Front cover

IBM z17 Technical Introduction

Bill White

Jacky Doll

Octavian Lascu

Artem Minin

Patrick Oughton

Ewerson Palacio

Martijn Raave

Jamie Roszel

John Troy

IBM Z

Redbooks

ibm.com/redbooks

IBM

Redbooks

IBM Redbooks

IBM z17 Technical Introduction

April 2025

SG24-8580-00

Note: Before using this information and the product it supports, read the information in “Notices” on page v.

First Edition (April 2025)

This edition applies to IBM z17 ME1.

Contents

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and customer examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

CICS®
Code Assistant™
Concert®
Db2®
DS8000®
FICON®
GDPS®
Guardium®
HyperSwap®
IBM®
IBM Cloud®
IBM Concert®
IBM Security®
IBM Spyre™
IBM Telum®
IBM watsonx®
IBM Z®
IBM z16®
IBM z17™
Language Environment®
Parallel Sysplex®
PIN®
RACF®
Rational®
Redbooks®
Redbooks (logo) ®
Resource Link®
Spyre™
watsonx®
watsonx Assistant™
watsonx Code Assistant™
WebSphere®
z/Architecture®
z/OS®
z/VM®
z15®
z16®
z17™
zEnterprise®

The following terms are trademarks of other companies:

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Zowe, are trademarks of the Linux Foundation.

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Red Hat, Ansible, OpenShift, Red Hat, are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Preface

The IBM Z® platform has been globally acknowledged for its security, resilience, performance, flexibility, and scalability. It forms the backbone of mission-critical workloads and is a key component in hybrid cloud environments and AI projects. With each new release, IBM® consistently enhances this solid foundation while expanding its benefits to empower businesses where it counts most.

This IBM Redbooks® publication introduces the newest member of the IBM Z family – the IBM z17™. The IBM z17 signifies the dedication of IBM to technological advancement, merging innovative features that address the rising demands for AI solutions and hybrid cloud infrastructures. The IBM z17 not only ensures reliability and security but also drives business operations forward while carefully managing risk.

The IBM z17 leverages AI for data-driven insights and automation, fine-tunes hybrid cloud strategies for unmatched agility, and supports robust application modernization. Furthermore, its cyber resiliency and security features ensure operations run smoothly with minimal disruptions and maximum system uptime – vital aspects in today's digital era.

In this IBM Redbooks publication, we look at each component of the IBM z17, offering insights and highlighting scenarios where it can redefine your organization's technological pathway. This guide will help you to quickly understand how your organization can take advantage of the capabilities of the IBM z17.

Authors

This book was produced by a team of specialists from around the world working with the IBM Redbooks, Poughkeepsie Center.

Bill White is an IBM Redbooks Project Leader and Senior IT Infrastructure Specialist at IBM Poughkeepsie, New York.

Jacky Doll has been with IBM for ten years, primarily working on IBM z/OS® product content design. Jacky helped deliver the first ever IBM Z Content Solution. She has recently joined the IBM Redbooks team as a Project Leader. Jacky is also pursuing her Ph.D. in Cognitive Science at RPI.

Octavian Lascu is a Senior IT Infrastructure Architect with Inter Computer, Romania. He has over 35 years of IT experience with IBM Z, IBM Power, and IBM Storage. Octavian was an IBM Redbooks Project Leader for over 20 years, where he has co-authored many IBM Redbooks publications covering IBM Z hardware, IBM Power, and various IBM solutions.

Artem Minin is currently a Technical Specialist in IBM's Washington Systems Center, a team of Subject Matter Experts that provides leading edge technical sales assistance for the design, implementation, and support of solutions that leverage IBM Z. Specifically, Artem is responsible for supporting IBM Z Data and AI solutions through PoCs, custom demos, and client workshops. He focuses on supporting client engagements which leverage open-source AI software, Machine Learning for z/OS, Cloud Pak for Data, Data Gate, DVM for z/OS, and SQL Data Insights.

Patrick Oughton is an IBM Z Brand Technical Specialist in New Zealand. He joined IBM in 2015 after working as a z/OS Systems Programmer for 30 years. His areas of expertise include IBM Z installation (hardware and operating system) and IBM Parallel Sysplex® Implementation. He has written three other IBM Redbooks publications.

Ewerson Palacio is an IBM Redbooks Project Leader. He holds a bachelor's degree in Math and Computer Science. Ewerson worked for IBM Brazil for over 40 years and retired in 2017 as an IBM Distinguished Engineer. Ewerson has co-authored many IBM Z Redbooks publications and created and presented IBM Redbooks seminars around the globe.

Martijn Raave is an IBM Z and LinuxONE Client Architect and Hardware Technical Specialist for IBM Northern Europe. Over a period of 27 years, his professional career has revolved around the mainframe platform, supporting several large Dutch customers in their technical and strategic journey on IBM Z. His focus areas are hardware, resiliency, availability, architecture, but he is interested in any IBM Z related topic.

Jamie Roszel has spent four years at IBM, initially creating technical documentation for IBM Cloud® Databases and now leading projects for IBM Redbooks. Jamie specializes in developing clear, comprehensive technical content that bridges the gap between complex systems and user needs.

John Troy is an IBM Z and storage hardware National Top Gun in the northeast area of the US. He has over 40 years of experience in the service field. His areas of expertise include IBM Z servers and high-end storage systems technical and customer support and services. John has also been an IBM Z hardware technical support course designer, developer, and instructor for the last eight generations of IBM high-end servers.

Thanks to the following people for their contributions to this project:

Jonathan Bradbury, Marc Coq, Anne Dames, Michael Grötzner, Dave Hollar, Richard Kisley, Nicolas Mäding, Purvi Patel, Priyal Shah, André Spahni, Dave Surman, Benedikt Wenz
IBM

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an IBM Redbooks residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks

- Send your comments in an email to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, IBM Redbooks
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

1

Attaining outcomes and driving value with the IBM z17

More than ever, businesses and organizations are looking for artificial intelligence (AI) solutions that are cost-effective to build and run securely at scale. At the same time, utilizing automation, transaction processing, and hybrid cloud practices to establish and govern those AI solutions appropriately are a must.

Many enterprises rely heavily on a hybrid cloud infrastructure with high-speed transaction processing for their business operations. While some are already using AI in transaction samplings, they actually envision having fully embedded, real-time AI integration - making use of AI and generative AI in business crucial workflows has become vital to delivering desired outcomes and driving value.

The newest addition to the IBM Z family, the IBM z17, addresses these demands by offering accelerated artificial intelligence capabilities, enhanced cyber resiliency and security, sustainable operations, and support for a modernized hybrid cloud infrastructure.

This chapter outlines features of the IBM z17 and illustrates the resulting business benefits. The following topics are covered:

- 1.1, "Modern challenges and IBM z17 solutions" on page 2
- 1.2, "IBM z17 technical highlights" on page 3
- 1.3, "AI, automation, and security: Exploring IBM z17 use cases" on page 7

1.1 Modern challenges and IBM z17 solutions

In today's rapidly evolving digital landscape, enterprises are under pressure to innovate, optimize resources, and maintain robust security postures. The convergence of AI and hybrid cloud strategies has become a powerful catalyst for transformation, enabling organizations to unlock new opportunities and drive growth.

Navigating challenges in AI and hybrid cloud initiatives requires understanding of the unique capabilities of underlying platforms, particularly transaction processing systems (TPS). These TPS are crucial for facilitating data sharing across hybrid cloud architectures, providing a robust foundation for enterprise transformation. The IBM z17 is specifically designed to address these challenges head-on. As enterprises strive to leverage AI and hybrid cloud strategies for innovation and growth, they must confront several pivotal challenges inherent in these initiatives. The IBM z17 offers targeted solutions designed to address these obstacles effectively, enhancing both performance and security while supporting sustainable operations, including:

- **Data management and performance**
  - **Challenge:** Efficient management of vast data volumes and transaction throughput.
  - **Solution:** IBM z17 delivers industry-leading performance with:
    - The IBM Telum® II processor chip, featuring a higher core density, additional cores, and improved architecture over its predecessor.
    - Large-scale memory for faster data processing.
    - Unique cache design optimizing overall performance.
    - Accelerated I/O bandwidth handling massive data volumes.
- **Data security, compliance, and resilience**
  - **Challenge:** Protection of sensitive information against current and future threats while ensuring compliance with regulations.
  - **Solution:** IBM z17 provides robust security and resilience features:
    - Advanced cryptography for comprehensive data protection.
    - Instant recovery mechanisms to minimize downtime during outages.
    - Dynamic production capacity activation across sites for enhanced disaster recovery (DR).
- **AI-Driven innovation and security**
  - **Challenge:** Harnessing AI to foster innovation, improve predictive capabilities, and ensure secure data usage.
  - **Solution:** IBM z17 advances the AI journey with:
    - Enhanced AI prediction accuracy using LLMs in real-time transaction processing.
    - AI acceleration on IBM Z with the IBM Spyre™ Accelerator[1]
    - Resource-efficient environments supporting sustainable AI workloads.
    - Additionally, IBM z17 enhances security by utilizing AI-powered tools to proactively identify and mitigate risks. It also simplifies compliance processes to save time and resources while accelerating a quantum-safe journey to address future threats.

[1] Statement of general direction: IBM Spyre Accelerator is planned to be available starting in 4Q 2025, in accordance with applicable import/export guidelines.

- **Sustainability**
  - **Challenge:** Reducing the environmental footprint of IT infrastructure without compromising performance.
  - **Solution:** IBM z17 supports sustainability by:
    - An energy-efficient design that reduces power consumption by approximately 17% compared to a similarly configured IBM z16® system[2].
    - High-density computing capabilities to minimize data center footprints.
- **Operational efficiency**
  - **Challenge:** Automating IT operations to increase market speed, modernize efficiently, and reduce risks.
  - **Solution:** IBM z17 transforms operations with:
    - AI-driven user experience enhancements fostering skill development.
    - Faster time-to-market through accelerated processes.
    - Increased pace of modernization while reducing risks through automation and standardization.

The IBM z17 surpasses conventional transaction processing systems (TPS) with a high-value, purpose-built architecture tailored for escalating AI and hybrid cloud needs. It delivers superior performance, security, and efficiency, empowering businesses to drive innovation, bolster cybersecurity, and optimize resource management during their digital transformation.

1.2 IBM z17 technical highlights

The IBM z17 maintains compatibility with its predecessor's form factor, adhering to a 19-inch rack mount design. This versatile architecture allows for scalability from a single frame up to four frames based on the specific system requirements and configurations. The 19-inch frames support American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE) Class A3 data centers.

[2] Disclaimer: This description of an IBM z17 system's expected configuration assumes typical settings, derived from historical averages observed in IBM z16 systems. The proposed IBM z17 setup includes a maximum capacity of 90 processors, supported by 8 TB memory and 5 I/O Acceleration (ICA-SR) 2.0 features. It incorporates three PCIe Generation 4+ Input/Output (I/O) drawers, housing 43 versatile I/O adapters that cater to networking, external storage, and security functionalities. The IBM z16 is configured to provide the same hardware capability. Power consumption is based on the Power Estimation Tool.

Figure 1-1 shows the diverse IBM z17 configuration possibilities, ranging from a single 19-inch frame up to four frames.

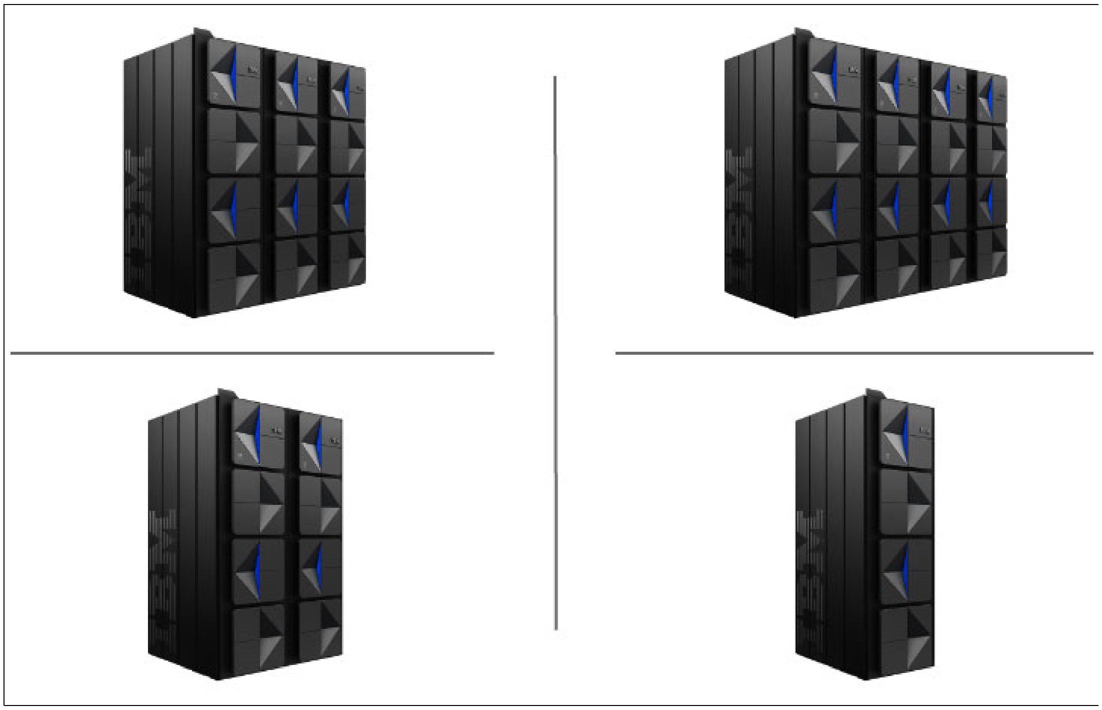

Figure 1-1 IBM z17 configuration options (cannot display covers till announce day

The IBM z17 is designed for seamless integration and future-proofing, inheriting compatibility with both IBM z16 and IBM z15® systems. This continuity supports a range of upgrade paths through five distinct features: Max43, Max90, Max136, Max183, and Max208. Each feature's name reflects the maximum number of characterizable processor units (PUs) available for configuration.

Table 1-1 lists some of the IBM z17 ME1 technical capabilities compared to the IBM z16 A01.

Table 1-1

	IBM z17 differentiation[a]	IBM z17 ME1	IBM z16 A01
Processor chip	► 20% core processor area reduction ► 17% power reduction ► 11% single thread performance improvement	► 5nm technology ► 5.5 GHz ► 8 cores per chip ► 24.1 miles of wire per chip ► 43B transistors	► 7nm technology ► 5.2 GHz ► 8 cores per chip ► 18.8 miles of wire per chip ► 22.5B transistors
Capacity	► 20% greater capacity for standard drawer models ► 15% greater capacity on the maximum configuration model	208 characterizable processor units	200 characterizable processor units
Cache	Up to 40% more shared cache per core compared to IBM z16.	► 36 MB L2 ► 360 MB virtual L3 ► 2.8 GB virtual L4	► 32 MB L2 ► 256 MB virtual L3 ► 2 GB virtual L4
Total system memory	60% system memory growth	► 4U DDR5 DDIMM ► 64 TB max memory	► 4U DDR4 DDIMM ► 40 TB max memory
On-chip AI acceleration	► Support for LLM compute primitives ► Improved quantization: Int8, FP16 datatypes	Telum II	Telum I
Off-chip PCIe Accelerator card	Available only on z17	► IBM Spyre Accelerator ► 32 Gen AI-ready cores on extended adapters ► Up to 48 adapters per system	Not available
System I/O	► Reduced power for I/O management ► Double density with new IBM FICON® Express and Network Express features	On-processor chip I/O Data Processing Unit (DPU)	Off-chip I/O processing (ASIC chip)

a. Disclaimer: Calculations presented in this column were established through internal measurements. Standard models include IBM z17 Max43, Max90, Max136 and Max183 and IBM z16 Max39, Max82, Max125, and Max168. Maximum configuration models are IBM z17 Max208 and IBM z16 Max200. Results may vary based on individual workload, configuration, and software levels. For more information, see IBM Z Large Systems Performance Reference.

The IBM z17 also provides the following:

- Support for six logical channel subsystems (LCSSs)[3], four subchannel sets, and 85 logical partitions (LPARs).
- A larger fixed Hardware System Area (884 GB) that is managed separately from ordered memory.
- A single-instruction, multiple-data (SIMD) processor increases parallelism to accelerate analytics and AI processing. In addition, simultaneous multithreading (SMT) increases processing efficiency and throughput and raises the number of instructions in flight. Special coprocessors and new hardware instructions for accelerating selected workloads is also available.

[3] Each LCSS supports 63,25K devices in the first subchannel set and 64K devices in each alternate subchannel sets.

- IBM Virtual Flash Memory (VFM) can be used to handle z/OS paging workload spikes and improve availability. Up to 6 TB, in 12 increments of 0.5 TB, is orderable.
- The IBM Z Sort accelerator helps reduce CPU costs, speed up the sorting process, and improve database functions.
- IBM Integrated Accelerator for zEnterprise® Data Compression (zEDC) improves data compression operations by having one dedicated compression coprocessor per processing unit (on-chip compression), and new hardware instructions.
- For improved I/O channel performance, the ASIC functions that are part of the I/O features have moved to assist processors in the processing unit (PU) chip, called the Data Processing Unit (DPU). The corresponding I/O features are:
  - FICON Express32-4P (4 ports) for storage connectivity
  - Network Express (2 ports) for network connectivity
- Just-in-time deployment of processor resources. The Capacity on Demand (CoD) function can dynamically change available system capacity. This function can help respond to new business requirements with flexibility and precise granularity.
- IBM Tailored Fit Pricing for IBM Z options are designed to deliver unmatched simplicity and predictability of hardware capacity and software pricing, even in the constantly evolving era of hybrid cloud.
- The same high quality of service and reliability, availability, and serviceability (RAS) that is traditional in the IBM Z platform is provided. The RAS strategy uses a building-block approach that meets the stringent requirements for achieving continuous, reliable operation.
- Enhance resiliency with flexible capacity to make system resources available across locations to proactively avoid disruptions.
- Integrated quantum-safe protection is provided through quantum-safe cryptography APIs and crypto-discovery tools. Quantum-safe secure boot technology helps protect IBM z17 firmware from quantum attacks through a built-in dual signature scheme with no configuration changes required for enablement.

For more information about the IBM z17 configuration options, hardware components, and upgrade paths, see Chapter 2, “IBM z17 ME1 hardware overview” on page 11.

For more information regarding cryptographic features and storage, network, and clustering connectivity options, see Chapter 3, “IBM z17 supported features and functions” on page 27.

1.3 AI, automation, and security: Exploring IBM z17 use cases

This section focuses on three key use cases of IBM z17 to foster innovation and growth, enhance operational efficiency, and bolster data security:

- Leveraging AI for ground-breaking innovation and growth opportunities.
- Automating processes to revolutionize efficiency.
- Employing robust security measures to protect sensitive business information.

Each use case provides an exploration into the transformative potential of IBM z17, offering practical insights for businesses looking to optimize their operations and maintain a competitive edge in the modern marketplace.

1.3.1 Leveraging IBM z17 for innovation and growth through AI

IBM z17 introduces a transformative era for enterprise AI through its innovative features:

- **Composite AI**: The distinctive Composite AI of IBM z17 amalgamates multiple AI models - Machine Learning (ML), Deep Learning (DL), and Large Language Models (LLMs) - into an integrated framework. This fusion amplifies the collaborative problem-solving potential of diverse AI technologies leveraging unstructured data as well.
- **IBM Telum II Processor**: With unparalleled capacity, this processor supports real-time scoring for millions of transactions per second, enabling 100% in-transaction AI insights. It enhances transactional intelligence via swift inferencing, without sacrificing performance.
- **Integrated AI Accelerator**: The second generation on-chip AI accelerator on IBM z17 significantly boosts the AI inferencing capacity as each core on the chip can access all AI accelerators within the same drawer. This has resulted in a 7.5x inference throughput increase on IBM z17 compared to IBM z16® for a Credit Card Fraud Detection use case. This acceleration propels the AI innovation cycle, enabling organizations to maintain a competitive edge.
- **Secure and Scalable Environment**: IBM z17 prioritizes the secure execution of AI workloads. It implements hardware-based encryption, isolated execution enclaves, and stringent security measures to protect intellectual property while upholding data privacy regulations. This ensures that innovation flourishes within a robustly protected ecosystem.
- **IBM Spyre Accelerator**: Complementing the Telum II Processor, the Spyre Accelerator presents an adaptable architecture capable of integrating multiple AI models and LLMs seamlessly. This adaptability allows organizations to easily scale their AI capabilities in line with evolving business demands.

By capitalizing on these advanced functions, IBM z17 can help move businesses towards growth and innovation:

- **Accelerated Innovation**: The synergistic effect of Telum II Processor, Integrated AI Accelerator, and Spyre Accelerator rapidly facilitates the development and deployment of AI models. This agility enables organizations to promptly react to market changes and seize emerging opportunities.
- **Enhanced Predictive Capabilities**: By uniting diverse models, businesses gain an all-encompassing understanding of their operations. This holistic view empowers more precise forecasting and strategic planning across departments.

- **Regulatory Compliance**: IBM z17 prioritizes data security and privacy, ensuring enterprises can responsibly leverage AI technologies while adhering to strict regulations.
- **Scalability**: The platform's design effortlessly scales AI capabilities via the Spyre Accelerator, accommodating changing business needs without disruption. This adaptability ensures organizations can extend their AI initiatives smoothly as required.

Embrace IBM z17 to redefine your enterprise's AI strategy, blending advanced technologies with a secure and scalable infrastructure for sustainable growth and innovation. The robust security framework of IBM z17 harmonizes its advanced encryption functions with sophisticated anomaly detection mechanisms, featuring:

- **Encryption**: Utilizing 256-bit AES encryption across the inter-drawer connections, IBM z17 secures data integrity while preserving observability for detecting anomalous activities. This comprehensive encryption allows the anomaly detection system to inspect encrypted data streams for unusual patterns without compromising security protocols.
- **AI-driven Anomaly Analysis**: Equipped with an Integrated AI Accelerator and optional Spyre Accelerator, IBM z17 leverages advanced machine learning models for real-time examination of encrypted traffic, system behaviors, and user actions. This AI-enhanced approach identifies subtle anomalies often missed by conventional rule-based systems, thereby strengthening defenses against stealthy threats.

IBM z17 stands at the forefront of enterprise AI, offering a secure, scalable environment that supports rapid innovation and precise predictive capabilities while ensuring regulatory compliance.

