.5GHz
- 8 cores with 20% area reduction and improved microprocessor power management
- 40% more cache per core
- 24.1 Miles (39 KM) of wire per chip
- 43.0 Billion (Milliarden) transistors
- **NEW:** On-chip Data Processing Unit (DPU): Increased I/O performance with 70% reduction in power for I/O management, RAS, reduced latency
- 2nd-gen AI Accelerator for high-speed inferencing with fine tuning
- 8x dedicated AI processing per core



IBM Telum II™ Processor

10 - 36MB L2s

40% more cache per core over z16

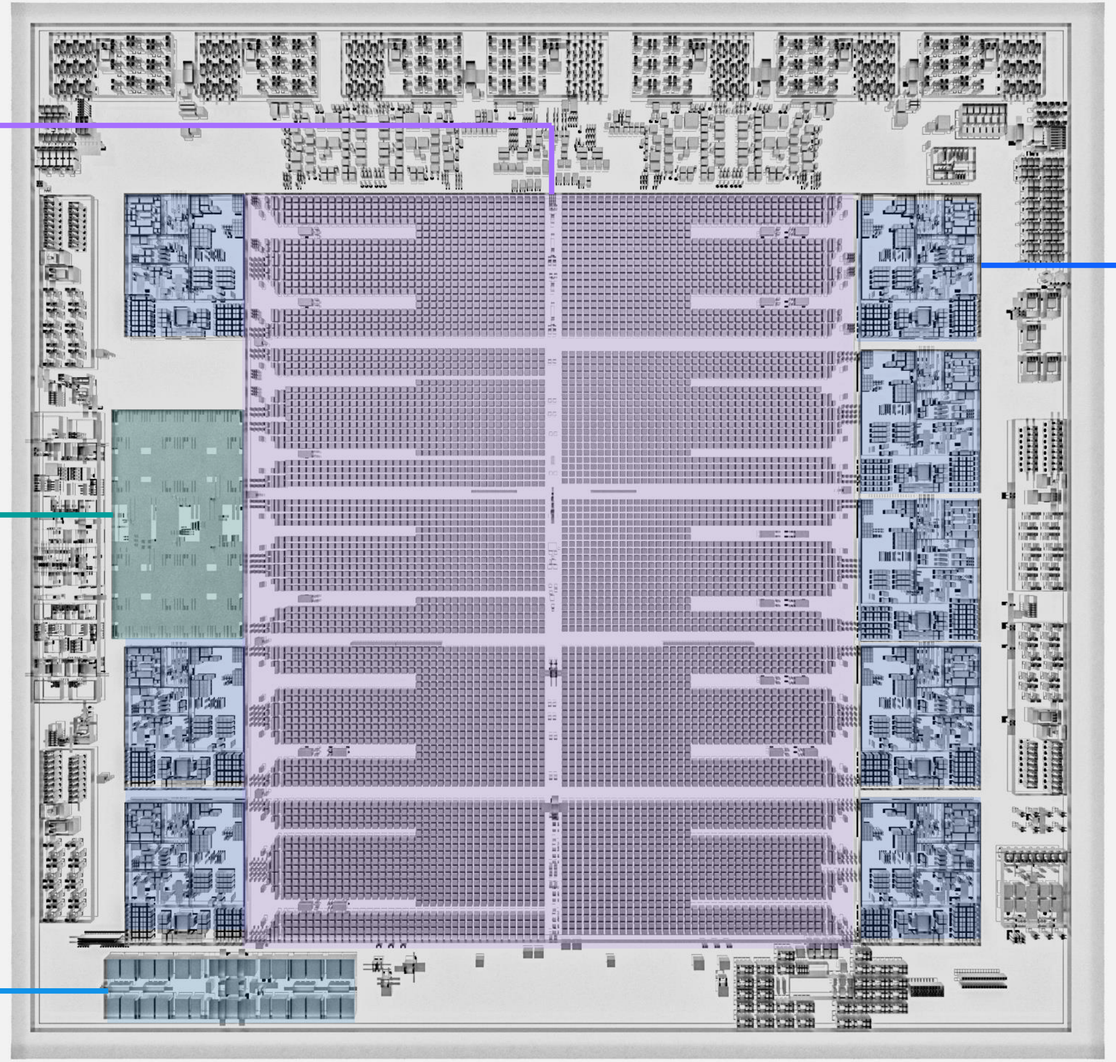
I/O DPU

A redesigned I/O subsystem resulting in power and data center footprint reduction

2nd Gen AI accelerator

Improved quantization and matrix operations

8x accelerators available per core



8 - 5.5GHz cores

+11% Single thread performance

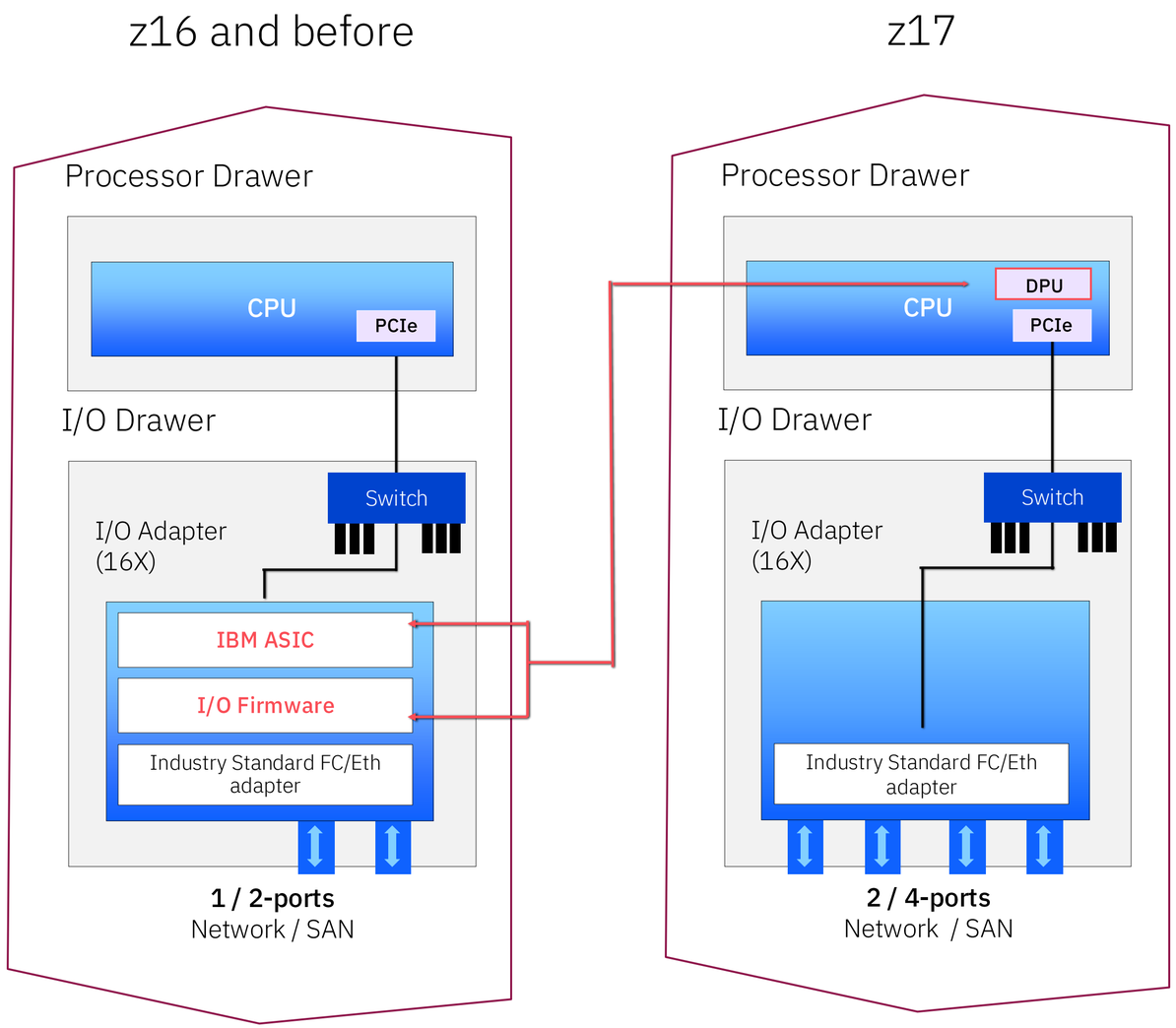
20% area reduction and 15% power reduction

Process up to **450 billion (Milliarden)** inference operations per day with **1 ms** response time, a **50%** increase over z16

IBM z17 vs. z16

	z16	z17	z17 differentiation
Processor Chip	7nm technology 5.2G Hz 8 cores per chip 18.8 Miles of wire per chip 22.5B transistors	5nm technology 5.5 GHz 8 cores per chip 24.1 Miles of wire per chip 43B transistors	20% core processor area reduction 15% power reduction +11% single thread performance
Capacity	200 cores	208 cores	+12-20% capacity
Cache	32MB L2 256MB virtual L3 2GB virtual L4	36MB L2 360MB Virtual L3 2.8GB virtual L4	+40% cache growth
Total system memory	4U DDR4 DDIMM 40TB max memory	4U DDR5 DDIMM 64TB max memory	+60% system memory growth
On-chip AI acceleration	Telum	Telum II	More AI processing per chip Up to 8x on-chip AI processors available per CPC drawer
Off-chip PCIe Accelerator card	N/A	Spyre AI accelerator chip 32 Gen AI-ready cores on extended adapters 75W PCIe gen5 x16 adapter Up to 48 adapters per system	Available only on z17
System I/O	Off-chip I/O processing	On-processor chip I/O DPU	70% Reduced power for I/O management Double density with new FICON Express 32G (4-port) Double density with converged Network Express adapter (2-port)

IBM z17 I/O - Next-gen I/O Infrastructure

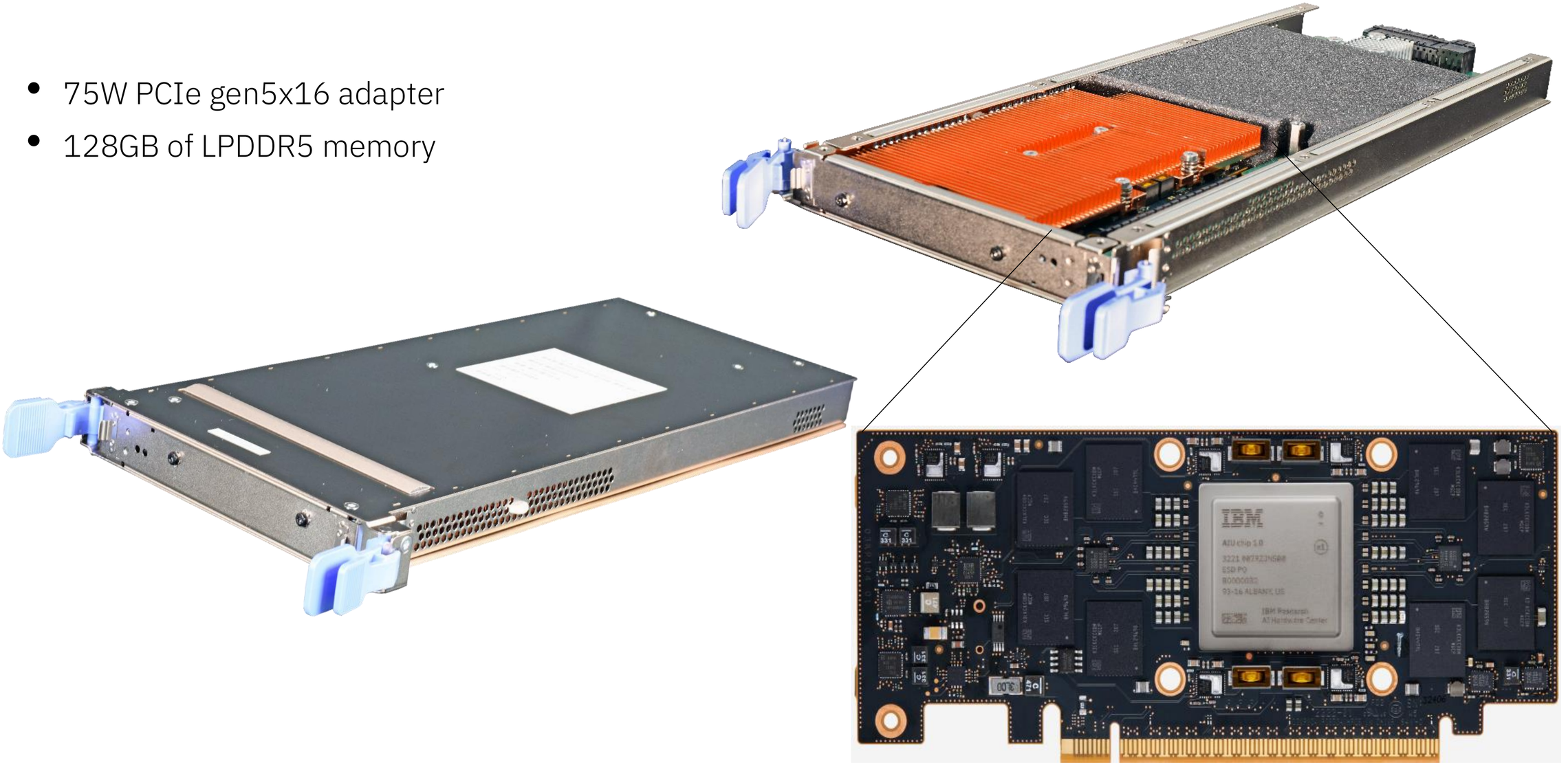


IBM z17 - New Build (NB) I/O Features

Description	Feature Code	Ports	Max Features	Comments- CHPID Types
• IBM Spyre AI Reserve Slot • Spyre AI Adapter	• 0061 • 0463	N/A	48	Sets of 8
FICON Express32-4P LX	0387	4	96	FC, FCP
FICON Express32-4P SX	0388	4	96	FC, FCP

IBM z17 Artificial Intelligence Accelerator (Spyre)

- 75W PCIe gen5x16 adapter
- 128GB of LPDDR5 memory



New FICON / FCP Express32-4P –(4 Ports)

– CHPID types supported: FICON (FC) and FCP

– Four PCHIDs/CHPIDs

– NO mixed CHPIDs for same card – only FC or FCP

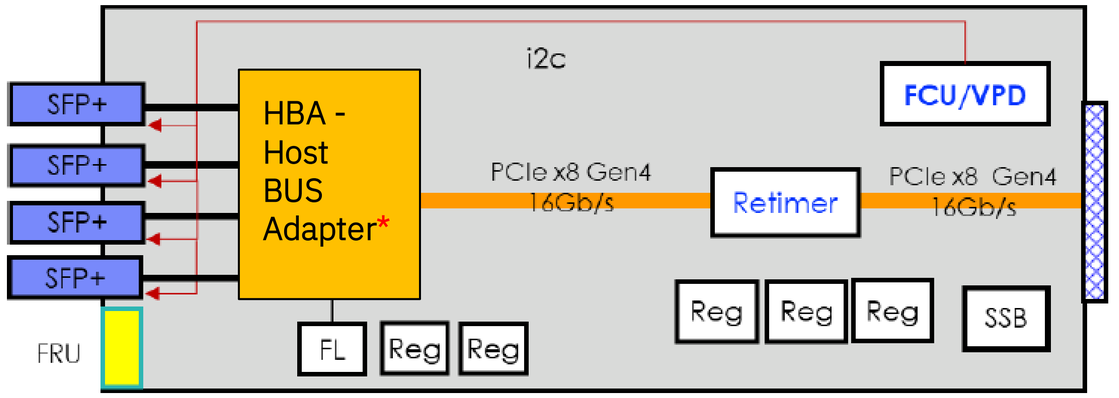
– Supports EDiF / FCES

– Auto-negotiates to 8, 16, or 32 Gbps
– Negotiation to 2 or 4 Gbps NOT supported (Switch needed)

– Max. 96 features per system- total: 384 CHNs

– 10KM LX - 9-micron single mode fiber
  • Unrepeated distance - 10 kilometers (6.2 miles)
  • Receiving device must also be LX

– SX - 50- or 62.5-micron multimode fiber
  • Distance variable with link data rate and fiber type
  • Receiving device must also be SX



* HBA is used to translate PCIe to FC protocol

IBM z17 - New Build (NB) I/O Features

Description	Feature Code	Ports	Max Features	Comments - CHPID Types (FID Types)
ICA SR2.0	0216	2	48	CS5
Coupling Express3 LR 10GB	0498	2	32	CL5
Coupling Express3 LR 25GB	0499	2	32	CL6
Network Express SR 10G	0524	2	48	OSH / NETH
Network Express LR 10G	0525	2	48	OSH / NETH
Network Express SR 25G	0526	2	48	OSH / NETH
Network Express LR 25G	0527	2	48	OSH / NETH

Network / OSA on IBM Z today

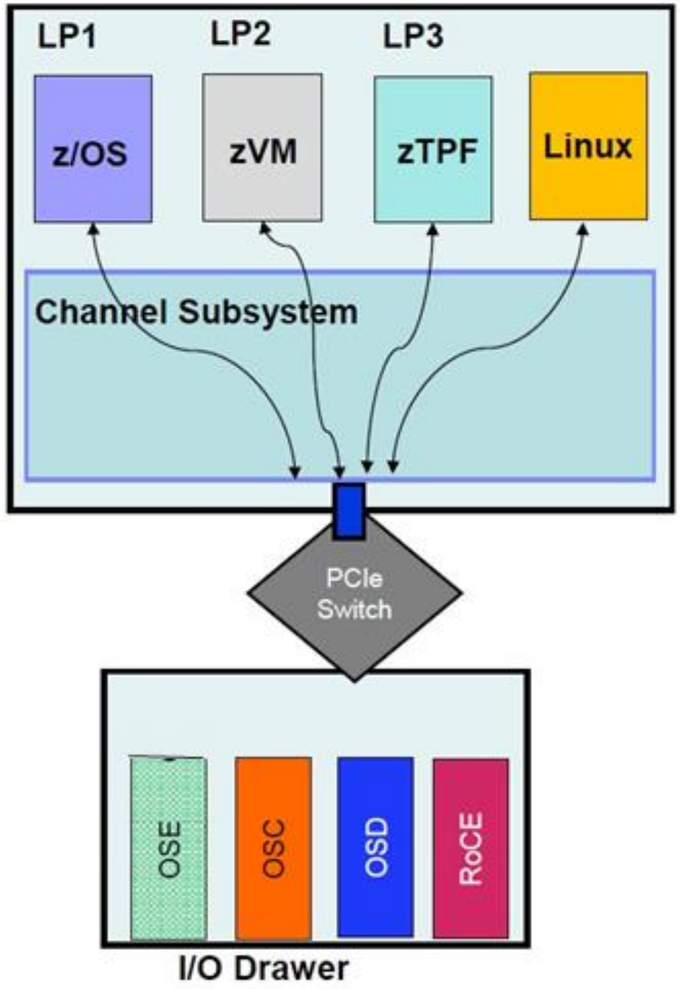
IBM Z currently has multiple unique functions that ultimately result in some protocol flowing over an Network link.
Each requires a unique channel type (with unique protocol driver) for a separate physical port:

- OSD – general TCP/IP, UDP, etc.
- OSC – Console controller functionality
- RoCE RDMA capability used in SMC-R protocol
- OSE [1] SNA (LSA) and TCP/IP (LCS)

1- IBM z17 does not support OSE

Considering redundancy requirements and bandwidth for each protocol shared across all LPARs, the current system Networking design can require many:

- I/O card slots
- Switch ports



Converged Multi-Function Network Adapter – Network Express

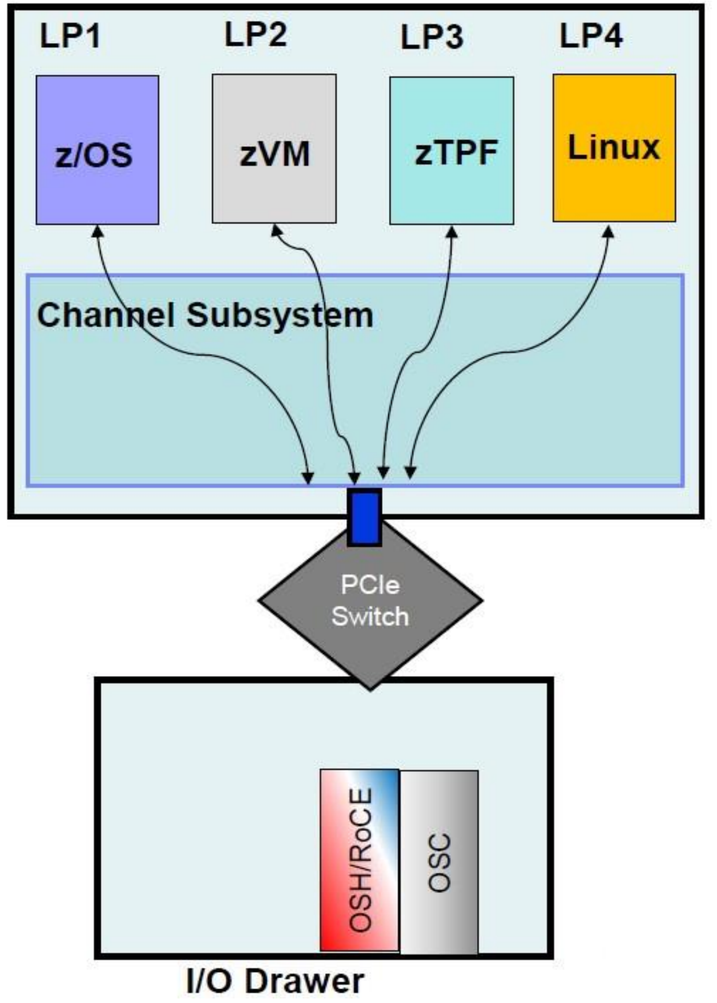
– A single port on the new adapter can simultaneously have two ‘personalities’:

- **OSH** using the new Enhanced QDIO protocol capability
- **NETH** for SMC-R RDMA or Linux native usage (TCP/IP, etc.)

