Erich Amrehn Distinguished Engineer & Versatilist
CTO WW Client Center
Member of IBM Academy of Technology, TEC & WW zChampion Leader
Research & Development Boeblingen

DPM & SSC on IBM Z

GSE Hamburg Oktober, 2017

Thanks to

Carl Mayer
Andreas Bieswanger
Stefan Roscher
Roland Seiffert

AGENDA

- DMP Dynamic Partition Manager intro ,what & how
- SSC Secure Service Container intro, what & how

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

BigInsights	DFSMSdss	FICON*	IMS	RACF*	System z10*	zEnterprise*
BlueMix	DFSMShsm	GDPS*	Language Environment*	Rational*	Tivoli*	z/OS*
CICS*	DFSORT	HyperSwap	MQSeries*	Redbooks*	UrbanCode	zSecure
COGNOS*	DS6000*	IBM*	Parallel Sysplex*	REXX	WebSphere*	z Systems
DB2*	DS8000*	IBM (logo)*	PartnerWorld*	SmartCloud*	z13	z/VM*
DFSMSdfp						

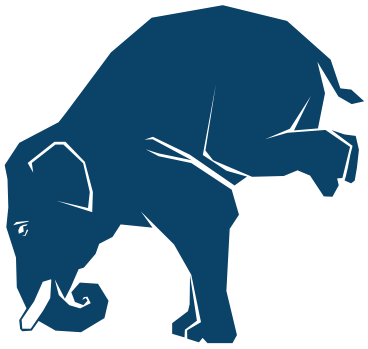
* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
Java and all Java based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
OpenStack is a trademark of OpenStack LLC. The OpenStack trademark policy is available on the OpenStackwebsite.
TEALEAF is a registered trademark of Tealeaf, an IBM Company.
Windows Server and the Windows logo are trademarks of the Microsoft group of countries.
Worklight is a trademark or registered trademark of Worklight, an IBM Company.
UNIX is a registered trademark of The Open Group in the United States and other countries.
* Other product and service names might be trademarks of IBM or other companies.

Notes:
Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the 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.
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.
This information provides only general descriptions of the types and portions of workloads that are eligible for execution on Specialty Engines (e.g, zIIPs, zAAPs, and IFLs) ("SEs"). IBM authorizes customers to use IBM SE only to execute the processing of Eligible Workloads of specific Programs expressly authorized by IBM as specified in the "Authorized Use Table for IBM Machines" provided at www.ibm.com/systems/support/machine_warranties/machine_code/aut.html ("AUT"). No other workload processing is authorized for execution on an SE. IBM offers SE at a lower price than General Processors/Central Processors because customers are authorized to use SEs only to process certain types and/or amounts of workloads as specified by IBM in the AUT.

The Host learns new Tricks



DPM & SSC

Mainframing made easier

IBM Dynamic Partition Manager Intro

What if

you are now able to create a new partition including I/O configuration within 10 minutes through a single management endpoint?

Back to reality

Deep mainframe knowledge required

Several management endpoints

Complex platform management

IBM

We built it DPM

Dynamic Partition Manager

Overview

What is DPM

Power of DPM

Making of DPM

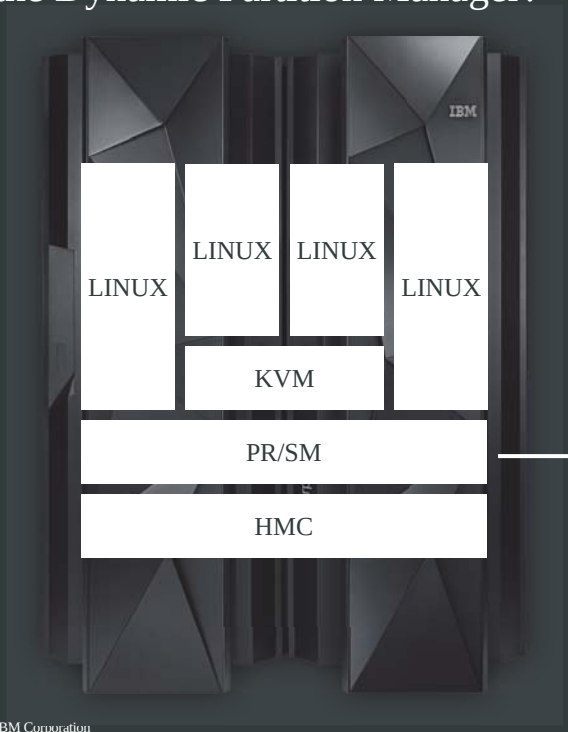
Overview

What is DPM

Power of DPM

Making of DPM

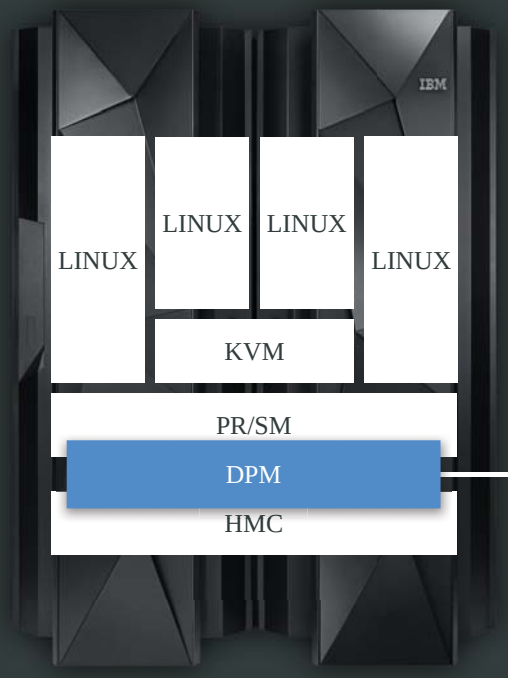
What is the Dynamic Partition Manager?



PR/SM

Powerful but complex

What is the Dynamic Partition Manager?



PR/SM + DPM

Powerful and easy

Overview

What is DPM

Power of DPM

Making of DPM

Introducing Adele

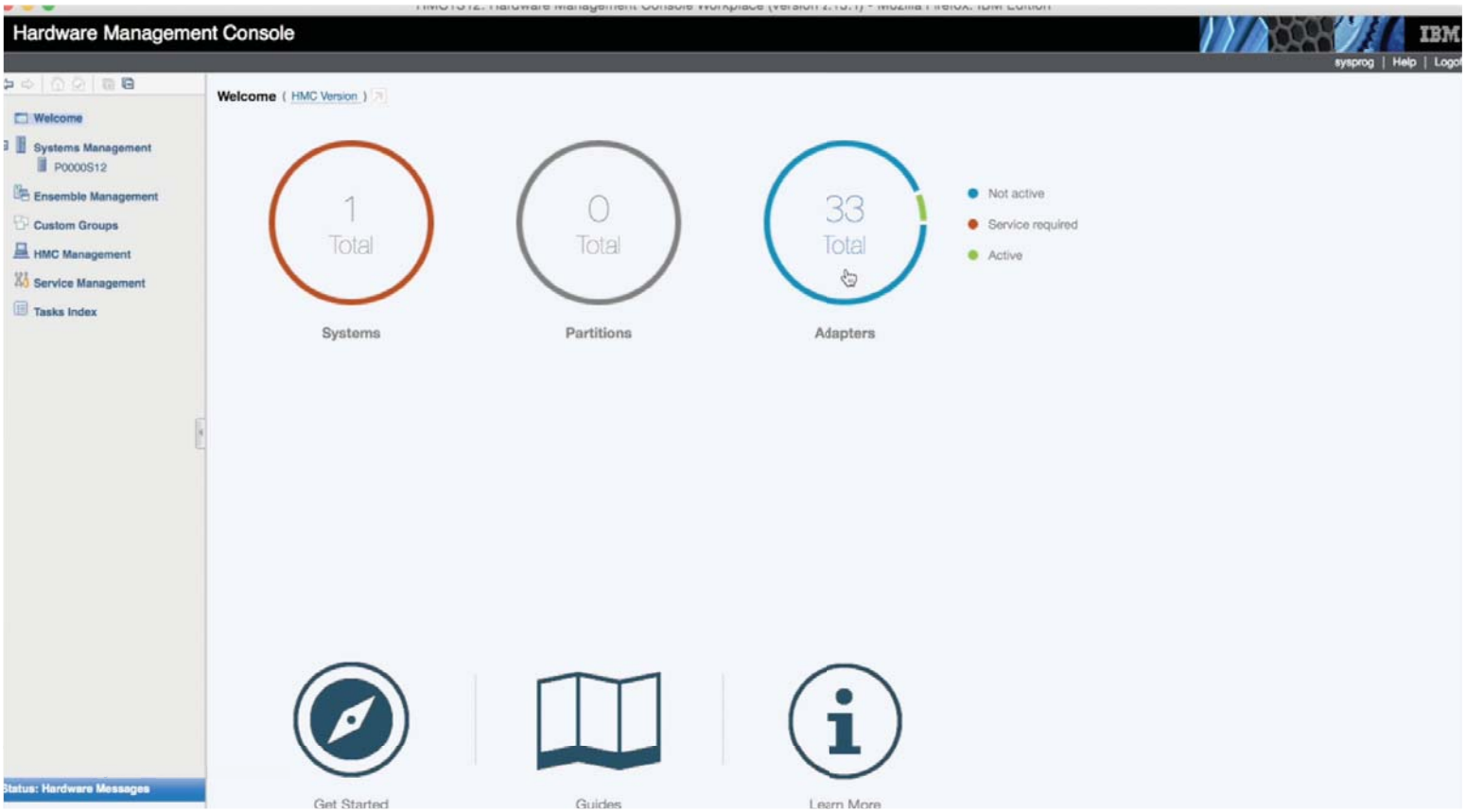
System Administrator
29 years old
From New York, NY

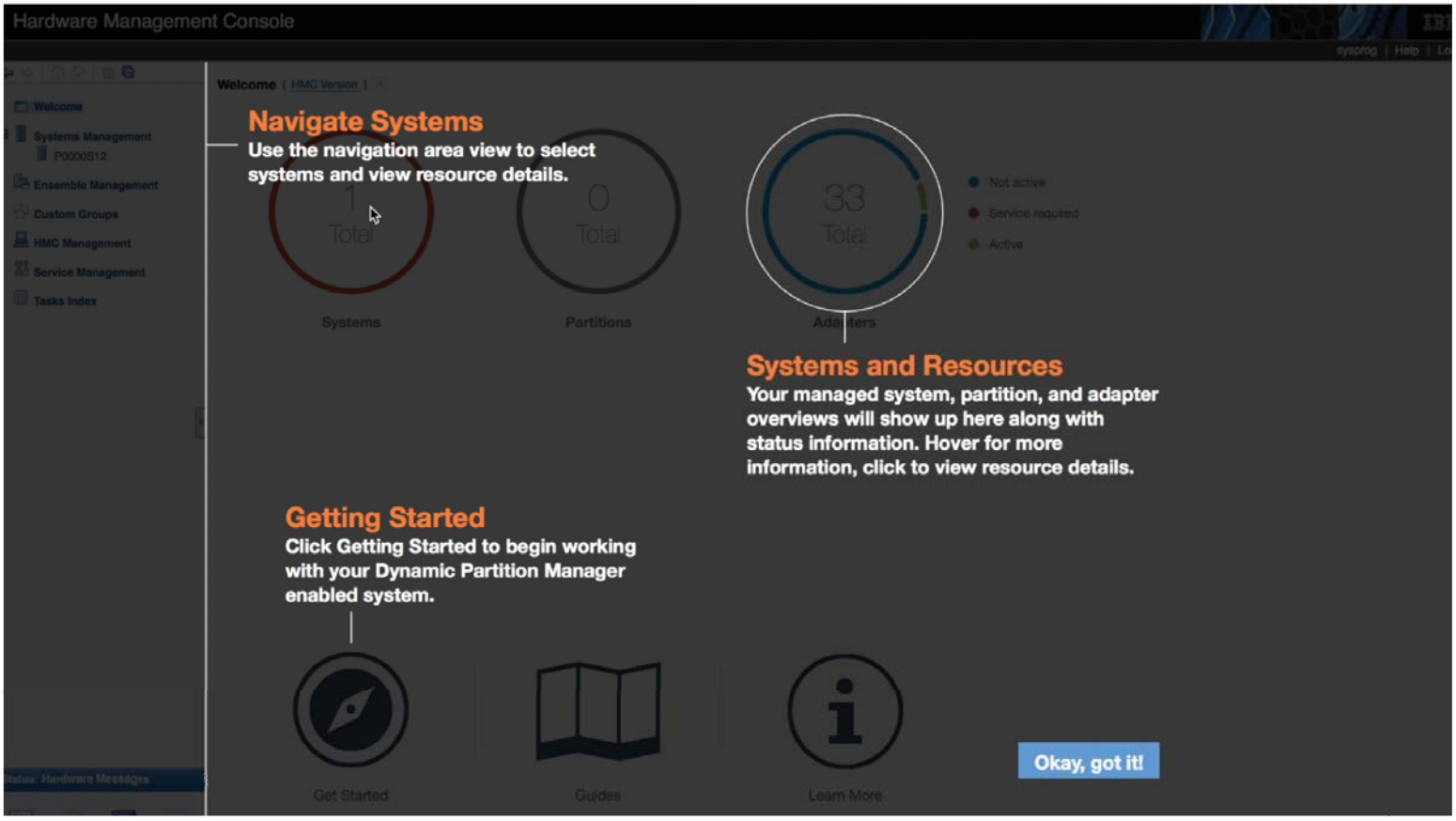
General virtualisation management skills
New to the mainframe