1.3.2 Maximizing efficiency gains on IBM z17 through transformative automation

IBM z17 offers several distinct features that contribute to efficiency gains:

- **AI-driven Automation**: Built-in AI capabilities automate repetitive tasks, allowing employees to focus on higher-value work. Features like Autonomics and z/OS Container Extensions (zCX) streamline operations by automating routine maintenance, updates, and scaling processes.
- **Enhanced Processing Power**: The advanced processor design of IBM z17 provides unparalleled performance for transactional workloads. This results in faster processing times and improved efficiency across critical business applications.
- **Scalable Infrastructure**: With its modular architecture, IBM z17 offers unmatched scalability. The system allows businesses to add or remove resources seamlessly, ensuring optimal performance during peak demands while minimizing costs during low-activity periods. This flexibility supports efficient resource management and cost control.
- **Advanced Security & Compliance**: Robust security features, including Pervasive Encryption and hardware-based cryptographic capabilities, protect sensitive data without impacting performance. This ensures compliance with stringent regulatory requirements while maintaining efficiency in data handling and transmission.
- **Resilient & Reliable Operations**: IBM z17 is engineered for uninterrupted service, offering advanced availability features like Parallel Sysplex and Geographically Dispersed Parallel Sysplex (IBM GDPS®). These capabilities minimize downtime and ensure business continuity, directly contributing to operational efficiency.

By leveraging these specific features of IBM z17, businesses can achieve substantial efficiency gains through accelerated processing, automated operations, scalable infrastructure, seamless cloud integration, robust security, and uninterrupted service delivery.

1.3.3 Safeguarding Vital Assets with IBM z17 for data security mastery

IBM z17 offers a multitude of robust features designed to safeguard vital assets and ensure data security mastery:

- **Pervasive Encryption**: This feature encrypts data at rest, in flight, and in use across various components, providing comprehensive protection without compromising performance. It covers databases, applications, storage devices, and even network traffic, ensuring that sensitive information remains secure throughout its lifecycle.
- **Hardware-based Cryptographic Capabilities**: IBM z17 incorporates dedicated hardware for cryptographic operations, offloading these tasks from the main processors. This not only enhances security but also maintains system performance by preventing encryption and decryption processes from slowing down critical applications.
- **Tamper-resistant Hardware**: IBM z17 employs tamper-resistant hardware designs to deter physical intrusion attempts. This includes features like intrusion detection sensors and tamper-responsive mechanisms that can automatically respond to unauthorized access attempts, ensuring the integrity of data stored within the system.
- **Compliance with Regulatory Standards**: IBM z17 is engineered to meet stringent global compliance requirements for data protection, such as GDPR, HIPAA, and PCI DSS. It provides audit-ready logging and reporting capabilities, which are crucial for demonstrating adherence to regulatory standards and conducting internal security reviews.
- **Integrated Security Management**: IBM z17 offers centralized security management tools that simplify the administration of security policies across the enterprise. This includes features like Role-Based Access Control (RBAC) for fine-grained access management, and unified policy enforcement mechanisms to ensure consistent application of security measures across diverse environments.

By leveraging these robust security features, IBM z17 empowers organizations to achieve a high standard of data security mastery, effectively safeguarding vital assets from a wide array of threats while maintaining operational efficiency and regulatory compliance.

The IBM z17 capabilities that underpin these use cases are described in more detail in Chapter 4, “IBM z17 system design strengths” on page 41.

2

IBM z17 ME1 hardware overview

This chapter expands on the descriptions of the key hardware components of IBM z17 ME1 that are introduced in 1.2, "IBM z17 technical highlights" on page 3.

This chapter describes the following topics:

2.1 IBM z17 ME1 upgrade paths

IBM z17 ME1 is built by using the IBM Telum II processor design. Each processor chip consists of eight cores. Two processor chips are packaged in the dual-chip module (DCM). Each DCM can have 9 - 11 or 10 - 15 active processor unit (PU) cores, depending on the configuration. With IBM z17 ME1, the maximum number of characterizable processors is represented by the feature names (see Table 2-1): Max43, Max90, Max136, Max183, and Max208. Spare PUs, System Assist Processors (SAPs), and two Integrated Firmware Processors (IFPs) are included in the IBM z17 ME1 configuration.

The number of characterizable PUs, SAPs, and spare PUs for the various features is listed in Table 2-1. For more information about PU characterization types, see “PU characterization” on page 19.

Table 2-1 IBM z17 ME1 processor unit configurations

Feature name	Number of CPC drawers	Feature Code	Characterizable processor units	SAPs	Spares
Max43	1	0571	0 - 43	5	2
Max90	2	0572	0 - 90	10	2
Max136	3	0573	0 - 136	16	2
Max183	4	0574	0 - 183	21	2
Max208	4	0575	0 - 208	24	2

IBM z17 ME1 ensures continuity and upgrades from IBM z16 A01and IBM z15 T01. The supported upgrade paths are shown in Figure 2-1.

.

Figure 2-1 IBM z17 ME1 upgrade paths

If an upgrade request cannot be fulfilled by using the existing configuration, a hardware upgrade is required in which one or two CPC drawers are added to accommodate the necessary capacity. With IBM z17 ME1, CPC drawers can be installed concurrently from a Max43 to a Max90, and to a Max136.

Note: No field upgrade is available to a Max183 or a Max208; these two features are factory-shipped only.

With IBM z17 ME1, concurrent upgrades are available for central processors (CPs), Integrated Facilities for Linux (IFLs), Integrated Coupling Facilities (ICFs), and IBM Z Integrated Information Processors (zIIPs). However, concurrent PU upgrades require that more PUs are physically installed but not activated previously.

In the rare event of a PU failure, one of the spare PUs is immediately and transparently activated and assigned the characteristics of the failing PU. Two spare PUs are always available on an IBM z17 ME1.

IBM z17 ME1 offers 337 capacity levels. In all, 208 capacity levels are based on the number of physically used CPs, plus up to 129 subcapacity models for the first 43 CPs.

For more information, see 4.3.1, “Capacity settings” on page 50.

2.2 Frames and cabling

The IBM z17 ME1 employs 19-inch frames and adheres to industry-standard power and hardware norms. Configurable as a one-through four-frame system, it occupies merely two standard 24-inch (60-centimeter) floor tiles per frame, perfectly suiting contemporary data center layouts.

The IBM z17 configuration options as compared to previous IBM Z servers are listed in Table 2-2.

Table 2-2 IBM z17 ME1 configuration options compared to IBM z16 A01 and IBM z15 T01 configurations

System	Number of frames	Number of CPC drawers	Number of I/O drawers	I/O and power connections	Power options[a]	Cooling options
IBM z17 ME1	1 - 4	1 - 4	0 - 12	Rear only	PDU only	Radiator (air) only
IBM z16 A01	1 - 4	1 - 4	0 - 12[b]	Rear only	PDU or BPA	Radiator (air) only
IBM z15 T01	1 - 4	1 - 5	0 - 12[b]	Rear only	PDU or BPA	Radiator (air) or water-cooling unit (WCU)

a. The power distribution unit (PDU) option supports the air-cooling (radiator) option. The Bulk Power Assembly (BPA) option supports both air-cooling and water-cooling options.
b. Maximum of 12 if ordered with the PDU option or maximum of 11 if ordered with the BPA option.

The number of Peripheral Component Interconnect Express+ (PCIe+) I/O drawers can vary based on the number of I/O features, and number of CPC drawers that is installed. For a maximum configuration up to 12 PCIe+ I/O drawers can be installed. PCIe+ I/O drawers can be added concurrently.

Additionally, IBM z17 ME1 supports top-exit options for the fiber-optic and copper cables that are used for I/O and power. These options give you more flexibility in planning where the system is installed, eliminate the need for cables to be run under a raised floor, and increase air flow over the system.

IBM z17 ME1 supports installation on raised floor and non-raised floor environments.

Figure 2-2 shows the front view of a fully configured IBM z17 ME1 with radiator cooling, four CPC drawers, and 12 PCIe+ I/O drawers.

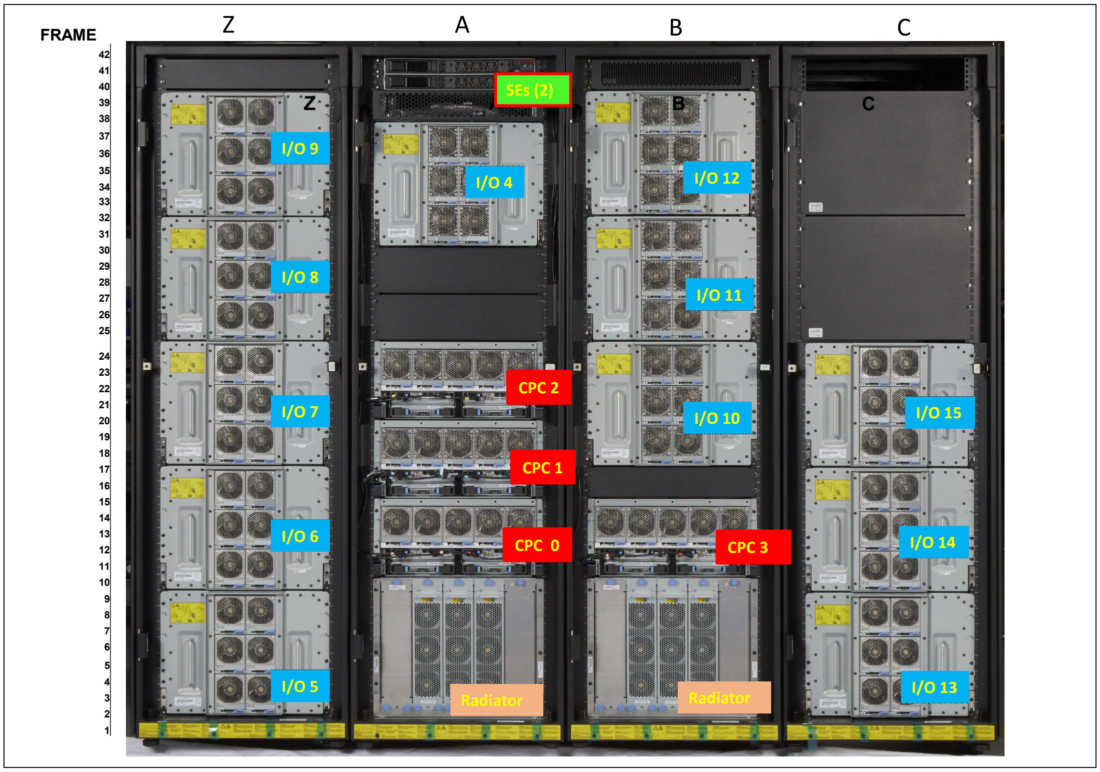

Figure 2-2 Front view of a fully configured IBM z17 ME1 with radiator cooling

Figure 2-3 shows the rear view of a fully configured IBM z17 ME1 with a total of 16 drawers (I/O and CPC combined), and two radiator cooling units.

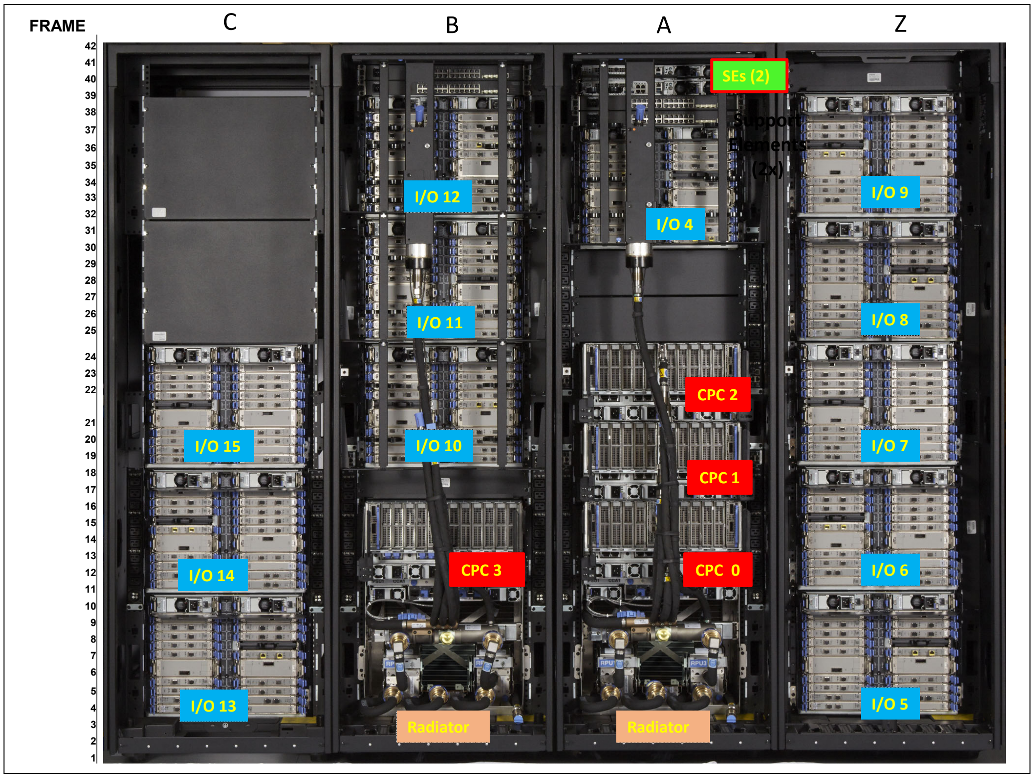

Figure 2-3 Rear view of a fully configured IBM z17 ME1

During the ordering process, the IBM configurator determines the necessary frame count and optimally positions CPC and PCIe+ I/O drawers.

Factors that determine the number of frames for an IBM z17 ME1 configuration include the following features:

- Number of CPC drawers
- Plan-ahead features for more CPC drawers
- Number of I/O features (determines the number of PCIe+ I/O drawers)
- Number of PDUs

2.3 CPC drawers

IBM z17 ME1 can be configured with up to four CPC drawers (three in the A Frame and one in the B Frame). Each CPC drawer contains the following elements:

- DCMs:

  Four DCMs with internal water loops providing dedicated cooling for every PU chip.

- Memory:
  - The memory allocation ranges from a base 512 GB to an extended 64 TB with four CPC drawer configurations, excluding the 884 GB reserved for the hardware system area (HSA). For more information, see Table 2-3 on page 20.
  - A CPC drawer can accommodate up to 48 dual inline memory modules (DIMMs), ranging in capacity from 32, 64, 128, 256, or 512 GB each.
- Fanouts:

  Each CPC drawer supports up to 12 Gen4 PCIe+ fanout adapters to connect to the Gen4 PCIe+ I/O drawers, and contains Integrated Coupling Adapter Short Reach (ICA SR) coupling links:

  - A 2-port Peripheral Component Interconnect Express (PCIe) 32 GBps I/O fanout. Each port supports one domain in the 16-slot Gen4 PCIe+ I/O drawers.
  - ICA SR2.0 PCIe fanouts for coupling links (two links of 8 GBps each).
- Four Power Supply Units (PSUs) that provide power to the CPC drawer and are accessible from the rear. Loss of one PSU leaves enough power to satisfy the power requirements of the entire drawer. The PSUs can be concurrently maintained.
- Two dual-function Base Management Cards (BMCs) or Oscillator Cards (OSCs) that provide redundant interfaces to the internal management network and provide clock synchronization to the IBM Z platform.
- Two dual-function Processor Power Cards (PPCs) that control Voltage Regulation, PSUs, and Fans. The PPCs are redundant and can be concurrently maintained.
- The CPC drawer features five front-mounted fans, ensuring efficient airflow and cooling for all components except the PU DCMs, which are internally cooled by using a water loop.

The CPC drawer communication topology is shown in Figure 2-4 on page 17. All CPC drawers are interconnected with high-speed communication link Symmetric multiprocessor-10 (SMP-10) Assemblies (A-Bus) directly attached to the DCMs. The SMP-10 cables are used to interconnect all the CPC drawers. The X-Bus provides connectivity between DCMs on the drawer, while the M-Bus connects the two PU chips on each DCM.

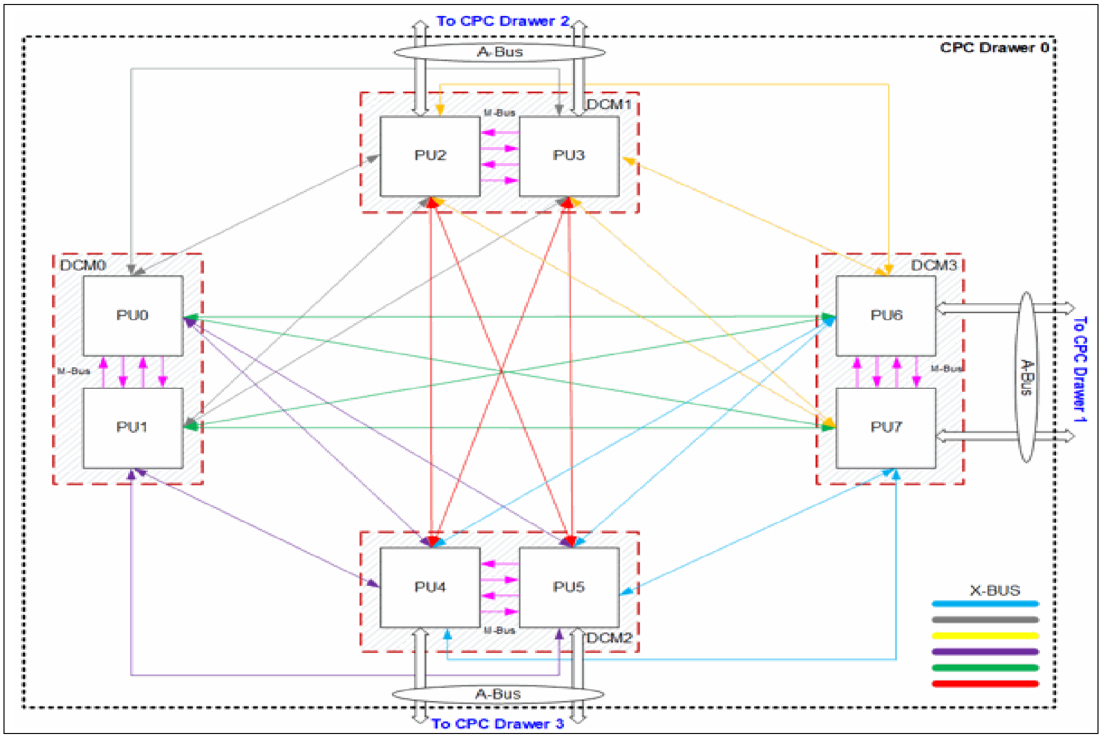

Figure 2-4 IBM z17 ME1 CPC drawer communication topology

Leveraging a dedicated connection between the PU and storage controls, the IBM Processor Resource/Systems Manager facility (PR/SM) enables seamless operation and management of this memory-coherent Symmetric Multiprocessing (SMP) system.

2.3.1 Dual-chip modules

A DCM contains two PU chips. Each PU chip contains eight general purpose PUs with a 128 KB Instruction and Data L1 cache and 10x 36 MB semi-private L2 caches. Each PU chip also has one Data Processing Unit (DPU) I/O Engine with access to the semi-private L2 caches for PCIe Gen5 x16 I/O operations.

2.3.2 Processor unit

PU is the generic term for an IBM z/Architecture® processor. Each PU is a superscalar processor with the following attributes:

- Up to six instructions can be decoded per clock cycle.
- Up to 10 instructions can run per clock cycle.
- Instructions can be issued out of order. The PU uses a high-frequency, low-latency pipeline that provides robust performance across a wide range of workloads.
- Memory accesses might not be in the same instruction order (out-of-order operand fetching).
- Most instructions flow through a pipeline with a varying number of steps for different types of instructions. Several instructions can be running at any moment, and they are subject to the maximum number of decodes and completions per cycle.

Processor cache structure

The on-chip cache for the PU (core) features the following design:

- Each PU core has an L1 cache (private) that is divided into a 128 KB cache for instructions and a 128 KB cache for data.
- Each PU core has a semi-private L2 cache of 36 MB, which is located next to the core.

> **Note:** L1 and L2 are physical cache and implemented in dense SRAM.

- Each PU chip contains 360 MB shared-victim virtual L3 cache, available to each PU core. The shared-victim virtual L3 cache is a logical construction that comprises all ten semi-private L2s (10 x 36 MB = 360 MB) belonging to all cores on the same chip[1].
- Each CPC drawer contains a 2.8 GB shared-victim virtual L4, consisting of all virtual L3 caches of the DCMs in the CPC drawer.

This on-chip cache implementation optimizes system performance for high-frequency processors and includes the following features:

- Cache improvements
- New translation and TLB2 design
- Pipeline optimizations
- Better branch prediction
- New accelerators and architectures
- Secure Execution support

The IBM z17 ME1 cache structure is shown Figure 2-5.

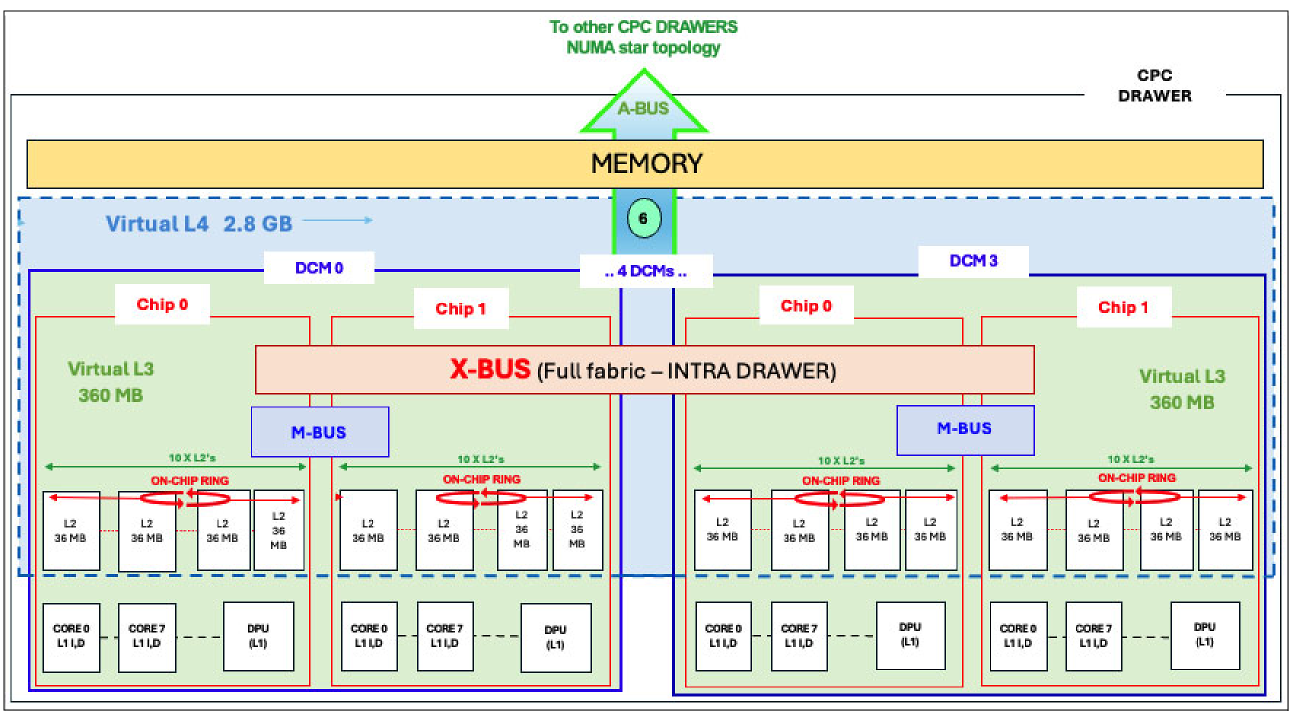

Figure 2-5 IBM z17 ME1 cache structure

[1] There are ten L2s in the pool (one per PU), plus one additional L2 to serve the DPU and one as part of the PU L2 pool.