– Each port can be configured to provide support for a single host protocol (EQDIO or native PCIe) or combination of host protocols

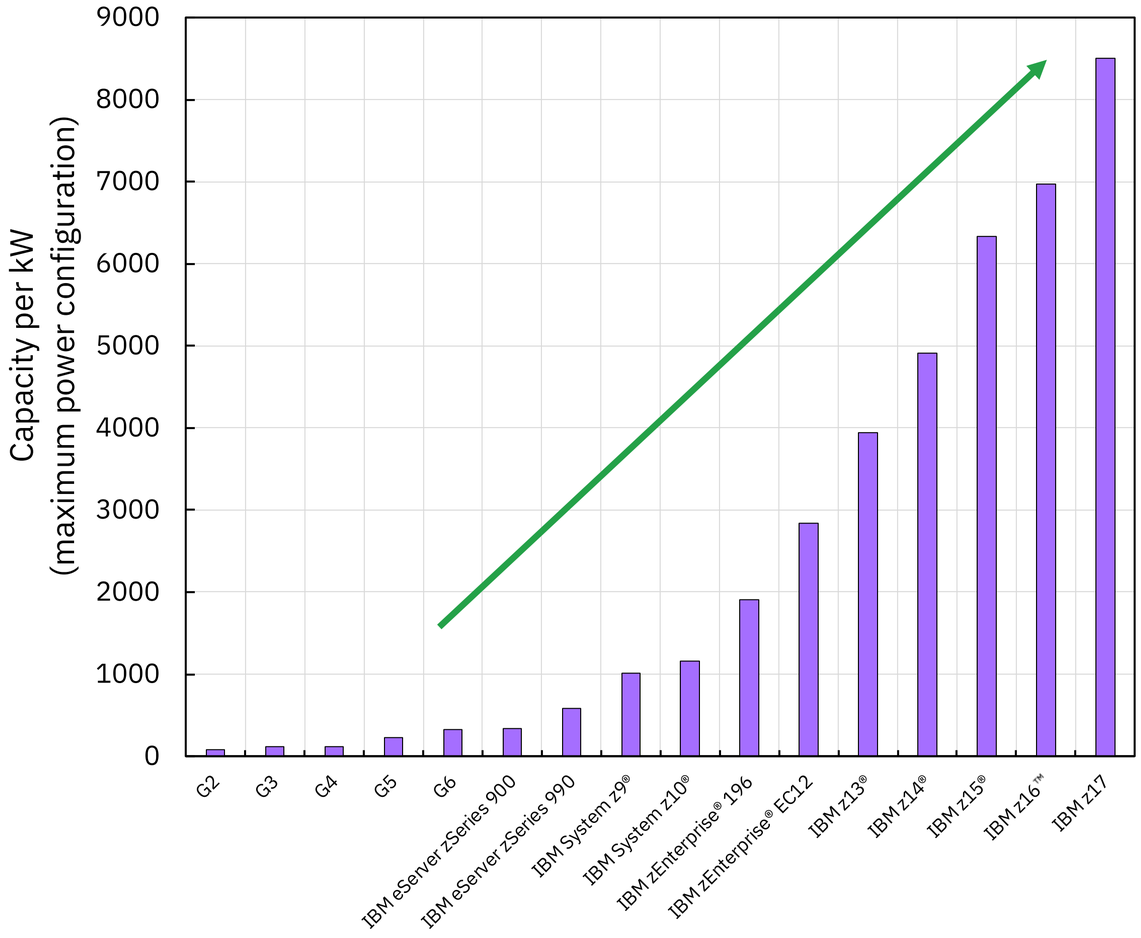
– Each entity can be independently manipulated (configured/deconfigured), affecting the underlying components of that entity (CHPIDs or FIDs)

Note: at GA1 CHPID type OSC requires an OSA Express7S 1.2 GbE SX/LX



IBM Z: continuous energy efficiency improvements & ESG focus

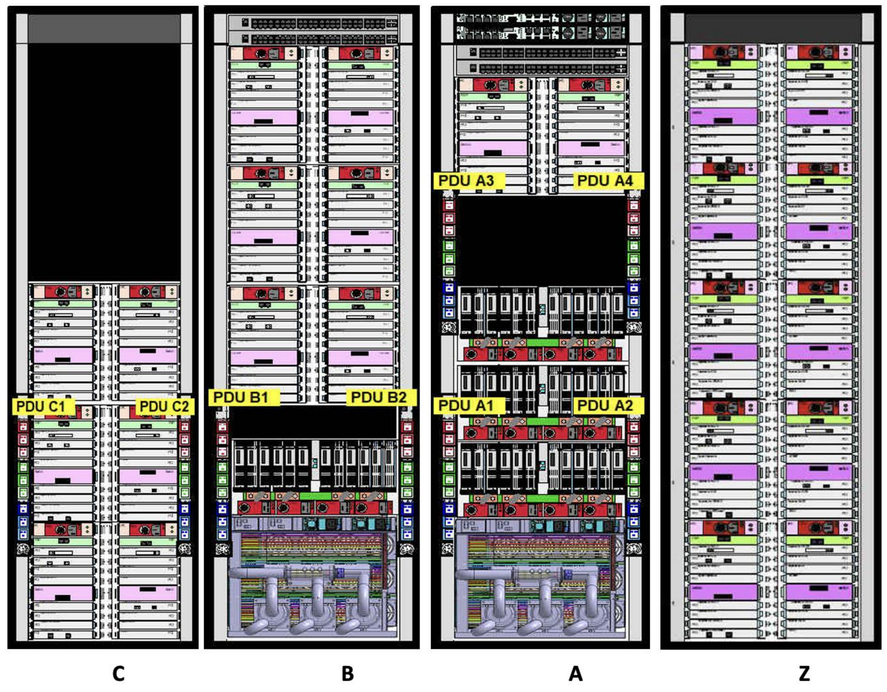
- 115X increased total capacity per kW over the last 15 generations
- IBM z17 reduces power consumption, weight, footprint compared to previous generations while increasing overall compute and capacity
- Lifecycle sustainability focus across every aspect including chip, prefilled coolant, packaging



Generation to generation power efficiency

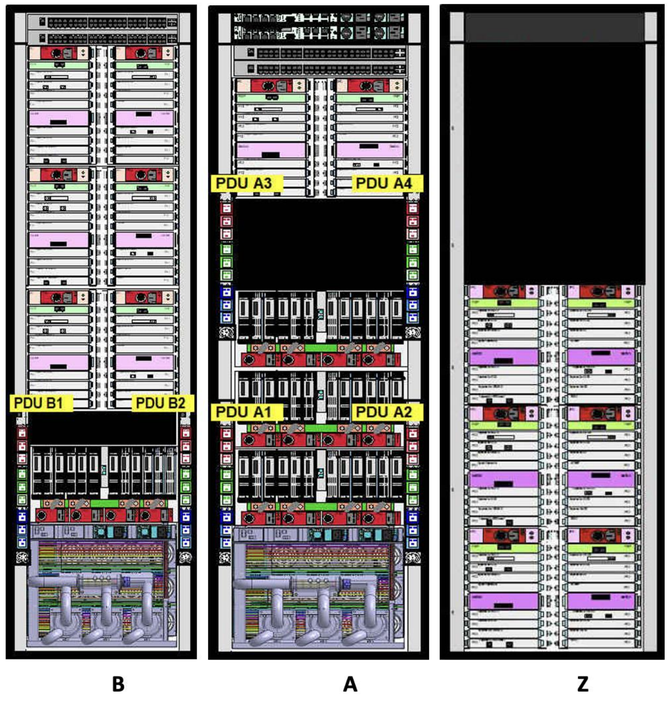
A large IBM z17 enables **more AI inferencing capability** with **lower power and a smaller data center footprint** than a similarly configured IBM z16.

IBM z16 Max200



Large z16 system
- 19,612 W
- 4 frames
- 8 power line cords

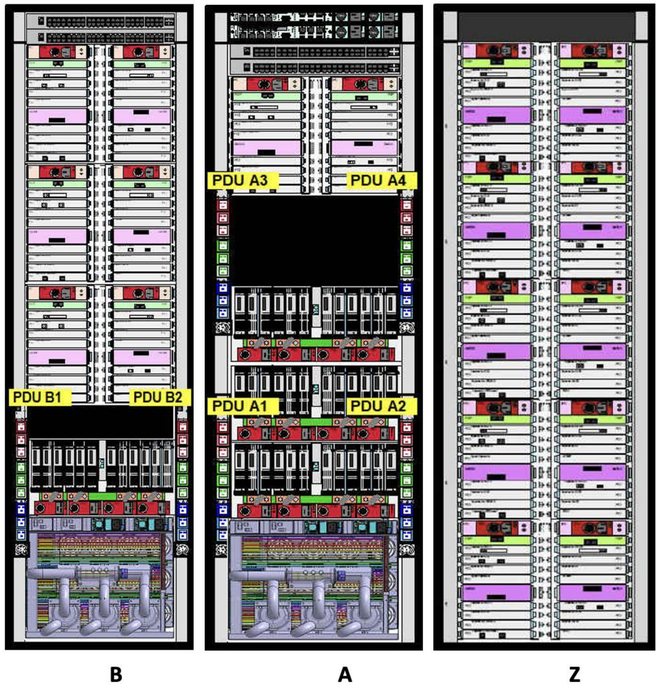
IBM z17 Max 208



Similar large z17 system
- 14,918 W (-24%)
- 3 frames
- 6 power line cords

Increased capabilities with **14% less power** and **25% smaller footprint than** similar z16

IBM z17 Max 208 + 40 Spyre

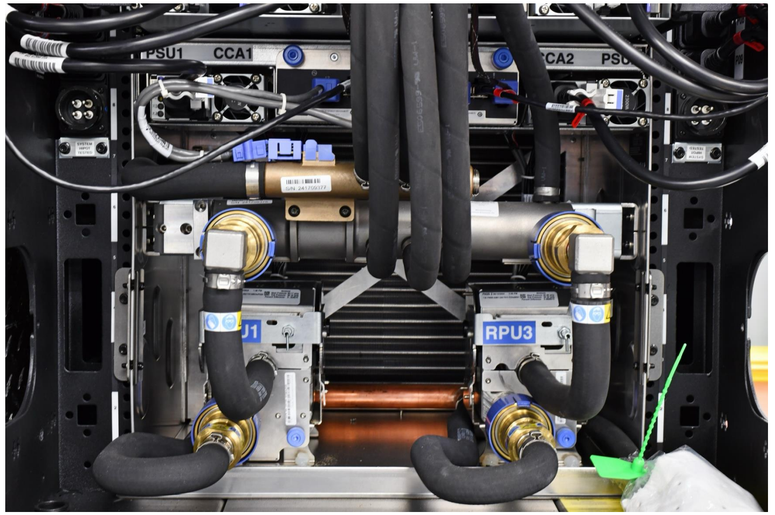


Similar large z17 system w/ 40 Spyre
- 18,450 W (-6%)
- 3 frames
- 6 power line cords

Significant AI inferencing capability with **3% less power** and **25% smaller footprint than** similar z16

Cooling

Cooling is similar to z16
– N+1 redundancy on fans (and their controls)
– N+1 redundancy on coolant pumps with N+2 cooling fan assembly
  • N+2 on coolant sensors



No fill and drain tool – (Not required with the Propylene Glycol Cooling)

IBM z17 Coupling Connectivity and Coexistence

IBM z17 ME1 (9175) ICA SR2.0 and CE3 LR

IBM z16 A01.A02 (3931 and 3932) ICA SR1.1 and CE2 LR

IBM z15 T01.T02 (8561 and 8562) ICA SR and CE LR

Coupling Express3 LR (CE3 LR)* 10G 10/100 km , 25G 10/100 km
IBM z17, IBM z16, IBM z15 to another IBM z17, IBM z16, IBM z15 Connectivity ONLY

IC (Internal Coupling Link)
Only supports IC-to-IC connectivity

IBM z15 Coupling Express LR and IBM z16 Coupling Express2 LR cannot be carried forward to IBM z17

Integrated Coupling Adapter (ICA SR, ICA SR1.1, ICA SR 2.0 – 8GBps up to 150 m
IBM z17, IBM z16, IBM z15 to another IBM z17, IBM z16, IBM z15 Connectivity ONLY

IBM z14, IBM z14 ZR1 and older systems
Not supported in the same Parallel Sysplex or STP CTN with IBM z17

Note: The link data rates do not represent the performance of the links. The actual performance is dependent upon including latency through the adapters, cable lengths, and the type of workload

Driver 61 / Version 2.17.0 (HMC/SE)

- HMC support to n-2 only
  - z14 no longer supported
  - same as SYSPLEX support

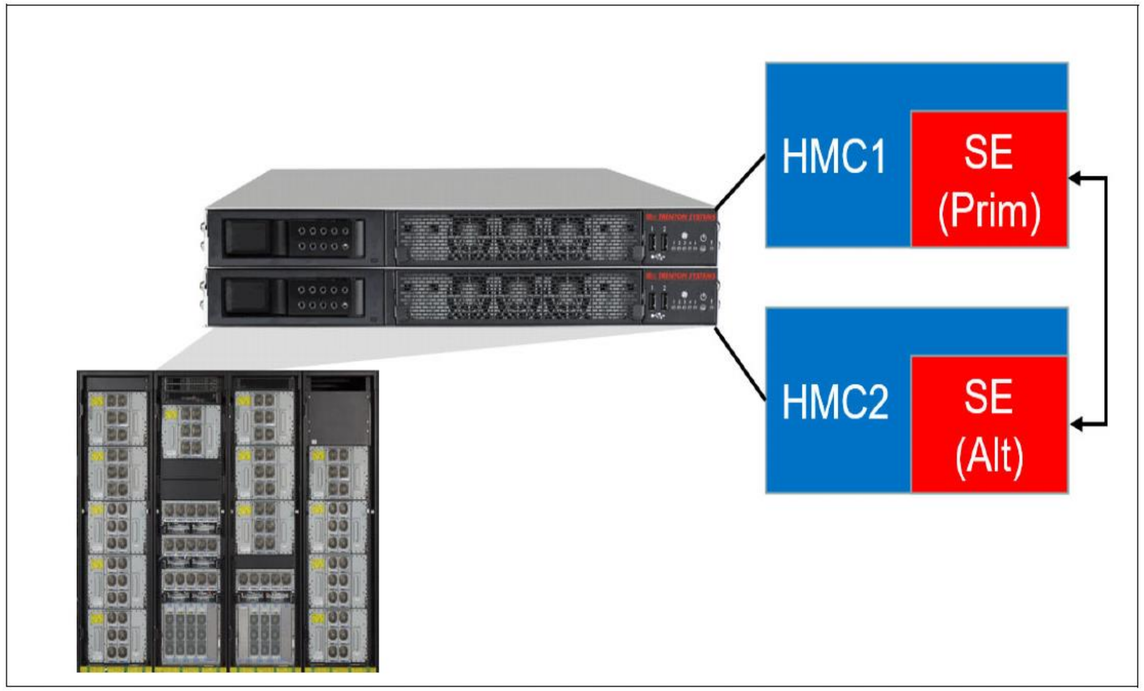
Machine Family	Machine Type	Firmware Driver	SE Version
IBM z17	9175	61	2.17.0
IBM z16	3931, 3932	51	2.16.0
IBM z15	8561, 8562	41	2.15.0

- Note:
  - HMC Driver 61 / Ver. 2.17.0 can be loaded on
    - z17 HMA (Hardware Management Appliance – 2 HMC / 2 SE)
    - IBM z16 HMA
    - IBM z15 HMA

  - Standalone HMC (Tower & Rack: no longer supported)

IMPORTANT
- Minimum 1 HMA per Data Center
- Maximum 2 HMAs per Data Center
- IBM z17 with SE only is available

What is an HMA?

