IBM zEnterprise System enhancements

Table of contents

1 Overview
1 Key prerequisites
2 Planned availability date
2 Description
4 Product positioning
5 Announcement countries

At a glance

The following are now being made available:

- Processor Unit (PU) ratio modification for the IBM zEnterprise EC12 (zEC12) and IBM zEnterprise BC12 (zBC12) servers
  - Now 2:1 ratio for IBM System z Integrated Information Processor (zIIP)/IBM System z Application Assist Processor (zAAP) to general purpose processor (CP)
- IBM WebSphere DataPower Integration Appliance XI50 for zEnterprise (DataPower XI50z) V5.0 firmware for the IBM zEnterprise BladeCenter Extension (zBX) Model 002
  - Increased governance with improvements to help control insight into your service-oriented architecture (SOA)
  - Enhanced security by enforcement of security industry standards to Web 2.0 infrastructure and mobile applications
  - Enhanced processing power with extended memory support
- Common Cryptographic Architecture (CCA) enhancements on the IBM zEnterprise 196 (z196) and IBM zEnterprise 114 (z114) servers when the Crypto Express3 PCIe adapter is configured as a CCA coprocessor

Overview

On July 23, 2013, IBM communicated a modification to the zIIP/zAAP ratio for the zEC12 and zBC12 servers, exclusively. The maximum ratio of zIIPs/zAAPs to CPs for zEC12 and zBC12 servers is now 2:1 such that you may now acquire up to two zIIPs and up to two zAAPs for every CP acquired for the server. Previously, the maximum allowed configuration ratio for zEC12 and zBC12 servers was one zIIP and one zAAP for every CP.

The IBM WebSphere DataPower Integration Appliance XI50 for zEnterprise (DataPower XI50z) is a multifunctional appliance that can help to simplify, govern, and enhance the network security for XML and web services. Today, IBM is announcing support for DataPower XI50z firmware V5.0 for the zBX Model 002.

Common Cryptographic Architecture (CCA) enhancements are now being offered for the z196 and z114 servers when the Crypto Express3 PCIe adapter is configured as a CCA coprocessor. These CCA enhancements were previously made available for the Crypto Express4S PCIe adapter on the zEC12 and zBC12 servers.

Key prerequisites

- There are no dependencies for support of a 2:1 ratio of zIIPs/zAAPs to CPs on the zEC12 and zBC12 servers.
• For zBX Model 002 support of the DataPower XI50z, refer to the zBX Model 002 Hardware requirements in the Description section.

• For Crypto Express3 CCA enhancements on the z196 and z114 servers, refer to the Hardware requirements and Software requirements in the Description section.

**Machine Change Levels (MCLs) may be required.**

Descriptions of the MCLs are available on Resource Link.

Access Resource Link at


Refer to: Mainframe products (select Product), Planning, Machine Information, EC/MCL report.

MCLs are designed to be applied concurrently. Contact IBM service personnel for further information.

---

**Planned availability date**

October 29, 2013

• A 2:1 ratio of zIIPs/zAAPs to CPs on the zEC12 and zBC12 servers

November 30, 2013

• DataPower XI50z V5.0 firmware for zBX Model 002

December 18, 2013

• CCA enhancements on the z196 and z114 servers when the Crypto Express3 PCIe adapter is configured as a CCA coprocessor

---

**Description**

**Modification to the zIIP/zAAP specialty engines to CP ratio**

On July 23, 2013, IBM communicated a modification to the IBM System z Integrated Information Processor (zIIP)/IBM System z Application Assist Processor (zAAP) to general purpose processor (CP) for the IBM zEnterprise EC12 (zEC12) and IBM zEnterprise BC12 (zBC12) servers, exclusively. The maximum ratio of zIIPs/zAAPs to CPs for the zEC12 and zBC12 servers is now 2:1 such that you may now acquire up to two zIIPs and up to two zAAPs for every CP acquired for the server. Previously, the maximum allowed configuration ratio for zEC12 and zBC12 servers was one zIIP and one zAAP for every CP.

This 2:1 ratio also applies to Capacity Backup (CBU). During configuration of CBU you will be able to apply the 2:1 ratio when ordering CBU zIIP features and CBU zAAP features.

IBM zEnterprise 196 (z196), IBM zEnterprise z114 (z114), and earlier servers continue to follow the maximum 1:1 ratio.

**Software requirements for modification of zIIP/zAPP specialty engines to CP ratio:**

If you plan to deploy the zIIP/zAAP to CP 2:1 ratio, the zEC12 or zBC12 server requires at a minimum:

• z/OS V2.1 with PTFs.
• z/OS V1.13 with PTFs.
• z/OS V1.12 with PTFs.

**Additional support for the IBM BladeCenter Extension (zBX) Model 002**

**Firmware V5.0 support for DataPower XI50z now available for the zBX Model 002:** The IBM WebSphere DataPower Integration Appliance XI50 for zEnterprise (DataPower XI50z) is a multifunctional appliance that can help to simplify, govern, and enhance the network security for XML and web services.