PU sparing

Hardware fault detection is embedded throughout the system design and combined with comprehensive instruction-level retry and dynamic PU sparing. This function provides the reliability and availability that is required for true IBM Z integrity.

On-core cryptographic hardware

Dedicated cryptographic hardware for each PU core includes extended key and hash sizes for the Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA). For more information, see 3.7, "Cryptography" on page 35. This cryptographic hardware is available with any processor type.

On-chip functions

Key on-chip dedicated coprocessors and accelerators to consider are:

- IBM Integrated Accelerator for Artificial Intelligence is designed for high-speed, real-time inferencing at scale.
- Data Processing Unit (DPU) helps improve I/O channel throughput along with improved I/O density.
- Central Processor Assist for Cryptographic Functions (CPACF) encrypts large amounts of data in real time.
- IBM Integrated Accelerator for IBM Z Sort uses the sort instruction (`SORTL`) to accelerate the sorting of data.
- IBM Integrated Accelerator for zEnterprise Data Compression is for data compression as defined by RFC195.

Software support

IBM z17 ME1 Processors (PUs) ensure complete compatibility with z/Architecture software while expanding the Instruction Set Architecture (ISA). These enhancements unlock improved functionality and enhanced performance, introducing new Artificial Intelligence Unit (AIU) instructions on the IBM z17 ME1.

PU characterization

PUs are ordered in single increments. The internal system functions are based on the configuration that is ordered. They characterize each PU into one of various types during system initialization, which is often called a power-on reset (POR) operation.

Characterizing PUs dynamically without a POR is possible by using a process that is called *Dynamic Processor Unit Reassignment*. A PU that is not characterized cannot be used. Each PU can be designated with one of the following characterizations:

- Central Processor (CP): these standard processors are used for general workloads.
- Integrated Facility for Linux (IFL): designates processors to be used specifically for Linux natively or on top of a hypervisor like IBM z/VM® or KVM.
- Unassigned Integrated Facilities for Linux (uIFL): allows you to directly purchase an IFL feature that is marked as being deactivated upon installation, which avoids software charges until the IFL is brought online for use.
- zIIP: an "Off Load Processor" that is used under z/OS for designated types of workloads. For a list of zIIP use candidates, see "Logical Processors" on page 46. zIIP also is used for the IBM System Recovery Boost (SRB) feature. For more information, see 4.7.3, "IBM Z System Recovery Boost" on page 59.

- Unassigned zIIP: a processor that is purchased for future use as a zIIP. It is offline and cannot be used until an upgrade for the zIIP is installed. It does not affect software licenses or maintenance charges.
- Integrated Coupling Facility (ICF): designates processors to be used specifically for Coupling Facility partitions. Coupling Facility partitions can run on shared or dedicated ICF processors, or on shared CP processors. On z17, the use of dedicated CP processors for Coupling Facility partitions was eliminated.
- Unassigned Integrated Coupling Facility (uICF): procure a deactivated feature during installation for later use.
- SAP: designates processors to be used specifically for assisting I/O operations.

Prior to acquiring zIIPs, at least one CP must be purchased. The maximum number of zIIPs available is limited to one fewer than the system's maximum PU configuration; for instance, IBM z17 ME1 Max208 can support up to 207 zIIPs. These guidelines apply similarly to unassigned zIIPs and IFL processors.

Converting a PU from one type to any other type is possible by using the Dynamic Processor Unit Reassignment process. These conversions occur concurrently with the system operation.

Note: The addition of ICFs, IFLs, and zIIPs does not change the system capacity setting or its millions of service units (MSU) rating.

2.3.3 Memory

The maximum physical memory size is directly related to the number of CPC drawers in the system. An IBM Z server includes more installed memory than was ordered because part of the installed memory is used to implement the redundant array of independent memory (RAIM) design. With IBM z17 ME1, up to 16 TB of memory per CPC drawer can be ordered, and up to 64 TB for a four-CPC drawer system.

Important: z/OS requires a minimum of 8 GB of memory (2 GB of memory when running under z/VM). z/OS V3R1 can support up to 16 TB of memory in an LPAR.

The minimum and maximum memory sizes for each IBM z17 ME1 feature are listed in Table 2-3.

Table 2-3 IBM z17 ME1 memory per feature

Feature name	CPC drawers	Memory
Max43 (Feature Code 0571)	1	512 GB - 16 TB
Max90 (Feature Code 0572)	2	512 GB - 32 TB
Max136 (Feature Code 0573)	3	512 GB - 48 TB
Max183 (Feature Code 0574)	4	512 GB - 64 TB
Max208 (Feature Code 0575)	4	512 GB - 64 TB

The HSA on IBM z17 ME1 has a fixed amount of memory (884 GB) that is managed separately from customer available memory.

However, the maximum amount of orderable memory can vary from the theoretical number because of dependencies on the memory granularity. On IBM z17 ME1, the granularity for memory is in 64, 128, 256, 512, 1024, and 2048 GB increments.

Physically, the memory is organized in the following ways:

- A CPC drawer always contains a minimum of 1024 GB to a maximum of 16 TB of installed memory.
- A CPC drawer can have more installed memory than is enabled. The excess memory can be enabled by a Licensed Internal Code (LIC) load.
- Memory upgrades are first satisfied by activating installed but unused memory capacity until it is exhausted. When no more unused memory is available from the installed cards, the cards must be upgraded to a higher capacity (replacing existing memory cards/DIMMs in the CPC drawer). Other options are when adding additional DIMMs into an existing drawer or when an additional CPC drawer with more memory must be installed (if permitted by the configuration).

Upon LPAR activation, PR/SM strives to assign PUs and memory within a single CPC drawer. If this allocation proves unfeasible, PR/SM can then utilize memory resources from any available CPC drawer. For instance, should the allocated PUs extend across multiple drawers, PR/SM will attempt to allocate memory from those specific drawers, even if sufficient memory exists in only one of them.

No matter which CPC drawer the memory is installed in, an LPAR can access that memory after it is allocated. IBM z17 ME1 is an SMP system because the PUs can access all of the available memory.

A memory upgrade is considered to be concurrent when it requires no change of the physical memory cards. A memory card change is disruptive when no use is made of Enhanced Drawer Availability (EDA). In a multiple-CPC drawer system, a single CPC drawer can be concurrently removed and reinstalled for a repair with EDA.

For model upgrades that involve the addition of a CPC drawer, the minimum usable memory increment (512 GB) is added to the system. During an upgrade, adding a CPC drawer and physical memory in the new drawer are concurrent operations.

Concurrent memory upgrade

When unused capacity is available on the installed memory cards, the total system memory can be upgraded concurrently through Licensed Internal Code Configuration Control (LICCC). The LICCC provides for system upgrades without hardware changes by activating extra (physically installed) unused capacity.

Redundant array of independent memory

RAIM technology makes the memory subsystem (in essence) a fully fault-tolerant N+1 design. The RAIM design automatically detects and recovers from failures of dynamic random access memory (DRAM), sockets, memory channels, or DIMMs.

The RAIM design is fully integrated in IBM z17 ME1 and enhanced to include one Memory Controller Unit (MCU) per processor chip, with eight memory channels and one DIMM per channel. The MCU enables memory to be implemented as RAIM. This technology has significant reliability, availability, and serviceability (RAS) capabilities in the area of error correction. Bit, lane, DRAM, DIMM, socket, and complete memory channel failures (including many types of multiple failures) can be detected and corrected.

For more information about memory design and configuration options, see *IBM z17 (9175) Technical Guide*, SG24-8579.

2.3.4 Hardware system area

The HSA is a fixed-size, reserved area of memory that is separate from the customer-purchased memory. The HSA is used for several internal functions, but the bulk of it is used by channel subsystem (CSS) functions.

Featuring a fixed-size 884 GB HSA, IBM z17 ME1 provides ample capacity to accommodate LPAR definitions or modifications, significantly reducing outage occurrences, and necessitating minimal planning.

A fixed, large HSA allows the dynamic I/O capability of IBM z17 ME1 to be enabled by default. It also enables the dynamic addition and removal of the following features:

- An LPAR to a new or existing CSS
- Devices, up to the maximum number permitted, in each subchannel set
- Logical processors by type
- Cryptographic adapters

2.4 I/O system structure

IBM z17 ME1 supports the PCIe-based infrastructure for the PCIe+ I/O drawers. The PCIe I/O infrastructure consists of the dual-port PCIe fanouts in the CPC drawers that support 32 GBps connectivity to the PCIe+ I/O drawer.

Ordering of I/O features: Ordering I/O feature types determines the suitable number of PCIe+ I/O drawers.

Figure 2-6 on page 23 shows a high-level view of the I/O system structure for IBM z17 ME1.

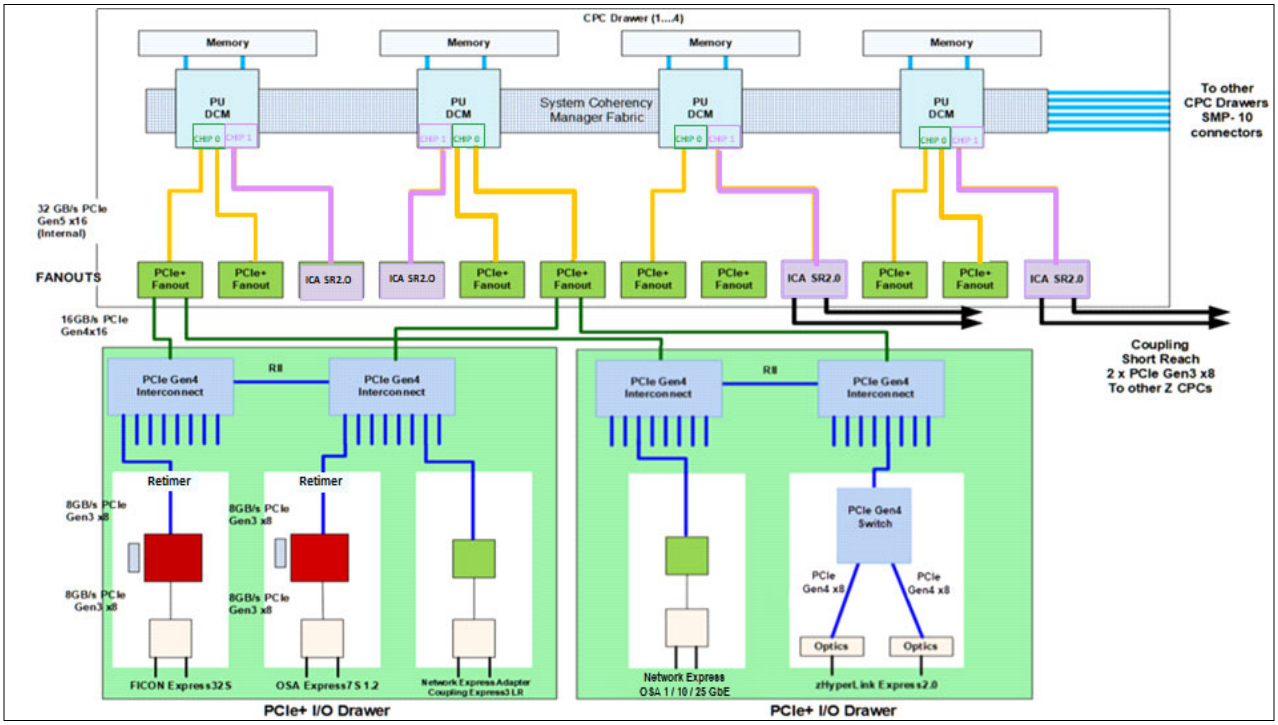

Figure 2-6 IBM z17 ME1 I/O system structure

The IBM z17 ME1 CPC drawer contains 12 fanout positions (LG01 through LG12). These slots can accommodate either:

- Dual-port PCIe+ fanouts for connecting to a PCIe+ I/O drawer
- ICA SR2.0 fanouts for coupling purposes
- Filler plates to assist with airflow cooling

For coupling link connectivity (IBM Parallel Sysplex and IBM Server Time Protocol (STP) configuration), IBM z17 ME1 supports the following link types:

- ICA SR2.0, to be installed in a CPC drawer
- Coupling Express3 Long Reach (CE LR), for installation within a PCIe+ I/O drawer

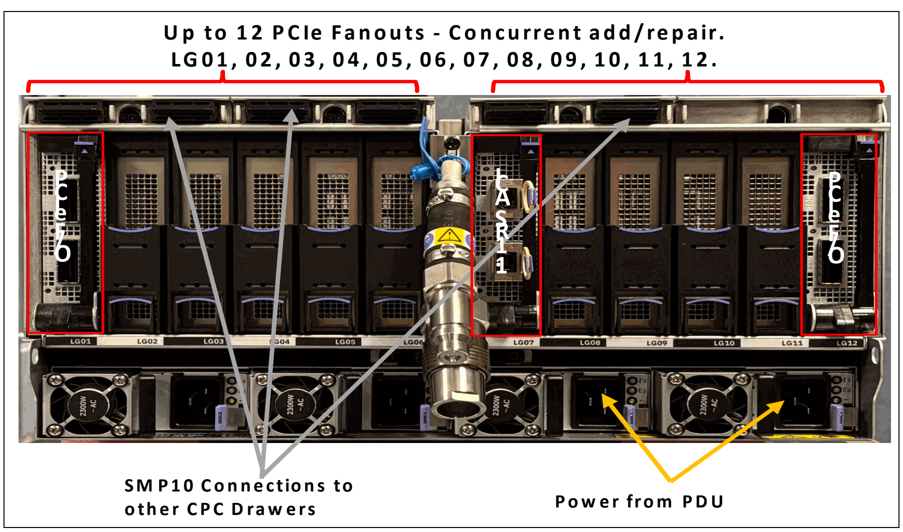

Figure 2-7 IBM z17 ME1 CPC drawer: Rear view

The PCIe+ I/O drawer (see Figure 2-8), is a 19-inch single side drawer that is 8U high. I/O features are installed horizontally, with cooling air flow from front to rear. The drawer contains 16 adapter slots and two slots for PCIe switch cards.

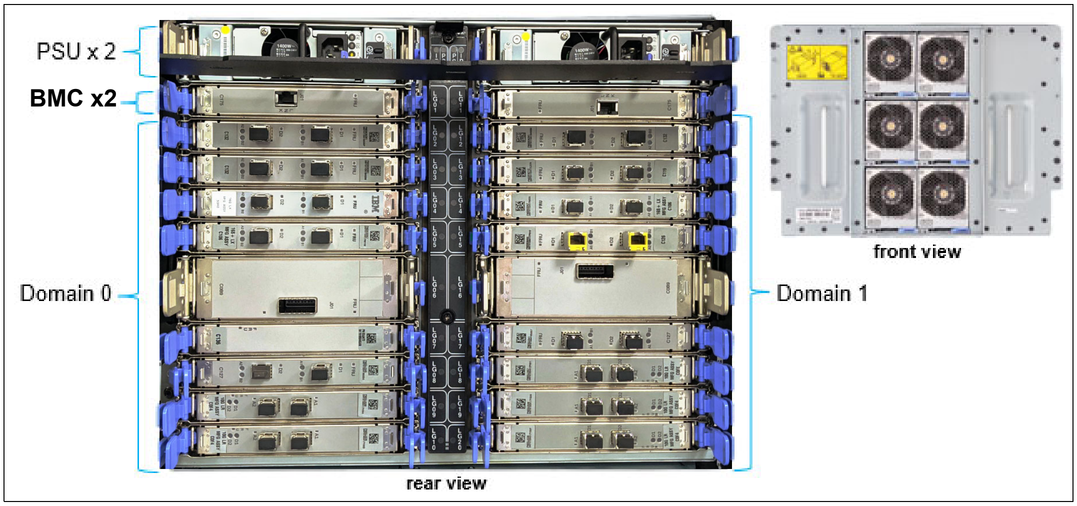

Figure 2-8 PCIe+ I/O drawer: Rear and front view

The two I/O domains per drawer each contain up to eight I/O features that support the following types:

- FICON Express32-4P, FICON Express32S, or FICON Express16SA
- OSA-Express7S 1.2 and OSA-Express7S
- Crypto-Express8S and Crypto-Express7S
- Network Express
- zHyperLink Express 2.0
- Coupling Express3 LR
- IBM Spyre Accelerator

For more information about the I/O features that are available with IBM z17 ME1, see Chapter 3, “IBM z17 supported features and functions” on page 27.

2.5 Power and cooling

IBM z17 ME1 meets the American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE) Class A3 specifications. ASHRAE is an organization that is devoted to the advancement of indoor-environment-control technology in the heating, ventilation, and air-conditioning industry.

2.5.1 Power options

The IBM z17 19-inch frames are available with the PDU power (BPA is not supported):

Using PDU for IBM z17 ME1 can enable fewer frames, which allows for extra I/O slots and improves power efficiency to lower overall energy costs. It offers some standardization and ease of data center installation planning. PDU-based system supports up to 12 PCIe+ I/O drawers. The loss of one power supply per set has no effect on system operation.

Depending on the configuration, the IBM z17 ME1 requires 2 to 8 PDU connections for full redundancy. Power cords support attachment to either 200-208V 30/60A 3 Phase (Low Voltage) or 380-415V 32A 3 Phase Wye (High Voltage).

Consider the following points about power:

- A total of one to four 42U 19-inch IBM frames are used.
- Air flow is front to rear. All blowers are mounted on the front of the frame.
- All external power cabling is at the rear of the frames (no power cabling in front).
- Top or bottom exit power is supported.
- No Emergency Power Off (EPO) switch is used.
- PDUs are different for Low Voltage vs High Voltage (never plug a High Voltage source to a Low Voltage PDU)

Specific power requirements depend on the number of frames, CPC drawers, and type of I/O features that are installed, which will dictate the number of PDUs necessary.

For more information about the maximum power consumption tables for the various configurations and environments, see *IBM 9175 Installation Manual for Physical Planning*, GC28-7049.

For more information about the power and weight estimation tool, see IBM Resource Link®.

2.5.2 Cooling options

The IBM z17 ME1 cooling system is available only with the Radiator (air) cooling option. The previous customer water-cooling solution that was available with IBM z15 is not offered with IBM z17.

DCMs are always cooled with an internal (closed) coolant loop. The liquid in the internal system is cooled by using an internal radiator. The radiator, PCIe+ I/O drawers, power enclosures, and CPC drawers are cooled by chilled air with blowers.

The air-cooling system in IBM z17 ME1 is redesigned for better availability and lower cooling power consumption. The radiator design is a closed-loop coolant pump system for the DCMs in the CPC drawers. It is designed with N+1 pumps, reservoir, blowers, controls, and sensors. The radiator unit is cooled by air.

The cooling loop liquid for IBM z17 ME1 is a Propylene Glycol + Water Solution instead of the previously used water solution. Systems will ship prefilled and sealed from manufacturing. The previous Fill Drain Tool and BTA water jugs are eliminated.

3

IBM z17 supported features and functions

IBM Z features and functions that are supported on IBM z17 are highlighted in this chapter. The information provided expands on the key hardware elements that are introduced in Chapter 1, “Attaining outcomes and driving value with the IBM z17” on page 1 and Chapter 2, “IBM z17 ME1 hardware overview” on page 11.

For more information about the key capabilities and enhancements, see *IBM z17 (9175) Technical Guide*, SG24-8579. For details on the I/O features and functions, see *IBM Z Connectivity Handbook*, SG24-5444.

This chapter describes the following topics:

3.1 IBM z17 I/O connectivity overview

IBM z17 provides a Peripheral Component Interconnect Express (PCIe)-based infrastructure for the PCIe+ I/O drawers to support the following features:

- Storage connectivity:
  - zHyperLink Express2.0 (new build only)
  - FICON Express32-4P (new build only)
  - FICON Express32S (carry forward only)
  - FICON Express16SA (carry forward only)
- Network connectivity:
  - Network Express 25G (new build only)
  - Network Express 10G (new build only)
  - OSA-Express7S 1.2 (new build or carry forward)
  - OSA-Express7S (carry forward)
  - OSA Express 1000BASE-T 7S (carry forward from IBM z15 only)
- Clustering connectivity:
  - Integrated Coupling Adapter2.0 (ICA SR2.0) (new build only)
  - Two types of Coupling Express3 Long Reach (LR) (new build only):
    - Coupling Express3 LR 25G
    - Coupling Express3 LR 10G
- Cryptographic features:
  - Crypto Express8S, one or two hardware security modules (new build or carry forward)
  - Crypto Express7S, one or two hardware security modules (carry forward only)

More information about these features is provided in IBM Z Functional Matrix, REDP-5157 and IBM Z Connectivity Handbook, SG24-5444.

The following features that were supported on earlier IBM Z platforms are *not* orderable and *cannot* be carried forward to IBM z17:

- zHyperLink Express1.1 and zHyperLink Express
- FICON Express16S+, FICON Express16S, and FICON Express8S
- OSA Express6S and OSA-Express5S
- RoCE Express3, RoCE Express2.1, and RoCE Express2
- Crypto Express6S and Crypto Express5S
- IBM zEnterprise Data Compression (zEDC)
- Coupling Express2 LR and Coupling Express LR
- ICA SR1.1 and ICA SR

> **Note:** The LC Duplex connector type is used for all fiber optic cables, except the cables used for zHyperLink Express, and ICA SR2.0 connections, which have multi-fiber termination push-on (MTP) connectors.