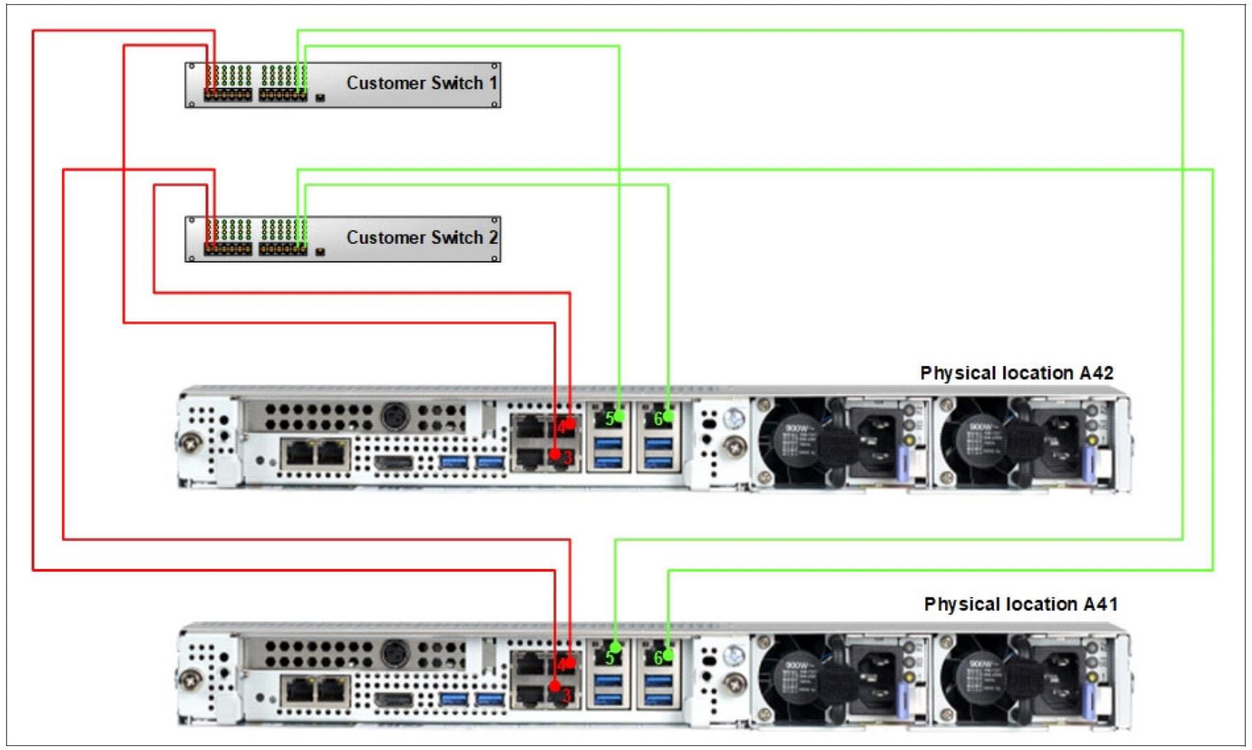


Hardware Management Appliance

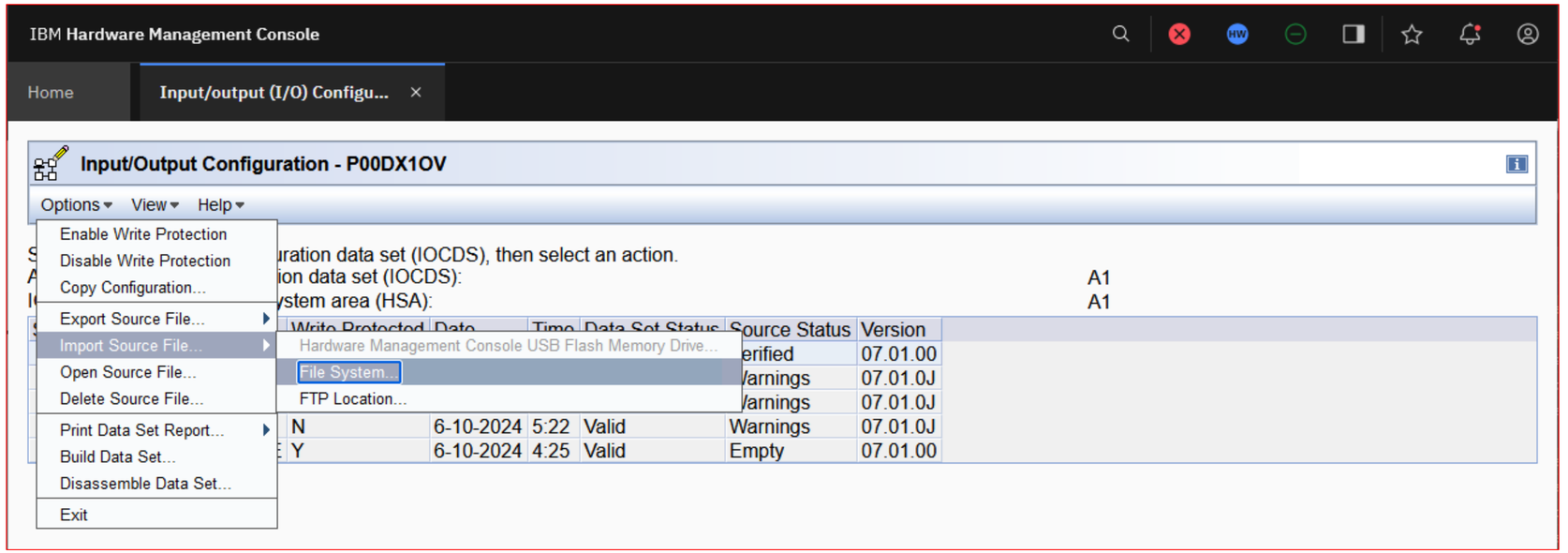
HMA is an Appliance feature consist of:

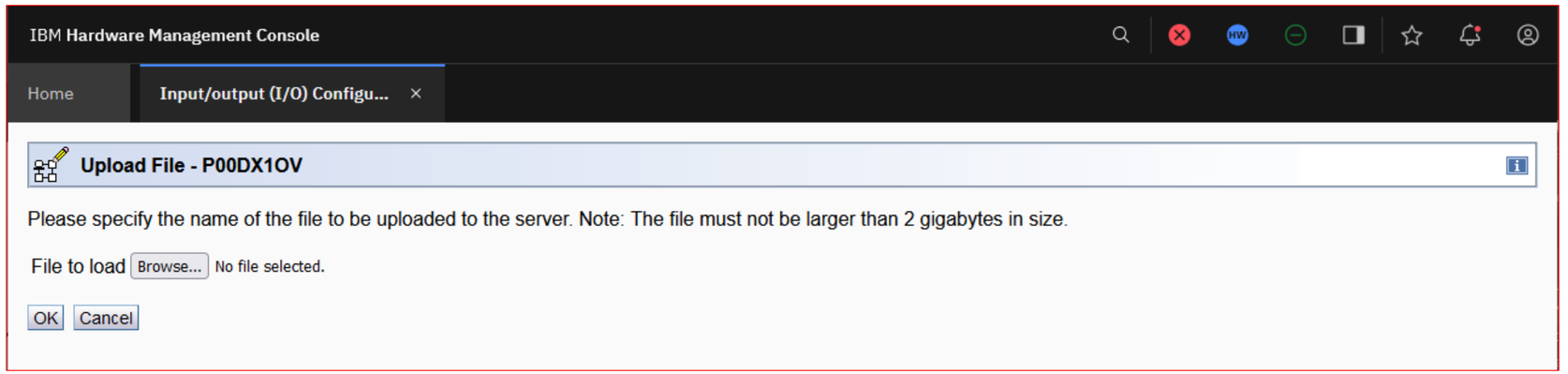
- Two HMCs
- Two SEs

- Each HMC and SE has own 2 physical Network Ports which has to be connected to a customer provided Switch
- The SE runs virtual on the HMC -> if HMC must be restarted also the SE will be restarted.



Import/Export Remote File System





Provide option to import/export files directly from/to client workstation remotely connecting to the HMC Addresses

- USB access to HMA HMC in the Data Center
- Complexity of SFTP/FTPS
- Secure connection

Import/Export Remote File System

Import/Export from Remote Browsing File System

As with Driver 61/Version 2.17.0, only HMAs are supported; most clients will use the HMC via remote connections. For the tasks listed below, Import/Export from Remote Browsing File System is supported:

- Fibre Channel Endpoint Security
- Secure Boot Certificate Management
- Certificate Management
- System Input/Output Configuration Analyzer
- Analyze Console Internal Code
- Change Console Internal Code
- FCP Configuration
- Audit log Scheduled Operations
- Export/Import IOCDS
- Save/Restore Customizable Console Data
- Crypto Configuration
- View/Archive Security Logs
- Advanced Facilities
- OSA Advanced Facilities
- Crypto UDX configuration
- Transmit Service Data
- Transmit VPD
- Import Secure Execution Keys
- Export/Import Profiles
- Reassign HMC
- Manage Firmware Features
- System I/O Configuration Analyzer
- Perform Model Conversion

Security Enhancements: Dual Control

Dual Control Value Proposition

Dual control adds an extra layer of security for critical tasks on the HMC.

Dual control enabled tasks require another level of verification from an approver before they can be run.

Requirements/Value

- Industry or Company Security Standard

- User action error protection
  - Unintended activation of a wrong active LPAR

- Fraud Protection (most likely insider)
  - Misuse of Crypto
  - Security Attack (take down one or more LPARs)

- Financial Protection or Workload Performance Degradation
  - Capacity on Demand (eg. On/Off Capacity on Demand)
  - User mistake or Fraud protection

Dual Control Design Highlights

Dual Control definitions in User Management roles

- Optionally assigned to users

Dual Control available to z17, z16, z15 using HMC 2.17.0

Dual Control Target per User Role

- Object and
- Task

Dual Control Approver per User Role

- Any User Role for task/object authorization control
- Can also create special User Role with list of specific users for DC approval

Dual Control Management Execution Requests for Approval

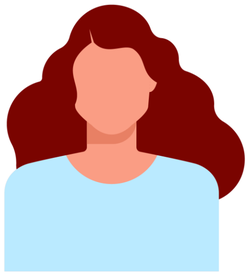
- Run by requester restricted to time window in the future
- Run by requester
  - No time window restriction
- Run immediately
  - Automatically without requester further involvement
- Run on a specific date and time

Dual Control CPCs supported (Requires z17 HMC 2.17.0)

- z17 CPC (no restrictions)
- z16 & z15 CPCs
  - Should remove Single Object Operations in any role applied to a User under Dual Control
  - *Perform Model Conversion (Capacity on Demand)* & *Change LPAR Cryptographic Controls* tasks not available for HMC 2.17.0 z16 & z15 targets

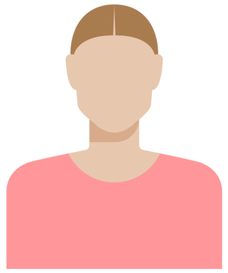
Dual Control external interfaces (UIs, WS APIs, BCPii v2, IBM HMC Mobile)

Primary user personas



Noëmi
Junior system administrator

Daniel
Experienced system administrator



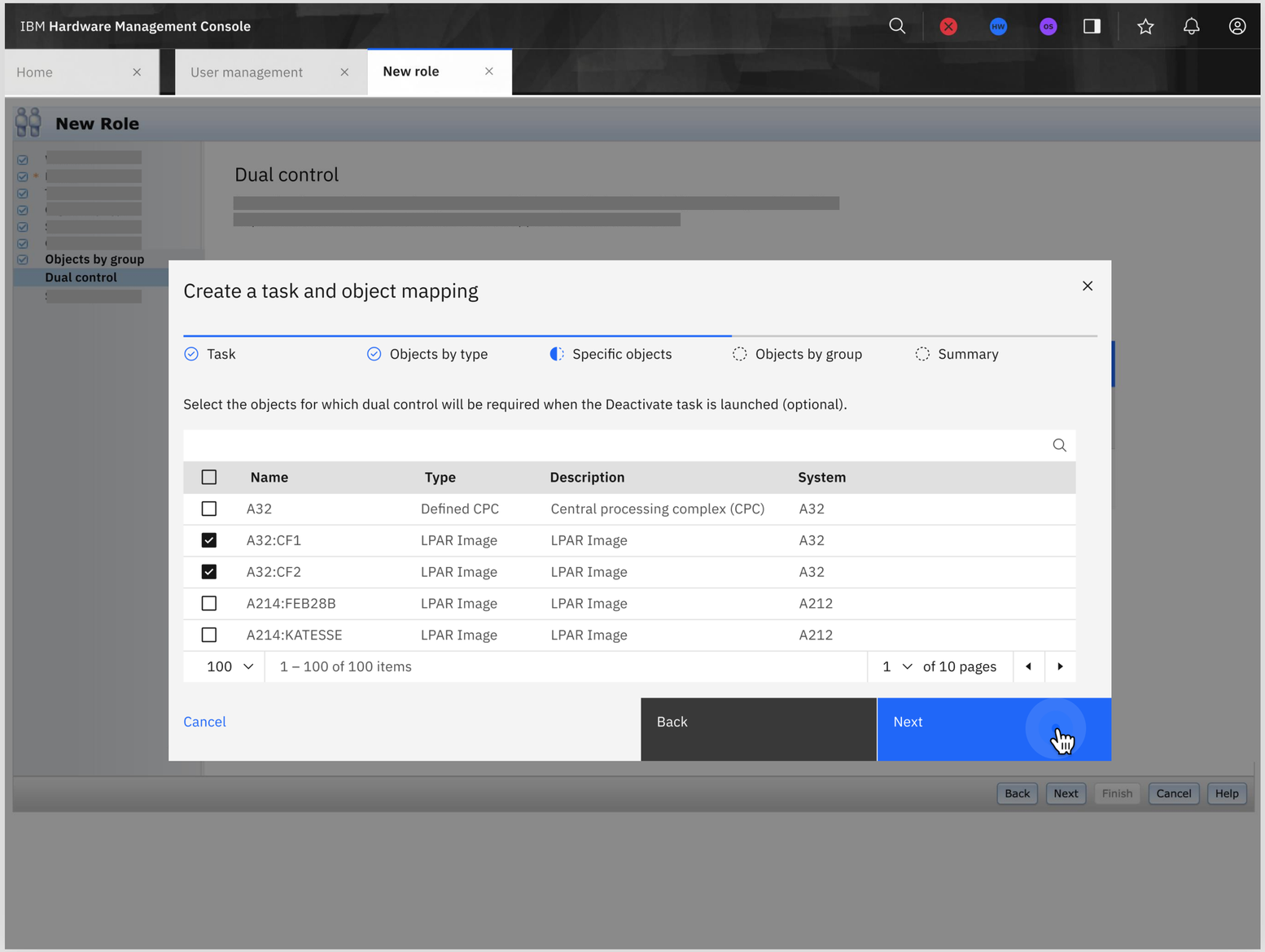
Marco
Security administrator

Hardware management

Security

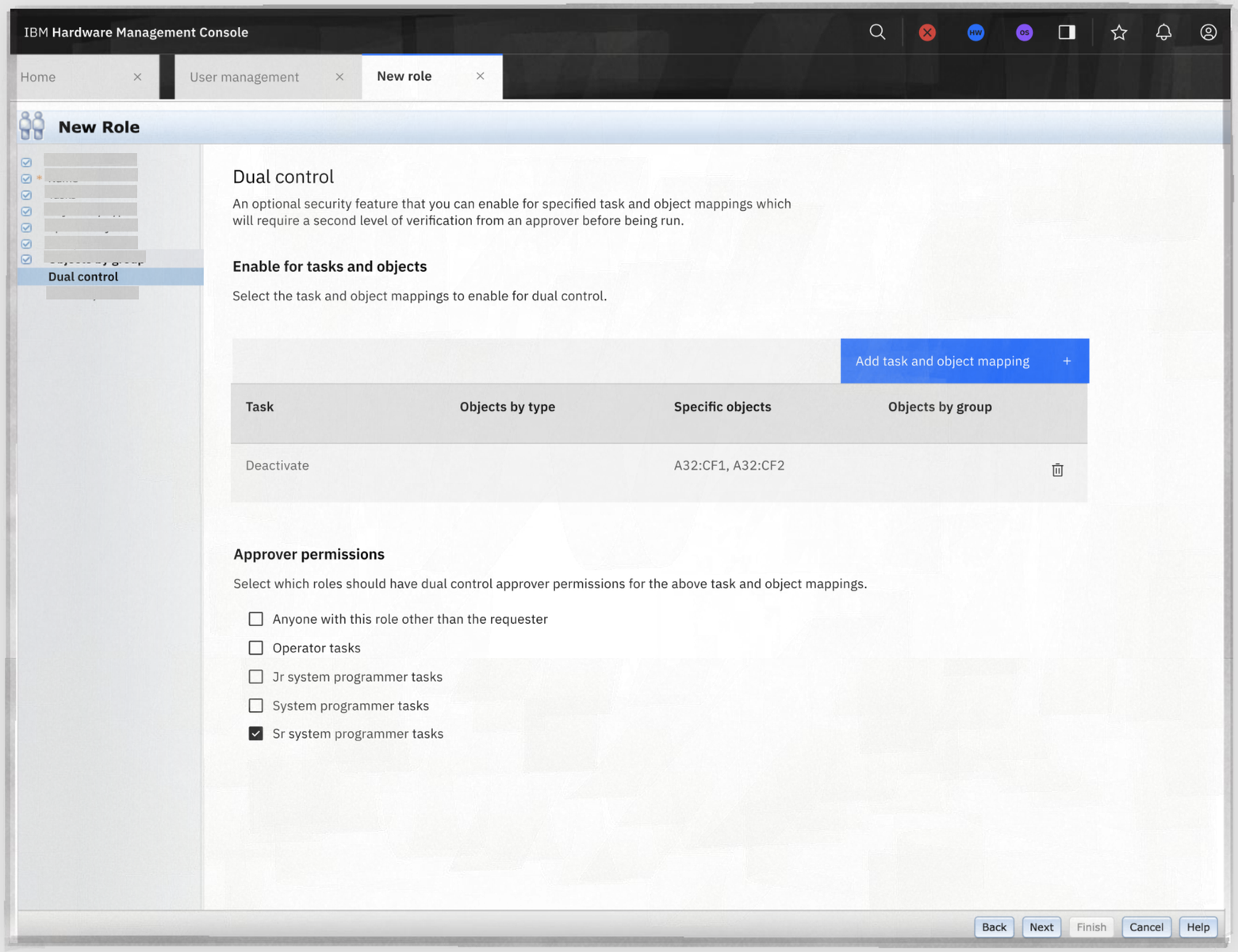
Dual control set-up for the deactivate task

Marco selects the objects that should be enabled for dual control with the deactivate task

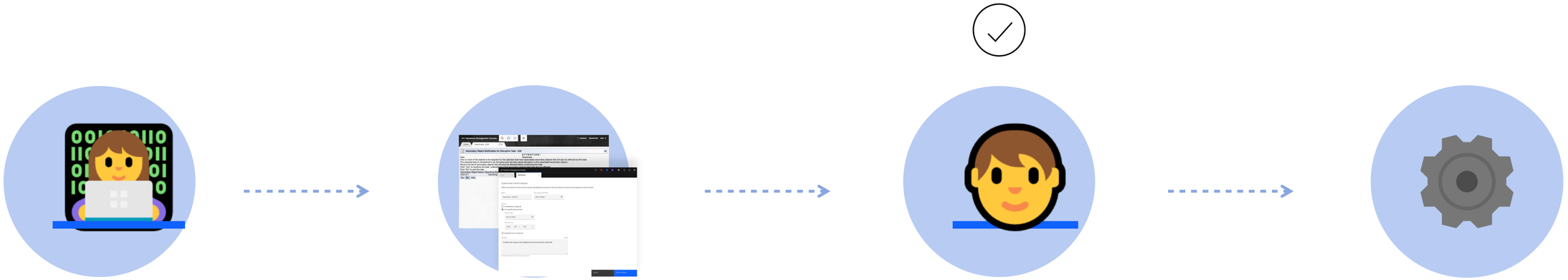


Defining approver permissions

Once all the tasks and object mappings are defined, Marco selects the roles of the users that should have approver permissions for the designated task and object mappings.