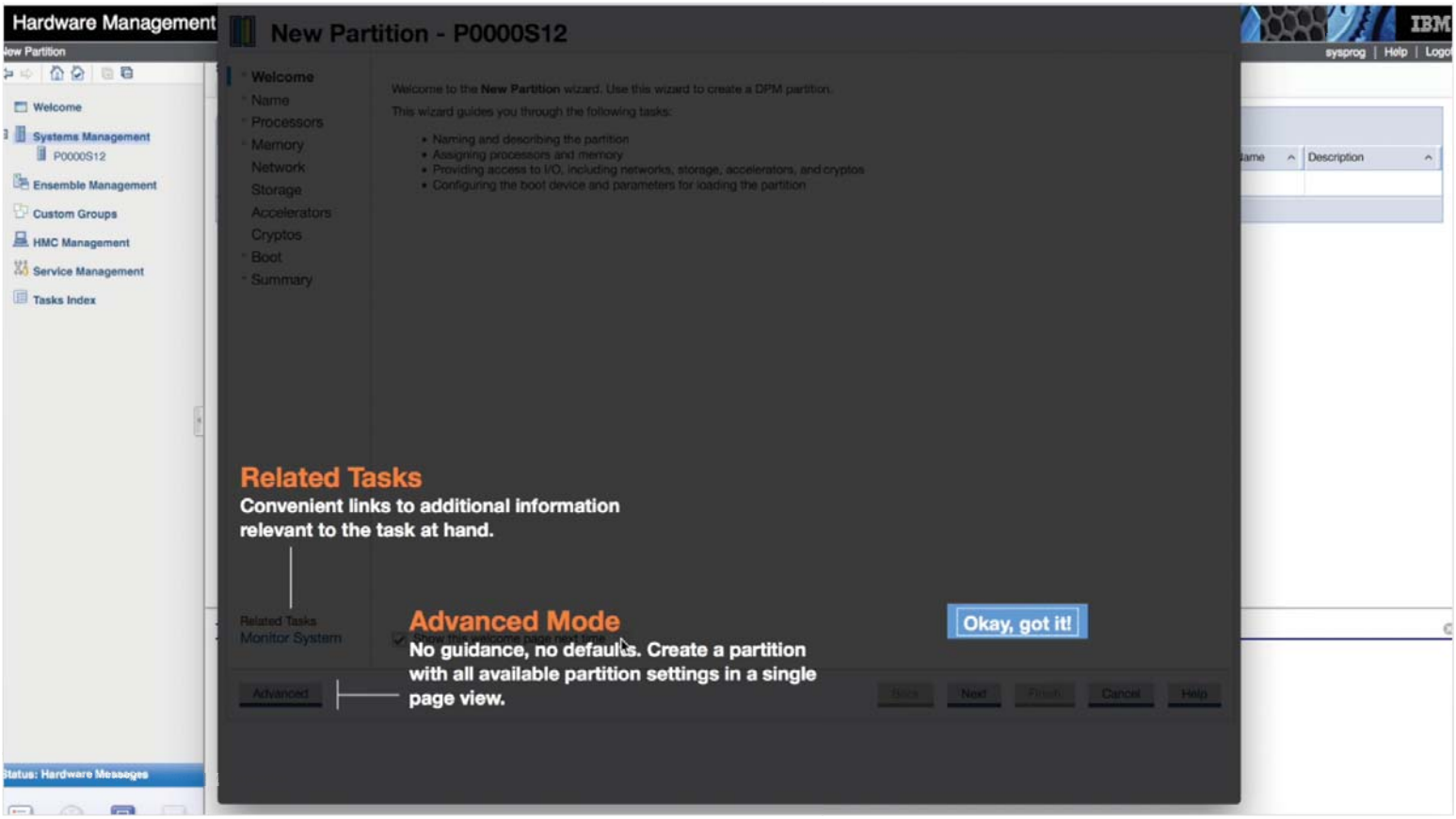
The Power of DPM

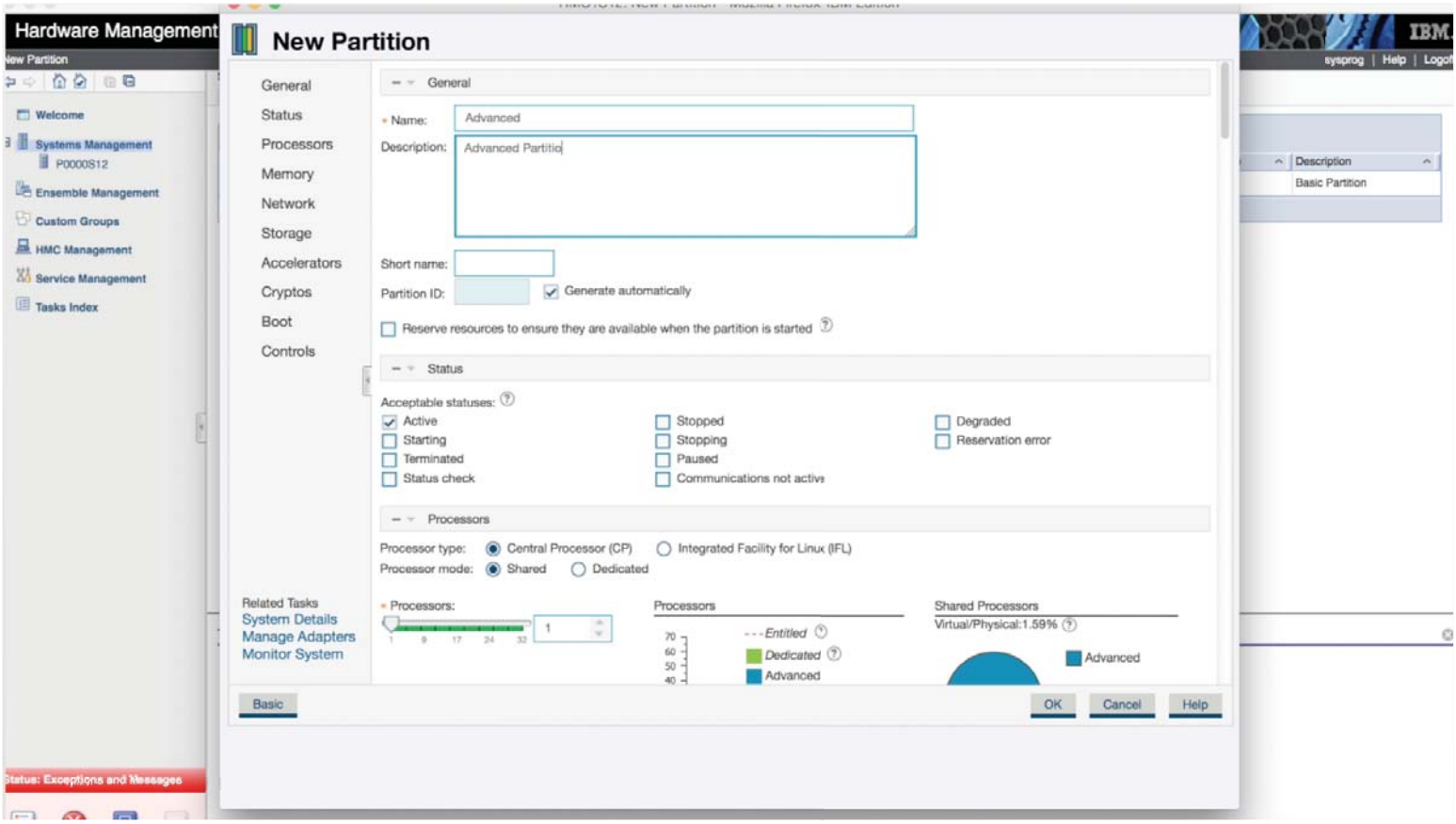
“I want to create a new partition including I/O configuration, within 10 minutes just by myself.”

Adele
System Administrator


Hardware Management Console
IBM
sysprog | Help | Logo
Welcome
Welcome (HMC Version)
Welcome
Systems Management
P0000S12
Ensemble Management
Custom Groups
HMC Management
Service Management
Tasks Index
1
Total
Systems
0
Total
Partitions
33
Total
Adapters
Not active
Service required
Active
Get Started
Guides
Learn More
Status: Hardware Messages


Hardware Management Console
sysprog | Help | Lo
Welcome
Welcome (HMC Version)
Systems Management
P0000512
Ensemble Management
Custom Groups
HMC Management
Service Management
Tasks Index
Navigate Systems
Use the navigation area view to select systems and view resource details.
1
Total
Systems
0
Total
Partitions
33
Total
Not active
Service required
Active
Systems and Resources
Your managed system, partition, and adapter overviews will show up here along with status information. Hover for more information, click to view resource details.
Getting Started
Click Getting Started to begin working with your Dynamic Partition Manager enabled system.
Get Started
Guides
Learn More
Okay, got it!


Hardware Management
New Partition - P0000S12
Welcome
Name
Processors
Memory
Network
Storage
Accelerators
Cryptos
Boot
Summary
Welcome to the New Partition wizard. Use this wizard to create a DPM partition.
This wizard guides you through the following tasks:
Naming and describing the partition
Assigning processors and memory
Providing access to I/O, including networks, storage, accelerators, and cryptos
Configuring the boot device and parameters for loading the partition
Related Tasks
Convenient links to additional information relevant to the task at hand.
Related Tasks
Monitor System
Advanced Mode
No guidance, no defaults. Create a partition with all available partition settings in a single page view.
Okay, got it!
Advanced
Back
Next
Finish
Cancel
Help
Welcome
Systems Management
P0000S12
Ensemble Management
Custom Groups
HMC Management
Service Management
Tasks Index
Status: Hardware Messages
IBM
sysprog | Help | Logo
Description

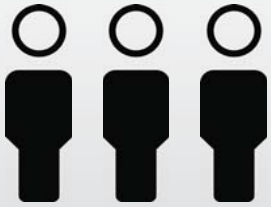

Hardware Management
New Partition
Welcome
Systems Management
P0000S12
Ensemble Management
Custom Groups
HMC Management
Service Management
Tasks Index
Status: Exceptions and Messages
IBM
sysprog | Help | Logoff
Description
Basic Partition
New Partition
General
Status
Processors
Memory
Network
Storage
Accelerators
Cryptos
Boot
Controls
General
Name: Advanced
Description: Advanced Partitio
Short name:
Partition ID:
Generate automatically
Reserve resources to ensure they are available when the partition is started
Status
Acceptable statuses:
Active
Starting
Terminated
Status check
Stopped
Stopping
Paused
Communications not active
Degraded
Reservation error
Processors
Processor type: Central Processor (CP) Integrated Facility for Linux (IFL)
Processor mode: Shared Dedicated
Related Tasks
System Details
Manage Adapters
Monitor System
Processors:
1
1 9 17 24 32
Processors
70
60
50
40
Entitled
Dedicated
Advanced
Shared Processors
Virtual/Physical:1.59%
Advanced
Basic
OK
Cancel
Help