3.2 Introducing the IBM z17 I/O design

The IBM Z platform is designed to meet the growing demands of modern businesses by providing advanced features and functions that enhance I/O throughput and connectivity. The IBM Z I/O stack for storage and network connectivity has advanced on application-specific integrated circuit (ASIC) chips for over 30 years. With IBM z17, a novel I/O design featuring a Data Processing Unit (DPU) is introduced to enhance performance and boost I/O rates for FCP, FICON, High Performance FICON, and OSA protocols. The DPU is an on-chip processor that integrates I/O acceleration directly onto the Telum II processor.

The DPU consists of 32 cores organized into four clusters of eight, executing firmware utilizing a standard instruction set architecture tailored to address IBM Z-specific I/O requirements. A PCIe Bridge Unit (PBU) offers system memory access, previously mediated by data routers in ASIC chips for prior IBM Z I/O features.

The architecture integrates additional offload/accelerator engines for both I/O and non-I/O functions alongside enhanced infrastructure management capabilities, underscoring its adaptability and future-readiness.

The IBM z17 also doubles port density for storage and network connectivity features, underscoring commitment by IBM to energy efficiency and capacity expansion.

> **Note:** Storage and network connectivity features on IBM z17, excluding those leveraging the Data Processing Unit (DPU), will continue to in utilize the ASIC chip design and I/O operations similar to IBM z16 and previous systems.

3.3 Storage connectivity

Storage connectivity is achieved through a variety of methods, including direct storage attachment to Storage Area Networks (SANs). The main focus for storage connectivity with IBM Z is to continuously improve the latency for I/O transmission. The new I/O design, including the DPU and the FICON Express32-4P (4-port feature), embodies that goal as does zHyperLink Express.

3.3.1 FICON Express features

FICON Express features in IBM z17 evolve, offering enhanced throughput, reliability, availability, and serviceability (RAS). In IBM z17, these features can provide connectivity to other systems, such as Fibre Channel (FC) switches and various devices in a SAN environment.

FICON Express features follow the established Fibre Channel (FC) standards to support data storage and access requirements, along with the latest FC technology in storage and access devices.

FICON Express features support the following protocols:

- FICON

  This enhanced protocol provides for communication across SAN Fabric switches, channel to channel (CTC) connectivity, and with FICON devices, such as disks, tapes, and printers.

- High Performance FICON

  The FICON Channel Enhancement boosts FICON channel performance by shifting I/O management tasks from the channel subsystem to the controller and host adapter, thereby optimizing system efficiency.

- Fibre Channel Protocol (FCP)

  This standard protocol is used for communicating with disk and tape devices through FC switches and directors. The FCP channel can connect to FCP SAN fabrics and access FCP and SCSI devices.

The FICON Express32-4P feature makes use of the DPU to move data to and from memory and storage devices. It supports the same protocols as its predecessor (FICON Express32S), but with higher port density (four versus two). Both features support a link data rate up to 32 Gbps and can auto-negotiate to 8, 16, or 32 Gbps.

The FICON Express32S implements PCIe cards, providing enhanced port granularity and superior capabilities compared to preceding FICON Express features.

3.3.2 zHyperLink Express

zHyperLink was created to provide fast access to data through low-latency connections between the IBM Z platform and storage.

With the zHyperLink Express2.0 feature, you can make synchronous requests for data that is in the storage cache of the IBM DS8000®. This process is done by directly connecting the zHyperLink Express2.0 port in the IBM z17 to an I/O bay port of the IBM DS8000. This short-distance (up to 150 m (492 feet)), direct connection is designed for low-latency read/write, such as with IBM Db2 for z/OS synchronous I/O reads and log writes.

zHyperLink has the ability to process more than 4K data transfers in a synchronous fashion, which is new for IBM z17, allowing additional software usage that was not possible with only data transfers of 4K or less.

Working in conjunction with the FICON SAN Infrastructure, zHyperLink improves application response time, which reduces I/O-sensitive workload response time by half without requiring application changes.

> **Note:** The zHyperLink channels complement FICON channels, but they do *not* replace FICON channels. FICON remains the main data driver and is mandatory for zHyperLink usage.

3.4 Network connectivity

Network connectivity covers the connections between the platform and external networks with Network Express (2-port features) and Open Systems Adapter-Express (OSA-Express) features. Intra-system communication is provided through IBM HiperSockets and Internal Shared Memory (ISM).

The new I/O design for network connectivity, including the DPU and the Network Express features, improves data transmission latency.

> **Note:** OSA-Express7S features are supported with the IBM z17. However, OSA-Express features can be replaced by Network Express features.
>
> IBM z17 does not support RoCE Express features; instead, it utilizes Network Express features.

3.4.1 Network Express and OSA-Express features

Network Express and OSA-Express features provide local area network (LAN) connectivity and comply with IEEE standards. Additionally, those features assume several functions of the TCP/IP stack that normally are performed by the processor unit (PU), which provides performance benefits by offloading processing from the operating system. For the Network Express feature these functions of the TCP/IP stack are handled by the DPU.

The OSA-Express and Network Express features continue to support fiber optic (single-mode and multimode) environments. The IBM z17 is the last generation to support copper connections and *only* through the OSA-Express7S 1000BASE-T, which is available as carry forward from IBM z15.

In addition to the traditional network connectivity, the Network Express feature is simultaneously able to provide fast memory-to-memory communications between two IBM Z servers using Remote Direct Memory Access (RDMA) over Converged Ethernet (RoCE).

These features help reduce consumption of CPU resources for applications that use the TCP/IP stack (such as IBM WebSphere®, which accesses an IBM Db2® database). These features can also help reduce network latency with memory-to-memory transfers by using Shared Memory Communications over RDMA (SMC-R).

With SMC-R, you can transfer very large amounts of data quickly and at low latency. SMC-R is transparent to the application and requires no code changes, which enables rapid time to value.

3.4.2 IBM HiperSockets

Referred to as the “network in a box”, IBM HiperSockets simulate local area network (LAN) environments exclusively within IBM Z servers. It enables direct data transfer between logical partition (LPAR) memories, facilitated by IBM Z firmware.

A component of the Licensed Internal Code (LIC), HiperSockets offers LAN connectivity across various system images within an IBM Z platform through secure, memory-to-memory data transfers.

By eliminating I/O subsystem operations and bypassing the need for external network connections between LPARs on an IBM Z platform, HiperSockets supports server consolidation through seamless virtual server interconnectivity and simplified enterprise networking.

3.4.3 ISM communications

The Internal Shared Memory (ISM), functioning as a virtual Peripheral Component Express (PCI) network adapter, facilitates direct access to shared virtual memory and offers an optimized interconnect for intra-communications on the IBM Z platform. It is utilized by Shared Memory Communications-Direct Memory Access (SMC-D).

SMC-D optimizes operating systems communications in a way that is transparent to socket applications. It also reduces the CPU cost of TCP/IP processing in the data path, which enables highly efficient and application-transparent communications.

SMC-D requires no extra physical resources (such as PCIe bandwidth, ports, I/O slots, network resources, or Ethernet switches). Instead, SMC-D uses LPAR-to-LPAR communication through HiperSockets, an OSA-Express, or a Network Express feature for establishing the initial connection.

z/OS and Linux on IBM Z platforms both support Shared Memory Communications (SMC), enabling memory-to-memory data sharing between the operating systems for enhanced efficiency and performance.

3.5 Clustering connectivity

IBM Parallel Sysplex is a clustering technology enabling multiple z/OS images to operate concurrently, appearing as one system to users. This configuration facilitates near-continuous availability. The Coupling Facility (CF), which supports parallelism, can function as a separate Logical Partition (internal CF) or within dedicated hardware (external CF).

What makes a group of such z/OS images into a sysplex is the inter-communication. This inter-communication is handled through coupling links. Coupling links enable all the z/OS to CF communication, CF-to-CF traffic, and Server Time Protocol (STP)[1].

For more information about options, see *Coupling Facility Configuration Options*.

There are three types of features that provide the Sysplex connectivity between or within IBM z17s, IBM z16s, and IBM z15s systems:

- **ICA SR2.0**

  Supports distances up to 150 meters, so mainly used for infra-site connectivity between systems.

- **Coupling Express3 LR**

  IBM z17 introduces Coupling Express3 LR 25G, a two-port 25 gigabit ethernet-based long reach coupling adapter that carries a new coupling channel type: CL6. Also available on IBM z17 is Coupling Express3 LR 10G, a two-port 10 gigabit ethernet-based long reach coupling adapter that carries the legacy coupling channel type CL5.

  Supports longer (unrepeated) connectivity to systems up to 10 kilometers, so mainly (not exclusively) used for inter-site connectivity between systems. Longer distances, up to 100 kilometers, are possible with the use of a DWDM extender.

- **Internal coupling peer (ICP)**

  Facilitates rapid and secure memory-to-memory communication between LPARs on the same system, running Coupling Facility (CF) and z/OS images. This connection is emulated in Licensed Internal Code (LIC), eliminating the need for physical cabling.

[1] All external coupling links can be used to carry STP timekeeping information.

3.5.1 Dynamic I/O configuration

Dynamic I/O configuration changes can be made to a stand-alone CF[2], Linux on Z, and z/TPF LPARs, without requiring a disruptive power on reset (POR).

The IBM z17 contains a firmware-based activation service that is used for dynamic I/O configuration changes to stand-alone CF, Linux on Z, and z/TPF partitions.

The firmware-based LPAR is driven by updates from an HCD instance that is running in a z/OS LPAR on a different IBM Z server that is connected to the same Hardware Management Console (HMC).

A firmware LPAR resides within the reserved range allocated by IBM, offering no attached I/O and thus consuming no configurable resources. Consequently, it remains invisible to clients.

3.5.2 Quantum-safe protection for CFCC

Quantum-safe protection covers Coupling Facility Control Code (CFCC). CFCC boot and the update processes are protected with Cryptographic Suite for Algebraic Lattices (Module-Lattice-Based Digital Signature (ML-DSA)), standardized by NIST, for quantum-safe digital signatures. For more information about quantum-safe digital signatures, see *Transitioning to Quantum-Safe Cryptography on IBM Z*, SG24-8525.

3.6 IBM Z coordinated server time

IBM Z coordinated server time ensures all systems within a network are synchronized to the same time. This is crucial for accurate logging of events, managing network traffic, executing time-sensitive transactions, and coordinate actions based on precise timestamps.

Server Time Protocol (STP) employs message transmission over coupling links between IBM Z servers for maintaining synchronized timekeeping. The IBM z17 can join an STP Coordinated Timing Network (CTN), a group of interconnected IBM Z servers that synchronize their time to Coordinated Server Time (CST).

STP is implemented in LIC as a system-wide facility of IBM z17 and is enabled by installing the STP feature. Extra configuration is required for an IBM z17 to become a member of a CTN.

For high availability (HA) purposes, nondisruptive capability is implemented in IBM z17 firmware that allows two CTNs to be merged into one, or to split one CTN into two, dynamically.

STP supports a multi-site timing network of up to 100 km (62 miles) over fiber optic cabling without requiring an intermediate site[3]. This protocol allows a Parallel Sysplex to span these distances for a multi-site Parallel Sysplex.

> **Note:** If an IBM z17 plays a CTN role (Primary Time Server (PTS), Backup Time Server (BTS), or Arbiter), the other CTN roleplaying IBM Z server must include direct coupling connectivity to IBM z15, z16, or z17.

[2] A stand-alone CF does not have any running instances of z/OS or z/VM.
[3] With dense wavelength-division multiplexing (DWDM).

3.6.1 STP implementation with IBM z17

The following are the STP implementation characteristics with IBM z17:

- NTPv4/Chrony will improve the overall resiliency of IBM Z NTP implementation for STP. It also will improve the accuracy and stability capabilities of IBM Z STP by making use of the full suite of NTP algorithms using Chrony.
- Network Time Security (NTS) protocol for NTP is an approved IETF standard (RFC 8915) that provides cryptographic security for the client-server mode of NTP. NTS uses Transport Layer Security (TLS) and Authenticated Encryption with Associated Data (AEAD) to:
  - Allow NTP users to obtain time in an authenticated manner.
  - Ensure that time data received is authenticated and secure.
  - Protect against attacks such as spoofing, man-in-the-middle and replay.
- Support of Mixed Mode of NTP and PTP improves the overall STP resiliency capabilities by allowing STP to use up to five external time sources (three NTP and two PTP) simultaneously. Mixed mode operation also improves STP accuracy and stability.
- Direct network connection to the IBM z17 CPC drawer of the External Time Source (ETS). ETS for Network Time Protocol (NTP), Precision Time Protocol (PTP), and Pulse per Second (PPS) network cables now connects directly to the IBM z17 central processor complex (CPC) drawers.[4] This connection provides greater accuracy to the external time reference.
- The n-mode Power STP Imminent Disruption Signal option. A loss of Primary Time Server (PTS) on IBM Z servers has severe implications for the timing network and the entire workload execution environment within an IBM Z sysplex.

3.6.2 Network Time Protocol Client support

Employing Network Time Protocol (NTP) servers as an External Time Source (ETS) typically meets the need for a time reference across diverse platforms, offering enhanced time accuracy compared to alternative methods.

NTP client support is available in the firmware partition that is running on IBM z17. The code interfaces with the NTP servers. This interaction allows an NTP server to become the single-time source for IBM z17 and for other servers that have NTP clients. The NTP Ethernet cable must plug directly into the Base Management Card (BMC) or Oscillator Card (OSC) ports on the IBM z17 CPC drawer. Redundant cabling and ETS must be configured.

3.6.3 Precision Time Protocol Client support

IEEE 1588 PTP is implemented on IBM z17 as an ETS for a CTN. The PTP Ethernet cable must plug directly into the BMC or OSC ports on IBM z17. Redundant cabling and ETS should be configured.

3.6.4 Pulse per Second support

Two OSCs,[5] which are included as a standard feature of IBM z17, provide a dual-path interface for the PPS signal. The cards contain a Bayonet Neill-Concelman (BNC) connector for PPS attachment at the front side of the CPC drawer. The redundant design allows continuous operation during the failure of one card and concurrent card maintenance.

[4] The ETS and PPS cables are connected to the Base Management Card (BMC) or Oscillator Card (OSC) adapters and from the front of the CPC drawer.

[5] The OSCs are combined with the BMCs.

STP tracks the highly stable and accurate PPS signal from the external time server. PPS maintains accuracy of 10 µs as measured at the PPS input of IBM z17.

A cable connection from the PPS port to the PPS output of an NTP server is required when IBM z17 is configured for NTP with PPS as ETS for time synchronization.

PPS is optional for PTP but might still be required for NTP to meet financial regulations regarding the accuracy of time synchronization between servers.

For more information, see *IBM Z Server Time Protocol Guide*, SG24-8480.

3.7 Cryptography

The IBM Z platform offers cryptographic engines that provide high-speed cryptographic operations:

- Central Processor Assist for Cryptographic Functions (CPACF)

  Cryptographic functions are provided through a set of instructions, which are available in the hardware on every processor unit (PU).

- Crypto Express features

  Cryptographic functions that are provided through high-security, tamper-sensing, and tamper-responding hardware security modules (HSMs).

The IBM Z platform provides cryptographic functions that can be categorized in the following groups from an application program perspective:

- Symmetric cryptographic functions,[6] which are provided by the CPACF or Crypto Express features when defined as an accelerator.
- Asymmetric cryptographic functions,[7] which are provided by the Crypto Express features.

Additionally, cryptographic features and functions are engineered to protect IBM z17 from attacks, including threats that might use quantum computers. The system includes the use of quantum-safe algorithms selected by NIST through the many firmware layers that are loaded during the boot process. Only authentic, IBM recognized firmware is accepted. This hardware-protected verification of the firmware uses a dual-signature scheme, consisting of a combination of both classical and quantum safe algorithms selected by NIST. The protection is anchored in the IBM Z *Root of Trust*.[8]

For more information about the quantum-safe algorithms selected by NIST utilized in IBM z17, see *Transitioning to Quantum-Safe Cryptography on IBM Z*, SG24-8525.

[6] With symmetric encryption, the same cryptographic key is used for encryption and decryption of the data (the sender and receiver of the data use the same key).

[7] With asymmetric encryption, the receiver's public key is used for encryption and the receiver's private key is used for decryption.

[8] Root of Trust is a source that can always be trusted within a cryptographic system.

3.7.1 Central Processor Assist for Cryptographic Functions

Each processor unit (PU) chip in the IBM z17 has an independent cryptographic engine (known as a cryptographic assist). The no-charge Central Processor Assist for Cryptographic Functions (CPACF) enablement feature offers a set of cryptographic functions for high-performance encryption and decryption with clear key operations for Secure Sockets Layer (SSL) and Transport Layer Security (TLS), VPN, and data-storing applications that do not require Federal Information Processing Standards (FIPS) 140-2 Level 4 security[9].

The CPACF-protected key is a function that facilitates the continued privacy of cryptographic key material while keeping the wanted high performance. CPACF ensures that key material is not visible to applications or operating systems during encryption operations. A CPACF-protected key provides substantial throughput improvements for large-volume data encryption and low latency for encryption of small blocks of data.

The cryptographic assist includes support for the following functions:

- Advanced Encryption Standard (AES) for 128-bit, 192-bit, and 256-bit keys
- Improved performance of AES Galois/Counter Mode (GCM) encryption
- Data Encryption Standard (DES) data encryption and decryption with single, double, or triple length keys
- Pseudo-random number generation (PRNG)
- Deterministic Random Number Generation (DRNG)
- True-random number generator (TRNG)
- Message authentication code
- Elliptic Curve Cryptography (ECC) support[10]
- Hashing algorithms: Secure Hash Algorithm (SHA)-1, SHA-2, and SHA-3, and Hash based message authentication (HMAC)

IBM Z servers inherently support SHA-1, SHA-2, and SHA-3 without the CPACF feature requirement. The CPACF functions are supported by z/OS, z/VM, 21 Century Software VSE^{n} V6.3, z/TPF, and Linux on IBM Z.

> **Attention:** Cryptographic methods like DES, along with hashing algorithms such as SHA-1, are deemed inadequate for current cybersecurity standards due to their vulnerability against contemporary attacks.
>
> This risk can be mitigated by switching to stronger algorithms, such as AES, SHA-256, SHA-3, Module-Lattice-Based Digital Signature (ML-DSA), and (Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM).
>
> IBM provides several tools that can aid in the management and discovery process:
>
> - IBM z/OS Integrated Cryptographic Service Facility (ICSF)
> - IBM Application Discovery and Delivery Intelligence (ADDI)
> - IBM Crypto Analytics Tool (CAT)
> - IBM z/OS Encryption Readiness Technology (zERT)
>
> These tools can help you identify certificates, encryption protocols, algorithms, and key lengths that are at risk in your IBM Z environment.

[9] FIPS 140-2 Security Requirements for Cryptographic Modules.

[10] Message-Security-Assist extension 9 is a hardware feature introduced in IBM z15 that provides the ECC capabilities, including message authentication, key generation, and scalar multiplication.

3.7.2 Crypto Express8S

The Crypto Express8S are Peripheral Component Interconnect Express (PCIe) cryptographic co-processors, which are an optional feature available on IBM z17. These co-processors are HSMs that provide high-security cryptographic processing as required by banking and other industries.

The Crypto Express8S is engineered with APIs that provide access to the quantum safe algorithms selected by NIST along with classical cryptographic algorithms to modernize existing applications and build new ones.

This feature provides a secure programming and hardware environment where crypto-processes are performed. Each cryptographic coprocessor includes general-purpose processors, nonvolatile storage, and specialized cryptographic electronics. All these features are contained within a tamper-sensing and tamper-responsive enclosure that wipes all keys and sensitive data on any attempt to tamper with the device. The security features of the HSM are designed to meet the requirements of FIPS 140-2 Level 4.

The Crypto Express8S (2-adapter) feature includes two Peripheral Component Interconnect Express Cryptographic Coprocessors (PCIeCCs), and the Crypto Express8S (1-adapter) feature includes one PCIeCC. For availability reasons, a minimum of two features is required for both features. Up to 30 Crypto Express8S (2-adapter) features are supported on IBM z17. The maximum number of the 1-adapter features is 16. The Crypto Express8S feature occupies one I/O slot in a PCIe+ I/O drawer.

The adapters can be configured as a Secure IBM Common Cryptographic Architecture (CCA) coprocessor, a Secure IBM Enterprise PKCS #11 (EP11) coprocessor, or as an accelerator.

Crypto Express8S provides domain support for up to 85 LPARs on IBM z17 ME1.

This accelerator function focuses on expediting SSL and TLS processes at the fastest possible speeds, rather than providing dedicated support for securing and storing financial application keys or secrets over extended periods. The Crypto Express8S can be configured as one of the following configurations:

- The Secure IBM CCA coprocessor includes secure key functions with an emphasis on the specialized functions that are required for banking and payment card systems. It is optionally programmable to add custom functions and algorithms by using User Defined-Extensions (UDXs).

  A mode called *Payment Card Industry PTS HSM* (PCI-HSM) is available in CCA mode. PCI-HSM mode simplifies compliance with Payment Card Industry requirements for HSMs.
- The Secure IBM EP11 coprocessor implements an industry-standardized set of services that adheres to the PKCS #11 specification 2.20 and more recent amendments. It was designed for extended FIPS and Common Criteria evaluations to meet industry requirements.

CCA features include the ability to use Advanced Encryption Standard (AES) keys for operations, such as data encryption, ISO and IBM PIN® processing, and PCI SSC compliant key wrapping to strengthen security. CCA is also extended for the support for the cryptographic requirements of the German Banking Industry Committee, Deutsche Kreditwirtschaft, and the NIST selected quantum-safe cryptographic algorithms.

The Crypto Express8S with CCA firmware adds secure key support for quantum-safe cryptographic private keys for signature and key encapsulation mechanism (KEM) purposes.

The CCA interface supports NIST standardized algorithm ML-DSA, including HashML-DSA, secure private keys usable for digital signature generation and verification. The CCA interface also supports NIST standardized algorithm ML-KEM. These components are also combined with Elliptic-curve Diffie-Hellman (ECDH) support to offer a quantum-safe cryptographic hybrid key exchange scheme. This hybrid scheme is engineered with secure CCA private keys for all involved private keys in scenarios where data needs enhanced authentication against future quantum computing attacks on conventional cryptography.

