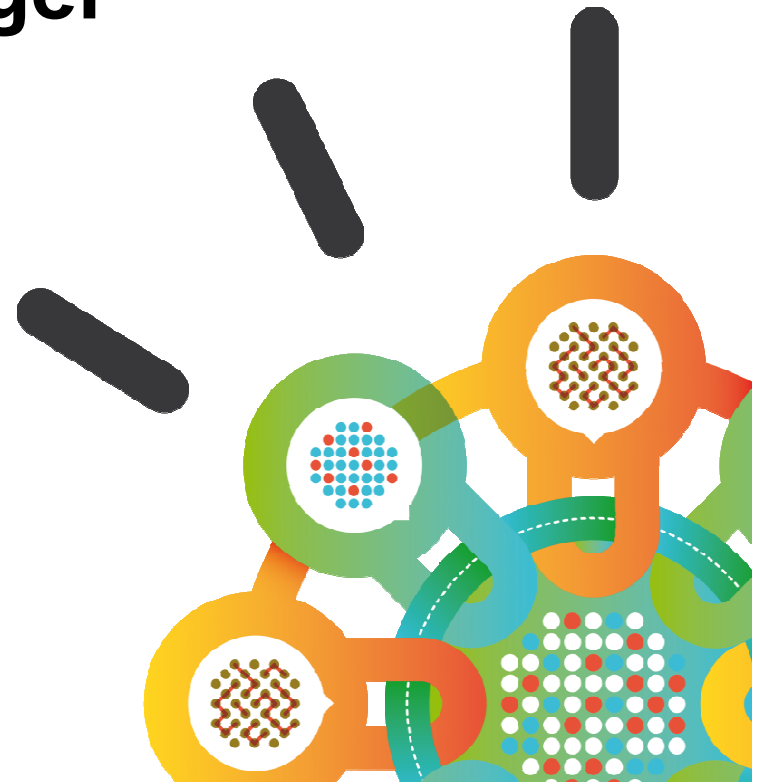
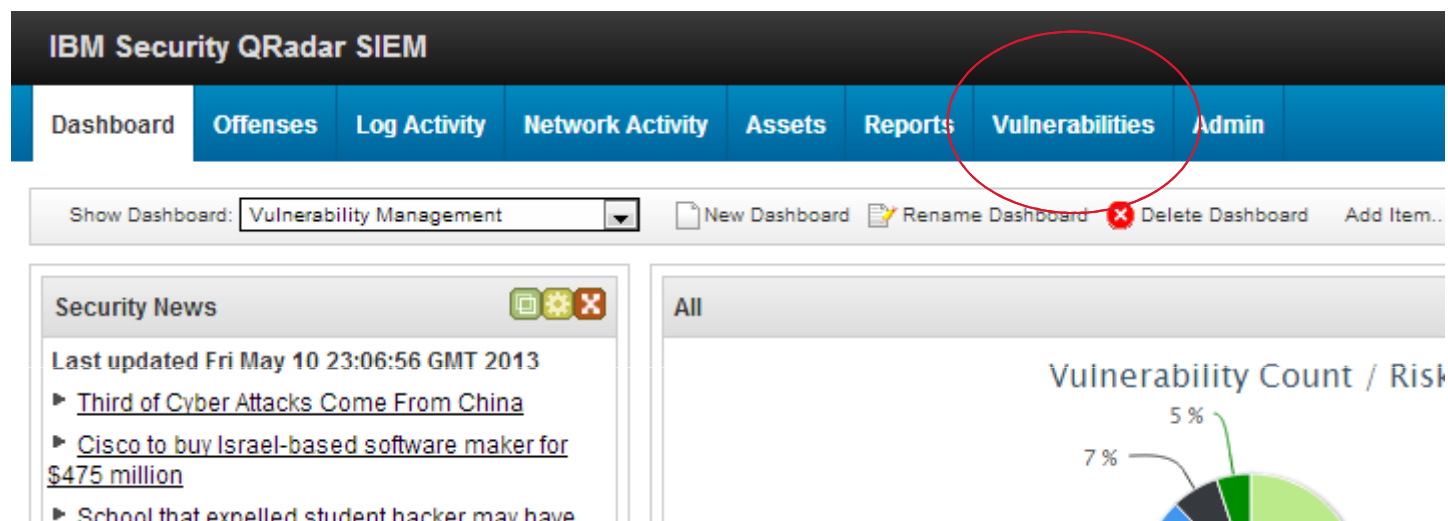