Days

10 minutes

Several
management endpoints

Single
management endpoint



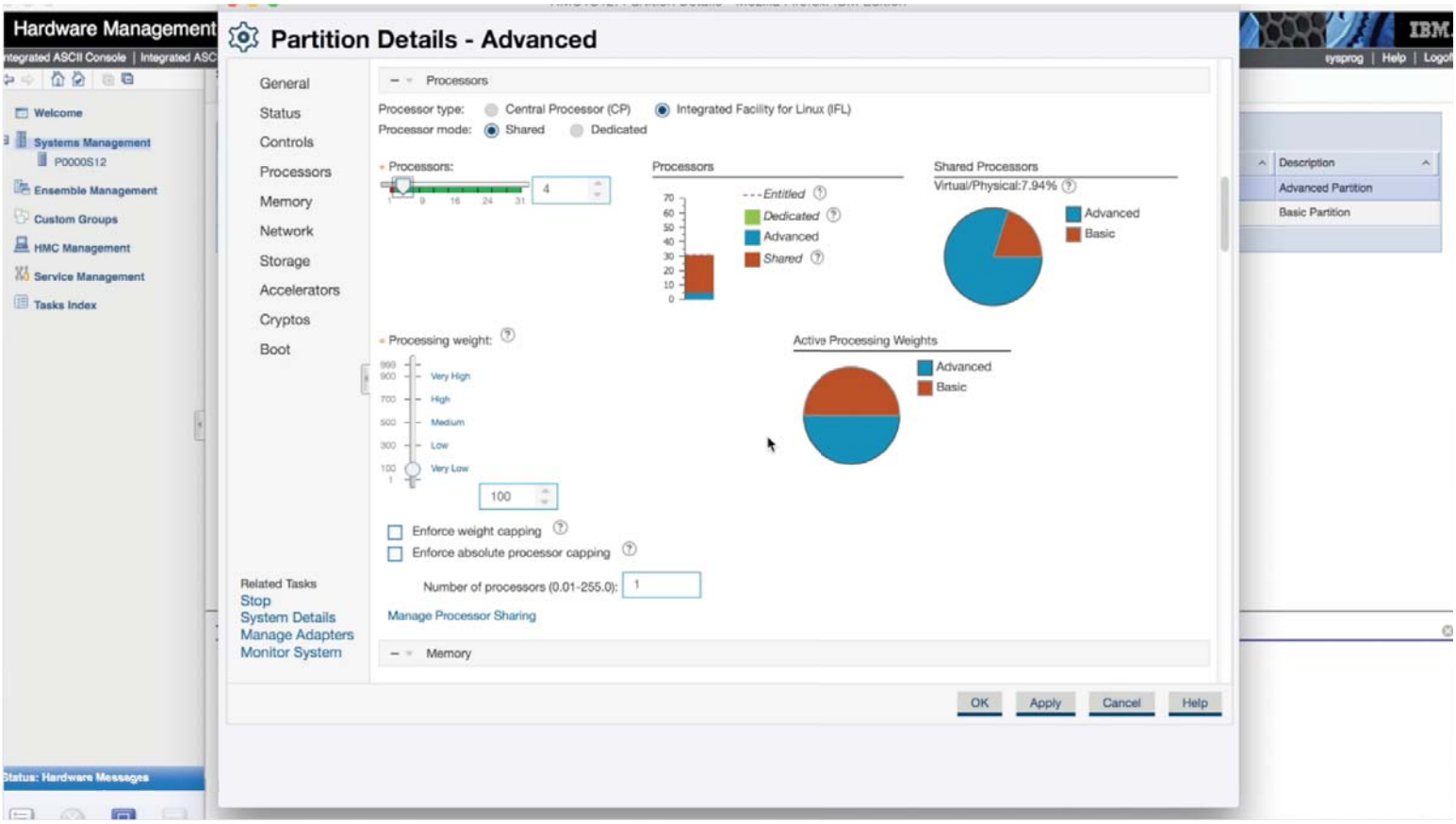
Several
System Administrators

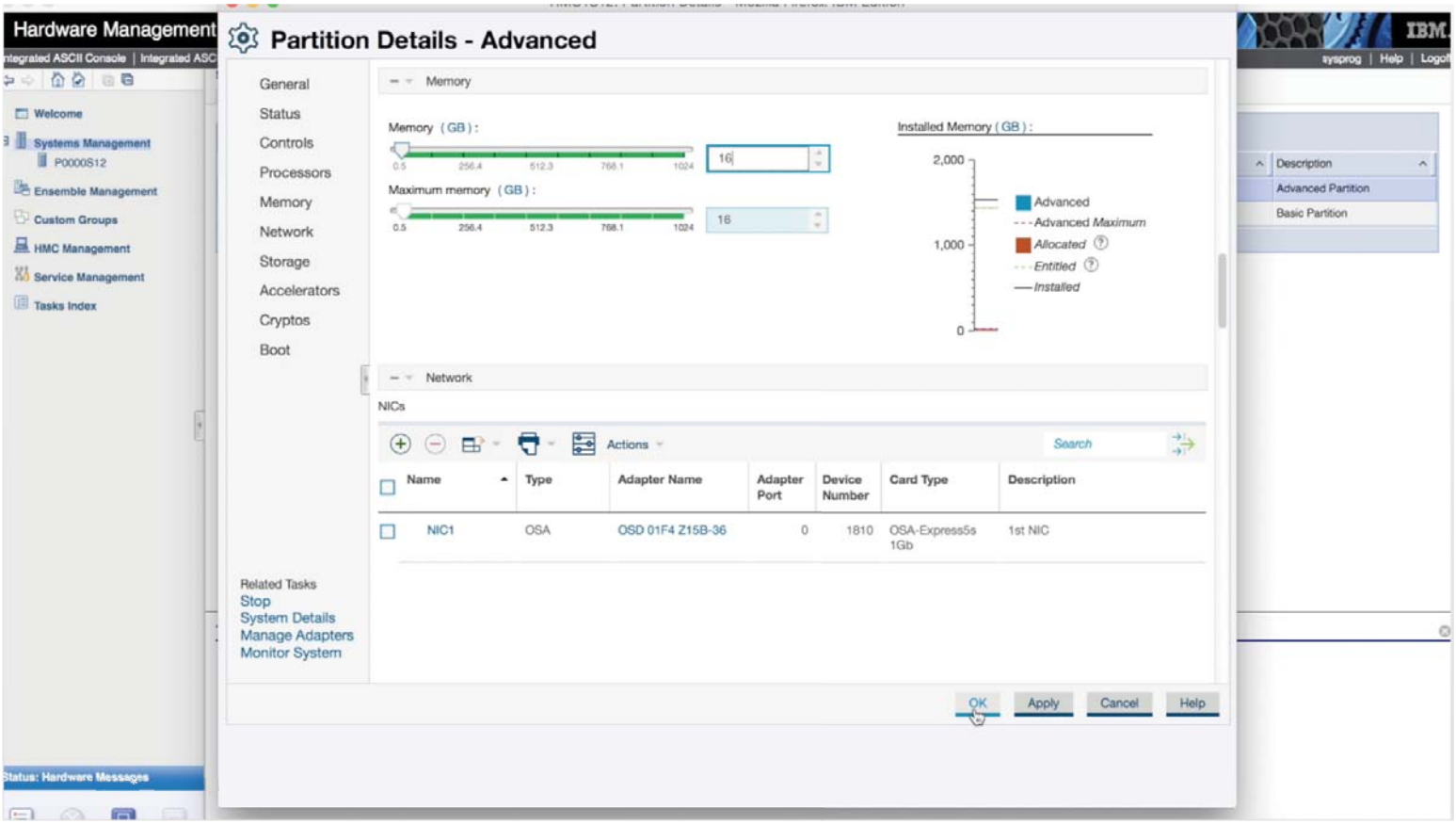
Single
System Administrator

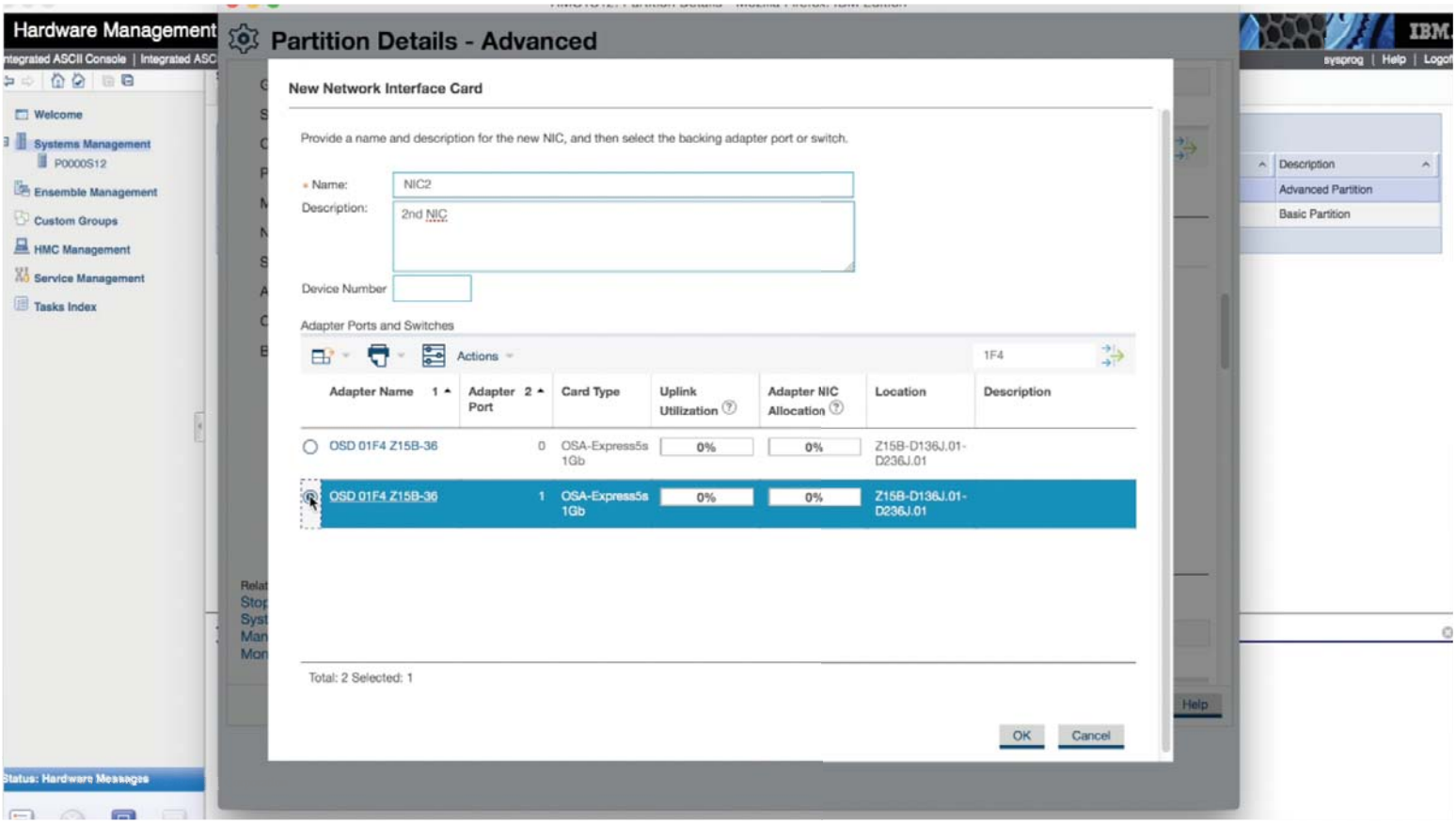
The Power of DPM

“I want to easily modify the system resources without interrupting the running workload by myself and within minutes.”

Adele
System Administrator


Hardware Management
Partition Details - Advanced
General
Status
Controls
Processors
Memory
Network
Storage
Accelerators
Cryptos
Boot
Processors
Processor type: Central Processor (CP) Integrated Facility for Linux (IFL)
Processor mode: Shared Dedicated
Processors:
4
Processors
Entitled
Dedicated
Advanced
Shared
Shared Processors
Virtual/Physical:7.94%
Advanced
Basic
Processing weight:
Very High
High
Medium
Low
Very Low
100
Active Processing Weights
Advanced
Basic
Enforce weight capping
Enforce absolute processor capping
Number of processors (0.01-255.0):
1
Manage Processor Sharing
Related Tasks
Stop
System Details
Manage Adapters
Monitor System
Memory
OK
Apply
Cancel
Help
Welcome
Systems Management
P0000S12
Ensemble Management
Custom Groups
HMC Management
Service Management
Tasks Index
Description
Advanced Partition
Basic Partition
sysprog | Help | Logoff


Hardware Management
Welcome
Systems Management
P0000S12
Ensemble Management
Custom Groups
HMC Management
Service Management
Tasks Index
Partition Details - Advanced
General
Status
Controls
Processors
Memory
Network
Storage
Accelerators
Cryptos
Boot
Memory
Memory (GB):
0.5
256.4
512.3
768.1
1024
16
Maximum memory (GB):
16
Installed Memory (GB):
2,000
1,000
0
Advanced
Advanced Maximum
Allocated
Entitled
Installed
Network
NICs
Actions
Search
Name
Type
Adapter Name
Adapter Port
Device Number
Card Type
Description
NIC1
OSA
OSD 01F4 Z15B-36
0
1810
OSA-Express5s 1Gb
1st NIC
Related Tasks
Stop
System Details
Manage Adapters
Monitor System
OK
Apply
Cancel
Help
Description
Advanced Partition
Basic Partition
Status: Hardware Messages

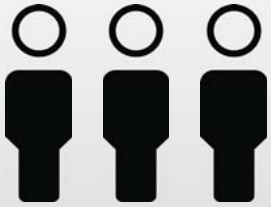

Hardware Management
Partition Details - Advanced
New Network Interface Card
Provide a name and description for the new NIC, and then select the backing adapter port or switch.
* Name:
NIC2
Description:
2nd NIC
Device Number
Adapter Ports and Switches
Actions
1F4
Adapter Name 1
Adapter Port 2
Card Type
Uplink Utilization
Adapter NIC Allocation
Location
Description
OSD 01F4 Z15B-36
0
OSA-Express5s 1Gb
0%
0%
Z15B-D136J.01-D236J.01
OSD 01F4 Z15B-36
1
OSA-Express5s 1Gb
0%
0%
Z15B-D136J.01-D236J.01
Total: 2 Selected: 1
OK
Cancel
Welcome
Systems Management
P0000S12
Ensemble Management
Custom Groups
HMC Management
Service Management
Tasks Index
Description
Advanced Partition
Basic Partition
Help
Status: Hardware Messages