Dual Control
Task use touch points



Noëmi

Selections made in task and approval request submitted

Daniel

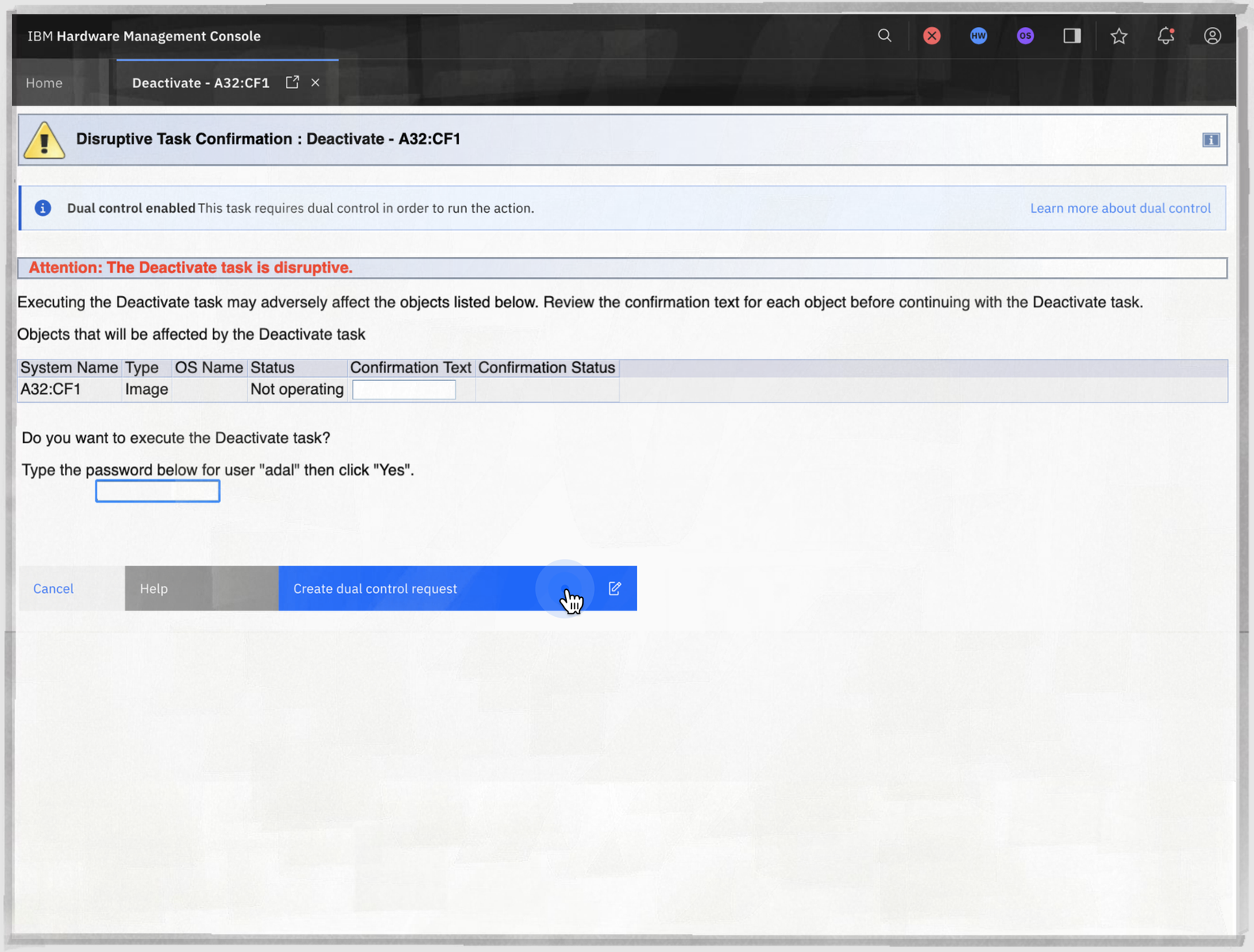
Approval/Rejection

Task is run

In task

Noëmi sees that this is a *dual control enabled task and object mapping*

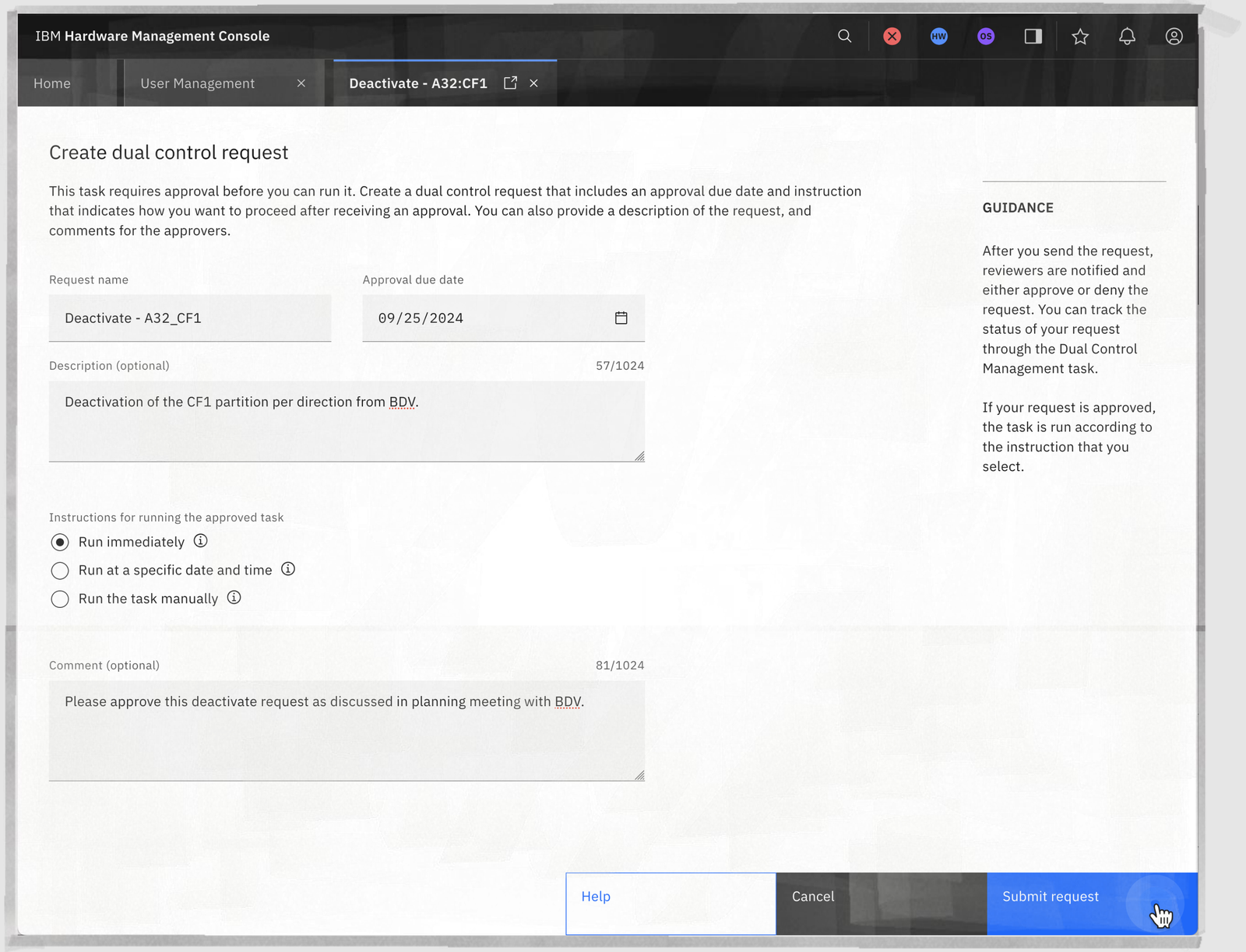
Once she has made her selections and is done within task, she *creates a dual control request*



Submitting a dual control request

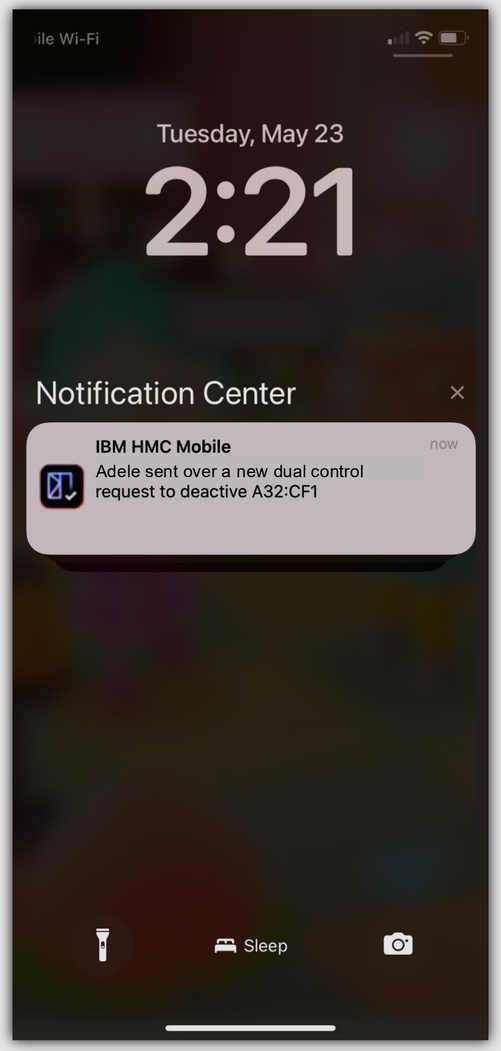
Noëmi selects an *approval due date*, and that the Deactivate should run immediately after it's approved.

She submits the request

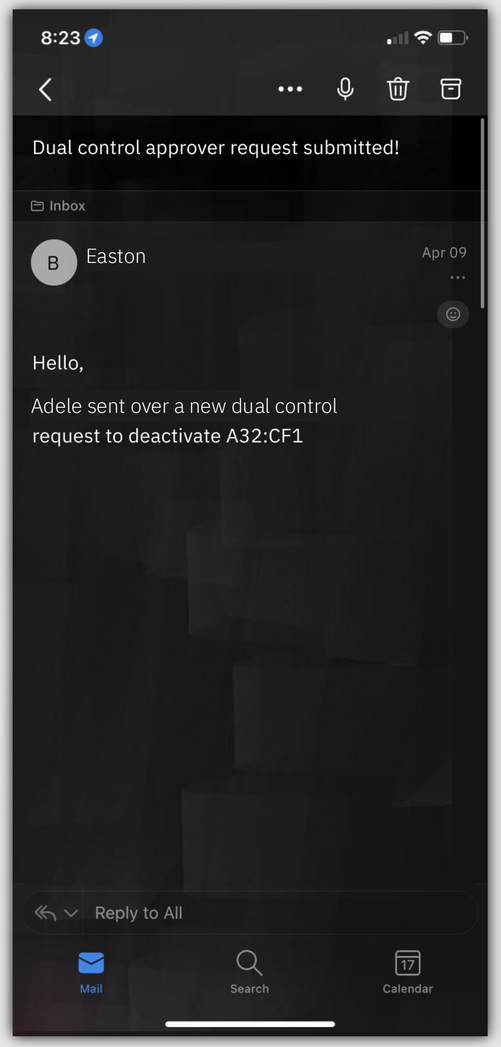


Approver notified of dual control request

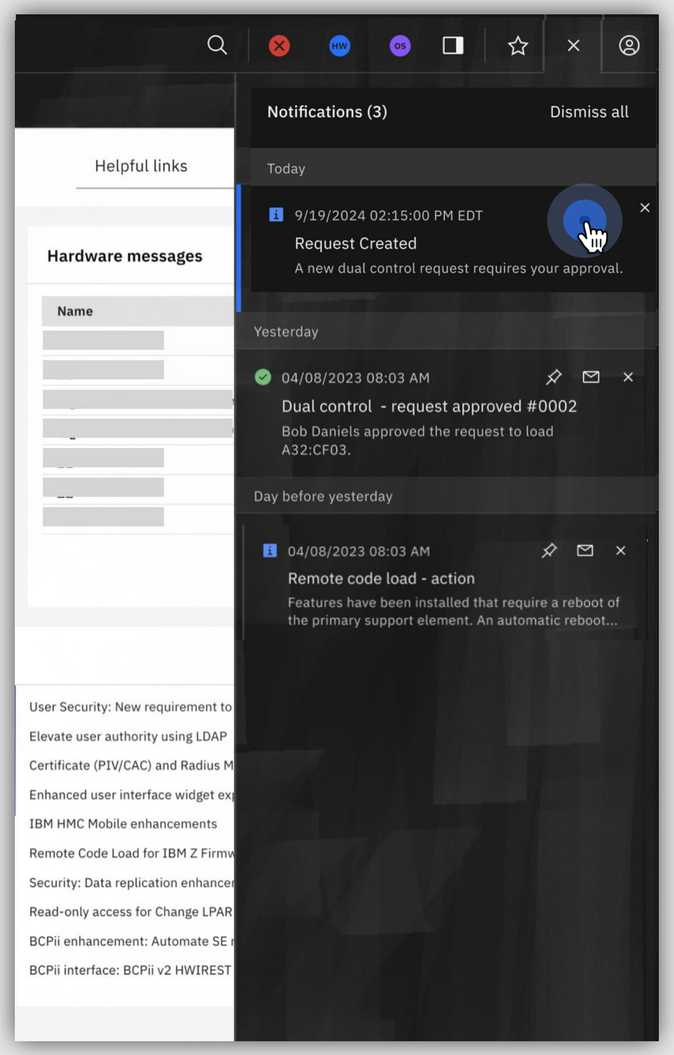
Daniel, a dual control approver, is notified of the request via mobile, email, APIs, BCPii, and the notification panel in the HMC



HMC Mobile



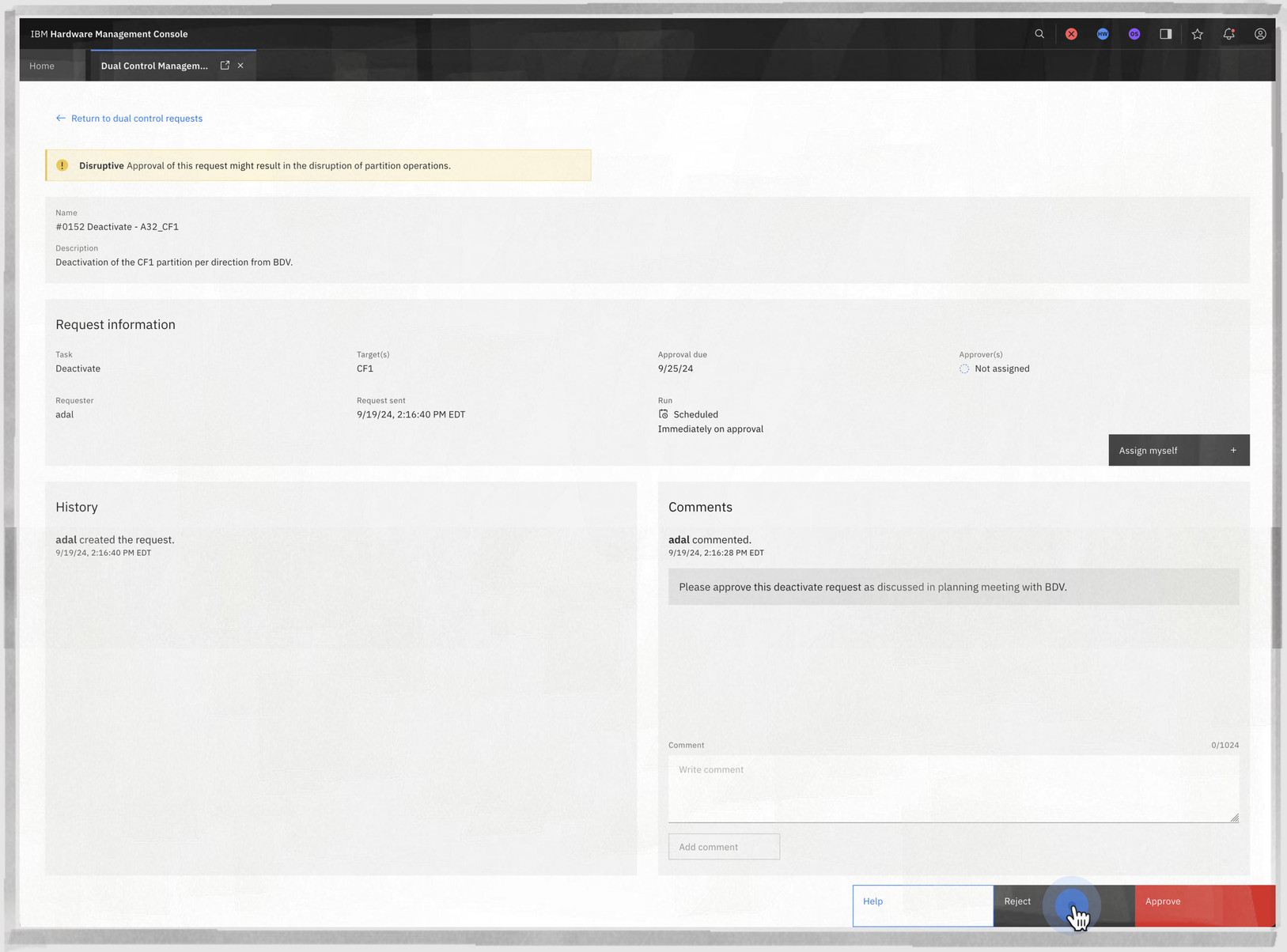
Email



Notification/Alert panel

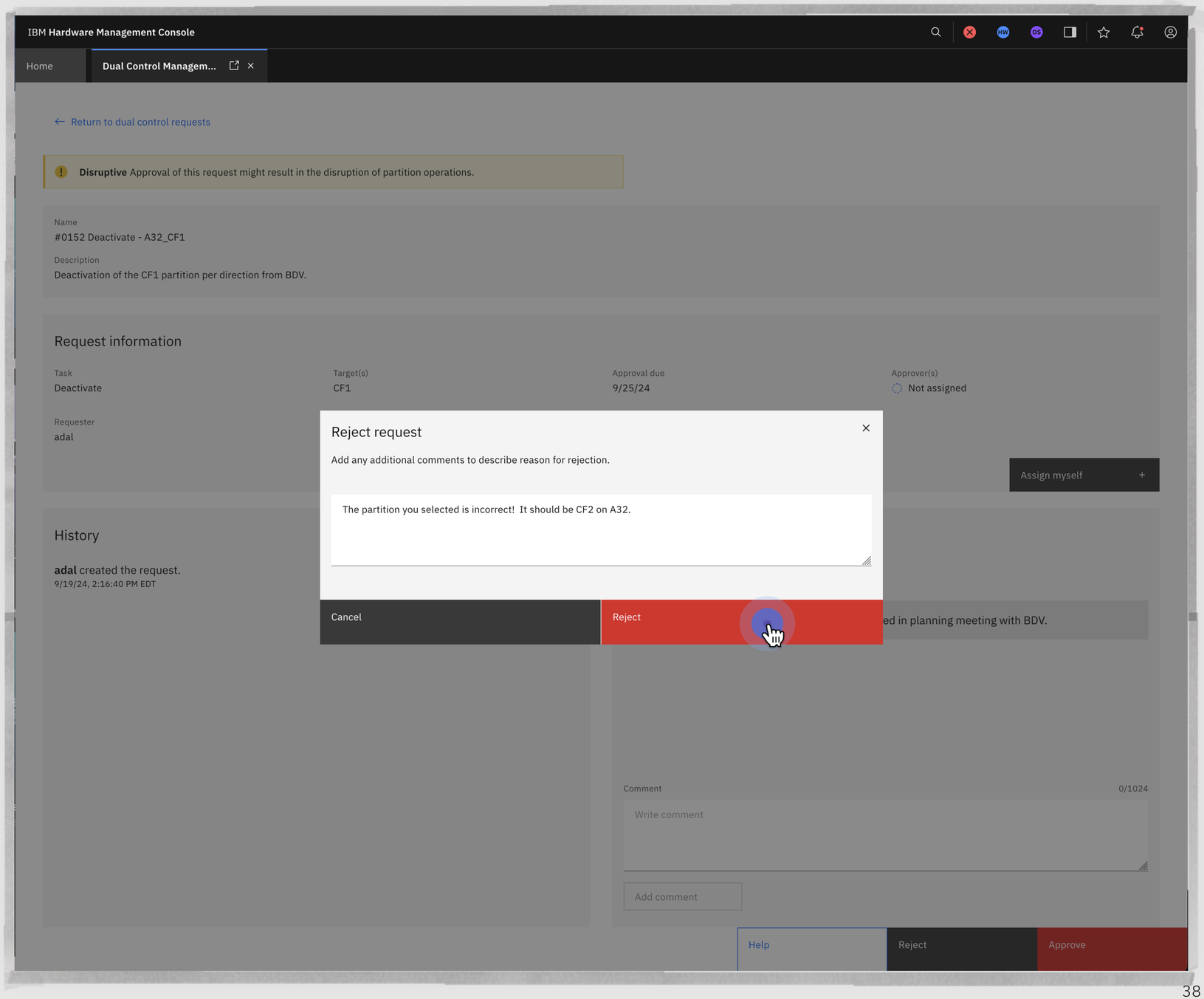
Approver reviews the request

Daniel reviews the request and sees that Noëmi selected the wrong partition to deactivate. He clicks reject.