New support in DataPower XI50z V5.0 for WebSphere Service Registry and Repository (WSRR) subscription can help to distinguish similar Saved Search Queries and support automatic synchronization and enforcement between WSRR and DataPower. This is designed to provide more consumable and centralized service level agreement (SLA) management. DataPower XI50z V5.0 appliances support the IETF Open Authorization (OAuth) 2.0 protocol. Using the OAuth protocol helps to decrease the need to share your credentials with third parties. It is designed to provide an authorization service separate and apart from the resource owner. OAuth is focused on the emerging Web 2.0 infrastructure and the popularity of APIs that exist to provide customizable access to an organization's applications. For example, eBay provides an API to provide enhanced shopping experiences by integrating with third-party applications; Twitter and Facebook provide APIs that extend their applications by providing content sharing capabilities. Each of these integrations requires focused attention on all aspects of security and the need to consider all access to be untrusted until proven otherwise.

**AAA expanded to support other service objects:** Authentication, Authorization, Accounting (AAA - "triple A") for user or entity security is a framework within the WebSphere DataPower firmware. DataPower takes advantage of AAA extensively to support the OAuth 2.0 protocol. AAA is used to authenticate both the resource owner's and OAuth client's identities. It is also used for authorizing a request. In release 3.8.1, DataPower introduced form-based authentication, which is tied closely with web application firewall. As of firmware V5.0 AAA has been expanded to support other service objects. DataPower XI50z V5.0 is designed to act to protect access to resources when defined as a Policy Enforcement Point (PEP) for a resource server receiving and authorizing OAuth 2.0 requests. DataPower XI50z V5.0 firmware is also designed to improve processing power with extended memory support removing some of the limitations for large files.

The DataPower XI50z V5.0 firmware was previously made available for the zBX Model 003.

**Hardware requirements for Firmware V5.0 support for DataPower XI50z on the zBX Model 002:**

The zBX (machine type 2458) Model 002 for the z196 and z114 requires the following:

<table>
<thead>
<tr>
<th>Family</th>
<th>Machine type</th>
<th>Firmware driver</th>
<th>SE version</th>
</tr>
</thead>
<tbody>
<tr>
<td>z196</td>
<td>2817</td>
<td>93 MCL</td>
<td>2.11.1</td>
</tr>
<tr>
<td>z114</td>
<td>2818</td>
<td>93 MCL</td>
<td>2.11.1</td>
</tr>
</tbody>
</table>

**Common Cryptographic Architecture (CCA) enhancements for the z196 and z114 servers**

When the Crypto Express3 PCIe adapter is configured as a CCA coprocessor, the following cryptographic enhancements are supported on select zEnterprise 196 (z196) and zEnterprise 114 (z114) servers:

**Export Triple Data Encryption Standard (TDES) key under Advanced Encryption Standard (AES) transport keys:** The AES encryption algorithm has greater security than the TDES encryption algorithm. CCA has added the ability to use AES key-encrypting keys (KEKs) to wrap your TDES keys to help begin moving to AES for key management. All of the TDES key wrapping functions are still available, but a parallel set of AES wrapping functions are now available for use.
**Diversified Key Generation Cipher Block Chaining (CBC) support:** During the Europay, Mastercard and Visa (EMV) smart card personalization process, session keys are derived and then used to secure messages to the EMV cards. Some EMV card personalization specifications require the use of TDES CBC mode to derive these session keys. This enhancement adds that capability to the existing key derivation options in CCA.

**Initial PIN Encrypting Key (IPEK) support:** The IPEK is the initial key that is loaded into a point-of-sale (POS) terminal before it is deployed for use, when that terminal will use the Derived Unique Key Per Transaction (DUKPT) key protocol. CCA has added a function that allows the Hardware Security Module (HSM) to securely derive an IPEK and return it to the application program in an encrypted key token, which can then be securely installed in a POS terminal.

**Remote Key Export (RKX) key wrapping method support:** In a previous release, CCA added the capability to wrap keys using a proprietary enhanced mode algorithm. This included the ability to set a default preference for the wrapping method to be used, as well as options to override that default in most CCA functions. The RKX function now supports that ability as well.

**Integration of User Defined Extensions (UDXs) into CCA:** A UDX is designed to allow you to add custom functions to the CCA application programming interface (API) running in the Hardware Security Module (HSM). CCA has included the following three UDXs in the standard CCA APIs, avoiding the requirement for a UDX: Recover PIN from Offset, Symmetric Key Export with Data, and Authentication Parameter Generate.

These CCA enhancements are supported by z/OS and by z/VM for guest exploitation.