Hours

Minutes

Several
management endpoints

Single
management endpoint



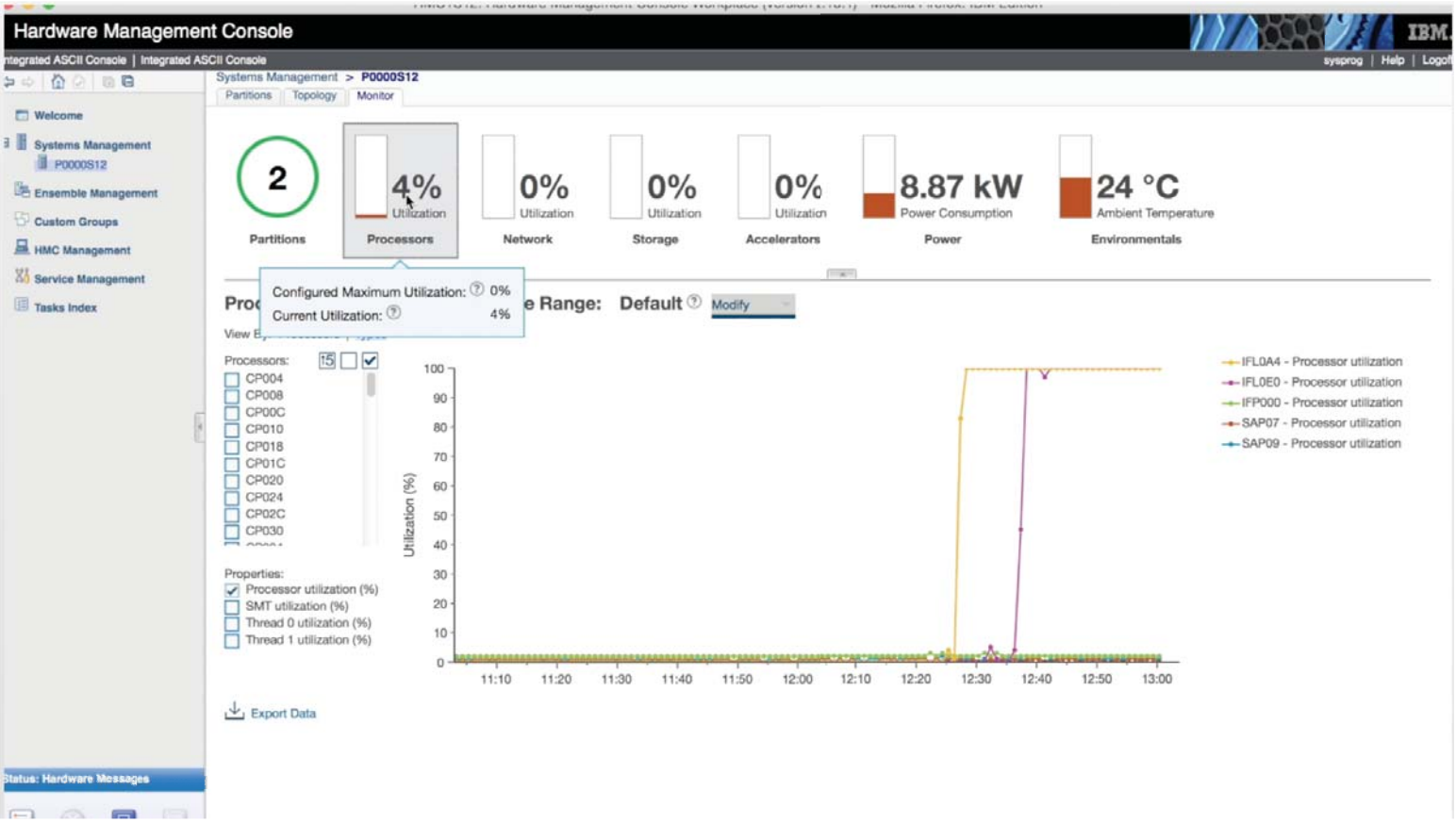
Several
System Administrators

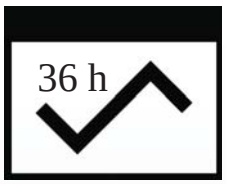
Single
System Administrator

The Power of DPM

“I need to get insights on how a system and its resources are doing over time.”

Adele
System Administrator


Hardware Management Console
IBM
Integrated ASCII Console | Integrated ASCII Console
sysprog | Help | Logoff
Systems Management > P0000S12
Partitions
Topology
Monitor
Welcome
Systems Management
P0000S12
Ensemble Management
Custom Groups
HMC Management
Service Management
Tasks Index
2
Partitions
4%
Utilization
Processors
0%
Utilization
Network
0%
Utilization
Storage
0%
Utilization
Accelerators
8.87 kW
Power Consumption
Power
24 °C
Ambient Temperature
Environmentals
Configured Maximum Utilization: 0%
Current Utilization: 4%
Range: Default
Modify
Processors:
CP004
CP008
CP00C
CP010
CP018
CP01C
CP020
CP024
CP02C
CP030
Properties:
Processor utilization (%)
SMT utilization (%)
Thread 0 utilization (%)
Thread 1 utilization (%)
Utilization (%)
100
90
80
70
60
50
40
30
20
10
0
11:10
11:20
11:30
11:40
11:50
12:00
12:10
12:20
12:30
12:40
12:50
13:00
IFL0A4 - Processor utilization
IFL0E0 - Processor utilization
IFP000 - Processor utilization
SAP07 - Processor utilization
SAP09 - Processor utilization
Export Data
Status: Hardware Messages



Monitoring data

Insights over time

Data scattered across several pages

All insights in one place

Web Services API


```
from vsmconst import *
from wsaconst import *
from wsautils import *
from vsmutils import *
import sys
import traceback


session = None

try :
    # Create session, then log onto target HMC ...
    session = session_startup()
    print '\nGet CPCs'
    cpcs = list_cpcs (session)
    cpcs_name= cpcs [0][ 'name' ]
    print
    print '----------------------------------------'
    print cpcs
    print
    print '\n CPC', cpcs_name
    raw_input('Press Enter to create new partition ...')

    cpcs_uri = cpcs [0][ 'object-uri' ]
    uri = cpcs_uri + "/partitions"
    inputBody = {
    "name":              "API Demo",
    "description":       "This partition is generated by the demo script",
    "initial-memory":    1024,
    "maximum-memory":    2048,
    "ifl-processors":    1,
    "processor-mode":    "shared",
    "boot-device":       "ftp",
    "boot-ftp-host":     "9.152.151.39",
    "boot-ftp-username": "hmcmanager", "boot-ftp-password": "        ",
    "boot-ftp-insfile" : "sample/sample.ins"
    }
    body = json.dumps(inputBody)
    print '----------------------------------------'
    print
    body = session.post(uri, body)
    print body
    print
    print 'New partition created!'
    print '----------------------------------------'
    print '----------------------------------------'
    raw_input('Press Enter to start partition ...')
    print '----------------------------------------'
    print
    newPartition_uri = body.body[ 'object-uri' ]
    start_uri = newPartition_uri + "/operations/start"
    print session.post(start_uri, None)
    print
    print 'Partition is starting ...'
    print '----------------------------------------'
    raw_input('Press Enter to stop partition ...')
    print '----------------------------------------'
    print
    stop_uri = newPartition_uri + "/operations/stop"
    print session.post(stop_uri, None)
    print 'Partition is stopping ...'
    print '----------------------------------------'
    raw_input('Press Enter to delete partition ...')
    print '----------------------------------------'
    print
    print session.delete(newPartition_uri)
    print
    print 'Partition deleted'
    print '----------------------------------------'

except ApiException as exception :
    # Exceptions raised due to an API error
    print exception
    print '\n\nFailed'
    sys.exit( WSA_EXIT_ERROR_API )
except ApiFatalException as exception :
    # Environmental exceptions
    print exception
    print '\n\nSetup failed'
    sys.exit( WSA_EXIT_ERROR_UNCAUGHT )
# Catch all for unexpected and uncaught exceptions ...
except Exception :
    traceback.print_exc()
    sys.exit( WSA_EXIT_ERROR_UNCAUGHT )

finally :
# Clean up active resource before exiting ...
    session_shutdown( session )

sys.exit(0)
```