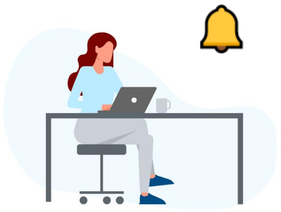


Approver rejects the request

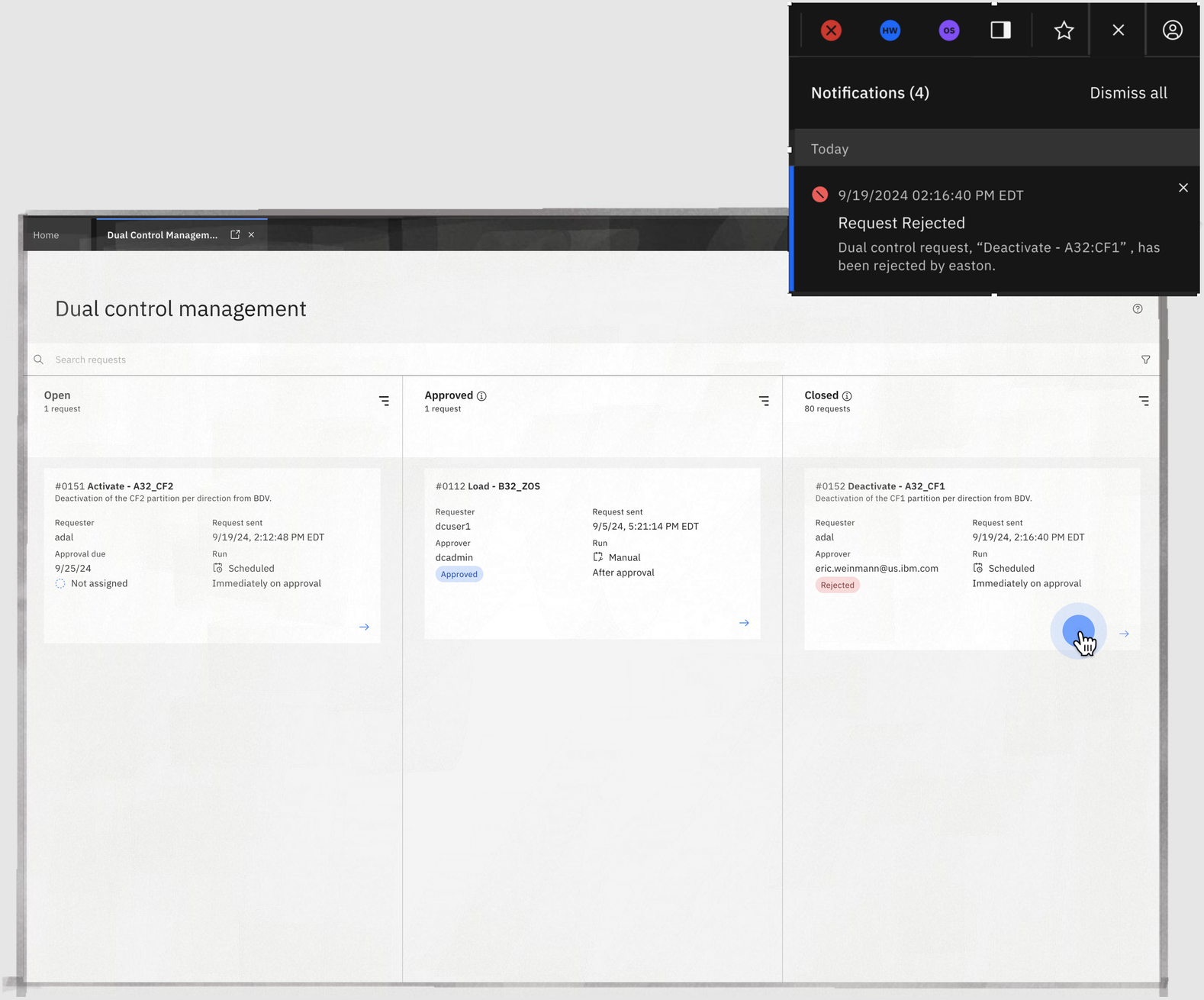
Daniel writes a comment to explain why it was rejected



Notified of rejection, launches the dual control management task

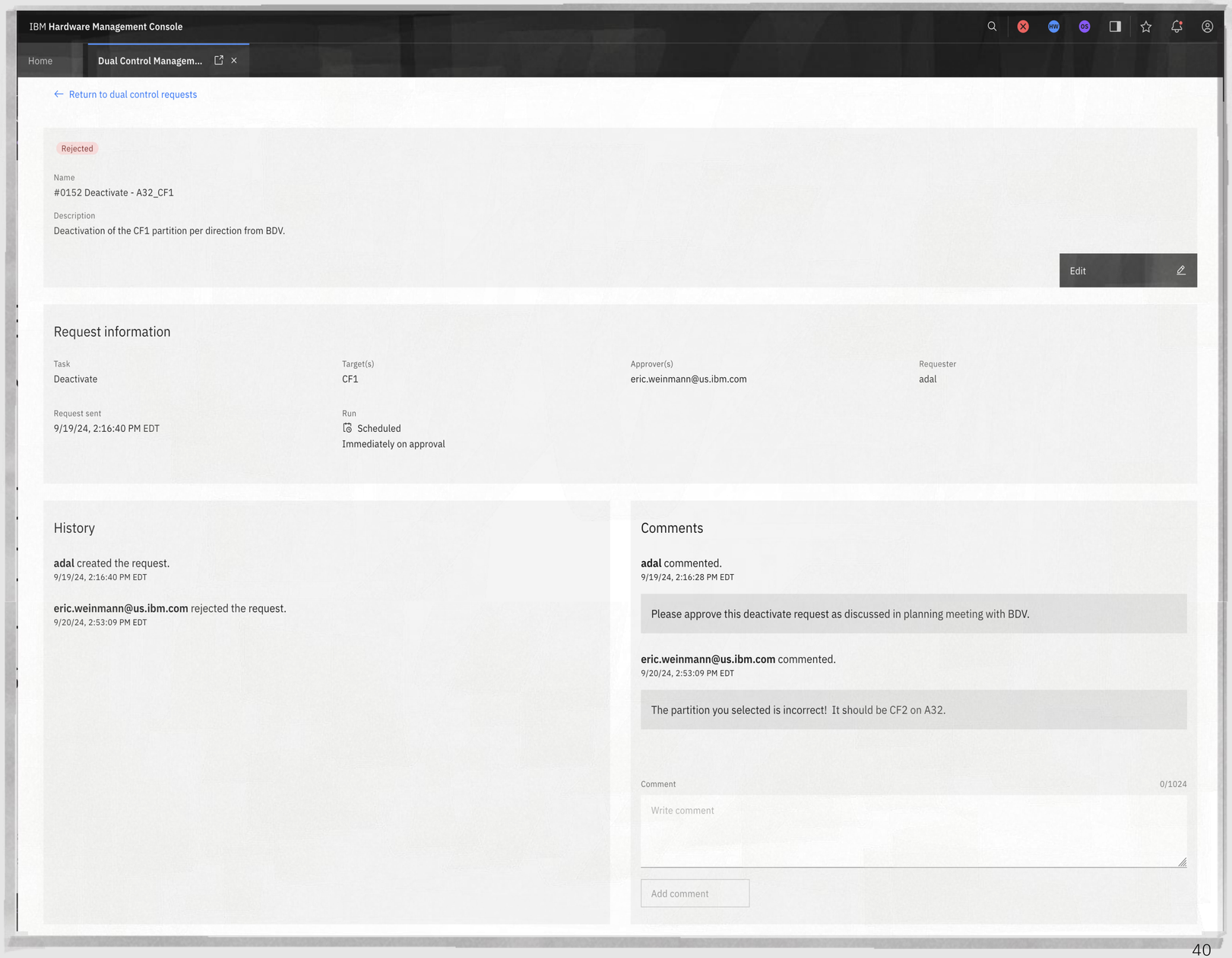


Noëmi
is notified that her request has been rejected so she launches the dual control management task and clicks into request card to view details



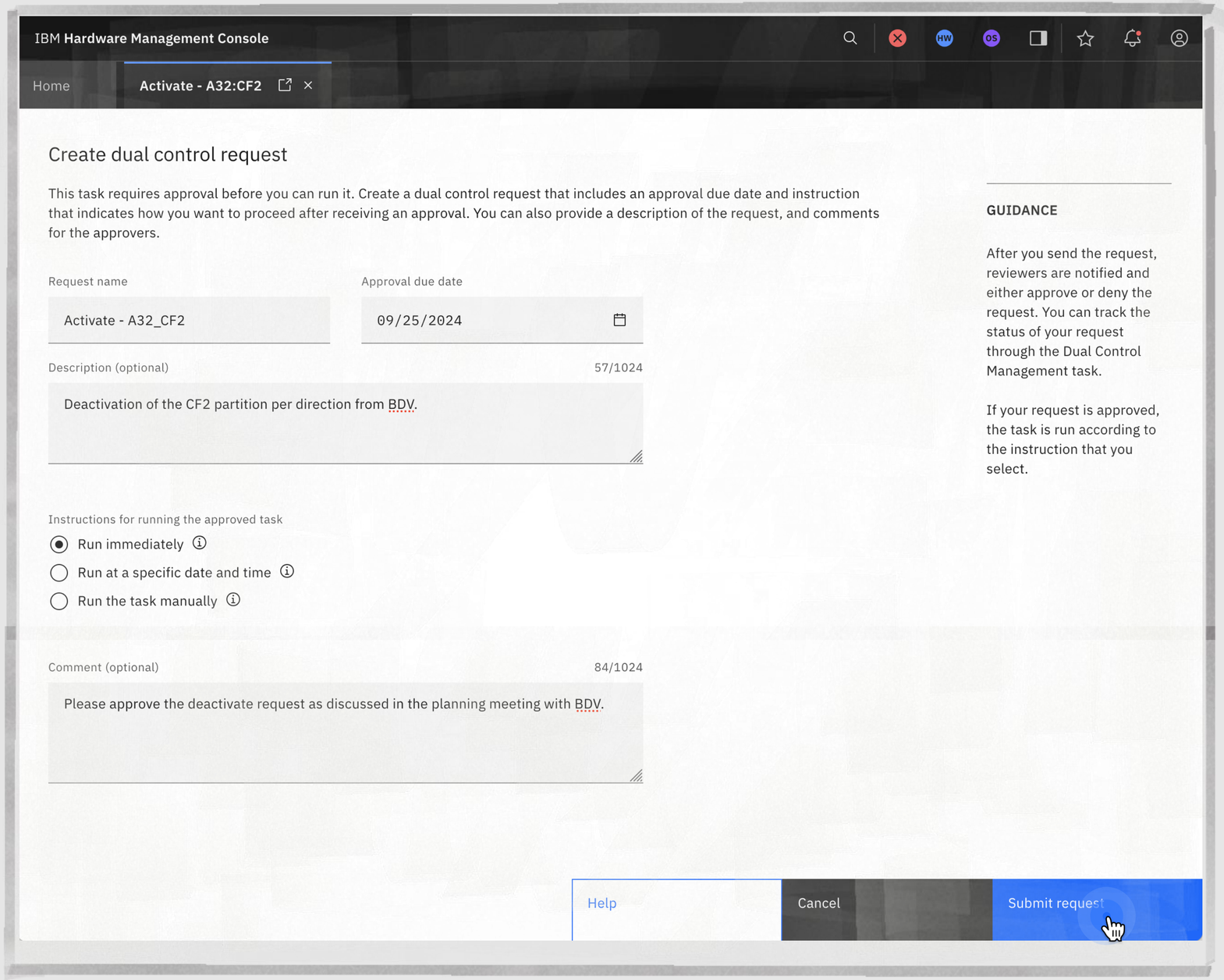
Realizing mistake

Noëmi
reads Daniels's comment about selecting the wrong partition.
She proceeds to submit a new request

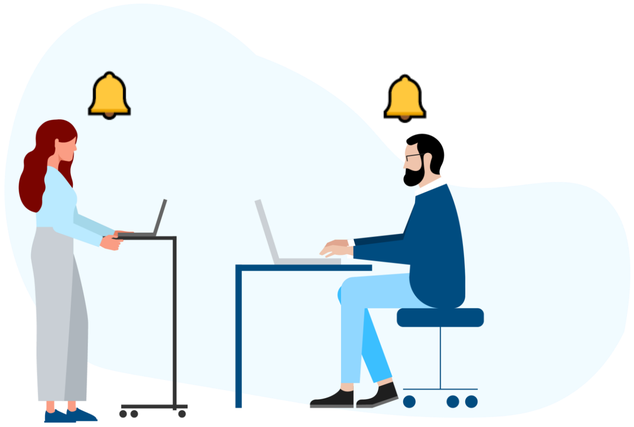


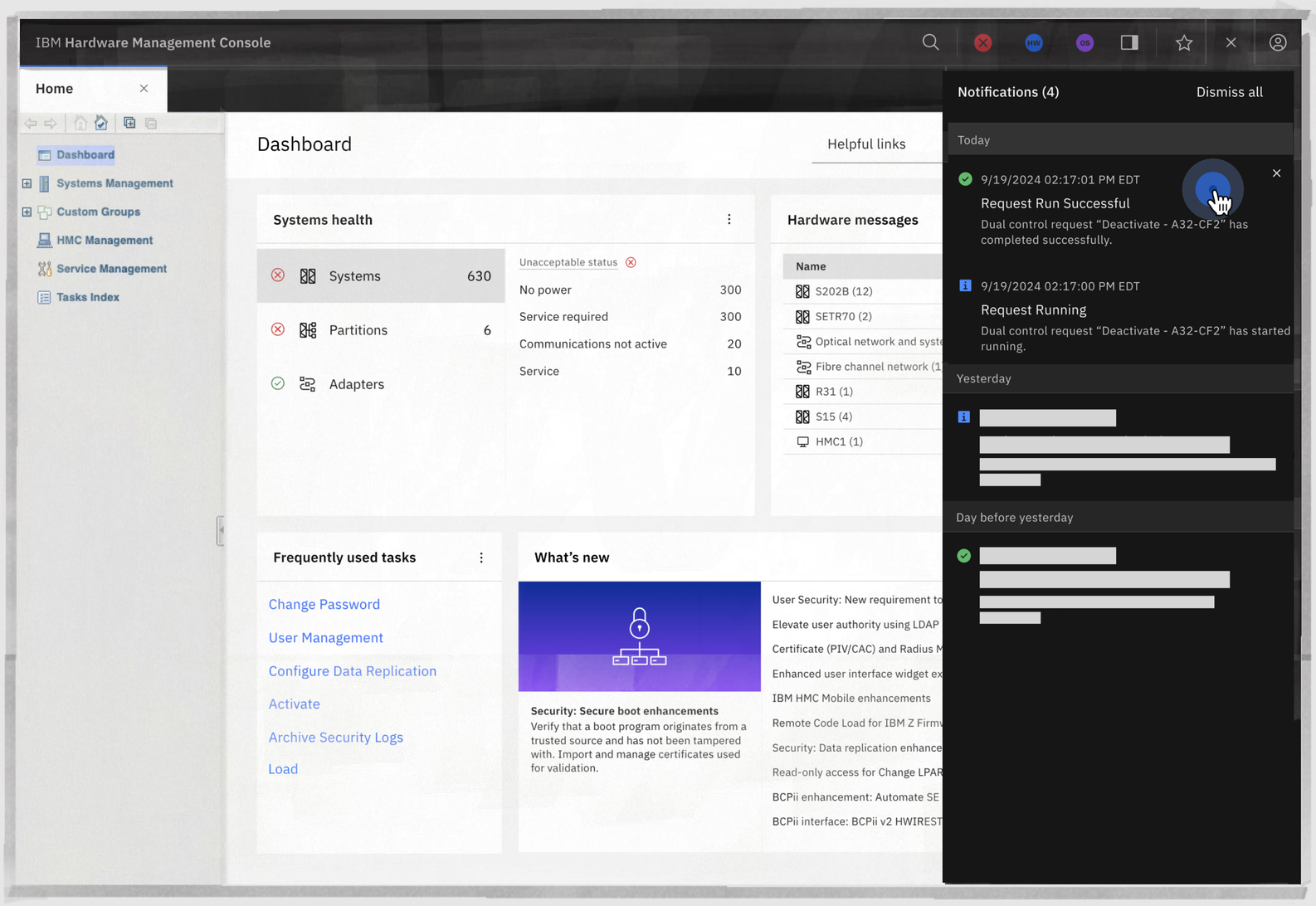
Submitting new request

Noëmi
makes her selections once again and ensures she has selected the correct partition to deactivate. She then submits the new request



Deactivate is run and both Noëmi and Daniel are notified





Noemi and Daniel are review the results

← Return to dual control requests

Successful

Name
#0160 Deactivate - A32 CF2

Description
Deactivation of the CF2 partition per direction from BDV.