Several features that support the usage of the AES algorithm in banking applications also were added to CCA. These features include the addition of AES-related key management features and the AES ISO Format 4 (ISO-4) PIN blocks, as defined in the ISO 9564-1 standard. PIN block conversion is supported and used in AES PIN blocks in other CCA callable services. IBM continues to add enhancements as AES finance industry standards are released.

Other enhancements for CCA on Crypto Express8S include:

- TR-31 (X9.143) native support in all operational APIs. TR-31 is the standard key block in the financial services industry. Users of the CEX8S are now able to create TR-31 keys under the CCA MK like any other key type and use them in CCA services. not just for key transport.
- SHA-3 is now available for hash services and digital signature generation/verification. The CCA host library for Linux on IBM Z also now has support to send SHA3 requests to the CPACF.

RSA updates include RSA 8192-bit key support, OAEP 2.1 encoding for RSA encryption, decryption, and import / export of RSA-AESKW wrapped keys - allowing key exchange between CCA and PKCS#11 APIs popular at major cloud cryptography service providers.

Enhancements for EP11 on Crypto Express8S include:

- An additional FIPS 140-2 approved image. Customers are able to switch from the regular to the FIPS approved image on a per AP basis if required by regulators. Usage of the regular image is preferred as it contains the latest features and bug fixes. The FIPS image will match the version as mentioned by the most recent CMVP certificate available for the module.
- A continuous update for z16 adds support for the BLS digital signature algorithm with the BLS12-381 pairing-friendly curve to EP11. BLS signatures are deterministic and non-malleable and used by the Ethereum 2 crypto currency system. It allows for both aggregation of signatures and public keys. Additionally, support for the key derivation required by deterministic hierarchical wallets as defined in EIP2333 is added.
- A continuous update for z16 adds support for assigning Crypto Adapters in EP11 mode to guest configurations running in secure execution mode. Adapters must be bound and associated with the guest configuration to become operational. Association employs a guest secret known to the owner of the image only to ensure generated secrets can be used by this secure guest image only, even if the adapter gets moved to a different configuration without zeroization.

3.7.3 Crypto Express7S (carry forward only)

The Crypto Express7S feature has one or two PCIeCC (HSMs) per feature. For availability reasons, a minimum of two features is required. Up to 16 Crypto Express7S single adapter or up to 30 Crypto Express7S 2-adapter features are supported on IBM z17.

The adapters can be configured as a Secure IBM CCA coprocessor, a Secure IBM EP11 coprocessor, or as an accelerator.

On the IBM z17 ME1, Crypto Express7S offers domain support for as many as 85 LPAR instances.

Trusted Key Entry (TKE) feature: The TKE Workstation feature is required to support the administration of the Crypto Express features when configured as an Enterprise PKCS #11 coprocessor or managing the CCA mode PCI-HSM.

Changes were made to the TKE feature to use the quantum-safe cryptographic algorithms selected by NIST when authenticating Crypto Express8S, verifying replies from the Crypto Express8S coprocessors, and protecting key parts in flight for the Common Cryptographic Architecture (CCA). Finally, the IBM Z pervasive encryption functions are updated to use the quantum-safe algorithms selected by NIST for key management.

3.8 Special-purpose features and functions

IBM takes a *total systems* view regarding the design and development the IBM Z platform. The IBM Z stack is built around digital services, agile application development, connectivity, and system management. This design approach creates an integrated, diverse platform with specialized hardware and dedicated computing capabilities.

IBM z17 delivers a range of features and functions so that CPUs can concentrate on computational tasks while distinct, specialized features take care of the rest.

The latest additions with the IBM z17 are the second-generation IBM Z Integrated Accelerator for AI and the IBM Spyre Accelerator, which provide enhanced AI capabilities. The Integrated Accelerator for AI (with the Telum II processor) delivers AI inference in real-time, at large scale and rate, without needing to offload data from IBM z17 to perform AI inference. The Spyre Accelerator is a PCIe-attached AI accelerator designed to handle larger, more complex AI use cases, and can be clustered together to provide scalable and sustainable AI capabilities.

For more information about the other IBM z17 on-chip features, see 4.1.1, “Processor design highlights” on page 42.

3.9 Hardware management

The Hardware Management Console (HMC) and Support Element (SE) are appliances that provide hardware management for IBM Z servers. Hardware platform management covers a complex set of configuration, operation, monitoring, and service management tasks, and other services that are essential to the operations of the IBM Z platform.

The minimum driver level for HMC and SE for IBM z17 is Driver 61. Driver 61 is equivalent to Version 2.17.0. The HMC with Driver 61 or Version 2.17.0 can manage N-2 generations of IBM Z servers and be installed on IBM z15 and IBM z16.

On IBM z17, two HMCs are delivered with the Hardware Management Appliance (HMA) feature. It is possible to order the HMA feature later. However, only new microcode is delivered without HMC hardware.

Note: The HMC code runs on the two integrated 1U rack-mounted servers on the top of the IBM z17 A frame. Stand-alone HMCs that are outside the IBM z17 HMCs (tower or rack mount) are no longer supported and can no longer be ordered.

As closed systems, Support Elements (SEs) and Hardware Management Consoles (HMCs or HMAs) cannot accommodate additional software installations beyond their intended functions.

With IBM z17 and HMA, the SE and HMC codes run *virtualized* on the integrated two SEs on the two integrated 1U rack-mounted servers on the top of the IBM z17 A frame. One SE is the Primary SE (active) and the other is the Alternative SE (backup).

The SEs are connected to Ethernet switches for network connectivity with IBM Z servers and the HMAs. An HMC/HMA can communicate with one or more IBM Z servers.

When tasks are performed on the HMC, the commands are sent to one or more SEs, which then issue commands to their respective CPCs.

The HMC Remote Support Facility (RSF) provides communication with the IBM Support network for hardware problem reporting and service.

4

IBM z17 system design strengths

Every new generation of the IBM Z platform introduces innovative features and functions to provide more velocity, security, agility, and flexibility for building new IT solutions and services.

The IBM Z hardware, firmware, and operating systems always conform to the IBM z/Architecture[1] to ensure support of current and future workloads and services. Whenever new capabilities are implemented, the z/Architecture is extended rather than replaced. This practice helps sustain the compatibility, integrity, and longevity of the IBM Z platform. Thus, investment protection for earlier versions of workloads and solutions is ensured.

The advancement of the IBM Z platform embodies a proven architecture that is open, secure, resilient, and adaptable. From the microprocessor and memory design to the artificial intelligence (AI), sort, and cryptography capabilities, and its unparalleled I/O throughput, and rich virtualization, the IBM z17 is built to respond with speed and versatility.

This chapter describes the following topics:

[1] IBM z/Architecture is the mainframe-computational architecture notation that defines its behavior. For more information, see *IBM z/Architecture Principles of Operation*, SA22-7832.

4.1 IBM z17 technology improvements

Computer systems achieve the levels of efficiency that are needed by businesses through an overall balanced design. Processor units (PUs), memory, I/O, and network communications must complement each other to achieve the required levels of performance. A balanced system design also incorporates all the enhancements in software, hardware, and firmware to accelerate specific type of operations, for example, sorting, inferencing, compressing, and encrypting data.

IBM z17 provides high levels of performance, scalability, resiliency, flexibility, and security when serving as a transaction processing system, a hybrid cloud platform, or both. IBM z17 can host thousands of virtualized environments.

Each generation of IBM Z servers provides more system capacity, which combines various system design enhancements. Within each single drawer, IBM z17 ME1 provides up to 20% greater capacity than IBM z16 A01 for standard models and up to 15% greater capacity on the max configuration model, enabling efficient scaling of partitions.

Also contributing to the extra capacity on IBM z17 are numerous improvements in processor chip design, including new instructions, multithreading, and redesigned and larger caches.

4.1.1 Processor design highlights

IBM z17 supports 64-bit addressing mode and uses Complex Instruction Set Computer (CISC), including highly capable and complex instructions. Most of the instructions are implemented at the hardware or firmware level for the most optimal and effective execution.

PU is the generic term for the z/Architecture CPU. Each PU is a superscalar processor, which can decode up to six complex instructions per clock cycle, running instructions out-of-order. The PU uses a high-frequency, low-latency pipeline that provides robust performance across a wide range of workloads.

z/Architecture addressing modes: The z/Architecture simultaneously supports 24-bit, 31-bit, and 64-bit addressing modes. This feature delivers compatibility with earlier software versions, which provides investment protection.

Compared to its predecessors, IBM z17 features the following processor design changes, improvements, and architectural extensions with the Telum II processor:

- Cross CPC drawer (A-Bus):
  - Improved resource management
  - Reduced interface latency (>10% reduction)
  - 10% more effective bandwidth
- Redesigned processor chip that uses 5-nm silicon wafer technology
- New cache structure is 40% larger:
  - L1D (data) and L1I (instruction) cache: ON-core (128 KB each)
  - L2 - dense SRAM: Outside the core, semi-private to the core = 36 MB
  - Virtual L3 cache (shared victim) = 360 MB
  - Virtual L4 cache (shared victim) = 2.8 GB

- New core-nest interface:
  - Increased capacity
  - Improved throughput
  - Enhanced security
- A new branch prediction design that uses SRAM
- Significant architecture changes (COBOL compiler and more)
- Dedicated coprocessors and accelerators for each PU core:
  - IBM Integrated Accelerator for Artificial Intelligence (AIU)

    This second generation on-chip AIU is designed for high-speed, real-time inferencing at scale. The on-chip AI acceleration adds more than 24 TFLOPS of processing power that is shared by all cores on the chip.

    This centralized AI design provides high performance and consistent low latency inferencing for processing a mix of transactional and AI workloads at speed and scale.
  - Central Processor Assist for Cryptographic Functions (CPACF)

    This component encrypts large amounts of data in real time. CPACF provides counters that track cryptographic compliance and instruction use, algorithms, bit length, and key security for a specific workload.
  - IBM Integrated Accelerator for IBM Z Sort

    This on-core accelerator for sort uses the sort instruction (`SORTL`) to accelerate the sorting of data. The IBM Integrated Accelerator for IBM Z Sort (zSort) feature helps reduce the CPU costs and improve the elapsed time for eligible workloads by speeding up the sorting process and improving database functions.
  - IBM Integrated Accelerator for z Enterprise Data Compression

    This on-chip accelerator for compression implements compression as defined by RFC195. It performs data compression with improved performance and simplified management on a processor chip level. The on-chip compression is designed to reduce the penalty of storing, transporting, and processing data without changing applications architecture.
- The new I/O design called a Data Processing Unit (DPU) is designed to improve channel performance and increase I/O rates for FCP, FICON (including HPF), and OSA protocols.

4.1.2 Memory

System memory stands as a foundational design element, its persistent improvements directly enhancing overall system performance.

Maximum physical memory size is directly related to the number of central processor complex (CPC) drawers in the system. An IBM Z server has more memory that is installed than was ordered because a portion of the installed memory is used to implement the redundant array of independent memory (RAIM) design (the technology that provides memory protection and excludes memory faults). You are *not* charged for the extra amount of memory that is needed for RAIM.

For example, with IBM z17 ME1, you have up to 64 TB of memory for a four-CPC drawer configuration (60% increase per drawer compared to IBM z16 A01).

The IBM z17 ME1 Hardware System Area (HSA) is 884 GB compared to 256 GB with the IBM z16 A01. The HSA area is a fixed size and not included in the memory that is ordered.

Each operating system can allocate the amount of main memory up to its supported limit.

Flexible Memory

Flexible memory supplies additional physical memory required for a specific situation involving an IBM z17 with numerous CPC drawers, including one currently non-operational. This scenario necessitates activation base memory and HSA functionality.

The IBM z17 ME1 allocates necessary extra resources for flexible memory configurations during the setup of memory features and entitlements. Flexible memory ranges from 512 GB to 41728 GB based on ordered feature (Max43, Max90, Max136, Max183, or Max208).

Virtual Flash Memory

IBM Virtual Flash Memory (VFM) is the replacement for the Flash Express features that were available on earlier IBM Z servers. With IBM z17 ME1, the VFM feature can be ordered in 512 GB increments up to 12 VFM features for a total of 6 TB.

Using VFM can help improve z/OS system availability by reducing latency from paging delays that can occur at the start of the workday or during other transitional periods. It is also designed to help eliminate delays that can occur when diagnostic data is collected during failures.

Therefore, VFM can help meet most demanding service-level agreements (SLAs) and compete more effectively. VFM provides rapid time to value.

4.2 IBM Z virtualization

Virtualization has been a key strength of the IBM Z platform for more than five decades. It is embedded in the hardware, firmware, and operating systems. All computing resources (such as CPU, memory, and I/O) are virtualized. Each set of the resources can be used independently within separate operating environments (known as *guest systems*).

The IBM Z platform is designed to concurrently run multiple virtual guest systems and provide each system with the required dynamic sharing of the resources with minimal costs and performance impact.

Virtualization management, which is called a *hypervisor*, operates on hardware and software levels of the IBM Z platform. The hardware hypervisor (first level or type 1) is PR/SM, which is integrated into the firmware. PR/SM runs the control code that manages the hardware resources and builds LPARs[2] that run operating systems, middleware, and software applications. PR/SM evolved over the decades on the IBM Z platform and is a proven, secure, and fundamental IBM Z technology. Every generation of the IBM Z platform brings PR/SM improvements that are aimed to demonstrate even better system performance.

The supported software hypervisors (type 2) are z/VM and KVM:

- z/VM supports the simultaneous execution of multiple virtual guest systems within an LPAR and nested (multi-level) virtualization. z/VM is a powerful hypervisor that can emulate various hardware devices to its guests.
- KVM[3] provides flexibility for your hypervisor choice and the unique combination of enterprise hardware and open source.

[2] LPAR technology was introduced more than four decades ago on the IBM Z platform to support virtualization and provide the highest level of isolation between guest systems.

[3] For more information about the use of KVM with IBM Z, see Virtualization Cookbook for IBM Z Volume 5: KVM, SG24-8463.

The KVM hypervisor is available in recent Linux on IBM Z distributions and enables you to share real CPUs (called IFLs), memory, and I/O resources.

z/VM and KVM interconnect with PR/SM and use its functions.

Multiple hypervisors can coexist and run simultaneously on the IBM Z platform so that you can create and build multiple virtualized guest systems that are running various open-source applications on the IBM Z platform with high levels of performance and integrated security.

IBM Z is continuously improving virtualization techniques IBM Z development provides highly scalable dynamic platforms that can host traditional and modern solutions (such as hybrid cloud and container technology) on the same footprint.

Figure 4-1 shows the diverse workloads that are supported and virtualized on a single IBM z17, and the co-existence of multiple hypervisors: PR/SM, z/VM, and KVM.

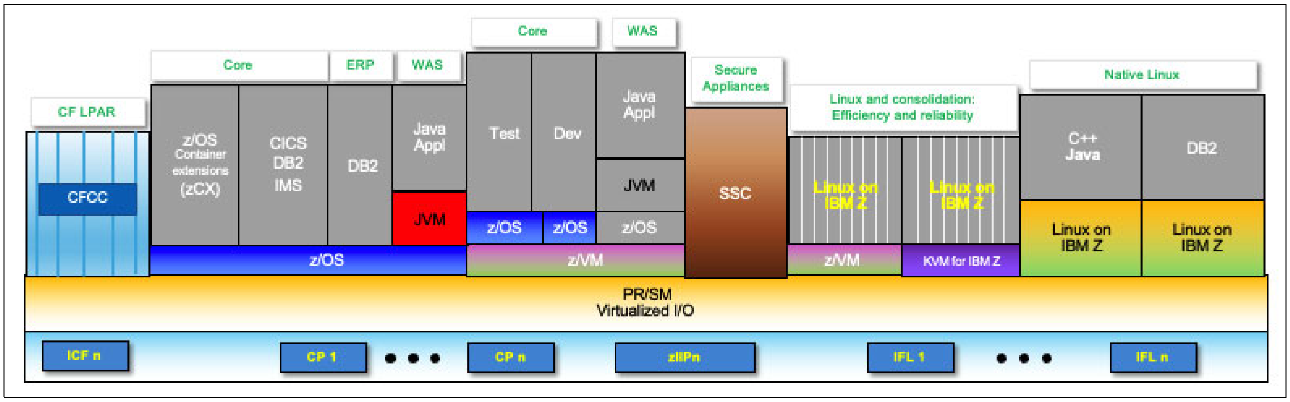

Figure 4-1 Virtualization on the IBM Z platform

4.2.1 Cloud environments

Virtualization is critical to the viability of cloud service offerings because it provides the elasticity that allows a platform to deal with the ebbs and flows of demands on IT resources. By virtue of the integration in the hardware, firmware, and operating systems, virtualization on IBM z17 is highly efficient, delivering up to 100% sustained resource use, and the highest levels of isolation and security. Therefore, the cloud solution costs (whether hardware, software, or management) are minimal.

Cloud elasticity requirements are covered by IBM z17 granularity offerings, including capacity levels, Tailor Fit Pricing (for unpredictable, high spiking, and business-critical workloads), and Capacity on Demand (CoD). These characteristics and others make the IBM Z platform the gold standard for the industry.

Additionally, managing a cloud environment requires tools that can leverage a pool of virtualized compute, storage, and network resources and present them to the consumer as a service in a secure way.

A *cloud management system* must enable the management of virtualized IT resources to support different types of cloud service models and cloud deployment models. OpenStack can satisfy a wide range of cloud management demands. OpenStack integrates various components to automate IT infrastructure service provisioning.

IBM z17 also can be tailored with a choice of IBM Z-backed services that are delivered through IBM Cloud to help transform your infrastructure, applications, and data by exposing and connecting assets with simplified and intelligent operations across the infrastructure.

The cloud-native capabilities are delivered as pre-integrated solutions called IBM Cloud Paks. This IBM certified and containerized software provides a common operating model and a common set of services.

With Red Hat, the hybrid cloud capabilities on the IBM Z platform are extended. Support for running Red Hat OpenShift and Linux on IBM Z provides expansive cloud capabilities, including open containers, tools, and access to an extensive open community.

For more information about hybrid cloud capabilities, see Hybrid cloud with IBM Z.

In addition, IBM has several offerings that can help organizations automate multi-cloud and hybrid environments, orchestrate workloads, and help improve network management, such as:

- IBM Vault Self-Managed, which provides a standardized enterprise secrets management solution that builds on the security, resiliency and scalability of IBM Z and LinuxONE.
- IBM Terraform, which provides capabilities enabling a standardized shared service across an organization to provision and manage Z infrastructure as code. Terraform includes governance features to help mitigate infrastructure risks, including policy as code, run tasks, audit logging, and configuration drift detection. Terraform is available as a self-managed installation on distributed platforms.

For more information on these offerings, see the announcement.

4.2.2 Hardware virtualization

The IBM Z platform is known for its unique virtualization capabilities, enabling you to deploy various workloads (traditional and modern) to achieve the highest performance and throughput metrics with the lowest costs and impact.

Workload separation is one of the most important parameters. PR/SM in IBM z17 is designed to meet the highest level of Common Criteria (EAL5+), similar to previous IBM Z platforms. This level of isolation ensures the integrity and security of the workloads and excludes the contamination of the running applications by other programs.

Logical Processors

All physical PUs are virtualized as logical processors on the IBM Z platform and can be characterized as the following types:

- Central processors (CPs) are standard processors that support all operating systems and user workloads.
- A zIIP is used under z/OS for designated workloads. These workloads include, but are not limited to, the following examples:
  - IBM z/OS Container Extensions (zCX)
  - IBM Java virtual machine (JVM)
  - Various XML System Services
  - IPsec offload
  - Certain IBM Db2 for z/OS processes
  - DFSMS System Data Mover for z/OS Global Mirror
  - IBM HiperSockets for large messages
  - IBM System Recovery Boost

- Certain AI and Python workloads
- The Integrated Facility for Linux (IFL) processor solely supports Linux on IBM Z, along with z/VM and KVM hypervisors for managing Linux VMs.
- An Internal Coupling Facility (ICF) processor is used for z/OS clustering and supporting the family of IBM Parallel Sysplex solutions. ICF is dedicated to this function and exclusively runs the Coupling Facility Control Code (CFCC).

The characterized PUs are aimed to streamline the specific workload. All engines architecturally and physically are the same.

Additionally, the following pre-characterized processors are part of the base system configuration and always are present:

- SAPs that run I/O operations
- Integrated Firmware Processors (IFPs) for native PCIe features and other firmware functions

PR/SM accepts requests for work by dispatching logical processors on physical processors. Physical processors can be shared across LPARs or dedicated to an LPAR. The logical processors that are assigned to an LPAR must be either all shared or all dedicated.

PR/SM ensures that the processor state is correctly saved and restored (including all registers) when you switch a physical processor from one logical processor to another one. Data isolation, integrity, and coherence inside the system are always strictly enforced.

Logical processors can be dynamically added to and removed from LPARs. Operating system support is required to use this capability. z/OS, z/VM, and 21st Century Software VSE^n V6.3, each can dynamically define and change the number and type of reserved PUs in an LPAR profile. No planning is required.

The newly assigned logical processors are immediately available to the operating systems and for z/VM to its guest images. Linux on IBM Z provides the Standby CPU activation and deactivation functions.

Memory

To ensure security and data integrity, memory cannot be concurrently shared by active LPARs. Strict LPAR isolation is maintained to avoid any workload contamination.

An LPAR can be defined with an initial and reserved amount of memory. At activation time, the initial amount is made available to the partition, and the reserved amount can be added later partially or totally. Those two memory zones do not have to be contiguous in real memory, but the addressing area (for initial and reserved memory) is presented as contiguous to the operating system that runs in the LPAR.

z/VM can acquire memory nondisruptively and quickly make it available to guests. z/VM virtualizes this support to its guests, which can also increase their memory nondisruptively. Releasing memory is still a disruptive operation.

LPAR memory is said to be virtualized in the sense that within each LPAR, memory addresses are contiguous and start at address zero. LPAR memory addresses are different from the system’s absolute memory addresses, which are contiguous and have a single address of zero. Do not confuse this capability with the operating system that virtualizes its LPAR memory, which is done through the creation and management of multiple address spaces.

The z/Architecture features a robust virtual storage architecture that allows LPAR-by-LPAR definition of an unlimited number of address spaces and the simultaneous use by each program of up to 1023 of those address spaces. Each address space can be up to 16 EB (1 exabyte = 2^{60} bytes). Thus, the architecture has no real limits. Practical limits are determined by the available hardware resources, including disk storage for paging.