Overview

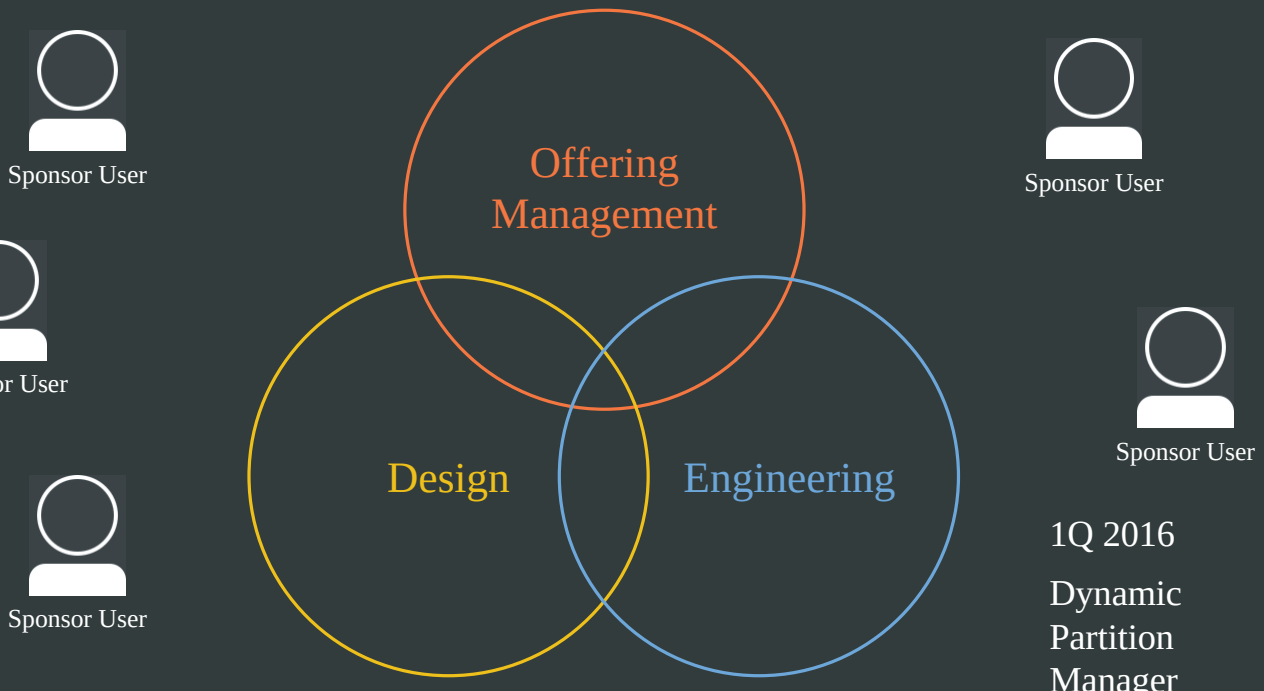
What is DPM

Power of DPM

Making of DPM

Making of the Dynamic Partition Manager

Making of the Dynamic Partition Manager



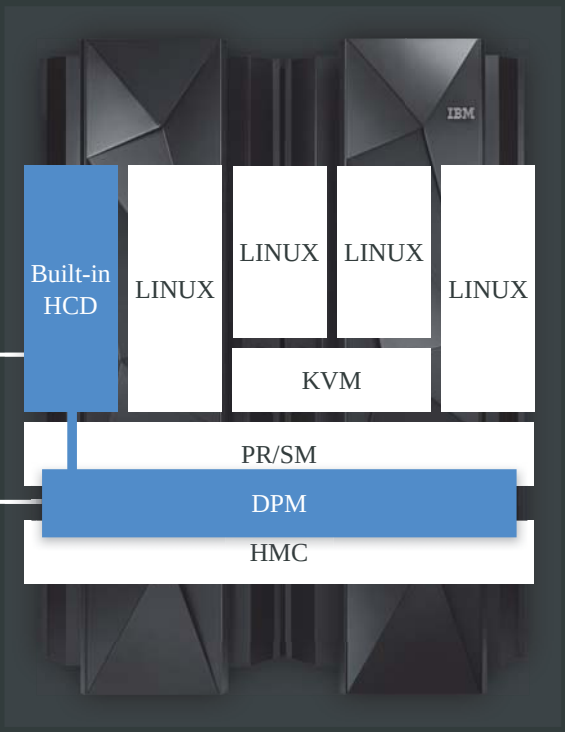
1Q 2016

Dynamic Partition Manager

Integrated, consistent User Experience

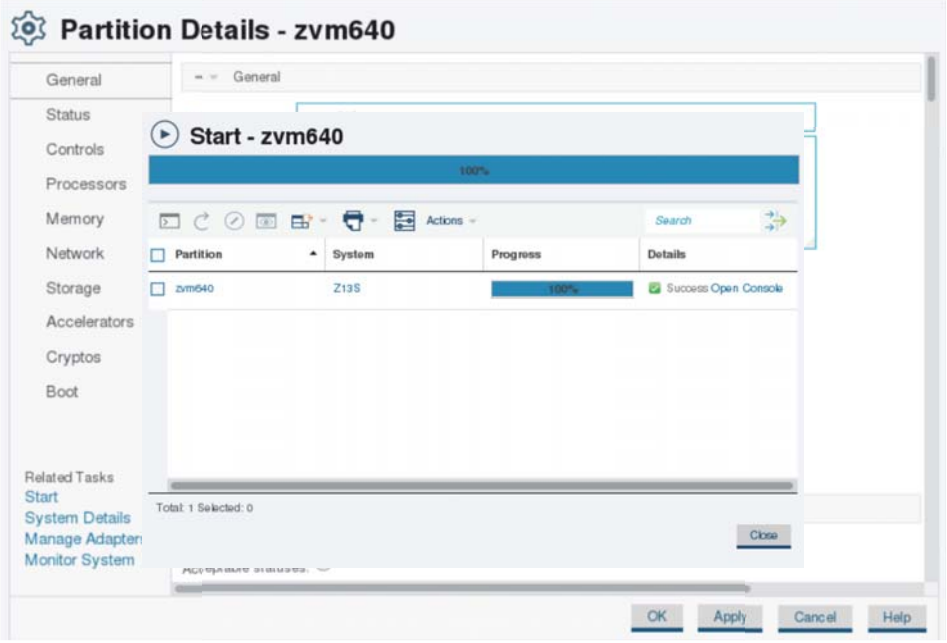
DPM + HCD

Hardware Configuration
Definition under the covers

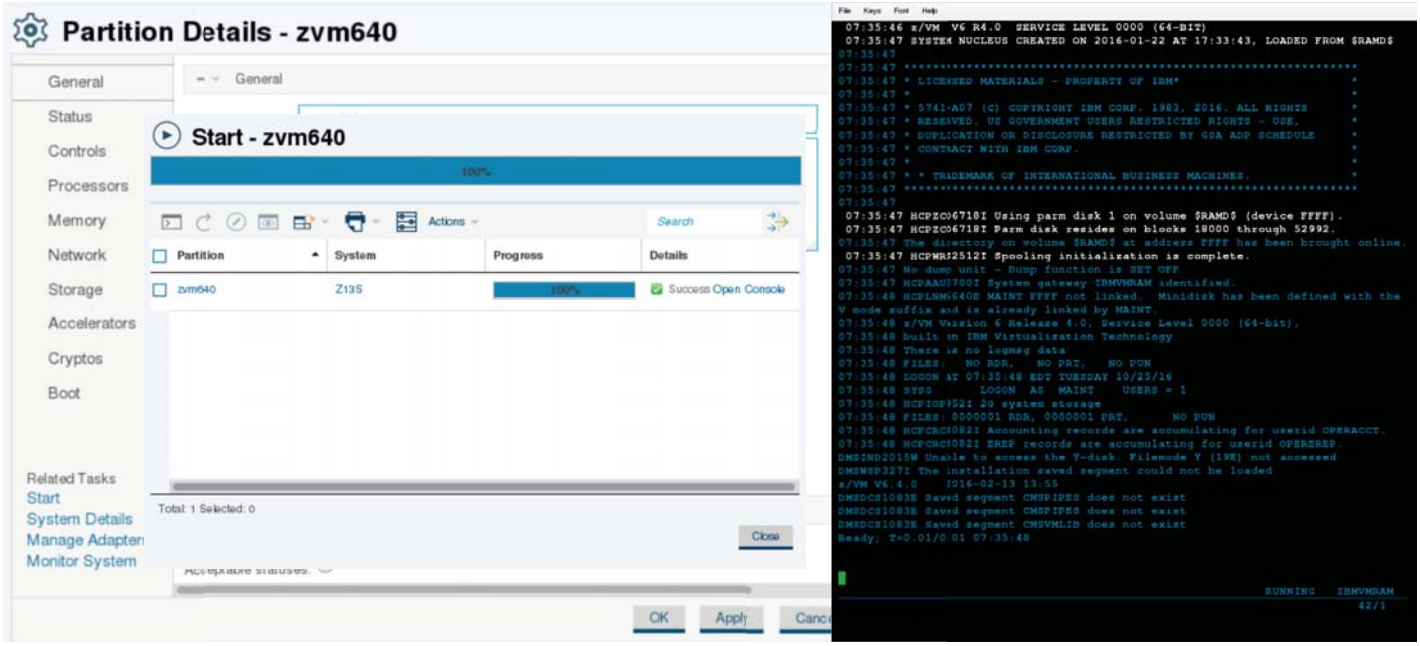


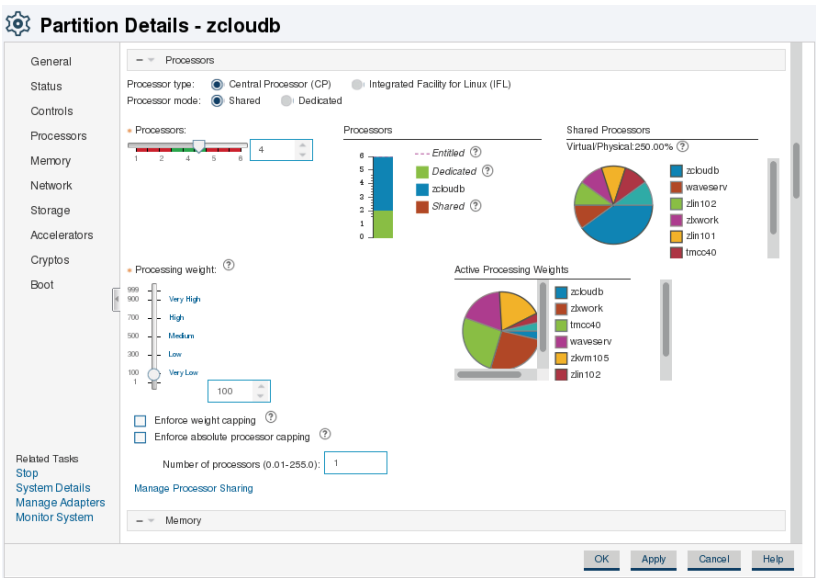
4Q16
z/VM support for FCP-only configurations with z/VM 6.4 GA

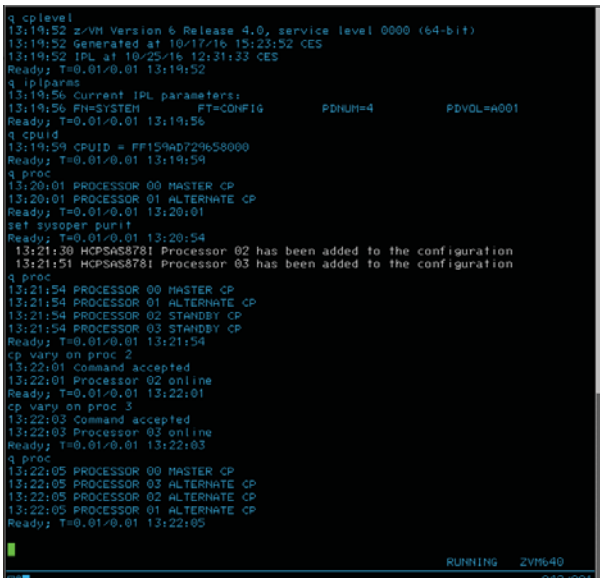
4Q16 - z/VM support for FCP-only configurations with z/VM 6.4 GA



4Q16 - z/VM support for FCP-only configurations with z/VM 6.4 GA



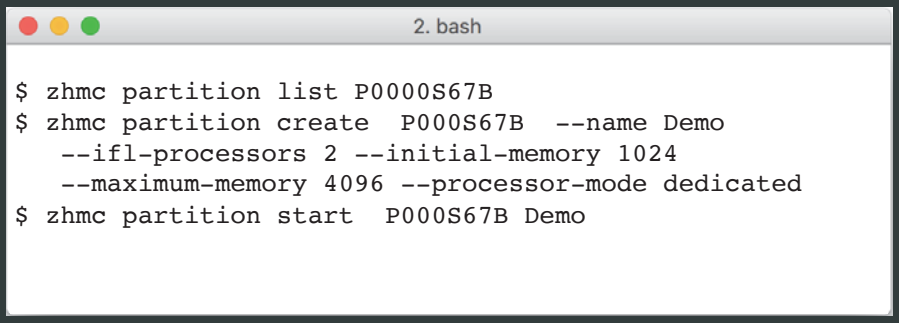




4Q16
zHMC Client
Python client library and CLI

4Q16 - zHMC Client - New python client library for HMC Web Services API

- Client library written in Python to easier consume HMC API
- Encapsulates REST over HTTPS and JMS protocols
- Enables automation with Ansible, Salt, Chef, Puppet, …
- Includes CLI with interactive and command mode



Currently support functionality:

- Start (a CPC in DPM mode)
- Stop (a CPC in DPM mode)
- New Partition
- Delete Partition
- Partition Details
- Start Partition
- Stop Partition
- Dump Partition
- PSW Restart (a Partition)
- Create HiperSockets Adapter
- Delete HiperSockets Adapter
- Adapter Details
- Manage Adapters
- Export WWPNs

Download: https://github.com/zhmcclient


```python
#!/usr/bin/env python
# Copyright 2016 IBM Corp. All Rights Reserved.

"""
Example shows lifecycle (Create-Read-Update-Delete) of a Partition.
"""

import sys
import logging
import yaml
import json
import requests.packages.urllib3
from pprint import pprint

import zhmcclient

requests.packages.urllib3.disable_warnings()

if len(sys.argv) != 2:
    print("Usage: %s hmccreds.yaml" % sys.argv[0])
    sys.exit(2)
hmccreds_file = sys.argv[1]

with open(hmccreds_file, 'r') as fp:
    hmccreds = yaml.load(fp)

partition_lifecycle = examples.get("partition_lifecycle", None)
if partition_lifecycle is None:
    print("partition_lifecycle not found in credentials file %s" % \
          (hmccreds_file))
    sys.exit(1)

hmc = partition_lifecycle["hmc"]
cpcname = partition_lifecycle["cpcname"]
partname = partition_lifecycle["partname"]

cred = hmccreds.get(hmc, None)
if cred is None:
    print("Credentials for HMC %s not found in credentials file %s" % \
          (hmc, hmccreds_file))
    sys.exit(1)

userid = cred["userid"]
password = cred["password"]

print("Using HMC %s with userid %s ..." % (hmc, userid))
session = zhmcclient.Session(hmc, userid, password)
cl = zhmcclient.Client(session)

timestats = partition_lifecycle.get("timestats", False)
if timestats:
    session.time_stats_keeper.enable()

print("Listing CPCs ...")
cpcs = cl.cpcs.list()
for cpc in cpcs:
    print(cpc)
```

```python
print("Finding CPC by name=%s ..." % cpcname)
try:
    cpc = cl.cpcs.find(name=cpcname)
except zhmcclient.NotFound:
    print("Could not find CPC %s on HMC %s" % (cpcname, hmc))
    sys.exit(1)

print("Finding Partition by name=%s on CPC %s ..." % (partname, cpc.name))
try:
    partition = cpc.partitions.find(name=partname)
except zhmcclient.NotFound:
    print("Partition %s does not exist yet" % partname)
else:
    print("Partition %s already exists - cleaning it up" % partition.name)
    status = partition.get_property('status')
    print("Partition %s status: %s" % (partition.name, status))
    if status == 'active':
        print("Stopping Partition %s ..." % partition.name)
        partition.stop()
    print("Deleting Partition %s ..." % partition.name)
    partition.delete()

properties = {
    'name': partname,
    'description': 'Original partition description.',
    'cp-processors': 2,
    'initial-memory': 1024,
    'maximum-memory': 2048,
    'processor-mode': 'shared',
    'boot-device': 'test-operating-system'
}
print("Creating a new Partition %s on CPC %s with following properties ..."
      % (partname, cpcname))
pprint(properties)
new_partition = cpc.partitions.create(properties)
print("New Partition %s created at: %s" %
      (new_partition.name, new_partition.uri))

print("Starting Partition %s ..." % new_partition.name)
new_partition.start()

print("Description of Partition %s: %s"
    % (new_partition.name, new_partition.get_property('description')))

new_description = "Updated partition description."
print("Updating partition description to: %s" % new_description)
updated_properties = dict()
updated_properties["description"] = new_description
new_partition.update_properties(updated_properties)

print("Refreshing properties of Partition %s ..." % new_partition.name)
new_partition.pull_full_properties()
print("Description of Partition %s: %s"
    % (new_partition.name, new_partition.get_property('description')))

print("Logging off ...")
session.logoff()

print("Done.")
```


1Q17
OpenStack for DPM enablement

1Q2017 - OpenStack for DPM Enablement

Initial deliverable available for OpenStack Ocata release (released 2/23/17)

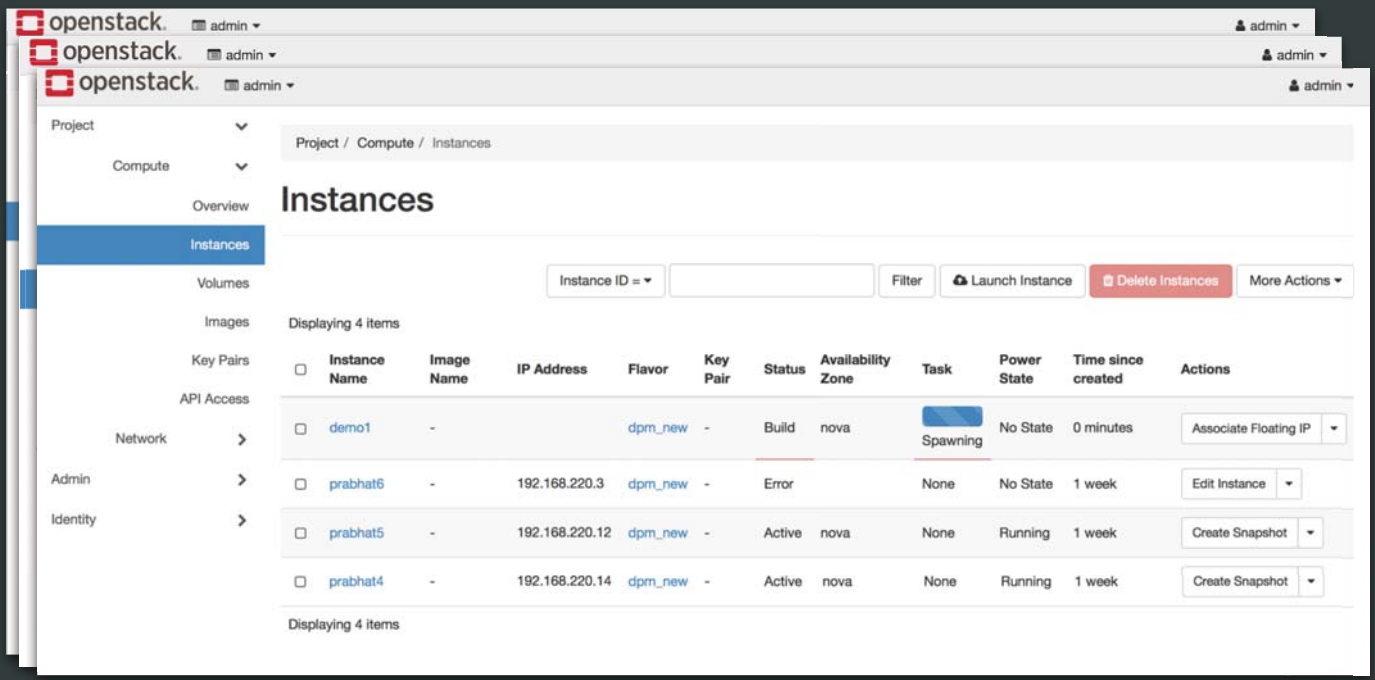
Feature Support Matrix

Feature	*Status*	IBM DPM
Guest instance status	mandatory	✔
Launch instance	mandatory	✔
Reboot instance	optional	✔
Shutdown instance	mandatory	✔
Block storage support	optional	✔
Block storage over fibre channel	optional	✔
Image storage support	mandatory	✔
Flat networking	*choice*	✔