Edit

Request information

Task
Deactivate

Target(s)
CF2

Approver(s)
eric.weinmann@us.ibm.com

Requester
adal

Request sent
9/23/24, 2:12:08 PM EDT

Run
Successful
9/12/24, 5:01:09 PM EDT

History

adal created the request.
9/23/24, 2:12:08 PM EDT

eric.weinmann@us.ibm.com approved the request.
9/23/24, 2:14:44 PM EDT

Deactivate has started.
9/23/24, 2:14:44 PM EDT

Deactivate has completed.
A32:CF2 is in a deactivated state.
9/23/24, 2:14:45 PM EDT

Comments

adal commented.
9/23/24, 2:12:08 PM EDT

Please approve the deactivate request as discussed in the planning meeting with BDV.

adal commented.
9/23/24, 2:13:37 PM EDT

Created a new request with the updated and correct partition CF2 selected!

Comment 0/1024

Dual Control Summary

01

Role-based task and object enablement

Security Administrators can enforce controls on which tasks & objects & users require Dual Control, and which users are granted permission to approve a Dual Control request.

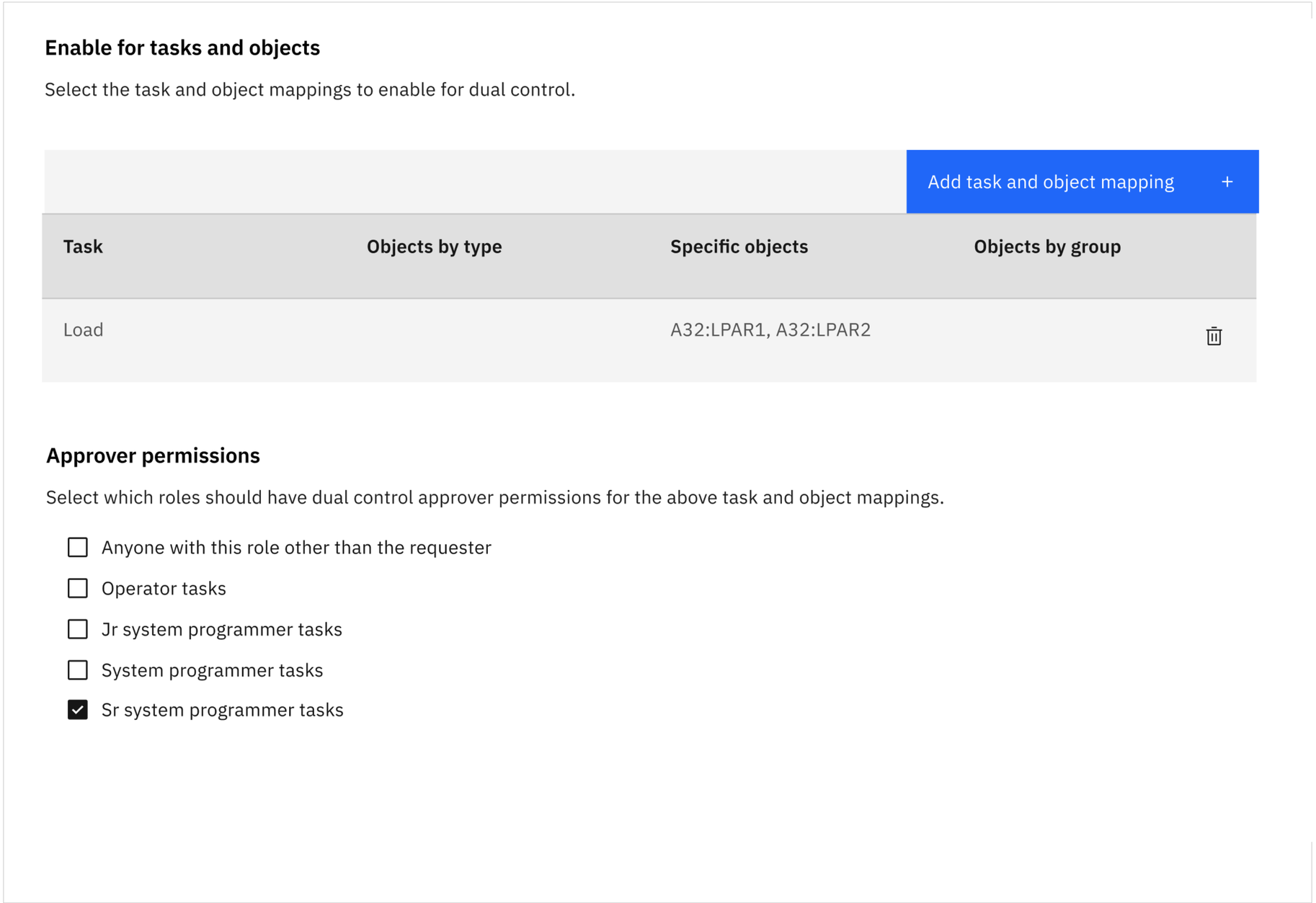


Image: Task and object mappings selection, approver permissions

Dual Control Summary

02

Flexible request options

Users can submit Dual Control requests for supported tasks with different run options:

- Run immediately
- Run at specific date and time
- Run manually by requester
- Run manually by requestor restricted to a time window

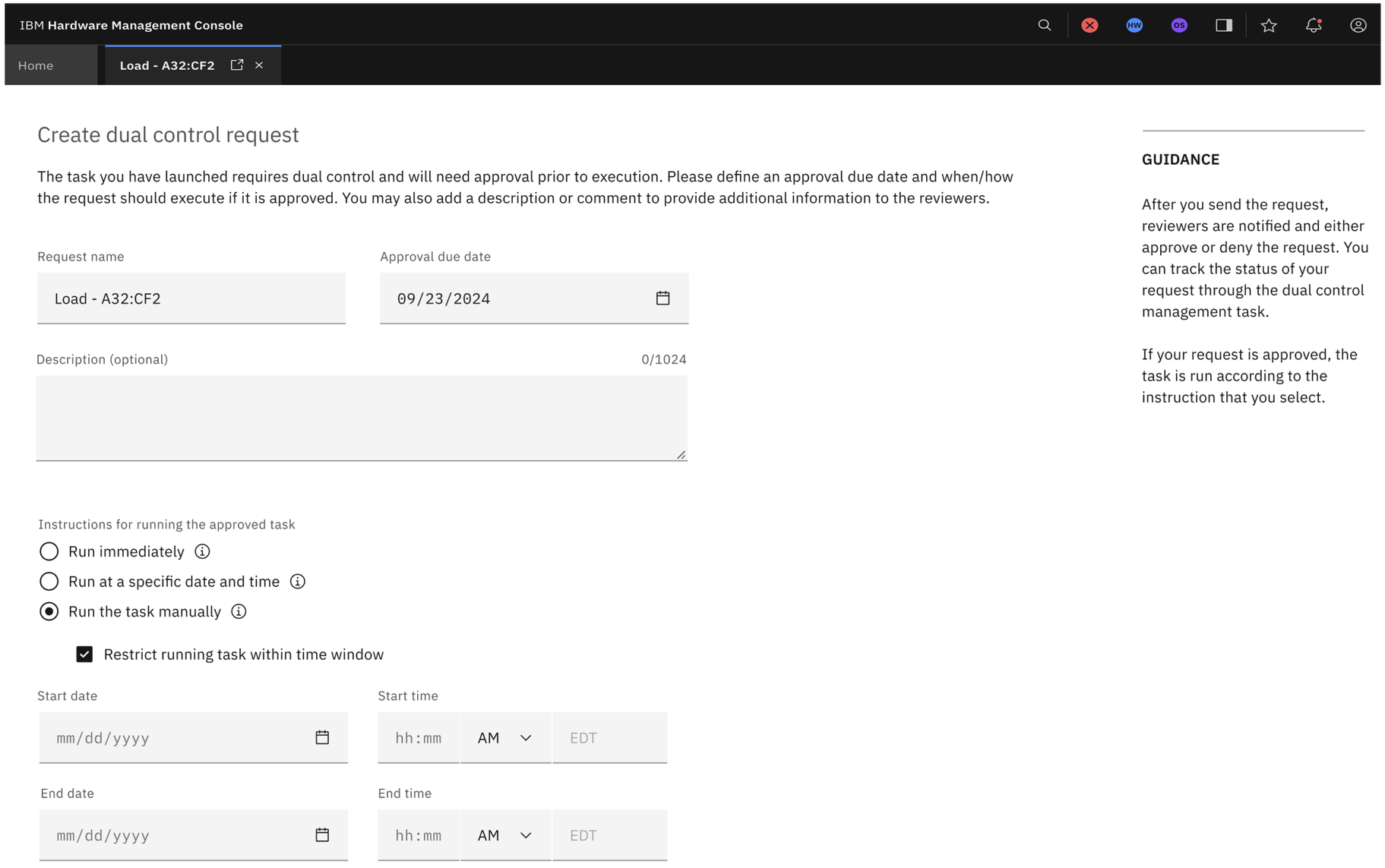


Image: Task to be run by requestor restricted to a time window

Dual Control Summary

03

Real-time notifications

Users are notified about the status of a dual control requests on the HMC, and through external methods (emails, HMC mobile notifications, APIs) to get as close to real-time visibility as possible.

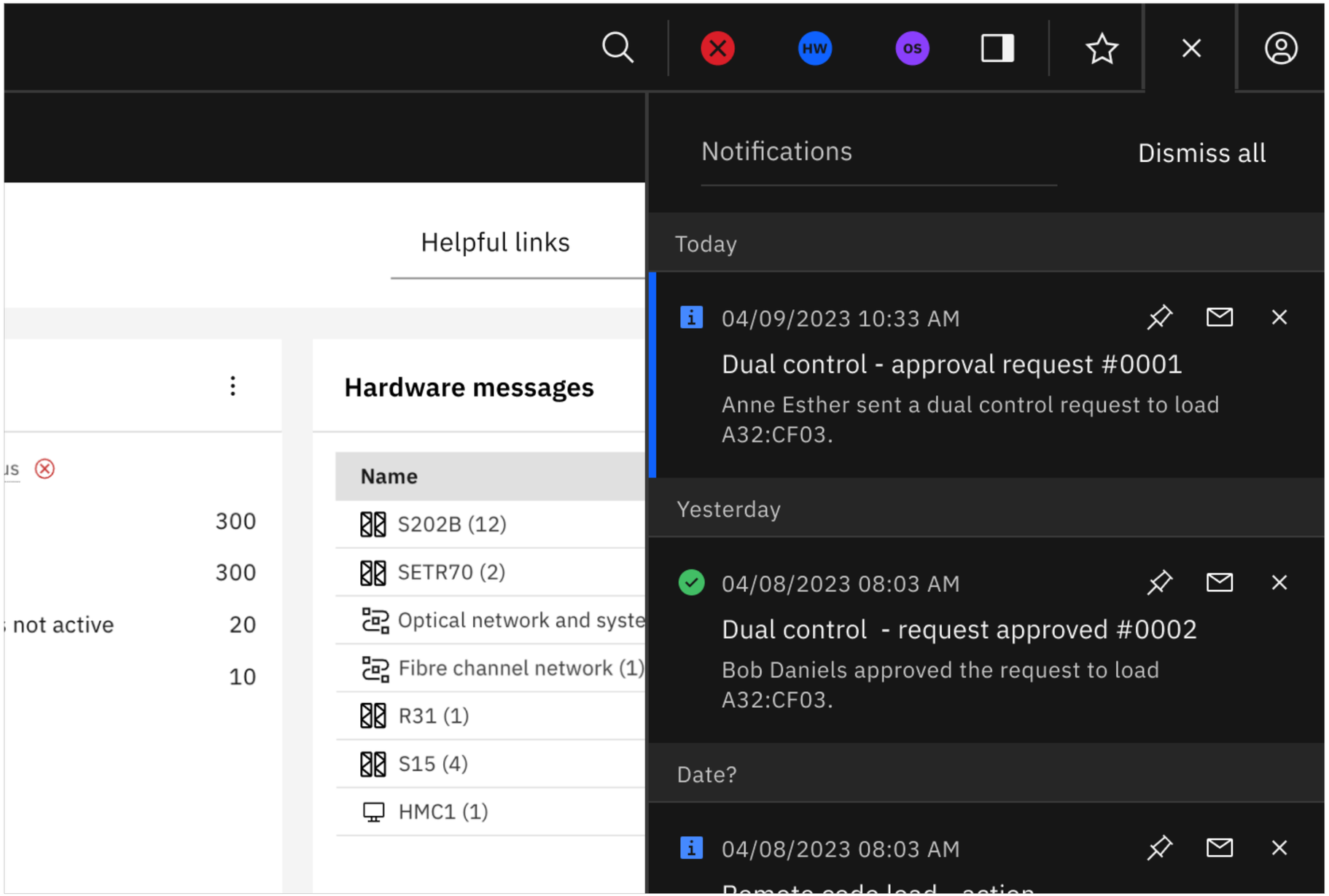


Image: Notifications panel on the HMC

Dual Control Summary

04

Request management and tracking

Requestors and approvers track the status of Dual Control requests in the Dual control management task.

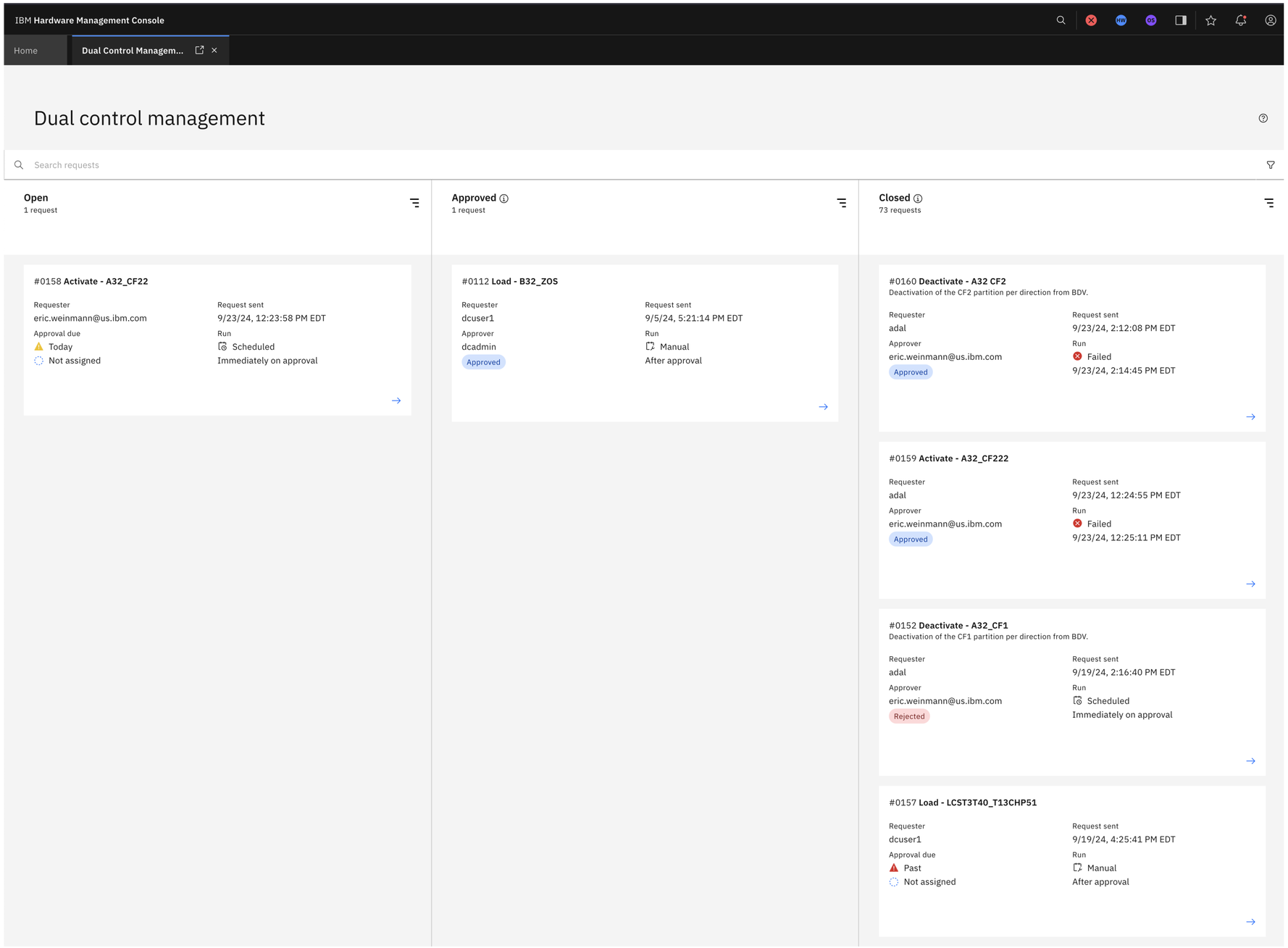


Image: Dual control management task kanban board

Dual Control Summary

05

Approver autonomy

Approvers can assign themselves to requests. They are provided with supporting information to make an accurate judgement to approve or reject a Dual Control request. Key information is:

- Requestor and approver information
- Task inputs
- History of events
- Comments
- Approval due date
- Run options
- Run time window