IBM Security QRadar Vulnerability Manager Architecture Overview



QVM Overview

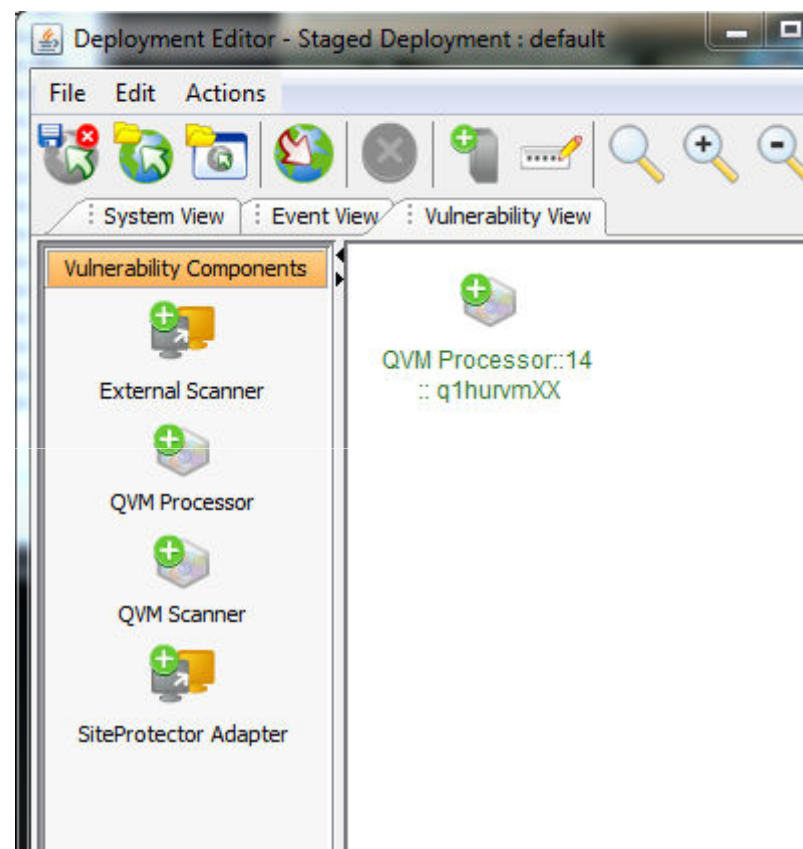
- New tab in QRadar



- Two new deployable components
 - QVM Console
 - Scan definitions, scan scheduling engine, scan results
 - QVM Scanner
 - Performs scan tasks as part of an overall scan
- Third component hosted by IBM
 - Hosted Scanner, scans a customers DMZ from the internet

Overview continued

- Licence able software component that is part of QRadar
 - Pre-installed on all 7.2 installations and above
- Supports all in one and distributed deployments
- Provides an internet hosted scanner for external DMZ scanning
- Deployments configured via deployment editor
- All communication between components is encrypted



Key Functional Areas

- Scan Management
 - Scan configuration
 - Scan scheduling
 - Scan results
- Manage Vulnerabilities
 - Searching, Filtering and Pivot
 - Exception and remediation processes
 - Research
 - Dashboards and reports
 - Includes 3rd party scan data