Open Stack Releases Overview

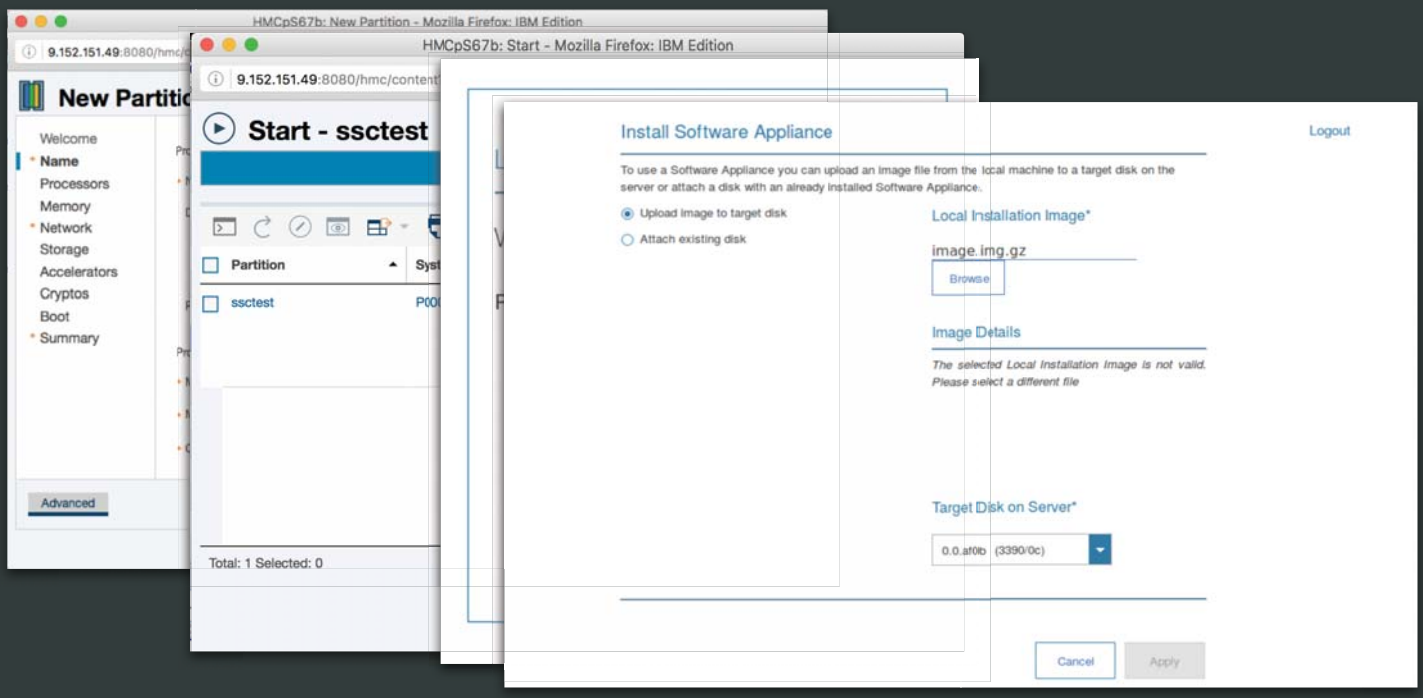
Series	Status	Initial Release Date	Next Phase	EOL Date
Queens	Under Development	scheduled		TBD
Pike	Phase I – Latest release	2017-08-30	Phase II – Maintained release on 2018-02-26	2018-09-03
Ocata	Phase II – Maintained release	2017-02-22	Phase III – Legacy release on 2018-02-26	2018-02-26
Newton	Phase II – Maintained release	2016-10-06	Phase III – Legacy release on 2017-10-09	2017-10-11
Mitaka	EOL	2016-04-07		2017-04-10
Liberty	EOL	2015-10-15		2016-11-17
Kilo	EOL	2015-04-30		2016-05-02
Juno	EOL	2014-10-16		2015-12-07
Icehouse	EOL	2014-04-17		2015-07-02
Havana	EOL	2013-10-17		2014-09-30

OpenStack with DPM Enablement



2Q17
IBM Secure Service Container Support

Deploying SSC-based workloads with DPM



DPM +  Secure Service Container = BLOCKCHAIN

Technical Specifications

- IBM z13 or IBM z13s, IBM z14
  IBM LinuxONE Emperor and II or
  IBM LinuxONE Rockhopper

  Feature Code #0016:
  Hardware Requirements for IBM DPM

  Two dedicated OSA-Express5S
  1000BASE-T Ethernet (#0417)

- FICON Express (Type FCP)
  OSA-Express
  Crypto Express
  zEDC Express
  10GbE RoCE Express
  HiperSockets

- KVM for IBM z & LinuxONE and/or
  Linux on IBM z & LinuxONE

  z/VM support for FCP-only configurations
  with z/VM 6.4 GA

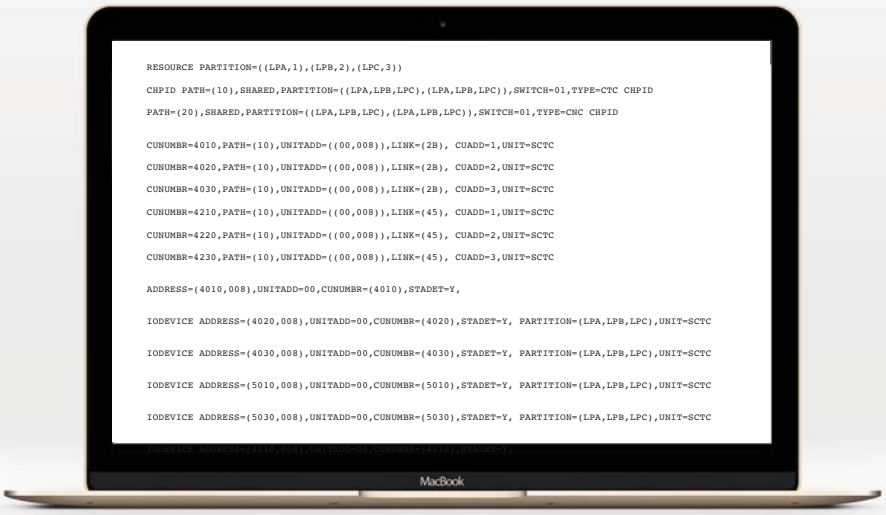
  Available now: Support for IBM Secure
  Service Container based workload

- No support yet for

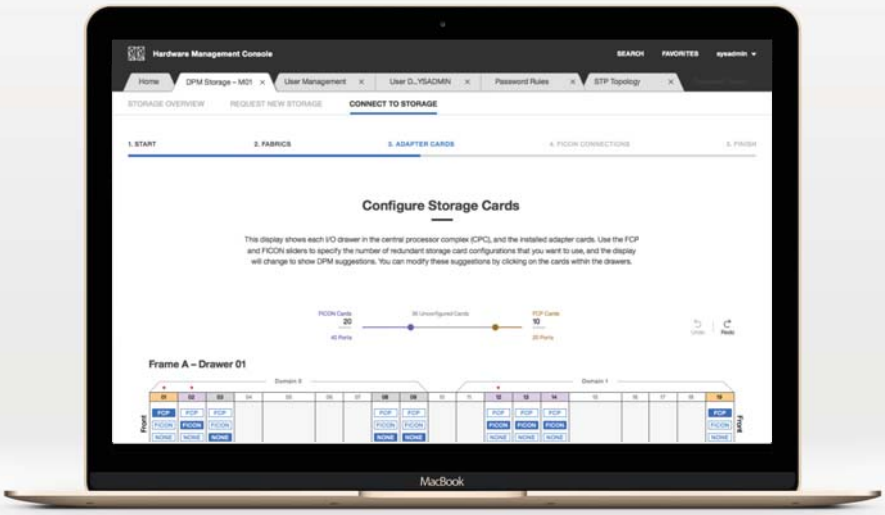
  z/OS, z/VSE, z/TPF
  GDPS® Virtual Appliance
  FICON Express (Type FC)

What's next?
DPM Release 3

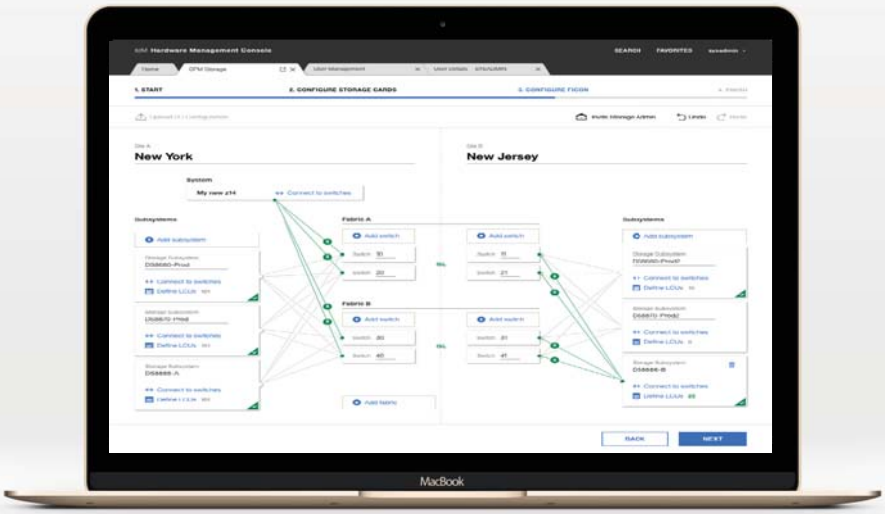
TURN THIS



INTO THAT



AND THAT




IBM
Q & A

Secure
Service
Container

Secure Service Container Introduction

Agenda

- **From Vision to Newspaper**
- **What**
  - **IBM Secure Service Container**
    What is it and what it's not
  - **Key Attributes**
  - **Building Blocks**
  - **Security Focus**
  - **Future**

What if …

Mainframe applications could be experienced almost as easily as **apps on a mobile device,** but with **industry leading security** ?

Keynote: Harnessing Billions to Save Millions - Barry Baker

View on YouTube

From Vision to Newspaper

Introduction

*» **IBM Secure Service Container** provides the base infrastructure for an **integration** of operating system, middleware and software components into an appliance, which works **autonomously** and provides **core services and infrastructure** focusing on **consumability** and **security**«*

Agenda

- **From Vision to Newspaper**
- **What**
  - **IBM Secure Service Container**
    What is it not and what is it
  - **Key Attributes**
  - **Building Blocks**
  - **Security Focus**
  - **Future**

Terminology

IBM z Systems™ Appliance

is an integration of operating system, middleware and Software components that work autonomously and provides core services and infrastructure focusing on consumability and security

Secure Service Container

provides the base infrastructure to create an **IBM z Systems™ Appliance** including operating system, middleware, SDK and firmware support

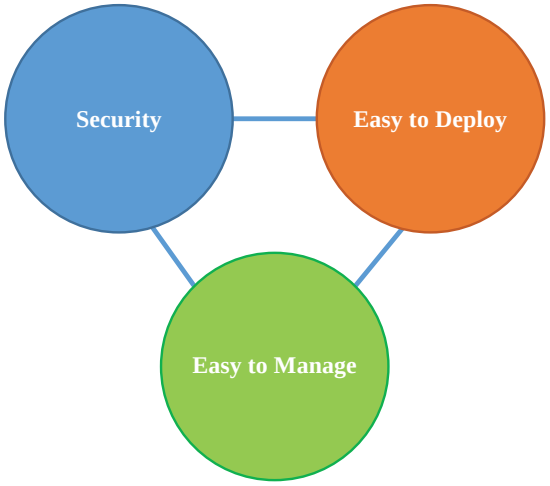
SSC Partition

A Partition type running an **IBM z Systems™ Appliance** based on **Secure Service Container**. The Partition type provides main aspects of the security features.

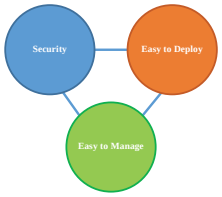
Secure Service Container is …

- … NOT a generic linux distribution
- … NOT yet another standalone product - it is a framework for solutions
- … NOT a white box for you to mangel with configuration internals
- … NOT a competition to Docker - it leverages / includes it
- … NOT the **single** answer to security for a solution

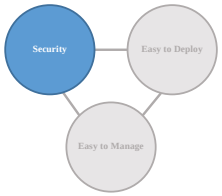
Key Attributes



Key Attributes



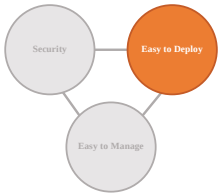
Key Attributes



Security

- The System Admin is a non trusted person
- The solution should leverage Security features without code changes
- Secure Service Container only boots untampered appliances
- All data and code is encrypted in flight and at rest
- System Admin can not access the memory
- Only well defined interfaces into and out of the appliance
- No direct OS level interaction

Key Attributes

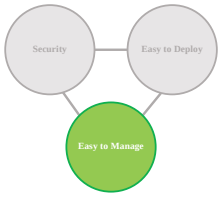


Easy to Deploy

- Deployment of a solution instead of different components
- Deployment without Operating System skills needed
- Deployment without solution skills needed

→ make a first step for cloud enablement with IBM Z

Key Attributes



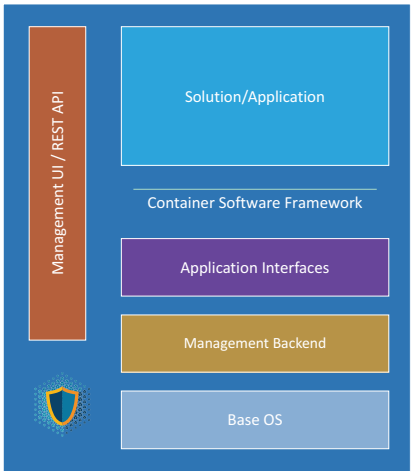
Easy to Manage

- Management of the appliance without Operating System skills
- Limited variance of settings
- RESTful APIs for automation
- UI for better user experience