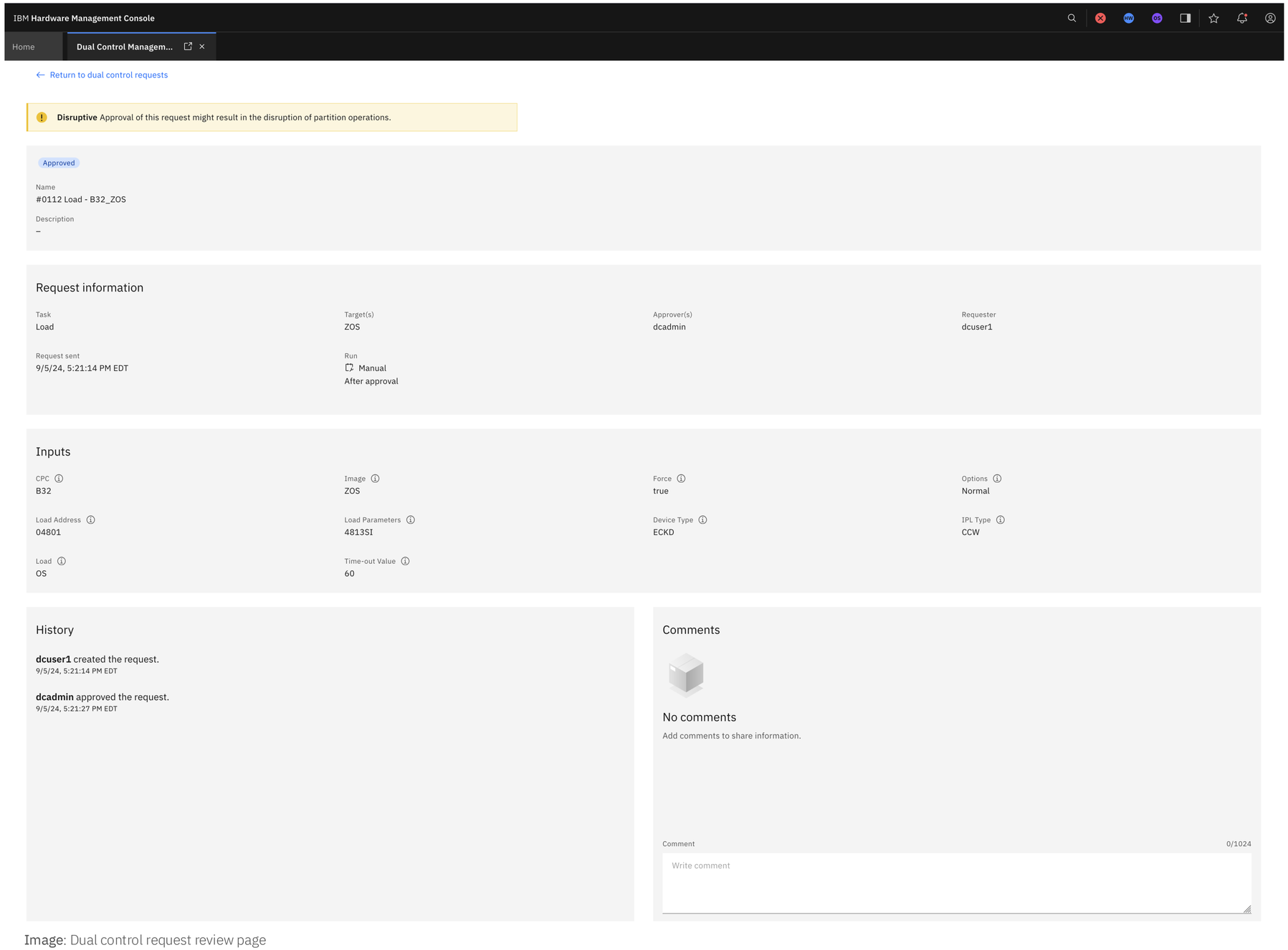
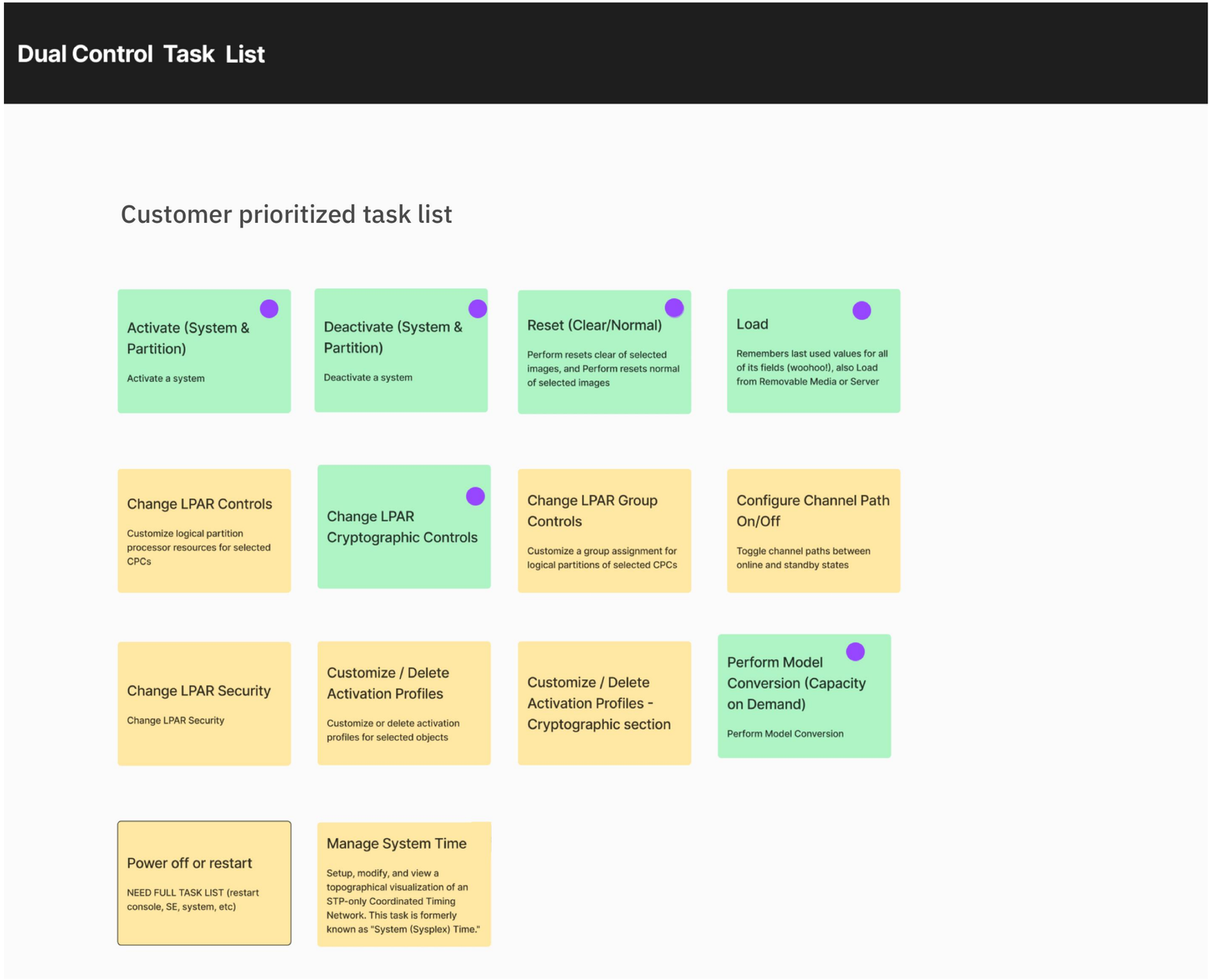


Image: Dual control request review page

Dual Control

Supported tasks

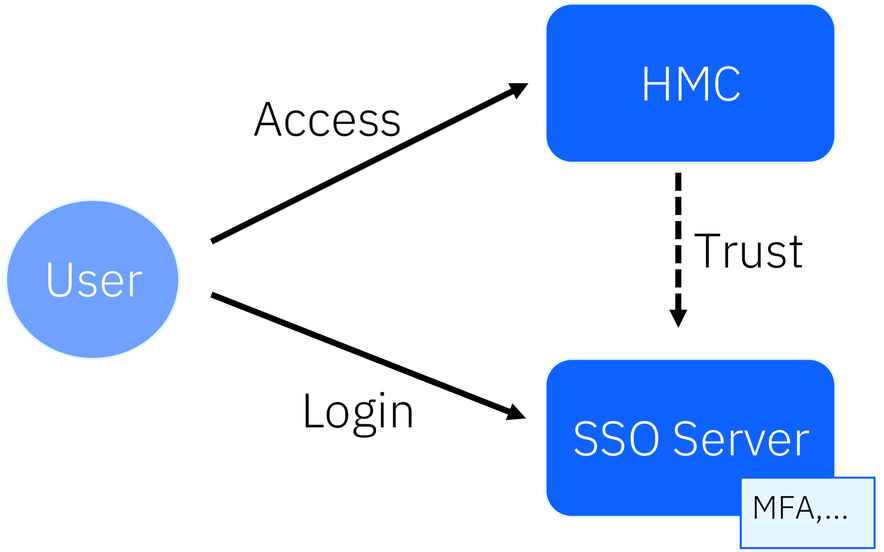
- Activate
- Deactivate
- Stop (DPM)
- Reset
- Load
- Change LPAR Cryptographic controls
- Perform Model Conversion



Single Sign On

Single Sign On (SSO)

- New authentication method for the HMC/SE
- HMC/SE never knows the user's credentials
- Allows for users to use existing credentials from other services on the HMC/SE
- OpenID Connect (OIDC) is the technology used
- **Note:**
  - SSO server provides the MFA support



Network Time Security

Network Time Security (NTS) And Other Enhancements

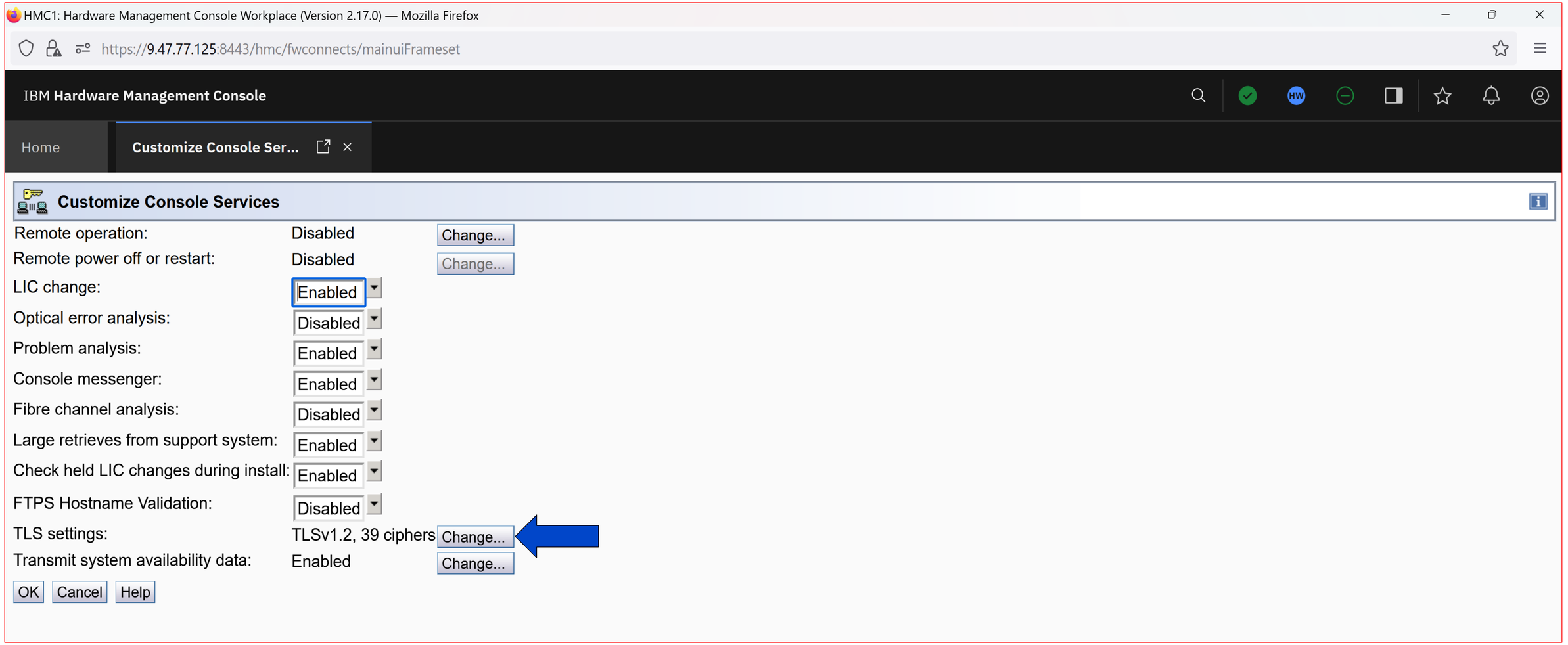
- HMC Manage System Time task Enhancements
  - Configure External Time Source (ETS) action
    - Support for 3 Network Time Protocol (NTP) servers
    - Support for 2 Precision Time Protocol (PTP) servers
    - Support for Mixed Mode (use of both NTP and PTP servers in parallel)
  - Manage CTN Certificates STP action
    - Allow use of certificates for secure NTS NTP communications between the CPC and configured ETS(es)
  - HMC Customize Console Date\Time task
    - NTP NTS support for HMC ↔ External Time Source connections
  - PTP Communication support
    - Multicast & Unicast (new)

TLS Cipher Suite Configuration

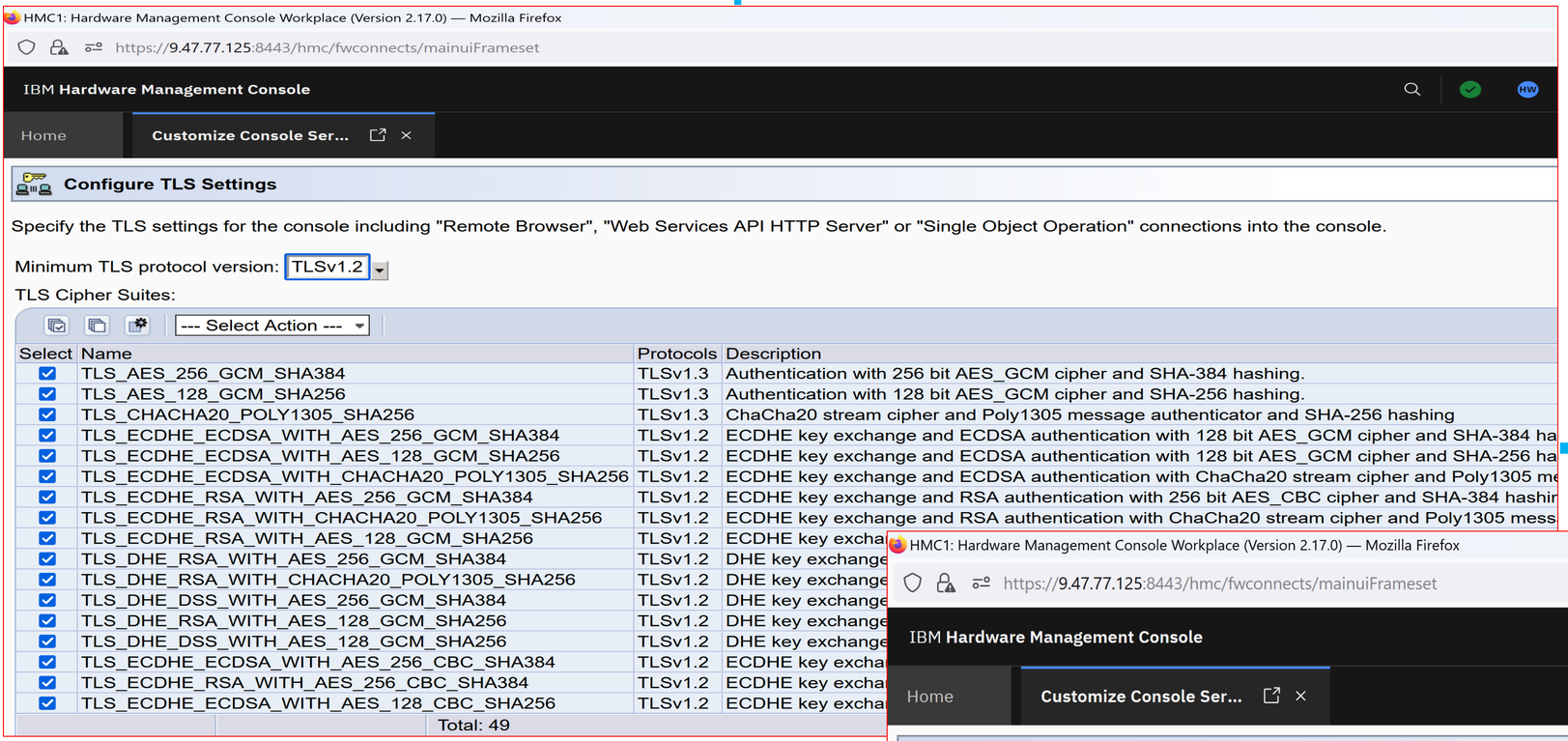
Cipher Suites Filtering per TLS

➢ Single Customize Console Services sub-task, Configure TLS Settings => mapped to Cipher Suites

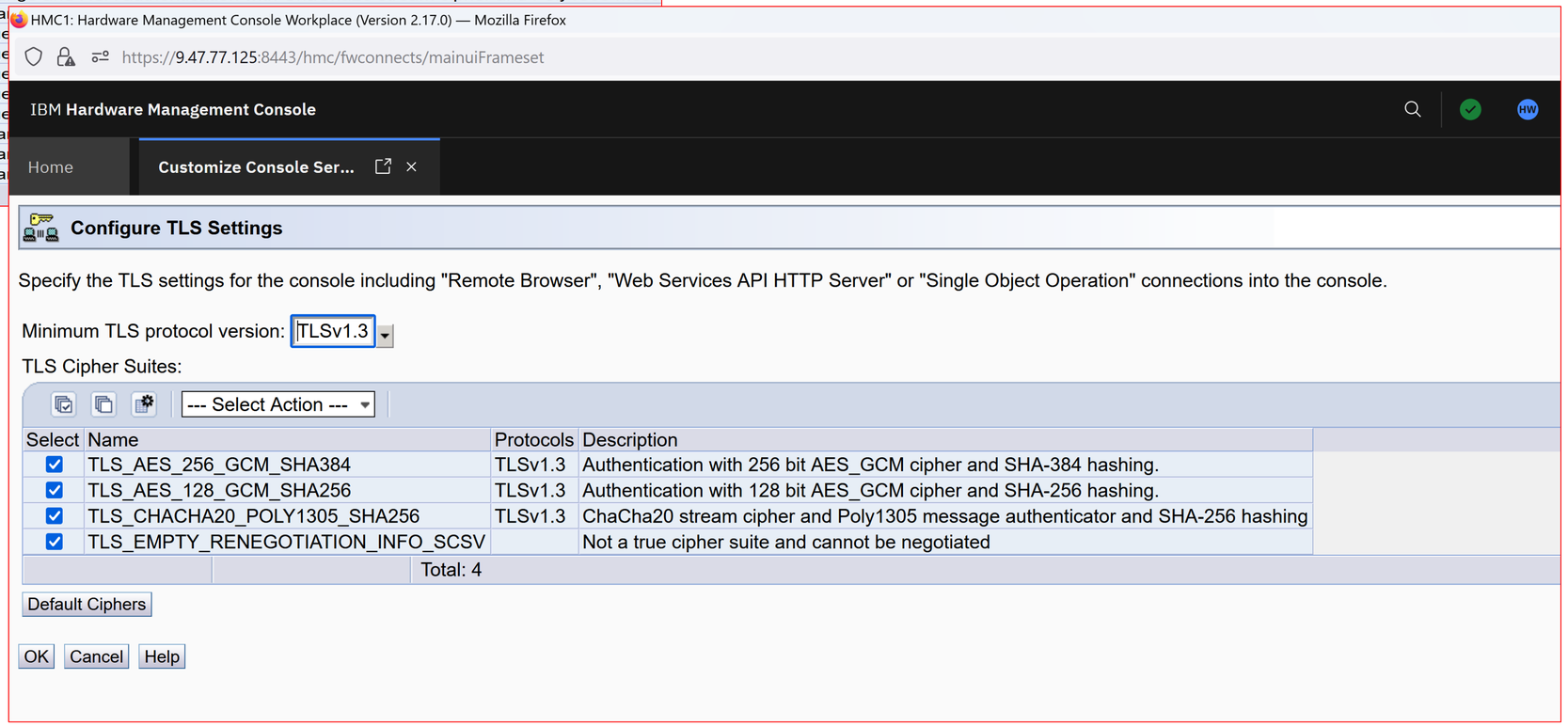
- Individual cipher suite shown for management based on Minimum TLS level



TLS 1.2 Filtered Ciphers



TLS 1.3 Filtered Ciphers



Complete HMC User configuration replication to SEs

HMC User Data Replicated to SE

➢ Strategy
- Provide ability to manage all user data in a single place, i.e., the HMC

➢ Existing support
- Standard HMC user definitions are replicated to managed SEs
- Clients can utilize these HMC user definitions to logon locally to the SE