**Hardware requirements for CCA enhancements:**

When the Crypto Express3 PCIe adapter is configured as a CCA coprocessor, the cryptographic enhancements identified in this announcement apply to the following:

<table>
<thead>
<tr>
<th>Family</th>
<th>Machine type</th>
<th>Firmware driver</th>
<th>SE version</th>
</tr>
</thead>
<tbody>
<tr>
<td>z196</td>
<td>2817</td>
<td>93 MCL</td>
<td>2.11.1</td>
</tr>
<tr>
<td>z114</td>
<td>2818</td>
<td>93 MCL</td>
<td>2.11.1</td>
</tr>
</tbody>
</table>

**Software requirements for CCA enhancements:**

When the Crypto Express3 PCIe adapter is configured as CCA coprocessor, Export TDES key under AES transport key, Diversified Key Generation CBC, IPEK, RKX key wrapping method, and Integration of UDX into CCA require at a minimum:

- z/OS V2.1 with the Cryptographic Support for z/OS V1R13-z/OS V2R1 web deliverable (FMID HCR77A1).
- z/OS V1.13 with the Cryptographic Support for z/OS V1R13-z/OS V2R1 web deliverable (FMID HCR77A1).
- z/VM V6.3 for guest exploitation.
- z/VM V6.2 with PTFs for guest exploitation.
- z/VM V5.4 with PTFs for guest exploitation.

For a complete list of functions supported by the Crypto Express3 PCIe adapter on the z196 and z114 servers when configured as a CCA coprocessor refer to

http://www-03.ibm.com/systems/z/advantages/security/zbc12cryptography.html#4

**Product positioning**

**zAAP on zIIP specialty engines:** The zEC12 and zBC12 are planned to be the last System z servers to offer System z Application Assist Processor (zAAP) specialty engines - in the future IBM System z plans to offer only System z Integrated Information Processors (zIIPs) specialty engines.
z/OS V1.11 and later was enhanced with a capability called zAAP on zIIP that is
designed to enable zAAP-eligible workloads to run on zIIP specialty engines. This
capability is designed to allow you to run zIIP- and zAAP-eligible workloads together
on one type of specialty engine - the zIIP.

This is ideal for environments without enough zAAP- or zIIP-eligible workload to
justify a specialty engine today; the combined eligible workloads may make the
acquisition of a zIIP more cost-effective. This capability is also intended to provide
more value for enterprises having only zIIPs by allowing Java and XML-based
workloads eligible to run on existing zIIPs.

The zAAP on zIIP capability is designed to help optimize server resources and
simplify systems management by reducing the need to plan for and manage multiple
types of specialty engines. The ratio change in zIIP/zAAP to general purpose (CP)
processor ratio from 1:1 to 2:1 is designed to allow for easier migration.

With the doubling of the zIIP and/or zAAP to CP ratio, along with the zIIPs and
zAAPs merging into one engine, you now have twice as many specialty engines as
before. Therefore, you have an opportunity to offload more workload. The zIIPs
serve double duty (they can be assigned to Java execution when there is major
demand, and DRDA processing when that is important - or both, in workload-
dependent ratios). You may also achieve higher utilization rate.

DataPower XI50z V5.0 firmware for the zBX Model 002: The physical
integration of the multifunctional WebSphere DataPower Integration Appliance
XI50 for zEnterprise (DataPower XI50z) into the zBX Model 002 is designed to
help increase collaborative synergy across the system. New capabilities in the
DataPower XI50 V5.0 firmware have been designed to help strengthen the security
and governance needed to embrace mobile devices and extend support of social
business.

CCA enhancements: If your enterprise has z196 or z114 servers installed, with
Crypto Express3 features, you may benefit from the Common Cryptographic
Architecture (CCA) enhancements (Export TDES key under AES transport key,
Diversified Key Generation CBC, IPEK, RKX key wrapping method, and Integration of
UDX into CCA) when the PCIe adapter is configured as a CCA coprocessor.

Reference information


Refer to Hardware Announcement ZG13-0195, dated July 23, 2013.

Announcement countries

All European, Middle Eastern, and African countries except:

- Sudan
- Iran, Islamic Republic of
- Syrian Arab Republic

Trademarks

zEnterprise, IBM, WebSphere, DataPower, System z, BladeCenter, Resource Link,
z/OS, z/VM and DRDA are registered trademarks of IBM Corporation in the United
States, other countries, or both.
Other company, product, and service names may be trademarks or service marks of
others.

Terms of use
IBM products and services which are announced and available in your country can be ordered under the applicable standard agreements, terms, conditions, and prices in effect at the time. IBM reserves the right to modify or withdraw this announcement at any time without notice. This announcement is provided for your information only. Reference to other products in this announcement does not necessarily imply those products are announced, or intend to be announced, in your country. Additional terms of use are located at:

Terms of use

For the most current information regarding IBM products, consult your IBM representative or reseller, or visit the IBM worldwide contacts page

http://www.ibm.com/planetwide/