Isolation of the address spaces is strictly enforced by the Dynamic Address conversion hardware mechanism. A program's right to read/write in each page frame is validated by comparing the page key with the key of the program that is requesting access.

Definition and management of the address spaces is under operating system control. Three addressing modes (24-bit, 31-bit, and 64-bit) are simultaneously supported, providing compatibility with earlier versions and investment protection.

Operating systems can enable sharing of address spaces, or parts of them, across multiple processes. For example, under z/VM, a single copy of the read-only part of a kernel can be shared by all VMs that use that operating system.
Known as *discontiguous shared segment* (DCSS), this shared memory use for many VMs can result in significant savings of real memory and improvements in performance.

I/O virtualization

IBM z17 ME1 supports six channel subsystems (CSSs), Each CSS can have up to 256 channels. In addition to the dedicated use of channels and I/O devices by an LPAR, the z/Architecture also enables sharing of the I/O devices that are accessed through these channels by several active LPARs. This function is known as *Multiple Image Facility* (MIF). The shared channels can belong to different CSSs, in which case they are known as *spanned channels*.

Data streams across sharing LPAR pairs traverse shared physical paths with complete isolation and integrity guarantees. PR/SM configures a single logical channel path per active LPAR with an online-configured channel for availability purposes. Critical devices, such as vital data set storage disks, require multiple logical channel paths to ensure redundancy and continuous operation.

When more isolation is required, you can use configuration rules to restrict the access of each LPAR to specific channel paths and specific I/O devices on those channel paths.

The parallel access volume (PAV) function enables access to a device through several addresses, normally one base address and an average of three aliases. This feature increases the throughput of the device by using more device addresses.

HyperPAV takes the technology a step further by allowing the I/O Supervisor (IOS) in z/OS (and the equivalent function in the Control Program of z/VM) to create PAV structures dynamically. The structures are created depending on the current I/O demand in the system, which lowers the need for manually tuning the system for PAV use.

SuperPAV is an extension of the HyperPAV architecture and implements multiple logical subsystems (LSSs) within an alias management group (AMG). SuperPAV enables the following solution:

- Problem: A new I/O request occurs and no alias PAV devices are available in the alias pool for the base PAV device's LSS.
- Solution: z/OS attempts to use an alias PAV device from another LSS within the AMG subgroup.

SuperPAV can provide relief for systems that experience high I/O queue time (IOSQ) during periods of peak I/O load. When few aliases are defined in an LSS, aliases might not be available during a heavy I/O period. z/OS checks peer LSS alias pools to borrow an alias to start I/O requests. Previously, these I/O requests were left queued when aliases are not available.

In large installations, the total number of device addresses can be high. Therefore, the concept of *subchannel sets* is part of the z/Architecture.

Subchannel sets

With IBM z17 ME1, up to four subchannel sets of approximately 64,000 device addresses are available. The base addresses[4] are defined to set 0 (IBM reserves 256 subchannels on set 0), and the aliases addresses are defined to set 1, set 2, and set 3.

Subchannel sets are used by the Metro Mirror (also referred to as *synchronous Peer-to-Peer Remote Copy* (PPRC)) function by having the Metro Mirror primary devices that are defined in subchannel set 0. Secondary devices can be defined in subchannel sets 1, 2, and 3, which provide more connectivity through subchannel set 0.

The IBM Z platform streamlines management of extensive I/O configurations with Extended Address Volumes (EAVs), offering vast storage capacity. Besides z/OS, both z/VM and Linux on IBM Z incorporate support for EAVs.

By extending the disk volume size, potentially fewer volumes are required to hold the same amount of data, which simplifies systems and data management. EAV is supported by the IBM Storage DS8000 series.

The dynamic I/O configuration function is supported by z/OS and z/VM. This function provides the capability of concurrently changing the active I/O configuration. Changes can be made to channel paths, control units, and devices. The fixed HSA area in IBM z17 greatly eases the planning requirements and enhances the flexibility and availability of these reconfigurations.

4.3 IBM z17 capacity

IBM z17 offers significant increases in capacity and performance over IBM z16. Several elements contribute to this effect, including many processors, individual processor performance, memory caches, SMT, and machine instructions, including the SIMD. Subcapacity settings continue to be offered.

The family of Capacity on Demand (CoD) offerings ensures a flexible addition of capacity when it is most needed, for example, during peak workload periods, scheduled maintenance, or in disaster recovery (DR) scenarios.

The IBM Tailored Fit Pricing for IBM Z options are designed to deliver unmatched simplicity and predictability of hardware capacity and software pricing, even in the constantly evolving era of hybrid cloud.

[4] Only a z/OS base device must be in subchannel set 0. Linux on IBM Z supports base devices in the other subchannels sets.

Note: Capacity and performance ratios are based on measurements and projections by using standard IBM benchmarks in a controlled environment. Actual throughput can vary depending on several factors, such as the job stream, I/O and storage configurations, and workload type.

4.3.1 Capacity settings

IBM z17 expands the offer on subcapacity settings. Finer granularity in capacity levels enables the growth of installed capacity to follow more closely the enterprise growth for a smoother, pay-as-you-go investment profile. Many performance and monitoring tools are available on IBM Z environments that are coupled with the flexibility of the CoD options (see 4.3.2, “CoD offerings” on page 51). These features help to manage growth by making capacity available when needed.

IBM z17 ME1 capacity levels

Regardless of the installed model, IBM z17 ME1 offers four distinct capacity levels for the first 43 CPs[5] that have three capacity levels (4xx, 5xx, and 6xx):

- One full capacity
- Three subcapacities

Full capacity CPs are identified as CP7. On IBM z17 ME1, up to 208 CPs can be configured as CP7. Up to 43 CPs can have subcapacity. The three subcapacity levels are identified by CP6, CP5, and CP4, and are displayed in hardware descriptions as feature codes (FC) on the CPs:

- Max43 - (FC 0571)
- Max90 - (FC 0572)
- Max136 - (FC 0573)
- Max183 - (FC 0574)
- Max208 - (FC 0575)

These processors deliver the scalability and granularity to meet the needs of medium-sized enterprises while also satisfying the requirements of large enterprises that have large-scale, mission-critical transaction and data processing requirements.

A capacity level is a setting of each CP to a subcapacity of the full CP capacity. The clock frequency of those processors remains unchanged. The capacity adjustment is achieved by using other means.

If more than 43 CPs are configured to the system, all must be full capacity because all CPs must be at the same capacity level. Granular capacity adds 129 subcapacity settings to the 208 capacity settings that are available with full capacity CPs (CP7) equaling 337 distinct capacity settings in the IBM z17.

A processor always is set at full capacity when it is characterized as anything other than a CP, such as a zIIP, an IFL, or an ICF. A distinct pricing framework governs non-Central Processor (non-CP) components, including acquisition and maintenance costs, along with diverse software licensing options tailored to these components.

[5] A CP is the IBM Z standard processor for use with any supported operating system. It is required to run z/OS.

To help size an IBM Z server to fit your requirements, IBM provides a no-cost tool that reflects the latest IBM Large Systems Performance Reference (LSPR) measurements, and it is called the IBM Z Processor Capacity Reference (zPCR). Download the tool from Getting Started with zPCR.

For more information about LSPR measurements, see LSPR for IBM Z.

4.3.2 CoD offerings

The IBM z17 maintains its Capacity on Demand (CoD) offerings, delivering flexibility, control, and administrative ease while addressing diverse resource needs across multiple scenarios with refined granularity over allocated resources.

IBM z17 can perform concurrent upgrades, which provide an increase of processor capacity with no platform outage. In most cases, with operating system support, a concurrent upgrade can also be nondisruptive to the operating system. It is important to consider that these upgrades are based on the enablement of resources that are physically present in IBM z17.

Capacity upgrades encompass both permanent and temporary adjustments to installed capacity, manageable through the Customer Initiated Upgrade (CIU) feature - no IBM service personnel intervention required. These modifications initiate online through IBM Resource Link, providing customers with self-sufficient control over their system's resource allocation.

Using the CIU facility requires a special contract between the customer and IBM. This contract specifies the terms and conditions for online CoD buying of upgrades, and other types of CoD upgrades are accepted. For more information, see IBM Resource Link.[6]

For more information about the CoD offerings, see *IBM z17 (9175) Technical Guide*, SG24-8579.

Permanent upgrades

Permanent upgrades of processors (CPs, IFLs, ICFs, zIIPs, and SAPs) and memory, or changes to a platform’s Model-Capacity Identifier (up to the limits of the installed processor capacity on an existing IBM z17), can be performed by customers through the IBM Online Permanent Upgrade offering by using the CIU facility.

Temporary upgrades

Temporary upgrades of an IBM z17 can be done by On/Off CoD or Capacity Backup (CBU) that is ordered from the CIU facility.

On/Off CoD function

On/Off CoD is a function that enables concurrent and temporary capacity growth of the CPC. On/Off CoD can be used for peak workload requirements for any period. On/Off CoD includes a daily hardware charge, and it can include an associated software charge. On/Off CoD offerings can be prepaid or post-paid.

When you use the On/Off CoD function, you can concurrently add processors (CPs, IFLs, ICFs, zIIPs, and SAPs), increase the CP capacity level, or both.

> **Prepaid On/Off CoD tokens:** New prepaid On/Off CoD tokens do *not* carry forward to future systems.

[6] IBM Resource Link ID is required.

Capacity backup function

CBU enables you to perform a concurrent and temporary activation of extra CPs, ICFs, IFLs, zIIPs, and SAPs, an increase of the CP capacity level, or both. This function can be used during an unforeseen loss of IBM Z capacity within the enterprise, or to perform a test of your disaster recovery (DR) procedures. The capacity of a CBU upgrade cannot be used for peak workload management.

CBU features are optional and require unused capacity to be available on CPC drawers of the backup system as unused PUs to increase the CP capacity level on a subcapacity system, or both. A CBU contract must be in place before the Licensed Internal Code Configuration Control (LICCC) code that enables this capability can be loaded on the system.

An initial CBU record provides for one test for each CBU year (each up to 10 days) and one disaster activation (up to 90 days). The record can be configured to be valid for up to 5 years. You also can order more tests for a CBU record in quantities of five, up to a maximum of 15 tests.

Suitable use of the CBU capability does not incur any other software charges from IBM.

Flexible Capacity for cyber resiliency

Flexible Capacity (FC 9933 together with FC 0376) can make production capacity available across sites between IBM z17 platforms for flexibility and elasticity in DR testing, planned maintenance, proactive outage avoidance, and actual DR scenarios.

Flexible Capacity works with other temporary record types, for example, On/Off CoD and Tailor Fit Pricing for Hardware (TPF-Hardware).

With Flexible Capacity, capacity can be allocated remotely without requiring onsite personnel (IBM or customer) after the initial set-up. Flexible Capacity provides the following benefits:

- Flexible duration of capacity (up to 1 year).
- Fully automated by using solutions such as IBM GDPS[7].
- Simplify compliance and improve confidence in DR scenarios, including tests.
- No need for CBU records by using this solution.

For more information, see *IBM Z Flexible Capacity for Cyber Resiliency*, REDP-5702.

z/OS capacity provisioning

Capacity provisioning helps you to manage the CP and zIIP capacity of an IBM z17 that is running one or more instances of the z/OS operating system. By using the z/OS Capacity Provisioning Manager (CPM) component, On/Off CoD temporary capacity can be activated and deactivated under control of a defined policy. Combined with functions in z/OS, the IBM z17 provisioning capability gives you a flexible, automated process to control the configuration and activation of On/Off CoD offerings.

4.3.3 IBM Tailored Fit Pricing for IBM Z

The Tailored Fit Pricing for IBM Z Hardware Consumption Solution provides an always-on, consumption-based capacity corridor that provides flexibility and control for unpredictable workload spikes throughout the day. It helps to scale IT demands and control behavior with a pay-for-use buffer and granular usage measurements.

[7] IBM GDPS (Geographically Dispersed Parallel Sysplex) is a collection of software offerings that help with disaster recovery and business continuity. GDPS can be used for single-site or multi-site environments. See *IBM GDPS: An Introduction to Concepts and Capabilities*, SG24-6374 for more information.

Tailored Fit Pricing for IBM Z helps to make embracing hybrid cloud easier with IBM Z. The pricing option delivers simplicity, flexibility, and predictability of pricing across the stack, even with constantly increasing unpredictability in business demand.

IBM Z Flexible Capacity for Cyber Resiliency can be used with TFP-Hardware. The Flexible Capacity limit is based on the Base Capacity. The presence or activation of TFP-Hardware does not affect the amount of capacity that can be activated by a Flexible Capacity Transfer record.

The Flexible Capacity Transfer record is considered to be the first record that was activated, regardless of the order in which temporary records or TFP-Hardware were activated.

For more information about the CoD offerings and Tailored Fit Pricing for IBM Z, see *IBM z17 (9175) Technical Guide*, SG24-8579.

4.4 IBM z17 performance

The IBM Z microprocessor chip for IBM z17 has a high-frequency design that uses IBM leading microprocessor technology and offers more cache per core than other chips. Additionally, an enhanced instruction execution sequence, along with processing technologies (such as SMT) delivers world-class per-thread performance. z/Architecture is enhanced by providing more instructions (including SIMD) that are intended to deliver improved CPU-centric performance and analytics.

For CPU-intensive workloads, more gains can be achieved by multiple compiler-level improvements. Improved performance of IBM z17 ME1 is a result of the enhancements that are described in Chapter 2, “IBM z17 ME1 hardware overview” on page 11 and 4.1, “IBM z17 technology improvements” on page 42.

4.4.1 LSPR workload suite: IBM z17 changes

To help you better understand workload variations, IBM provides a no-cost tool, zPCR, which is available at Getting Started with IBM z Processor Capacity Reference.

IBM continues to measure the performance of the systems by using various workloads and publishes the results at Large Systems Performance Reference (LSPR) report.

IBM also provides a list of millions of service units (MSU) ratings for reference.Capacity performance is closely associated with how a workload uses and interacts with a specific processor hardware design. Workload capacity performance is sensitive to the following major factors:

- Instruction path length
- Instruction complexity
- Memory hierarchy

The CPU Measurement Facility (CPUMF) data offers insight into the interaction of workload with the hardware design. CPUMF data helps LSPR to adjust workload capacity curves that are based on the underlying hardware sensitivities, in particular the processor access to caches and memory. The workload category is determined by the Level 1 Misses per 100 instructions (L1MP) and the *relative nest intensity* (RNI).

With the IBM Z platform, the LSPR introduced the following workload capacity categories that replace all prior primitives and mixes:

- LOW (RNI): A workload category that represents light use of the memory hierarchy.
- AVERAGE (RNI): A workload category that represents average use of the memory hierarchy. This category is expected to represent most production workloads.
- HIGH (RNI): A workload category that represents heavy use of the memory hierarchy.

These categories are based on the RNI, which is influenced by many variables, such as application type, I/O rate, application mix, CPU usage, data reference patterns, LPAR configuration, and the software configuration that is running. CPU MF data can be collected by z/OS SMF record type 113 or z/VM Monitor, using CPU Measurement Facility Host Counters.

Beyond traditional low, average, and high classifications, the newest zPCR introduces the low-average and average-high mixed categories, offering enhanced precision for workload characterization.

The LSPR tables continue to rate all z/Architecture processors that are running in LPAR mode and 64-bit mode. The single-number values are based on a combination of the default mixed workload ratios, typical multi-LPAR configurations, and expected early-program migration scenarios. In addition to z/OS workloads that are used to set the single-number values, the LSPR tables contain information that pertains to Linux on IBM Z and z/VM environments.

The LSPR contains the internal throughput rate ratios (ITRRs) for IBM z17 and the previous generations of processors. The report is based on measurements and projections by using standard IBM benchmarks in a controlled environment. The actual throughput that any user might experience varies depending on several factors, such as the amount of multiprogramming in the job stream, the I/O configuration, and the workload that is processed.

Experience demonstrates that IBM Z servers can run at up to 100% usage levels sustained. However, most users prefer to leave some white space and run at 90% or slightly under. For any capacity comparison, the use of “one number” (such as the MIPS or MSU metrics) is not a valid method. Therefore, use zPCR and involve IBM Support when you are planning for capacity.

For more information about IBM z17 performance, see *IBM z17 (9175) Technical Guide*, SG24-8579.

4.4.2 IBM z17 throughput optimization

The memory and cache structure implementation in the CPC drawers of IBM z17 are significantly enhanced compared to previous generations to provide sustained throughput and performance improvements. The memory is distributed throughout the CPC drawers and the CPC drawers have individual levels of cache that are private to the cores and shared by the cores. Nonetheless, all processors can access the highest level of cache and all the memory. Therefore, the system is managed as a memory-coherent symmetric multiprocessor (SMP).

Processors within the IBM z17 CPC drawer structure have different distance-to-memory attributes. CPC drawers are fully interconnected to minimize the distance. Other non-negligible effects result from data latency when grouping and dispatching work on a set of available logical processors. To minimize latency, the system attempts to dispatch and later redispatch work to a group of physical CPUs that share cache levels.

PR/SM manages the usage of physical processors by LPARs by dispatching the logical processors on the physical processors.

However, PR/SM is not aware of which workloads are being dispatched by the operating system in what logical processors. The Workload Manager (WLM) component of z/OS has the information at the task level but is unaware of physical processors.

This disconnect is solved by enhancements that enable PR/SM and WLM to work closely together. They can cooperate to create an affinity between task and physical processor rather than between LPAR and physical processor, which is known as *HiperDispatch*.

4.4.3 HiperDispatch

HiperDispatch combines two functional enhancements: in the z/OS dispatcher and in PR/SM. This function is intended to improve computing efficiency in the hardware, z/OS, and z/VM.

In general, the PR/SM dispatcher assigns work to the minimum number of logical processors that are needed for the priority (weight) of the LPAR. On IBM z17, PR/SM attempts to group the logical processors into the same logical cluster or in the neighboring logical cluster in the same CPC drawer and, if possible, in the same chip. This configuration results in reduction of multi-processor effects, maximizing the usage of shared cache, and lowering the interference across multiple partitions.

The z/OS dispatcher is enhanced to operate with multiple dispatching queues, and tasks are distributed among these queues. Specific z/OS tasks can be dispatched to a small subset of logical processors. PR/SM ties these logical processors to the same physical processors, which improve the hardware cache reuse and locality of reference characteristics, such as reducing the rate of cross communication.

To use the correct logical processors, the z/OS dispatcher obtains the necessary information from PR/SM through interfaces that are implemented on IBM z17. The entire IBM z17 stack (hardware, firmware, and software) tightly collaborates to obtain the full potential of the hardware. z/VM HiperDispatch provides support similar to the one in z/OS. It is possible to dynamically turn on and off HiperDispatch without requiring an initial program load (IPL).

IBM z17 includes several HiperDispatch algorithm enhancements, including the following examples:

- Improved memory affinity
- Improved LPAR placement based on IBM z16 experience
- Usage of a new chip configuration

Note: HiperDispatch necessitates Simultaneous Multithreading (SMT) activation, serving as an essential feature in IBM Z LSPR measurements, all conducted within z/OS environments with HiperDispatch enabled. It is advised to activate HiperDispatch for production workloads as a best practice.

4.5 IBM z17 AI acceleration

IBM z17 has enhanced AI acceleration capabilities with the introduction of the IBM Telum II processor Integrated AI Accelerator (on-chip AI accelerator) and Spyre Accelerator (PCIe-attached AI accelerator). They are built for high-speed inferencing—delivering deep learning and foundation model capabilities by using a multi-model method that focuses on performance and accuracy. This next-generation AI acceleration allows you to use more complex models for in-transaction workloads as well as certain generative AI use cases.

The Integrated AI Accelerator provides significant performance improvements, with a 4x increase in compute power, reaching 24 trillion operations per second (TOPS), and supports INT8 as a data type[8]. The IBM Spyre Accelerator enables the usage of foundation models and generative AI on the IBM Z platform. Now enterprises can securely and efficiently implement composite AI model architectures and AI assistants.

Composite AI refers to leveraging the strengths of multiple AI models, traditional and non-generative large language models, to improve the overall accuracy of a prediction, as compared to just using one. For example, composite AI can be used in insurance claim fraud detection, with a traditional neural network model being used to analyze and make a prediction based on structured data, while a large language model could then be used to extract information from the unstructured textual data associated with a claim, and generate a classification. This composite AI method can be applied for advanced detection of suspicious financial activities, support compliance with regulatory requirements, and mitigate the risk of financial crimes. With a composite AI architecture, business can reduce false positives and negatives, reduce potential losses, and reduce time spent on manual processing. On the IBM z17, such a composite AI architecture can be implemented to meet stringent transaction SLAs, allowing business decisions to utilize state of the art AI models in real-time.

Generative AI solutions such as IBM watsonx® Code Assistant™ for Z and IBM watsonx Assistant™ for Z will run on the IBM z17 platform utilizing IBM Spyre Accelerator cards.

IBM watsonx Code Assistant for Z helps to understand, optimize, refactor, transform, and validate COBOL code running on z/OS. This solution can accelerate the mainframe application lifecycle and streamline COBOL to Java modernization efforts. This solution is designed to increase developer productivity, reduce risks, costs, and time to value for a modernization initiative. Underneath, the solution leverages an IBM-trained foundation model fine-tuned for COBOL to Java translation.

IBM watsonx Assistant for Z can help unlock productivity for developers, operators, and programmers on the platform by providing a generative AI assistant that returns curated and site-specific responses to IBM Z-related questions. The assistant performs domain-specific Retrieval-Augmented Generation (RAG) to provide an accurate, detailed, step-by-step response based on a curated IBM Z knowledge base. This solution can also greatly reduce the learning curve needed for technical staff new to the IBM Z platform.

Notably, the watsonx Assistant for Z features integrated automation, allowing the execution of both routine and complex tasks on IBM Z through a chat interface. This automation can be triggered using Ansible or z/OSMF.

From the open-source perspective, IBM is offering several powerful containerized open-source AI solutions optimized to take full advantage of the hardware capabilities of the IBM Z platform. These container images are built from source, scanned for vulnerabilities, and can be retrieved free of charge from the IBM Z and LinuxONE container registry. However, enterprise organizations can face challenges adopting open-source offerings in critical business processes due to security, compliance, and support risks.

To alleviate this challenge, IBM has introduced the AI Toolkit for IBM Z and LinuxONE, which provides IBM Elite Support for several highly optimized AI runtime and serving solutions. In addition to support, these open-source AI solutions are built using IBM's secure engineering process, and are scanned and constantly monitored for vulnerabilities. The AI Toolkit for IBM Z and LinuxONE consists of the following AI solutions:

[8] INT8 uses 8-bit integers and integer math instead of floating-point numbers and floating-point math, reducing both memory and compute requirements.