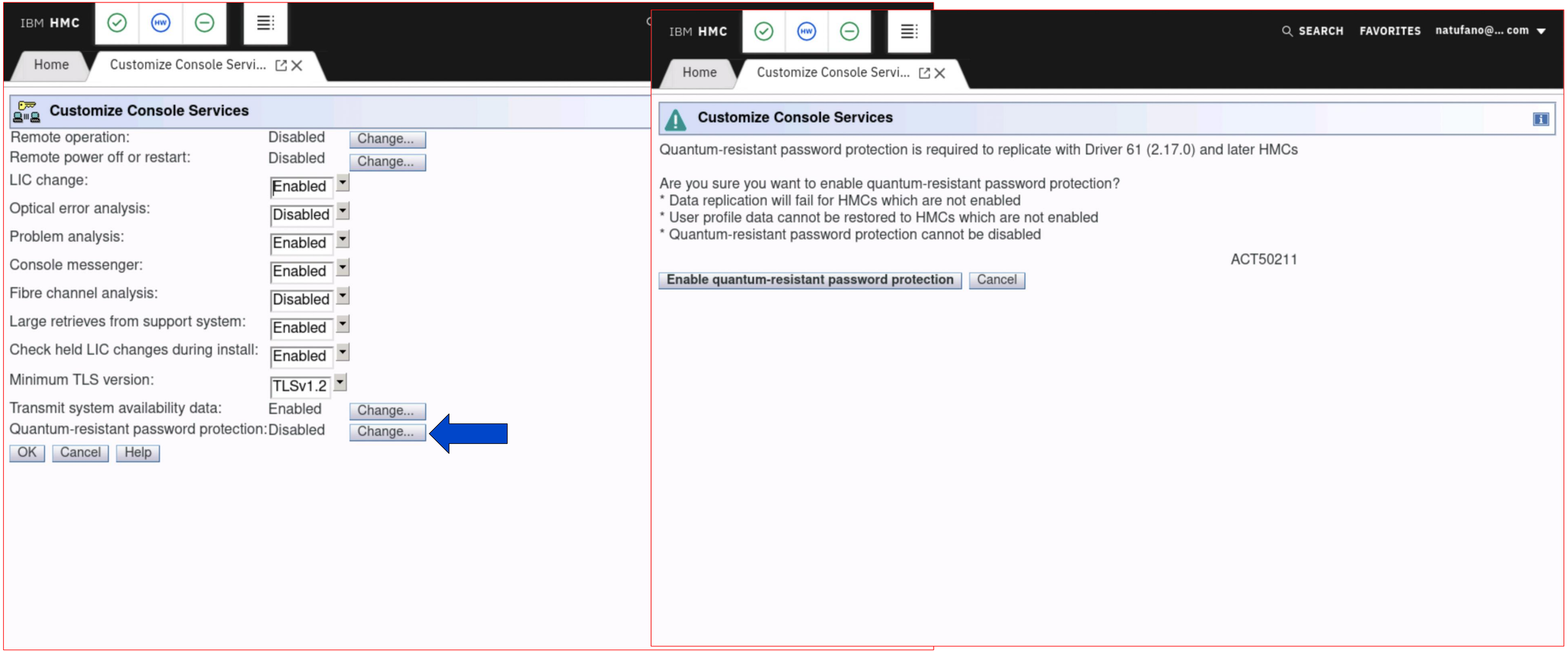
➢ What's changing?
- HMC defined user patterns and templates including LDAP Server definitions are now replicated to managed SEs
- Clients can utilize these HMC definitions to logon locally to the SE with pattern-based users
- Recommend doing all HMC User Data definitions (not just users) only on HMC, no User Mgmt on SE

Quantum-Resistant Password Hashing

Local Users Quantum-Resistant Password Hashing

- With z17, quantum-resistant hashing algorithm applied to storage of local users passwords
  - Prior to z17, local user password hashing used, but with z17, now it's quantum-resistant
  - **Note:** HMC/SE are also closed appliances with no access and additionally have an encrypted SSD
- User recommendation: define HMC Users on one HMC & allow replication to other HMCs and to SEs
- Implications of z17 HMC Local users replicated to other HMC/SE levels
  - **z17 HMCs/SEs:** none
  - **z16/z15 HMCs/SEs**
    - HMCs => HMC Data Replication of User Profile Data will be blocked until MCL/Opt In for new quantum-resistant
      - MCL Bundle: z16 – H31, z15 – H62
      - Must also Opt in ==> see next chart
    - SEs
      - For SE local console logon (not Single Object Operations), HMC user/password is normally authenticated to connected HMC
      - If no connection to HMC, SE local console logon would fail until Quantum Resistant MCL (z16 - S44, z15 – S98)/Opt In for new quantum-resistant
- **Note:** HMC LDAP or SSO authenticated users are not affected by this change

Quantum-Resistant Password Hashing – Opt In

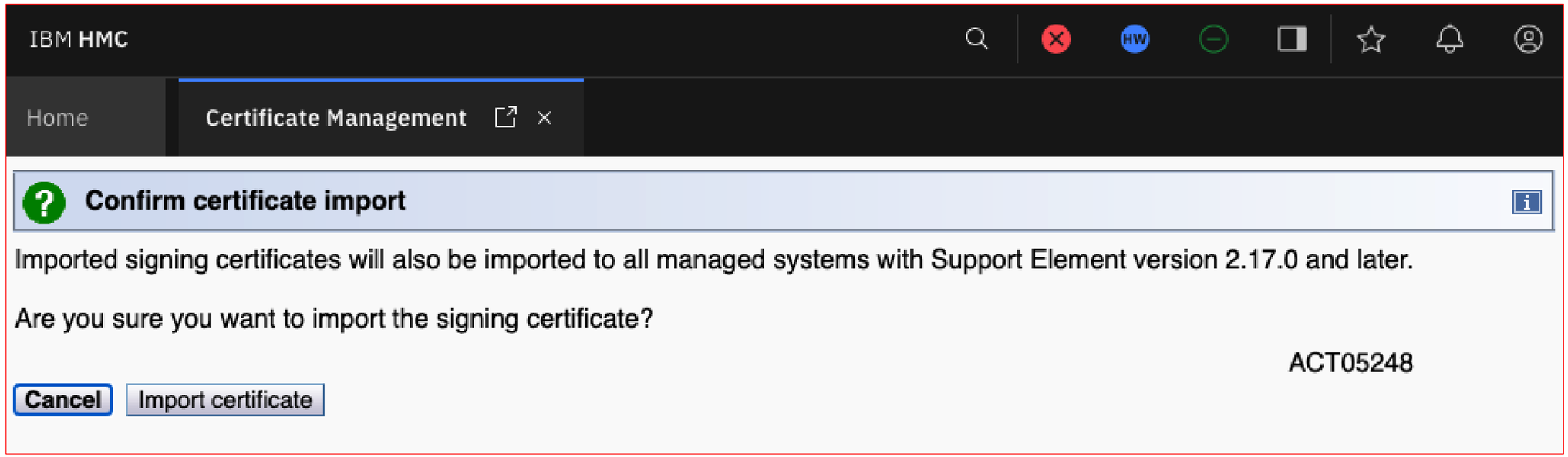


Replicate HMC Certificates to SE

Replicate HMC Certificates to SE

- Certificates imported to the HMC *Certificate Management* task will also be imported to managed IBM z17 SEs.
  - Certificates deleted from the Certificate Management task will also be deleted from managed IBM z17 SEs.
    - If multiple HMCs are managing the same SE, certificate is only deleted if no other HMC has that certificate imported.
    - If the HMC and SE stop communicating, certificates associated with that HMC are removed from the SE until communications are reestablished.
- Tasks/Options that can take advantage of this enhancement include:
  - LDAP
  - MFA
  - Remote Syslog Server
  - FTPS

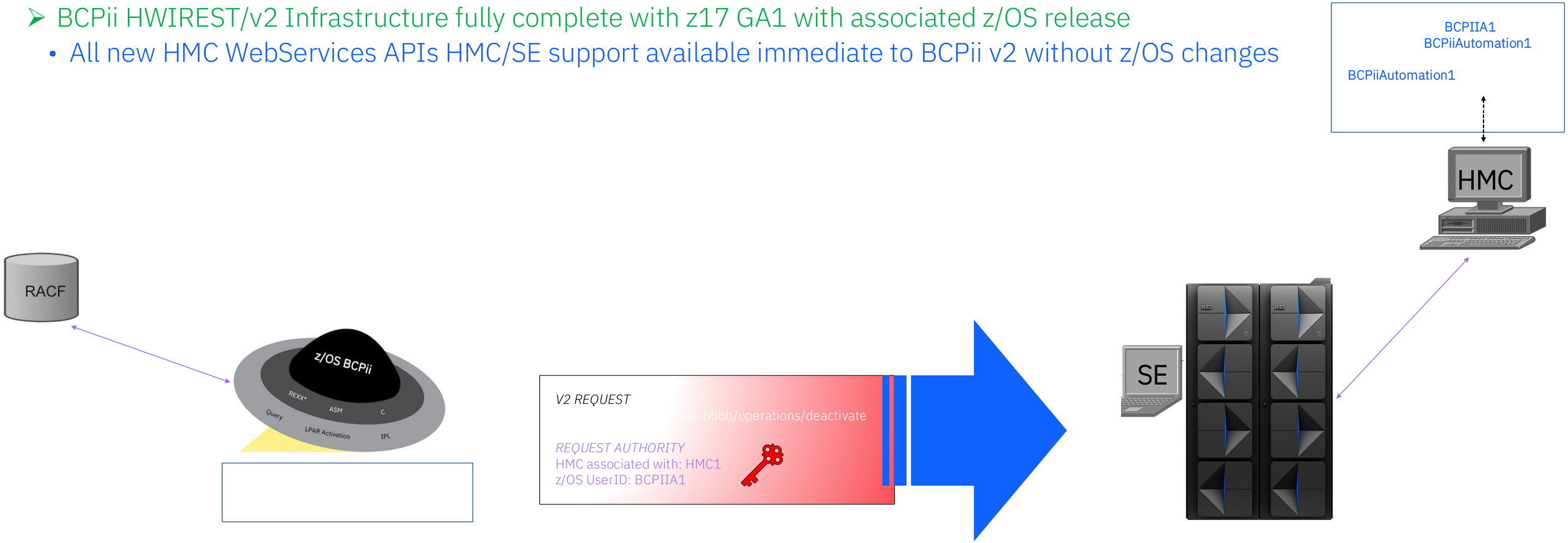
New Confirmation Dialogue



BCPii Enhancements/SOD

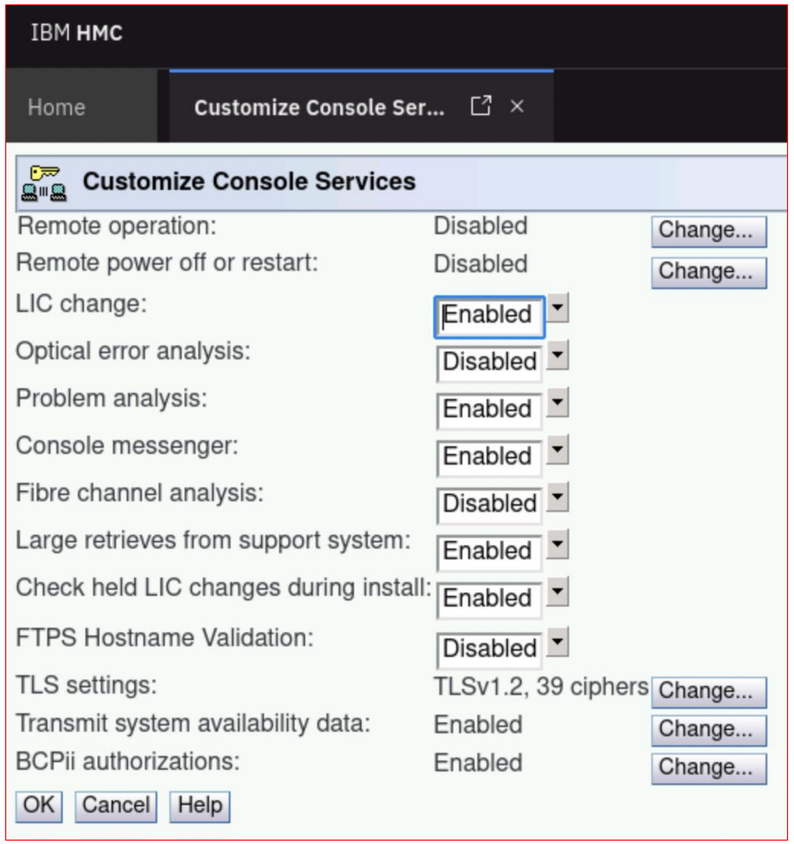
BCPii v2 Enhanced Security, HMC Target, Async support

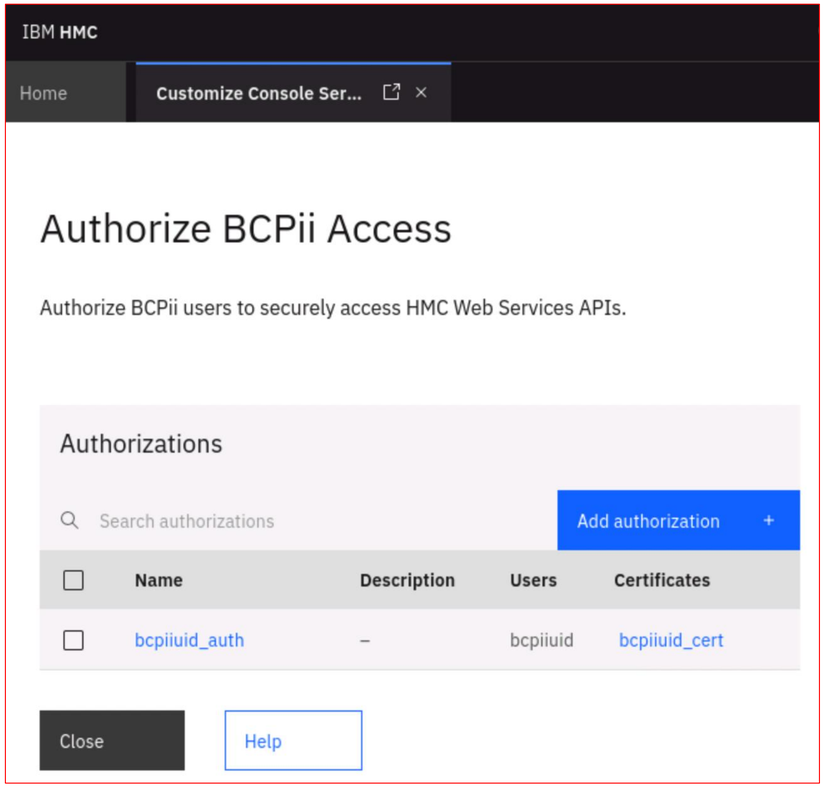
- BCPii HWIREST/v2 will pass the z/OS USER ID to SE/HMC via signed JSON Web Token (JWT)
  - *z/OS user mapped/limited to HMC user task/object permissions*
- Enhanced Security plus
  - *HMC Target support*
  - *BCPii HWIREST/v2 Asynchronous Notification support*
- BCPii HWIREST/v2 Infrastructure fully complete with z17 GA1 with associated z/OS release
  - All new HMC WebServices APIs HMC/SE support available immediate to BCPii v2 without z/OS changes

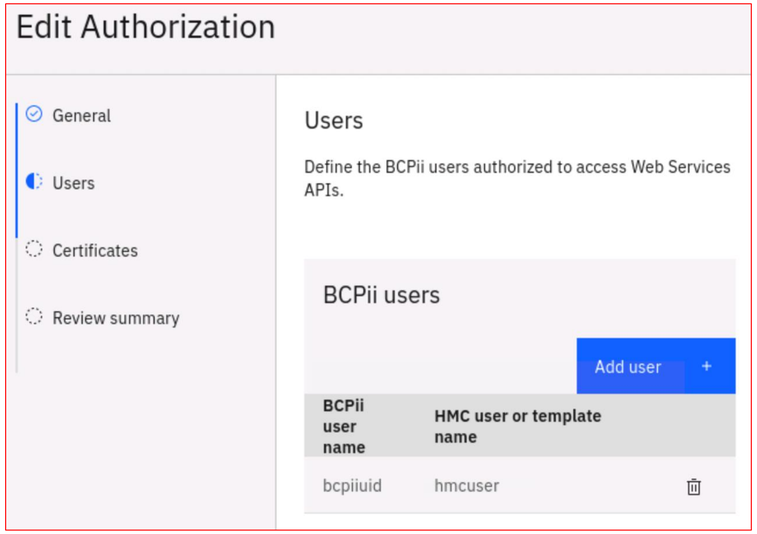


Configuring an HMC for BCPii Targeting

- The HMC needs to be configured to validate a JWT and map the z/OS BCPii ID to an HMC user
  - Import bcpii-authorization certificate used to validate JWT signature to HMC
  - Associate the certificate(s) with a BCPii to HMC user mapping
- The *Authorize BCPii Access* sub-task can be launched from *Customize Console Services*







SOD for BCPii v1/SNMP Deprecation

- z17 addresses BCPii v2 limitation on Asynchronous Notifications
- There will be no further feature enhancements in BCPii v1
  - Nor for the HMC/SE SNMP automation interface
- All future feature enhancements will only be for HMC/SE WS APIs & BCPii v2

- Above Translation: BCPii v1 & SNMP are being deprecated
  - BCPii v1 & SNMP are available or allowed; would recommend developing migration plan once a client has a z17 CPC
  - From Google:
    - A functionality that is deprecated is likely to be removed in the future, hence it is not advisable to use it.
    - Deprecated functional items are usually replaced or updated with newer versions.
  - IBM has no roadmap target to remove BCPii v1 (yet)
    - IBM also has no timeline to remove HMC/SE SNMP support (yet)

IBM z17 Redbooks and other interesting links

April 8th, 2025 – New and Updated Redbooks
- IBM z17 Technical Introduction, SG24-8580
- IBM z17 Technical Guide, SG24-8579
- IBM z17 Connectivity Handbook, SG24-5444-22

April 8th, 2025 – Updated Redpaper
- IBM Z Functional Matrix, REDP-5157-08

Jun 18th, 2025 – New and updated Redbook materials:
- IBM z17 Configuration Setup, SG24-8581
- IBM Z Time Synchronization Implementation Guide, SG24-8480-02

IBM z17 other interesting links
- IBM z17 interactive 3D Demo
- THIS is how IBM makes servers That cannot fail

Technology outlook for IBM Z

- Performance
- Capacity
- Data privacy & protection
- Resiliency
- Dedicated workload accelerators
- Sustainability
- Stack optimization
- Simplification

2019 — 2035

IBM z15

14nm

Accelerated Compression

Accelerated Sort

Secure Execution

System Recovery Boost

IBM z16

7nm

Accelerated AI

Quantum-Safe System

Secure Boot

Memory Encryption

Flexible Capacity for Cyber Resiliency

IBM z17

5nm

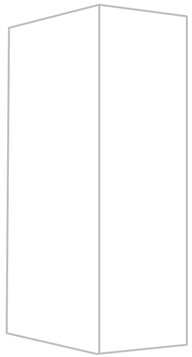
IBM Spyre Accelerator

Multi-model, agentic, & gen AI

Accelerated I/O

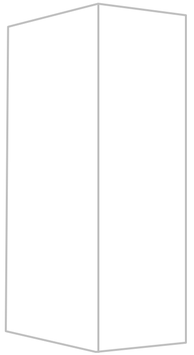
Standardized Quantum-Safe Algorithms

AI-powered security



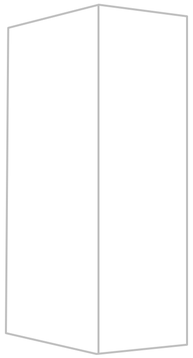
IBM zNext

3-2nm



IBM zNext +1

?nm



IBM zNext +2

?nm