Agenda

- **From Vision to Newspaper**
- **What**
  - **IBM Secure Service Container**
    What is it and what it's not
  - **Key Attributes**
  - **Building Blocks**
  - **Security Focus**
  - **Future**

Overview



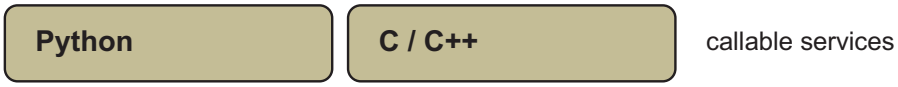
Building Blocks

Application Programming Interfaces

Extendable with Application-specific layer

- **Dojo Toolkit** for modular extensible client rendering
- **nginx** allows Application-specific web services
- **uwsgi** utilized to call Python “backend” services (or native services)

Container Framework Interfaces



callable services

Building Blocks

Application Programming Interfaces

Appliance Status	• Certificate Mgmt • User/Group Mgmt • Local or Remote LDAP Repository	• FICON DASD Volumes • FCP Volumes, • Disk Pools
Appliance Upgrade: 1. Export existing config 2. Reboot 3. Import config	• Alerts • Logging • Dump Services • Reboot to Installer	• NIC / VLAN Mgmt • Network Settings • Adapter Configuration

Extendable with Application-specific layer

- **Dojo Toolkit** for modular extensible client rendering
- **nginx** allows Application-specific web services
- **uwsgi** utilized to call Python “backend” services (or native services)

Container Framework Interfaces

Python	**C / C++**	callable services

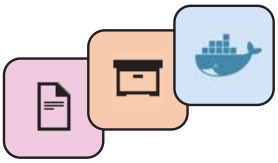
Appliance Build

- C /C++
- Python / Bash shell scripts, etc
- JavaScript / Dojo Toolkit
- …

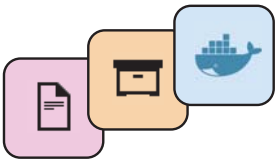
- RPM
- APT (future support)

- Docker engine supplied by Container Framework
- Docker Image Supplied by solution tam
- Launched by solution Application, e.g. using systemd init
- Container Life-cycle controlled by solution

Appliance Build



Appliance Build



Secure Service Container
Software Development Kit

Appliance Build

Appliance Build

- Create SSC-mode Image

Appliance Build

- Create SSC-mode Image

Appliance Build

Result:

"***Flat Image***"
for deployment [1)]

Secure Service Container
Software Development Kit

Appliance Deployment

"***Flat Image***"
for deployment [1)]

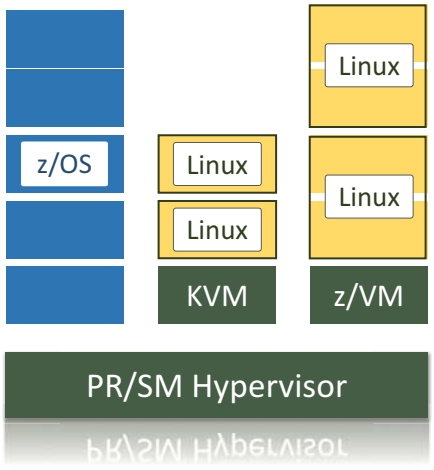
Appliance Deployment

"***Flat Image***"
for deployment [1)]

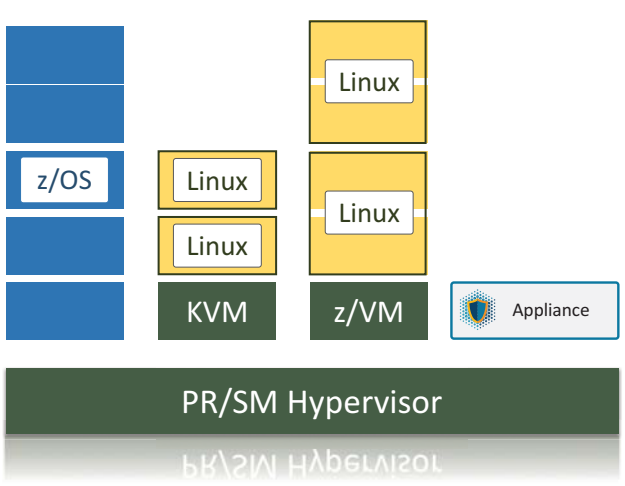
Appliance Deployment

Appliance Deployment

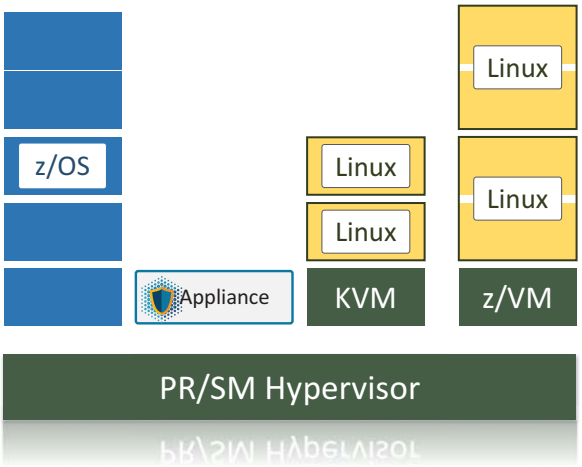
Appliance Deployment



Appliance Deployment



Appliance Deployment



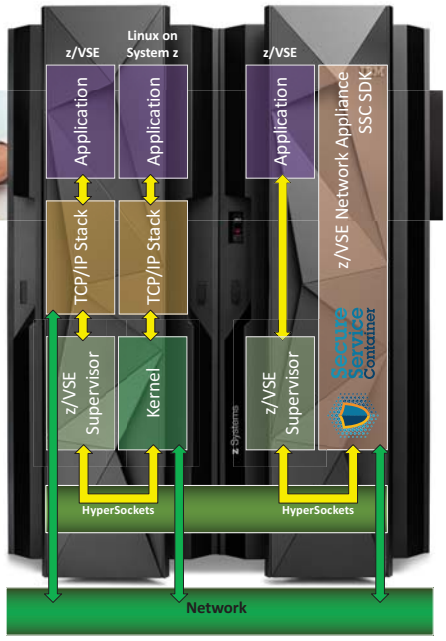
z/VSE Network Appliance

Better communications between z/VSE and Linux on z

- Existing z/VSE Linux Fast Pass (LFP) allows selected TCP/IP applications to communicate via the TCP/IP stack on Linux on z System without requiring a TCP/IP stack on z/VSE
- New no-charge z/VSE Network Appliance is an integrated solution providing TCP/IP stack functionality for TCP/IP applications running on z/VSE in LPAR
- Runs in SSC LPAR
- No Linux license, No TCP/IP product, No z/VM® required
- Supported on z/VSE 6.1, 5.2 and 5.1 and the z13 and z13s

Typical Client Use Cases:

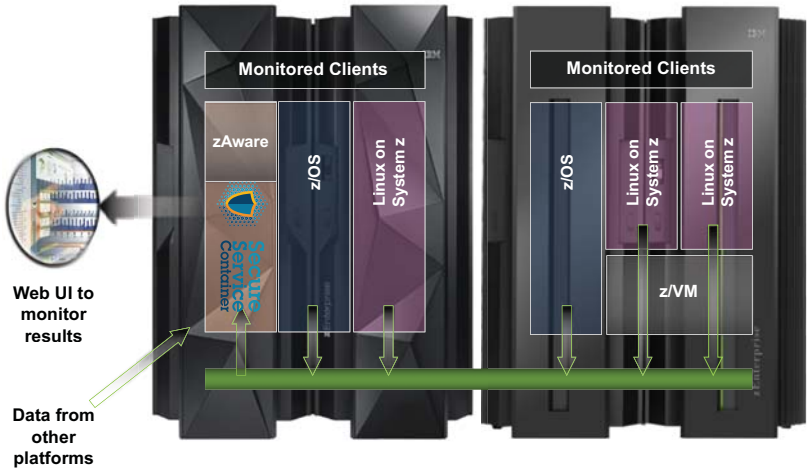
- Clients running z/VSE and DB2 on Linux, may increase performance and reduce costs
- For heavy loaded environments can free up z/VSE and CICS resources with elimination of TCP/IP stack
- For clients running z/VSE under z/VM, an equivalent LFP functionality is available using z/VSE z/VM IP Assist (VIA)



* Based on IBM measurements with high FTP workload
** IBM measurements: averaged value based on FTP and socket application use, bi-directional (z/VSE → Linux & Linux → z/VSE)
Actual results are heavily workload dependent and may vary for individual environments

Integated Analytics Software

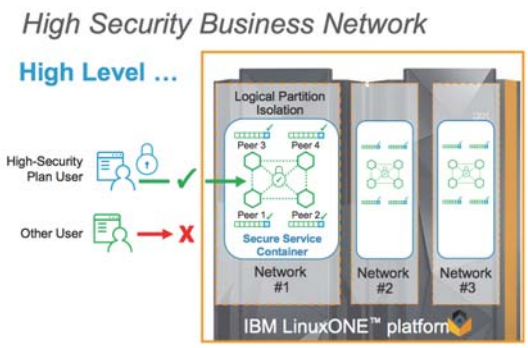
zAWARE based on Secure Service Container



Integrated Analytics Software Virtual Appliance

- Provides anomaly detection, search and reporting
- Identify unusual system behavior of z/OS and Linux on System z images
- Analyze message logs for all servers in the enterprise from single browser in real-time

IBM Blockchain



HYPERLEDGER PROJECT	Starter Plan	High Security Plan
Purpose	Development	Simulate a business network
4 nodes + Certificate Authority		
Dashboard for registration, monitoring, provisioning & documentation provided through Bluemix	✓	✓
Network Connections through SoftLayer	✓	✓
Cloud Provisioning & Self Service Enablement	✓	✓
Service Management and Billing through Bluemix	✓	✓
Customer Support through Bluemix	✓	✓
Environment	Shared, multi-tenant	Isolated, single tenant
Secure Service Container		✓
Highest levels of isolation in industry		✓
Compliance for highly regulated industries (Keys secured in HSM)		✓
Accelerated performance		✓

Agenda

- **From Vision to Newspaper**
- **What**
  - **IBM Secure Service Container**
    What is it and what it's not
  - **Key Attributes**
  - **Building Blocks**
  - **Security Focus**
  - **Future**

Security Basics

Right Access

to the

Right Resources

by the

Right Subject

at the

Right Time

Source: https://w3-connections.ibm.com/files/app#/file/d183941c-bb72-49c5-90f8-5a1e40b3de01

Security Claims

The Secure Service Container…

- provid(1)tamper protection during Appliance installation and runtime
- ensures confidentiality of data and code running within the Appliance – both at fligh(2)nd at rest

Signing

The Secure Service Container…

1. provides tamper protection during Appliance installation and runtime
   - provides tamper proof Software boot process
   - provides tamper detection of Appliance file system

Signing

The Secure Service Container…

1. provides tamper protection during Appliance installation and runtime
   - provides tamper proof Software boot process
   - provides tamper detection of Appliance file system

IBM Secure Service Container initiates a chain of trust in an external process:

➔ Limits bootable Software to a group of trusted vendors

➔ Allows to ensure integrity checking of Software boot process in z Firmware

Signing

The Secure Service Container…

1. provides tamper protection during Appliance installation and runtime
   - provides tamper proof Software boot process
   - provides tamper detection of Appliance file system

IBM Secure Service Container initiates a chain of trust in an external process:

➔ Limits bootable Software to a group of trusted vendors

➔ Allows to ensure integrity checking of Software boot process in z Firmware

IBM Secure Service Container uses Btrfs (file system) in conjunction with Chain of Trust and Encryption:

➔ Allows to detect tampering of Appliance file system during its online and offline state

Encryption

The Secure Service Container…

- provid(1)tamper protection during Appliance installation and runtime
- ensures confidentiality of data and code running within the Appliance – both at fligh(2)nd at rest

Encryption

The Secure Service Container…

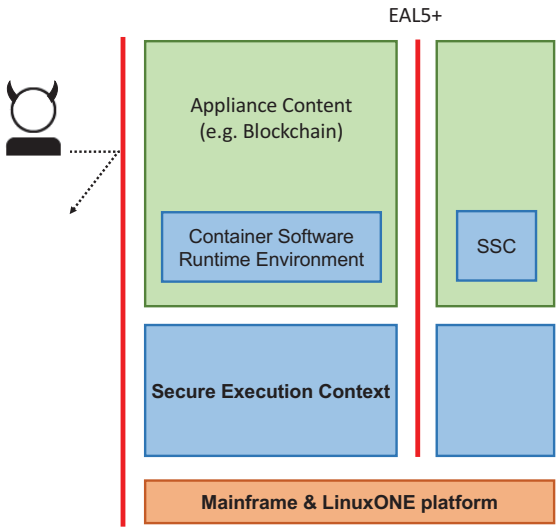
- provid(1)tamper protection during Appliance installation and runtime
- ensures confidentiality of data and code running within the Appliance – both at fligh(2)nd at rest

IBM Secure Service Container contains an encrypted LUKS partition:

➔ Dedicated to the established trust in a vendor

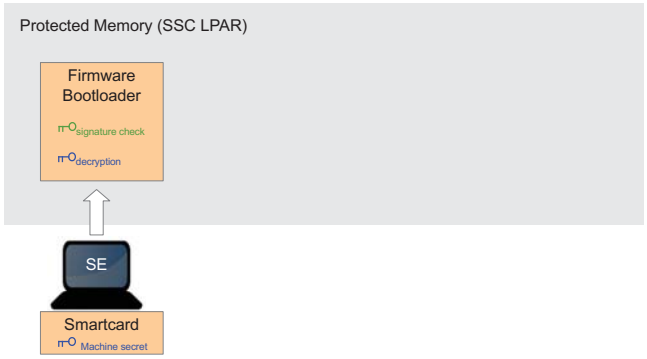
➔ Foundation to secure all data managed by the container