- **IBM Z Accelerated for TensorFlow**: A popular Machine Learning and Deep Learning (ML/DL) Python framework optimized to run on IBM Z and leverage the IBM Z Integrated Accelerator for AI.
- **IBM Z Accelerated for PyTorch**: A popular ML/DL Python framework optimized to run on IBM Z and leverage the IBM Z Integrated Accelerator for AI.
- **IBM Z Accelerated for SnapML**: A Python library that optimizes the training and scoring of popular ML models optimized to leverage the IBM Z Integrated Accelerator for AI.
- **IBM Z Accelerated Serving for TensorFlow**: A flexible and highly performant AI model serving platform which transparently leverages the IBM Z Integrated Accelerator for AI.
- **IBM Z Accelerated for NVIDIA Triton Inference Server**: A high-performance inference server that supports the deployment of AI models which transparently leverages the IBM Z Integrated Accelerator for AI.
- **IBM Z Deep Learning Compiler**: A compiler which generates an executable program from Open Neural Network Exchange (ONNX) DL models to execute on the IBM Z Integrated Accelerator for AI.

By offering several different popular open-source AI frameworks and inferencing solutions, IBM is helping organizations leverage existing skill-sets and expertise to seamlessly and quickly integrate AI solutions on the IBM Z platform, all while transparently leveraging the performant hardware capabilities.

4.6 IBM z17 sustainability

IBM z17 is designed for end-to-end sustainability, which can reduce total cost of ownership (TCO) and energy costs, while helping adhere to global environmental regulatory requirements.

IBM z17 optimizes energy consumption by reducing power and cooling demands, hence lowering costs and carbon emissions. When compared to running the same workloads on previous generation systems, immediate savings in energy consumption and carbon footprint are achieved through improved performance per kilowatt, reduced shipping impacts, floor space savings, and simplification.

Additionally, the z17 provides sustainability instrumentation, enabling real-time power consumption reporting and monitoring at the LPAR level, with support from the operating systems, including z/OS[9], z/VM[10], and Linux on Z. These features allow for better tracking and management of power usage, making it easier for organizations to measure and improve their sustainability.

4.7 IBM Z cyber resiliency

IBM Z cyber resiliency is about maintaining uninterrupted operations, safeguarding sensitive data and defending against evolving cyber events.

[9] Power information is available by using SMF records. Post-processing will provide approximations of z/OS service-class level power consumption.

[10] Power Consumption metrics are provided within z/VM monitor, including CPC and LPAR specific level power consumption information.

IBM Z cyber resiliency is an extension of traditional disaster recovery (DR) and business continuity (BC) solutions, including reliability, availability, and serviceability capabilities of the system (and redundant systems), multiple immutable copies of data, and replicating data to multiple locations - eliminating single points of failure.

Simply put, cyber resiliency is the ability to “bounce back” from a disruptive event. Being able to bounce back quickly begins a cyber resiliency solution with core capabilities in addition to standard backup and recovery of data or systems, and existing DR and BC solutions. For IBM Z, these include:

- Starting with a resilient and reliable base.

  IBM Z is known for its reliability, availability, and serviceability (RAS) capabilities. RAS is built into the hardware and software stacks of the IBM z/Architecture, where mean time between failures (MTBF) is measured in decades. The RAS strategy is to manage change by learning from previous generations of IBM Z platforms and investing in new RAS functions to eliminate or minimize all sources of outages.

- Minimizing the duration of outages with failover capability.

  IBM Parallel Sysplex technology is an IBM Z clustering technology that enables a highly resilient, highly scalable, dynamic, and robust IBM Z environment to achieve near-continuous services and application availability. Hardware, middleware, and software tightly cooperate to achieve this result.

- Reducing the impact of outages with fault-tolerant architecture and GDPS.

  Redundancy, by itself, does not necessarily provide higher availability. It is essential to design and implement the IT infrastructure using technologies such as system automation, Parallel Sysplex, and GDPS offerings. These technologies can take advantage of the redundancy and respond to failures with minimal impact on service levels.

- Lessening risk with validated immutable copies of business critical data.

  Regularly creating tamper-proof backups that are stored in a secured, isolated environment provide the ability to recover your business in the event of data corruption. The IBM Z Cyber Vault solution takes a holistic approach to help identify and safely recover from a cyberattack using validated immutable copies of your critical data.

4.7.1 IBM Z RAS

IBM z17 offers the same high quality of service and RAS capabilities that is traditional in the IBM Z platform. The RAS strategy uses a building-block approach that meets the stringent requirements for achieving continuous, reliable operation. The following RAS building blocks are available:

- Error prevention
- Error detection
- Recovery
- Problem determination
- Service structure
- Change management
- Measurement
- Analysis

RAS designs consistently evolve through the integration of novel technologies, structures, and requirements. These ongoing advancements are inherently linked with new features and functions, guaranteeing top-tier resilience for IBM Z platforms.

IBM Z RAS is accomplished with concurrent replace, repair, and upgrade functions for processing units, memory, CPC drawers and I/O drawers, as well as I/O features for storage, network, and clustering connectivity. IBM Z RAS also extends to the non-disruptive capability for installing firmware (known as LIC, Licensed Internal Code), updates. In most cases, a capacity upgrade can be concurrent, without a system outage.

4.7.2 IBM Parallel Sysplex and IBM GDPS

IBM Parallel Sysplex expands on IBM Z RAS design. It is a clustering technology for logical and physical systems that allows highly reliable, redundant, and robust IBM Z environments.

Parallel Sysplex is an active-active cluster with up to 32 members (z/OS systems). The underlying structure of the Parallel Sysplex remains transparent to users, networks, and applications.

Normally, two or more z/OS images are clustered to create a Parallel Sysplex. Multiple clusters can span several IBM Z servers, although a specific image (LPAR) can belong to only one Parallel Sysplex.

A z/OS Parallel Sysplex implements shared-all access to data. This configuration is facilitated by IBM Z I/O virtualization capabilities allowing several LPARs to share I/O paths in a secure way, which maximizes usage and greatly simplifies the configuration and connectivity.

A suitably configured Parallel Sysplex cluster is designed to maximize availability at the application level. Quick recovery after a failure is an essential part of sysplex recovery, and that is why SRB boosts sysplex recovery events. Sysplex also provides redundancy so that the workload can continue to run on other systems in the sysplex. Rather than a quick recovery from a failure, the Parallel Sysplex design objective is zero application downtime.

Additionally, IBM GPDS can be used for clustering and server management, storage replication, and automation to enable continuous availability, disaster recovery, and cyber resiliency. It manages the storage subsystem and remote copy configuration across platforms, automates Parallel Sysplex operational tasks and performs failure recovery from a single point of control to reach continuous availability of up to 99.999999%.

For more information about IBM Z resiliency, see *Getting Started with IBM Z Resiliency*, SG24-SG24-8446.

4.7.3 IBM Z System Recovery Boost

IBM System Recovery Boost with the optional temporary capacity is a function to accelerate operating system and services start and shutdown times. IBM z17 also provides boosted processor capacity and parallelism for specific events, such as middleware starts and restarts, SVC dump processing, and IBM HyperSwap® configuration load and reload to minimize the impact on running workloads.

For more information, see *Introducing IBM Z System Recovery Boost*, REDP5563.

4.7.4 IBM Z Cyber Vault solution

Designed for continuous availability and rapid disaster recovery, IBM Z provides industry-leading resiliency to protect the business from downtime. Implementing an IBM Z Cyber Vault solution will help optimize availability, keep systems running, detect problems in advance and recover critical data in the event of intentional or unintentional data corruption.

The IBM Z Cyber Vault solution is built on point-in-time immutable copies of data from a production environment, stored in an isolated, secure, clean location, on which regular and proactive data analytics run to validate the infrastructure, data structures, and data content.

In the event of logical data corruption the IBM Z Cyber Vault solution allows you to perform forensic, surgical or catastrophic recoveries to the production environment.

The IBM Z Cyber Vault solution consists of three critical layers:

- Storage: IBM DS8000 Safeguarded Copy provides the ability to capture immutable point-in-time copies of data that cannot be corrupted or erased.
- Automation: IBM GDPS Logical Corruption Protection Manager provides the ability to automate the capture and restoration of these point-in-time backup without manual intervention.
- Environment: A dedicated, secured vault environment, separated from production for validation and forensic analysis and any point-in-time backup.

For more information, see Server and cyber resiliency with IBM Z and *Getting Started with IBM Z Cyber Vault*, SG24-8511.

Early detection of cyber incidents regarding data access has become vital to limiting system downtime. IBM Threat Detection for z/OS (IBM TDz) is a lightweight AI software product that identifies anomalies in accessing z/OS-related data and issues alerts to indicate a potential cyberattack.

IBM TDz includes policy and exclusion lists to minimize false positives and provides tangible artifacts for diagnosis and remediation.[11] IBM TDz can also enhance your security posture while helping satisfy compliance regulations (like DORA), requiring anti-malware for z/OS.

4.8 IBM Z cybersecurity

While commonly mistaken for one another, cybersecurity and cyber resiliency serve different purposes. Cybersecurity strives to prevent cyberattacks, whereas cyber resiliency focuses on diminishing potential impacts of successful breaches on service delivery.

With IBM Z cybersecurity, there is a perception that IBM Z is the most secure platform in the industry. Nevertheless, we suggest the IBM Z platform is better referred to as the most securable in the industry. Even though security has been built into all layers of the IBM Z stack since inception, IBM has always given the flexibility to use those security features and functions based on distinct requirements. Therefore, it is important to understand which security mechanisms are available and consciously decide about their use, such as:

- Before accessing any data, a user must first authenticate themselves by providing credentials that verify their identity. This level of security can be enhanced by requiring multiple forms of identification, like IBM Z Multi-Factor Authentication (MFA), which can, for example, send a code to a phone that is used to further authenticate a user.
- Once authenticated, access control mechanisms determine what data or functions the user is allowed to access based on their role or permissions. For example, IBM Resource Access Control Facility (IBM RACF®) manages user identities and enforces access control policies. IBM RACF also supports a common access control method where users are assigned roles with specific permissions based on their job function, known as role-based access control (RBAC).[12]

[11] Future Direction for IBM Threat Detection for z/OS: IBM intends to add network anomaly detection to its IBM Threat Detection for z/OS product.

- Encryption safeguards data both in transit and at rest; without the decryption key, unauthorized access yields illegible information. A variety of encryption algorithms are supported on IBM Z, catering to varying security levels - including quantum computing threats. The IBM z17 incorporates a secure boot mechanism, fortified by quantum-safe technology across its firmware layers during initialization. Authentic, IBM-approved firmware is the sole admissible component in this process. Firmware verification on IBM z17 hardware leverages dual-signature schemes, quantum-safe and classical digital signatures, with protection anchored in the IBM Z Root of Trust[13].

Future direction for tagging sensitive data on IBM Z:
IBM intends to leverage the Telum Processor, artificial intelligence, and machine learning technology to identify and classify sensitive data in z/OS data sets. This will provide an automatic function to discover, classify, and tag data, which will support organizations in implementing more targeted and effective security measures to protect that information.

An automated compliance solution called IBM Z Security and Compliance Center (zSCC) is also available for the IBM Z platform, which gathers data from IBM software and products to simplify audits, saving time and effort. zSCC is enhanced with Security Patch Insights for IBM z/OS, Custom Goals for ISV's and users and IBM Concert® integration for enterprise compliance coverage. In addition, pre-defined compliance profiles can be used with zSCC, see *Keeping Up With Security and Compliance on IBM Z*, SG24-8540.

4.8.1 Pervasive encryption

Cryptography and corporate security always were a fundamental aspect of IBM Z platform development. The IBM Z platform continues to enhance and introduce new cryptography features and functions. These changes ensure the highest level of protection of your data and applications, making the platform compliant with the mandatory industry and regulatory standards.

The corporate security consists of many levels, with the strategies and policies for all components of the infrastructure: applications, databases, network, storage, and others. The traditional approach lays in defining the data perimeters and applying encryption selectively only to those perimeters.

Because the data is almost never static in the system as it flows between various systems and applications, this selective approach has a significant disadvantage: After the data leaves the defined perimeter, it becomes exposed.

The selective paradigm presumes complex management of the overall infrastructure, where the failure to protect one of the components might lead to the security breach and compromise of the whole landscape.

Today, businesses demand a more comprehensive approach because applications might be subject to various cyberthreat attacks (both external and internal). Regulations around data privacy and protection also are becoming more demanding, such as the European Union (EU) General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI-DSS), and Health Insurance Portability and Accountability Act (HIPAA).

Pervasive encryption shifts this paradigm to a data-centric one: Data is becoming the new perimeter, and encryption applies to all data regardless of its origin and location.

[12] RBAC is a policy-neutral access control mechanism defined around roles and privileges. It can also be used to help achieve separation of duties.
[13] Root of Trust is a source that can always be trusted within a cryptographic system.

At the same time, this approach does not require costly application changes, and it is transparent to the applications and their service consumers.

Pervasive encryption provides 360 degrees of data encryption for data at-rest (stored in persistent storage) and data in-flight (transactions). This approach reduces the risks of a security breach and financial losses that are associated with it and adheres to standards and compliance.

Pervasive encryption uses hardware cryptography acceleration in IBM z17, which is proven to be more effective, performant, and stable compared to software encryption.

Pervasive encryption is enabled by using tight integration between IBM Z hardware and software, and includes the following features:

- Integrated cryptographic hardware:
  - CPACF is a coprocessor on every PU that accelerates symmetric encryption operations.
  - Crypto-Express features are hardware security modules (HSMs)[14] with the following features:
    - Compliance with Federal Information Processing Standards (FIPS) 140-2 Level 4, the highest level of compliance within this standard.
    - Acceleration of diverse cryptographic algorithms, including digital signature sign and verification processes.
    - Tamper-proof storage for private keys and other highly sensitive data.
  - The CPACF and Crypto-Express usage is implemented on the hardware level, and supported natively by all IBM Z operating systems, which provides the highest encryption performance.
- Data set and file (also known as volume) encryption: Linux on IBM Z volumes and z/OS data sets are protected by using policy-controlled encryption, without any need to change or modify the applications.
- Network encryption: Network data traffic is protected by using standards-based encryption from endpoint to endpoint.
- Storage encryption: Encrypting the storage subsystem disks and its file systems.
- CF encryption: This encryption secures the Parallel Sysplex infrastructure, including the CF links and data that stored in the CF, by using policy-based encryption.

Encryption key management

Unified Key Orchestrator for IBM z/OS is a centralized key management software that securely orchestrates the lifecycle of encryption keys across an enterprise's on-premises and cloud environments. It provides a single, trusted user interface to manage encryption keys, supports multiple cloud environments, and is designed for key management specific to IBM z/OS data set encryption. UKO offers various features, including data set dashboard, security-rich key generation, policy-based key generation, role-based access and dual control, external RESTful APIs, advanced auditability and compliance, key rotation, and multi-tenancy. Overall, UKO aims to help enterprises manage and secure their encryption keys, comply with security standards, and simplify their key management processes.

[14] An HSM is a hardware computing device that safeguards and manages digital keys for strong authentication and accelerated crypto-operations and algorithms.

4.8.2 Quantum-safe algorithms

IBM recognizes that with any new technology that new threats exist, and as such, suitable counter measures must be taken.

Quantum technology can be used for incredible good, but in the hands of an adversary, it has the potential to weaken or break core cryptographic primitives that were used to secure systems and communications. This potential leaves the foundation for digital security at risk.

The National Institute of Standards and Technology (NIST) has published the finalized standards for quantum-safe algorithms that would block attacks from both conventional and quantum computers.

IBM z17 uses quantum-safe standards to help protect your business-critical infrastructure and data from potential attacks, these include:

- FIPS 203 - ML-KEM

  Formerly known as CRYSTALS-Kyber, FIPS 203 - ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) is the primary algorithms NIST recommends to be implemented for most use cases around public-key encryption and key encapsulation mechanism (KEM). Among its advantages are comparatively small encryption keys that two parties can exchange easily, as well as its speed of operation.

- FIPS 204 - ML-DSA

  Module-Lattice-Based Digital Signature (ML-DSA) is the primary quantum-safe digital signature algorithm standard that should be used for use case around authentication and digital signatures. It was formerly known as CRYSTALS-Dilithium.

IBM z17 Secure Boot technology protects system firmware integrity by using quantum-safe and classical digital signatures to perform a hardware-protected verification of the Initial Machine Load (IML) firmware components. This protection is anchored in a hardware-based root of trust to help ensure that the system starts safely and securely by keeping unauthorized firmware (or malware) from taking over the system during startup.

IBM z17 enables the following quantum-safe capabilities:

- Key generation
- Encryption
- Key encapsulation mechanisms (KEMs)
- Hybrid key exchange schemes
- Dual digital signature schemes

In addition to the quantum-safe cryptographic capabilities, tools such as IBM Application Discovery and Delivery Intelligence (ADDI), IBM z/OS Integrated Cryptographic Service Facility (ICSF), and IBM Crypto Analytics Tool (CAT) can help you discover where and what cryptography is used in applications. These tools can aid in developing a cryptographic inventory for migration and modernization planning.

For more information, see *Transitioning to Quantum-Safe Cryptography on IBM Z*, SG24-8525.

4.8.3 Secure Boot for z/OS

IBM z17 provides support for performing a Validated Boot (IPL) of z/OS systems by using IPL volumes that are defined and built for Extended Count Key Data (ECKD) DASD devices.

The solution uses digital signatures to provide an IPL-time check that the z/OS system, including z/OS nucleus and LPA load module executable files, is intact, untampered with, and originates from a trusted source from the time at which it was built and signed. This approach enables the detection of subsequent unauthorized changes to those software executable files, whether those changes are accidental or malicious in nature.

When a z/OS server is built and digitally signed as part of the client's secure build process, the target system can undergo IPL by using List-Directed IPL (LD-IPL) with digital signature validation in either Enforce or Audit mode, or undergo IPL without digital signature validation by using channel command word IPL (CCW-IPL).

- In *Enforce mode*, an IPL stops if there are validation failures for any of the load modules that are protected by Validated Boot or if the necessary configuration requirements are not met.
- In *Audit mode*, the IPL continues, but audit records are produced to describe the problems that are encountered.

Using Validated Boot for z/OS is entirely optional and bimodal. A z/OS server can continue to be built without supporting or being signed for use with Validated Boot, and a z/OS server that has been built and signed for use with Validated Boot can undergo IPL either with or without validation.

4.8.4 IBM Secure Execution for Linux

IBM Secure Execution for Linux is the confidential computing technology of IBM Z that establishes a Trusted Execution Environment (TEE) to protect data and workloads inside a KVM LPAR. The workloads running in the KVM LPAR (as guests) are protected from inspection or modification. This protection defends against attacks from malicious software hypervisors, negligent or malicious hypervisor administrators, and negligent or malicious system administrators. It covers non-denial of service attacks that an infrastructure service provider can execute against a deployed workload using system interfaces. Combined with IBM Z pervasive encryption to protect data at rest and in flight, IBM Secure Execution for Linux adds data-in-use protection, ensuring data is safeguarded throughout its lifecycle.

IBM Secure Execution for Linux enables the deployment of workloads from encrypted and integrity-protected images. It ensures both confidentiality and integrity of workload data from the start to the termination of the secure guest, including data in memory that might be swapped out by the hypervisor. Dumps of a secure guest are encrypted using a cryptographic key provided by the workload owner. Secure guest attestation provides proof to an appraiser that a guest is running as a secure guest and identifies a specific secure guest instance. Additionally, attestation can prove to the appraiser that certain data originates from a given secure guest. Secure guests can use IBM Crypto Express adapters in accelerator or EP11 mode. A TEE based on IBM Secure Execution for Linux can maintain secrets on behalf of a secure guest. This feature restricts the usage of hardware security module (HSM) protected keys to the secure guest that generated the keys, preventing access by any other guest configured to access the HSM. Such keys are cryptographically bound to the given secure guest workload.

While an encrypted secure guest image might contain secrets (for example, passwords and cryptographic keys) that clearly identify the owner of a workload, a software vendor might want to sell a generic integrity-protected plaintext workload image that becomes a personalized instance when started by any customer. The IBM z17 system generation introduces a new class of secrets maintained by the TEE of IBM Secure Execution for Linux, allowing instance owners to securely and exclusively insert their secrets into a running secure guest using a mechanism called adding retrievable secrets.

These secrets can be retrieved by the IBM Secure Execution for Linux guest instance from the TEE as Crypto Processor Assist Facility (CPACF) protected keys. CPACF protected keys are bound to a specific guest and do not reveal the plaintext value of the key. Inside the instance, they can be used to perform cryptographic operations in the CPACF cryptographic accelerator of the z17 processor chip. With retrievable secrets, an IBM Secure Execution for Linux guest can securely generate protected keys without requiring a Crypto Express adapter. Additionally, a workload owner might request that dumps be disabled or encrypted using a newly provided key. These features support customers in securely personalizing a secure guest whose boot image was a generic image provided by a software vendor or IBM Hyper Protect.

On an IBM z17, the attestation result reflects the secrets that the TEE based on IBM Secure Execution for Linux maintains on behalf of the secure guest. IBM z17 provides additional on-chip AI capabilities through the integrated Accelerator for AI, which is within the data-in-use protection boundary provided by IBM Secure Execution for Linux. Solutions running with the TEE provided by IBM Secure Execution for Linux can seamlessly benefit from this accelerator.

Securing critical data in a hybrid cloud environment typically relies on operational assurance to ensure a service provider does not access customer workloads or data through specific procedures and measures. However, in today's dynamic cyberthreat landscape, characterized by relentless and unpredictable attacks, operational assurance alone is insufficient. A robust, hardware-based technical assurance approach is indispensable.

The IBM Hyper Protect product family leverages the unique capabilities of IBM Secure Execution for Linux to apply Confidential Computing in enterprise environments more easily. As containers are the state-of-the-art artifact for workloads, IBM Hyper Protect abstracts confidential computing to this layer. IBM Hyper Protect provides pre-built and hardened images that can only be deployed in IBM Secure Execution for Linux and enables workloads to be provided as OCI images, deployable in the provided container runtime after validation against policies. IBM Hyper Protect introduces an encrypted Hyper Protect contract concept to enable the cryptographic isolation of personas and roles (for example, Workload/Solution provider, Data Controller, Model Owner, Environment Operator, Auditor/Compliance Officer). The contract may also contain encrypted policies enforced by the Hyper Protect Layer within the TEE, ensuring sensitive data, AI models, and IP are protected and cannot be accessed or altered from outside the TEE. Hyper Protect validates that workloads deployed come from a trustworthy CI/CD and are signed to enforce supply chain protection.

The secure guest attestation of IBM Secure Execution for Linux can enforce the deployment of containerized workloads on defined systems as specified in the contract. The secure guest attestation results are part of the encrypted attestation record of a given IBM Hyper Protect instance. IBM Hyper Protect is designed to leverage the new technical features of IBM Secure Execution for Linux to provide a seamless container experience without the risk or complexity of third-party attestation or key management. IBM Secure Execution for Linux can maintain secrets on behalf of the secure guest, enhancing the capabilities and use cases of the encrypted Hyper Protect Contract. This contract enables proof of workload identity, time-based one-time passwords, zero-knowledge proofs, or Multiple-Key-Encryption combined with Keep-your-own-key for data-at-rest or data-in-transit protection within a TEE based on IBM Secure Execution for Linux.

The solution provides a TEE, set of secure processes, and patterns. See *IBM Hyper Protect Platform: Applying Data Protection and Confidentiality in a Hybrid Cloud Environment*, SG24-8555 for details. For more information, see IBM Secure Execution and IBM Hyper Protect Services.

4.8.5 Secure Service Container

In a production environment, applications are subject to any number of external (cyberattacks) or internal (malicious software, system administrators who use their privileged rights for unauthorized access, and many others) security risks. Secure Service Containers provide trusted execution environments for applications by using tamper protection during installation and run time, restricted administrator access, and encryption of data in-flight and at-rest.

A Secure Service Container is an integrated IBM Z appliance and hosts the most sensitive workloads and applications. It acts as a highly protected and secured digital vault that enforces security by encrypting the entire stack. The application that is running inside the Secure Service Container is isolated and protected from outsider and insider threats.

Secure Service Containers combine hardware, software, and middleware, and it is unique to the IBM Z platform. Although referred to as a container, it should not be mistaken for purely open-source containers like Docker or container platforms such as Kubernetes. A Secure Service Container is a pre-packaged appliance deployed to an IBM Z LPAR, which must be defined as a Secure Service Container via the IBM Hardware Management Console (HMC).

A Secure Service Container features the following key advantages:

- Existing applications require zero changes to use Secure Service Container. Software developers do not need to write any Secure Service Container specific programming code.
- End-to-end encryption of data-in-flight and data at-rest:
  - Encryption for both data in transit and at rest is facilitated through automatic mechanisms, including Transport Layer Security (TLS) and IPsec for data in motion, as well as various encryption algorithms for data at rest.
  - Automatic volume encryption (Linux Unified Key Setup (LUKS)): Data at-rest. LUKS is the standard way in Linux to provide volume encryption. A Secure Service Container encrypts all data with a key that is stored within the appliance.
  - Protected memory: Up to 16 TB can be defined per Secure Service Container LPAR.
- Encrypted Diagnostic Data.

  All diagnostic information (debug dump data and logs) is encrypted and do not contain any user or application data.
- No operating system access.

  After the Secure Service Container appliance is built, the Secure Shell (SSH) and command-line interface (CLI) are unavailable. This configuration ensures that even system administrators cannot access the contents of a Secure Service Container and do not know what application is running there.
- Applications that run inside a Secure Service Container are accessed externally by RESTful APIs only.
- Tamper-proof Secure Boot for a Secure Service Container.

  Eligible applications are booted into a Secure Service Container by using a verified start sequence, in which only software code that is trusted and digitally signed and verified by IBM is uploaded into the Secure Service Container.
- Vertical workload isolation is provided by PR/SM. PR/SM in IBM z17 is designed to meet the highest level of Common Criteria (EAL5+), similar to previous IBM Z servers.
- Horizontal workload isolation: Separation from the rest of the host environment.

4.8.6 IBM Fibre Channel Endpoint Security

IBM Fibre Channel Endpoint Security adds endpoint authentication and encryption to data in-flight. It can help reduce insider threats of unauthorized access to the data by using traces or switch logs, and it can help technicians who use Fibre Channel (FC) analyzers to examine the packets during problem determination.

IBM Fibre Channel Endpoint Security is designed to help ensure the integrity and confidentiality of all data that flows on the channels between trusted entities within and across data centers. The trusted entities are IBM z17 and the IBM Storage subsystem (select IBM DS8000 storage systems). No application or middleware changes are required. Fibre Channel Endpoint Security supports all data in-flight from any operating system.

IBM Security® Guardium® Key Lifecycle Manager acts as a trusted authority for key generation operations and as an authentication server. It provides shared secret key generation in a relationship between an FC initiator (IBM Z) and the IBM Storage target. The solution implements an authentication and key management solution that is called IBM Secure Key Exchange (SKE).

Before establishing the connection, each channel must be authenticated, and if successful, then it becomes a trusted connection. A policy sets the rules, for example, enforcing trusted connections only. If the link goes down, the authentication process starts again.
The secure connection can be enabled automatically if both the IBM Z and IBM Storage endpoints are encryption-capable.

Data in-flight (to or from IBM Z and IBM Storage systems) is encrypted when it leaves either endpoint (source), and then it is decrypted at the destination. Encryption and decryption are done at the FC adapter level.

In endpoint security-related operations, the operating system that runs on the IBM Z platform is not involved. Tools are provided at the operating system level for displaying information about encryption status.

IBM Fibre Channel Endpoint Security is an orderable feature for IBM z17 (FC 1146) and requires Central Processor Assist for Cryptographic Functions (CPACF) enablement (Feature Code 3863), specific storage (DS8900), and FICON Express32S or FICON Express32-4P features.

For more information and implementation details, see the *IBM Fibre Channel Endpoint Security for IBM DS8900F and IBM Z*.

4.9 Automation on IBM Z

IBM automation solutions for IBM Z can provide real-time visibility, streamlined workloads, and security for application development and integration.

The key benefits of IBM Z automation are to help optimize IT processes, simplify management, reduce skill requirements, improve performance, and enable system self-management.

Automation on IBM Z is a well-established collection of tools and services that automate repetitive tasks across many diverse areas, including:

- Performance observability
- Resiliency

- Monitoring
- Data migration
- System management

For more information about the tools and services that make up IBM Z system automation, see IT automation for IBM Z.

IBM Z integrates automated resiliency solutions to ensure business continuity and improve data movement across hybrid cloud environments, such as:

- IBM Z System Automation and NetView – Provides policy-driven failover automation, disaster recovery orchestration, and proactive incident response, reducing manual intervention in system failures.
- The GDPS LCP manager – Provides disaster recovery, continuous availability, and data replication across multiple sites, ensuring minimal downtime and data loss.

See IBM Z System Automation for more information about other automation products for managing hardware and software resources.

In addition, automation through Red Hat Ansible Automation Platform and IBM Terraform, improving both infrastructure provisioning and system management.

- Red Hat Ansible Automation Platform simplifies z/OS software management, system configurations, and hybrid cloud orchestration. With Ansible Certified Content for IBM Z, IT teams can automate LPAR provisioning, middleware deployment (like IMS and IBM CICS®), and security updates using declarative, repeatable playbooks. This reduces skill requirements and accelerates DevOps adoption.
- IBM Terraform for IBM Z enables Infrastructure-as-Code (IaC), allowing teams to provision, update, and version IBM Z resources with declarative configurations. This eliminates configuration drift, ensures consistency, and integrates IBM Z with cloud automation workflows.

Together, Ansible and Terraform unify automation across IBM Z and hybrid cloud environments, reducing complexity and accelerating IT modernization efforts. For details on infrastructure automation see Red Hat Ansible Automation Platform and “What is Terraform?”.

AI-driven automation advancements with IBM Z also offer numerous benefits, including task automation, improved efficiency, reduced human error, and enhanced application development and integration. By pairing AI and automation, operations can be streamlined and improved service can be provided with IBM Z AIOps.

4.9.1 Automation in IBM Z AIOps

IBM Z AIOps leverages AI and ML algorithms to analyze, detect, and predict system behaviors in real time. This approach reduces downtime, improves efficiency, and proactively resolves issues before they impact critical workloads. On IBM Z, AIOps delivers:

- Real-Time performance observability – AI continuously monitors system performance, detecting anomalies and predicting failures to ensure system stability.
- Automated incident response – By using ML-driven root cause analysis, z17 reduces mean time to resolution (MTTR) by automatically identifying the source of issues.
- Optimized workload Execution – AIOps dynamically adjusts workloads and system resources, ensuring high performance while minimizing costs.

These capabilities allow IBM z17 to self-manage IT processes, reducing operational complexity while increasing system reliability. For more information, see AIOps for IBM Z.

4.9.2 Application development and integration

IBM z17 automates software development and integration workflows to optimize DevOps pipelines and enhance productivity can be provided with the following:

- watsonx Assistant for Z – AI-driven natural language automation helps operators troubleshoot and execute tasks using an AI-powered assistant trained on IBM Z operations.
- IBM watsonx® Code Assistant™ for Z – Accelerate the application lifecycle and streamline COBOL to Java modernization efforts.
- IBM Test Accelerator for Z – Automates unit and integration testing, allowing developers to rapidly validate z/OS applications in virtual environments, improving code quality.
- z/OS Cloud Broker and Wazi Developer for Workspaces – Provides self-service access to z/OS

These tools reduce software development time, improve application reliability, and enable AI-assisted DevOps automation on IBM z17, see AI on IBM Z for more information.

5

IBM z17 software support

This chapter outlines the supported operating systems and accompanying software for the IBM z17 ME1 and its respective features.

The following major operating systems are supported:

- IBM z/OS
- IBM z/VM
- IBM z/TPF
- 21st Century Software VSE^n
- Linux on IBM Z and the Kernel-based Virtual Machine (KVM) hypervisor

> **Note:** Operating systems or software versions that have reached end-of-service status.

Support and usage of hardware functions depend on the operating system version and release. The information in this chapter is subject to change. For the most current information, see *Preventive Service Planning for IBM Z.*

This chapter describes the following topics:

5.1 Software support

The software portfolio for IBM z17 includes various operating systems and middleware that support the most recent and significant technologies. IBM Z software engineering prioritizes hybrid cloud capabilities, robust security features, resilience, artificial intelligence (AI) integration, and support for application modernization initiatives. For more information, see Mainframe software for IBM Z.

5.1.1 Application development and languages

Software developers can leverage the multiple programming language environments that run on the IBM Z platform. Compilers and development tool support for the IBM Z platform are continuously extended to provide developers with agile and modern development methods.

Application Development for Linux on IBM Z mirrors that of Linux on distributed systems; therefore, this chapter concentrates on providing insights into the z/OS environment.

In addition to the traditional COBOL, PL/I, Fortran, and assembly languages, the IBM Z platform supports:

- C
- C++
- Java (including Java Platform, Enterprise Edition, and batch environments)
- Go
- Swift
- Python
- JavaScript
- Node.js

IBM actively embraces open-source projects to extend z/OS functions. For example, the Zowe open-source project brings together industry experts to drive innovation for the community of next-generation mainframe developers. This framework enables an ecosystem of software solutions that are intended to provide a simple, intuitive environment for various IT professionals that are performing administrative, development, test, and operation tasks on z/OS.

The IBM z/OS Container Extensions (zCX) feature enables you to run Docker containers natively under z/OS. For more information, see z/OS Container Extensions (zCX).

An extensive set of advanced integrated development environments (IDEs) and integration tools are available for continuous development, testing, and deployment of application code.

The IBM DevOps offerings, such as IBM Application Delivery Foundation for z/OS and IBM Rational® Team Concert, can be coupled with IBM Application Discovery and Delivery Intelligence (ADDI) to enable developers to understand the applications, gain cognitive insights into the process, and “evolve” those valuable older assets at speed with reduced risk to the enterprise.

Modern development practices are supported by IBM Rational Team Concert and open-source-based Git Version Control Tools for IBM z/OS (ported by Rocket Software), which are modern source code managers that run on and support z/OS.

For more information about software for the IBM Z platform, see the Products catalog.

Note: Leveraging up-to-date compiler versions ensures access to the most recent advancements in IBM Z technology - including novel cache structures, machine instructions, and instruction execution enhancements - which collectively bolster performance gains.

IBM z17 inherits the features and functions from its predecessor, such as on-chip compression and sort, and single-instruction multiple-data (SIMD) architectural notation, which provides efficient vector processing.

Java applications benefit from Guarded Storage Facility (GSF), which enables pause-less garbage collection.

Operating systems that run on IBM z17 can use IBM System Recovery Boost (SRB) to accelerate recovery after an outage.

The following security functions were introduced to complement the IBM Z security stack:

- Secure Execution: Provides better isolation and security for second-level guest systems that are running under the KVM hypervisor for IBM Z servers.
- Secure Boot: A feature for verifying an open-source operating systems' kernel to ensure that it comes from the trusted provider.
- Quantum-safe cryptography algorithms.
- Fully homomorphic encryption.
- Processor Activity Instrumentation to count cryptographic operations.
- z/OS Validated Boot (initial program load (IPL)).

5.1.2 Supported IBM compilers

Each new version of the following IBM z/OS compilers underscores the continuing IBM commitment to the COBOL, PL/I, and C/C++ programming languages on the z/OS platform:

- Enterprise COBOL

  The most recent version of Enterprise COBOL delivers improved performance and advanced optimization. It supports the following items:

  – COBOL to Java Interoperability (for example, Java can call COBOL and vice versa).
  – UTF-8.
  – 64-bit JSON support.
  – JSON Boolean support for Parse and Generate.
  – Binary coded decimal (BCP to hex floating point (HFP) conversions.
  – Numeric editing operation.
  – Zoned decimal operations.

- IBM Automatic Binary Optimizer for z/OS

  The Automatic Binary Optimizer for z/OS improves the performance of compiled COBOL programs. It does not require source code, source code migration, or the tuning of performance options. It uses modern optimization technology to accelerate the performance of COBOL objects that are compiled by VS COBOL II V1.3 and later.

- Enterprise PL/I provides the following functions:
  - More hardware use: Perform Timing Facility Function (PTFF) instruction.
  - Enhanced diagnostics for SUBSCRIPTRANGE.
  - Modernization enhancements:
    - Enhanced COMPARE for XML and JSON.
    - Support for Extended Binary Coded Decimal Interchange Code (EBCDIC) JSON.
- z/OS XL C/C++

  z/OS XL C/C++ enables developing high-performance-oriented applications through the services that are provided by IBM Language Environment® and Runtime Library extension base elements. It also works with z/OS Problem Determination Tools.

  The latest version has the following features:

  - High-performance math libraries:
    - Mathematical Acceleration Subsystem (MASS).
    - Replace Atlas with OpenBLAS.
  - Metal C for modernization of IBM High Level Assembler (HLASM) applications.
  - Neural Network Processing Assist (NNPA) Facility.
- Java

  The latest version of Java supports the following features:

  - On-chip zEnterprise Data Compression (zEDC) support.
  - Crypto: Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic-curve Diffie-Hellman (ECDH) acceleration.
  - Zoned Decimal operations in the Data Access Accelerator (DAA) library for enhance interoperability.
  - Java enablement of Deep Learning Containers (DLC) models that use IBM Z Integrated Accelerator for Artificial Intelligence (AIU).

  IBM Enterprise COBOL and Enterprise PL/I support are strategic components (separately orderable products) for IBM Rational Developer for IBM Z software. These features provide a robust IDE for COBOL and PL/I and connecting web services, Java Platform, Enterprise Edition (Java EE) applications, and traditional business processes.

  z/OS XL C/C++ programmers also can use IBM Developer for z/OS to help boost productivity by editing, compiling, and debugging z/OS XL C and XL C++ applications from the workstation.
- IBM Open Enterprise SDK for Python

  Also available on z/OS is the IBM Open Enterprise SDK for Python (current version 3.13), which is based on the popular Python interpreter from Python Software Foundation (PSF):

  - z/OS LE-based, 64-bit only.
  - Runs on z/OS UNIX System Services environment with no prerequisites.
  - Supports ASCII, EBCDIC, and Unicode (UTF-8).
  - Includes selected Python Package Index (PyPI) packages.

For more information, see IBM Open Enterprise SDK for Python.

5.2 Support by operating system

This section lists the support of in-service operating systems. The current and minimum operating system levels required to support IBM z17 are listed in Table 5-1.

Table 5-1 Operating system requirements

Operating system	**End of service**	**Notes**
z/OS 3.1	September 30, 2028.	See IBM Fix Category Values.
z/OS 2.5	September 30, 2026.	
z/OS 2.4	September 30, 2024.	
z/VM 7.4	March 31, 2029	
z/VM 7.3	March 31, 2027	
z/TPF 1.1	Not announced.	
Linux on IBM Z	Support information is available for SUSE, Red Hat, and Canonical.	For more information about minimal and recommended distribution levels, see the Linux distributors' websites.
KVM hypervisor		
21st Century Software VSE^{n} V6.3.1 (plus PTFs)	Not announced.	For more information, see 21st Century Software.

Note: Program temporary fixes (PTFs) and Fix Categories: The usage of several features depends on a particular operating system. In all cases, PTFs might be necessary for the operating system level that is indicated. Review the IBM Z hardware Fix Categories (FIXCAT) before the operating system is installed. PTFs for z/OS, and z/VM can be ordered electronically from IBM Shopz.

For more information about obtaining access to download the z/TPF and z/TPFDF APAR packages, contact TPFQA@us.ibm.com.

For Linux on IBM Z distributions and the KVM hypervisor, see the distributor's support information.

Fix packs for IBM software products that are running on Linux on IBM Z can be downloaded from IBM Fix Central.

For more information about IBM z17 and its features, see *IBM z17 (9175) Technical Guide*, SG24-8579.

For more information about all of the I/O features, see *IBM Z Connectivity Handbook*, SG24-5444.

5.2.1 z/OS

As a pivotal IBM Z operating system, z/OS supports IBM z17. However, IBM z17 features and functions vary based on the specific z/OS version deployed.

The z/OS release cycle was extended with IBM Software Support Services to provide the ability to purchase extended defect support service for previous versions of the operating system.

The supported versions of z/OS include the following:

- z/OS 3.1 + PTFs
- z/OS 2.5 + PTFs
- z/OS 2.4[1] + PTFs

For more information about the IBM z17 features and functions that are supported by z/OS, see *IBM z17 (9175) Technical Guide*, SG24-8579.

For more information, see:

- IBM Support
- IBM z/OS
- IBM Resource Link

5.2.2 z/VM

IBM z16 support is provided with PTFs for z/VM 7.3 and 7.4.

For more information about z/VM, see IBM z/VM and for PTF availability, see z/VM Continuous Delivery News.

For more information about the IBM z17 features and functions that are supported by z/VM, see *IBM z17 (9175) Technical Guide*, SG24-8579.

5.2.3 z/TPF

IBM z17 support is provided by z/TPF 1.1 plus PTFs.

For more information, see z/TPF.

For more information about the IBM z17 features and functions that are supported by z/TPF, see *IBM z17 (9175) Technical Guide*, SG24-8579.

[1] z/OS 2.4 requires a service extension and offers toleration support only (no support of new IBM z17 functions).

5.2.4 Linux on IBM Z

The Red Hat, SUSE, and Ubuntu releases that are supported on IBM z17 are listed in Table 5-2.

Table 5-2 Linux on IBM Z distributions

Linux on IBM Z distribution	**Version and release**
SUSE Linux Enterprise Server	SUSE Linux Enterprise Server 16 with service
SUSE Linux Enterprise Server	SUSE Linux Enterprise Server 15 SP6 with service
SUSE Linux Enterprise Server	SUSE Linux Enterprise Server 12 SP5 with service (not as a Secure Execution KVM host)
Red Hat Enterprise Server	RHEL 9.4 with service
Red Hat Enterprise Server	RHEL 8.10 with service
Red Hat Enterprise Server	RHEL 7.9 with service (not as a KVM host)
Canonical	Ubuntu 24.04 LTS with service
Canonical	Ubuntu 22.04 LTS with service
Canonical	Ubuntu 20.04.1 LTS with service

For more information about the IBM z17 features and functions that are supported by the Linux on IBM Z distributions, see *IBM z17 (9175) Technical Guide*, SG24-8579.

For more information about Linux on IBM Z, see Linux on IBM Z.

5.2.5 Kernel-based Virtual Machine hypervisor

For IBM z17, the KVM is delivered and supported by the Linux distribution partners. For more information about KVM support for the IBM Z platform, see:

- The documentation for your distribution
- *Virtualization Cookbook for IBM Z Volume 5: KVM*, SG24-8463

5.3 Software licensing

The IBM Z software portfolio includes operating system software (that is, z/OS, z/VM, and z/TPF) and middleware that runs on these operating systems. The portfolio also includes middleware for Linux on IBM Z environments. For IBM z17, the following metric groups for software licensing are available from IBM (depending on the software product):

- Monthly license charge (MLC)

  MLC pricing metrics feature a recurring monthly charge. In addition to permission to use the product, the charge includes access to IBM product support during the support period. MLC pricing applies to z/OS, and z/TPF operating systems. Charges are based on processor capacity, which is measured in millions of service units (MSU) per hour.

- IBM Tailored Fit Pricing for IBM Z for software

  Tailored Fit Pricing for IBM Z is a flexible software pricing model that dramatically simplifies the pricing landscape through flexible deployment options that are tailored to your IBM Z environment.

Two new pricing solutions, Enterprise Consumption and Enterprise Capacity, offer alternatives to the rolling four-hour average (R4HA)-based pricing model for new and existing workloads.

- IBM International Program License Agreement (IPLA)

  IPLA metrics feature a single, up-front charge for an entitlement to use the product. An optional and separate annual charge, called *subscription and support*, entitles you to access IBM product support during the support period. With this option, you can also receive future releases and versions at no extra charge.

For more information about software licensing, see IBM Software Licensing, and for IBM Z pricing, see Pricing on IBM Z.

Subcapacity pricing terms for z/VM and select z/VM based programs

Subcapacity pricing is available to clients running on the z/VM 7 platform. Software pricing at less than full machine capacity can provide more flexibility and improved cost of computing as a client manages the volatility and growth of new workloads.

For more information about subcapacity pricing terms for z/VM and z/VM based programs, see Sub-capacity pricing terms for z/VM and select z/VM based programs help improve flexibility and price and performance.

For more information about software licensing options, see *IBM z17 (9175) Technical Guide*, SG24-8579.

Redbooks

IBM z17 Technical Introduction

(0.2”spine)
0.17”<->0.473”
90<->249 pages

SG24-8580-00

ISBN 0738461083

Printed in U.S.A.