Secure Service Container Protection



- No system admin access
  - Once the appliance image is built, OS access (ssh) is not possible
    - Only Remote APIs available
  - Memory access of system admin is disabled
  - Encrypted disk
  - Debug data (dumps) encrypted
- Strong isolation between container instances
  - Based on LinuxONE EAL5+ protection profile
  - Requires dedicated HW

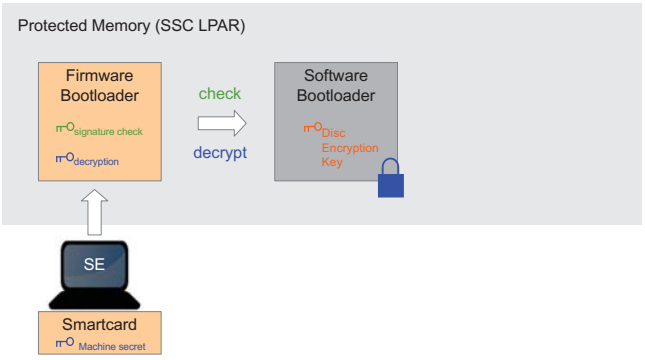
Encrypted, Signed, Tamper Resistant, Protected



Boot sequence

1. Firmware bootloader is loaded in memory
2. Firmware loads the software bootloader

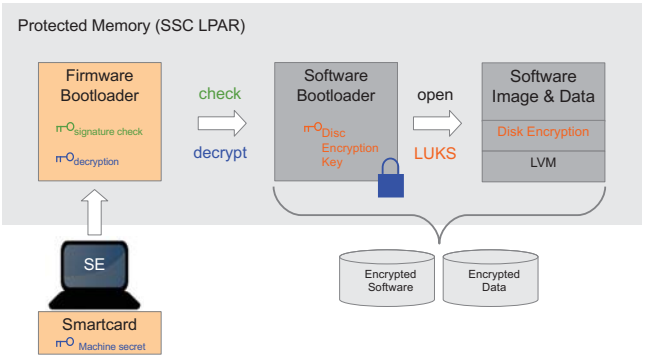
Encrypted, Signed, Tamper Resistant, Protected



Boot sequence

1. Firmware bootloader is loaded in memory
2. Firmware loads the software bootloader from disk
   1. Check integrity of software bootloader
   2. Decrypt software bootloader
3. Software bootloader activate encrypted

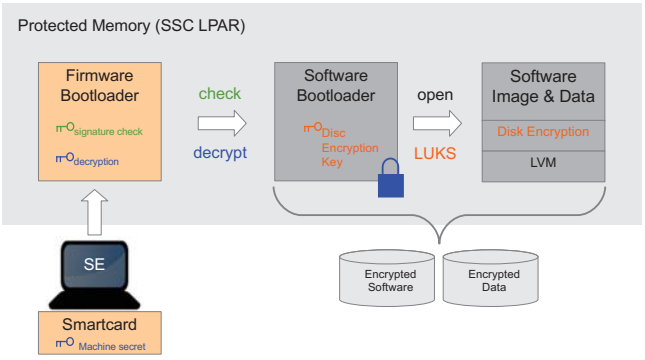
Encrypted, Signed, Tamper Resistant, Protected



Boot sequence

1. Firmware bootloader is loaded in memory
2. Firmware loads the software bootloader from disk
   1. Check integrity of software bootloader
   2. Decrypt software bootloader
3. Software bootloader activate encrypted disks
   1. Key stored in software bootloader (encrypted)
   2. Encryption/decryption done on the flight when accessing appliance code&data
4. Appliance designed to be managed by

Encrypted, Signed, Tamper Resistant, Protected



Boot sequence

1. Firmware bootloader is loaded in memory
2. Firmware loads the software bootloader from disk
   1. Check integrity of software bootloader
   2. Decrypt software bootloader
3. Software bootloader activate encrypted disks
   1. Key stored in software bootloader (encrypted)
   2. Encryption/decryption done on the flight when accessing appliance code&data
4. Appliance designed to be managed by remote APIs only
   - REST APIs to configure Linux and apps
   - No ssh (allowed in dev mode)

Agenda

- **Who am I**
- **Why: From Vision to Newspaper**
- **What**
  - **IBM Secure Service Container**
    What is it and what it's not
  - **Key Attributes**
  - **Building Blocks**
  - **Security Focus**
  - **Future**

need a bright chart as future no content just a picture or so

Text for example sCaaS, your solution here (appliance)

Example vIDAA

SDK / ISV infos chart (dinane Hendersen)

Broadening Solutions

Different Exploiters working on their first GA or refresh their solution

- zAWARE
- zVSE/NA
- HSBN Blockchain

Upcoming Appliance

- **vIDAA** is working towards a first release 2017
- ……..
- ……..

➔Enable ISVs to provide solutions within that framework

IDAA Deployment Options

The IDAA concept of HTAP can be implemented within different operating environments :

- on an on-premises appliance
- on a SW appliance installed on the mainframe

Both options will offer:

- same functionality
- same API
- same implementation

This provides:

- Coexistence and combination of deployment options, fully transparent for Db2 applications
- Flexibility in moving data for query acceleration as workload demands grow or change
- Consistency and efficiency in managing different IDAA environments

IBM Db2 Analytics Accelerator for z/OS Version 7.1, deployment on IBM Z

Announcement 10/17/2017
Availability 11/24/2017

Announcing Db2 Analytics Accelerator Version 7.1

Delivering new flexible, integrated deployment options

High-speed analysis of your enterprise data for real-time insight under the control and security of IBM Z

- Introduces new flexible, integrated deployment options
  - **Accelerator on IBM Z**
    - Unified homogeneity of service, support and operations
    - Flexible Capacity
  - **Accelerator on IBM Integrated Analytics System**
    - Fast, simple deployment on pre-configured hardware and software
    - Flexible and elastic data storage
- Based on IBM's premier analytical engine, Db2 Warehouse software
- Transition easily between deployment options
  - One API
  - One database engine

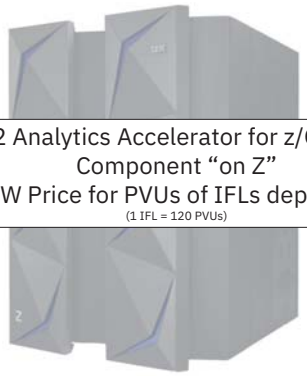
Product ordering: deployment option on IBM Z

1 Hardware – z14

Option 1:
Use IFLs and memory available on z14 system.

Option 2:
Add a full drawer of resources (35 IFLs and memory) to z14 system. Special pricing available for this option.

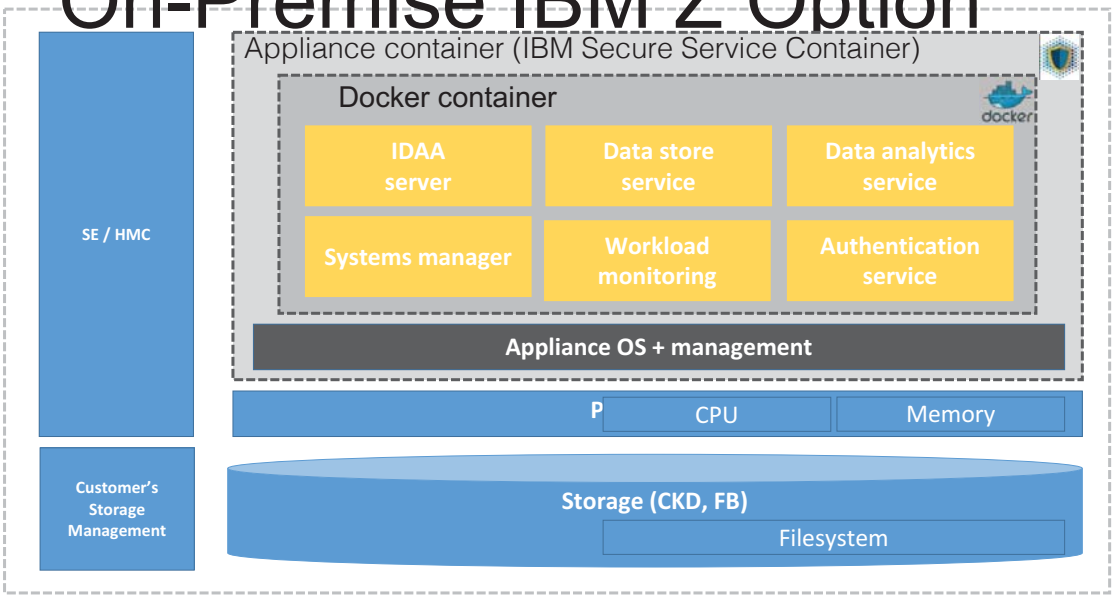
2 Software



Db2 Analytics Accelerator for z/OS V7.1
Component “on Z”
SW Price for PVUs of IFLs deployed
(1 IFL = 120 PVUs)

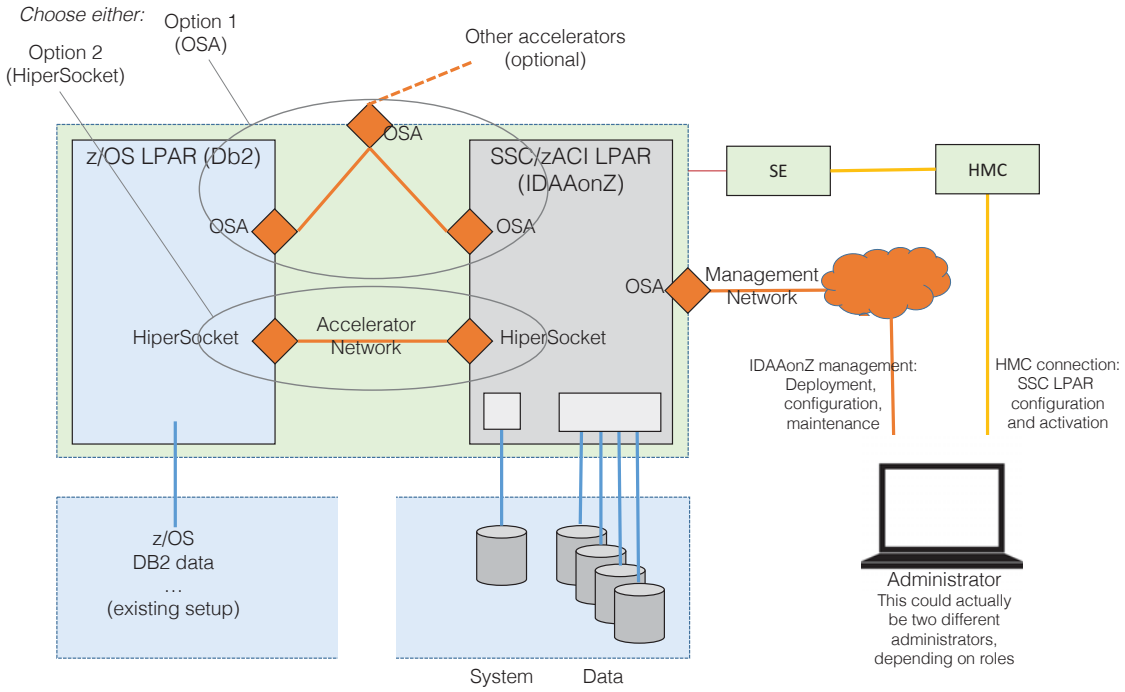
IDAA on IBM Z – High-Level Architecture

On-Premise IBM Z Option

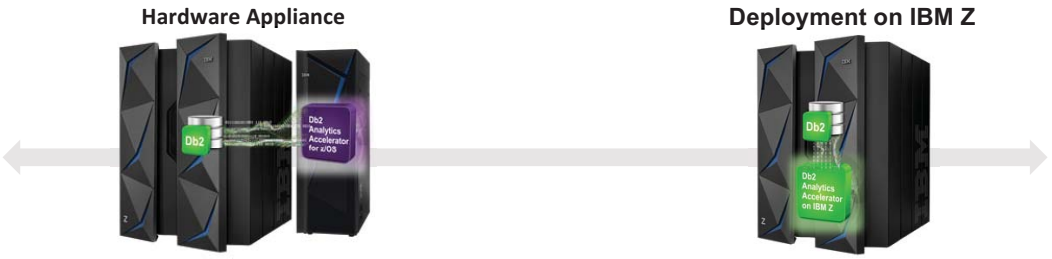


CPU, Memory, IO according to your requirements and infrastructure availability

IDAA on Z – Basic Setup (here: co-located with Db2 z/OS)



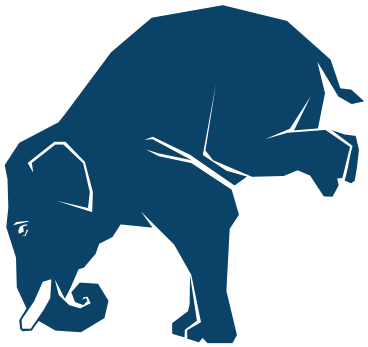
Summary: One API – One implementation – Two deployment options



Uniform experience, simultaneous use, and easy transition between different implementations

Common analytics engine across all the platforms: Db2 Warehouse

The Host learns new Tricks



DPM & SSC

Questions?

Thank you!

?

IBM

Erich Amrehn
Distinguished Engineer & Versatilist
CTO WW Client Centers

Schoenaicher Str. 220
D-71032 Boeblingen

+49-171-2213538
AMREHN@DE.IBM.COM