IBM Security QRadar SIEM

Dashboard

Offenses

Log Activity

Network Activity

Assets

Reports

Vulnerabilities

Admin

Vulnerabilities

My Assigned Vulnerabilities

▼ Manage Vulnerabilities

By Network

By Asset

By Vulnerability

By Open Service

Scan Results

Vulnerability Exception

► Research

▼ Administrative

Scan Profiles

Scan Exclusions

Operational Window

Search ▼

 Save Search Criteria

Quick Searches ▼

Actions ▼

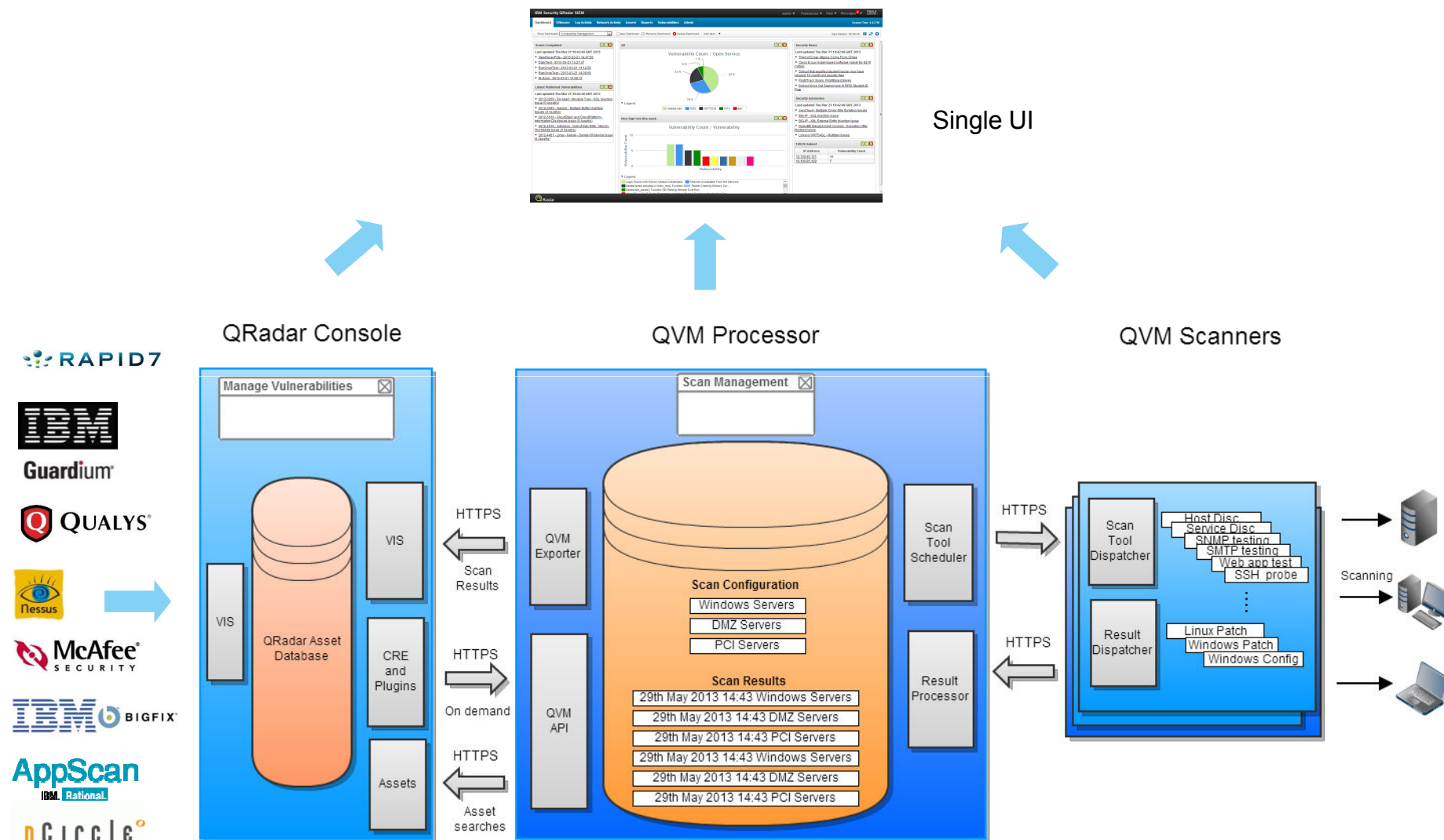
Quick Filter...

Manage Vulnerabilities > By Vulnerability Instances

Vulnerability Instances (No Search Parameters)

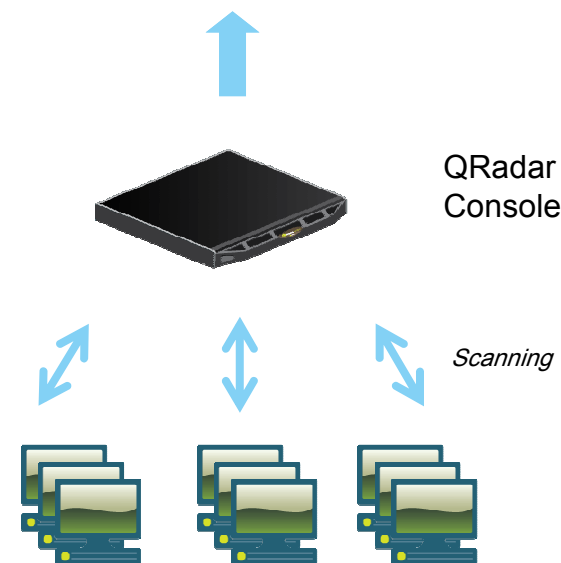
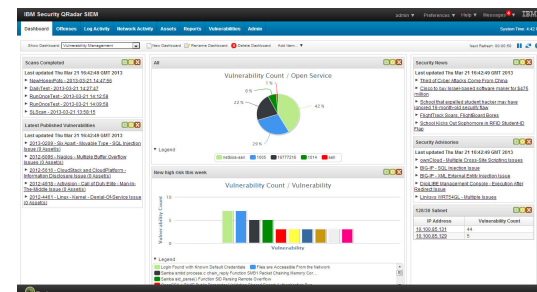
IP Address	Asset Name	Vulnerability
10.100.85.122	Ubuntu-7-04	2006-1608 - PHP - Security Byp
10.100.85.52	10.100.85.52	2011-5000 - OpenSSH - Denia
10.100.85.126	Ubuntu-9-04	2008-5161 - SSH - Tectia Clie
10.100.85.117	REDHAT9	2009-4022 - ISC - BIND - Cach
10.100.85.117	REDHAT9	2005-2666 - OpenSSH - Inform
10.100.85.22	10.100.85.22	2012-0814 - OpenSSH - Inform
10.100.85.122	Ubuntu-7-04	2006-4486 - PHP - Integer Ove
10.100.85.115	MANDRIVA-ENTERP	2011-2724 - Samba - Denial-Q
10.100.85.113	MANDRAKELINUX	PHP - Remote Arbitrary Locatio
10.100.85.18	10.100.85.18	2011-5000 - OpenSSH - Denia
10.100.85.130	FreeBSD5.labs.critic...	Remote Procedure Call Service
10.100.85.121	10.100.85.121	2012-0814 - OpenSSH - Inform
10.100.85.139	WIN2KSRV-SP4	Information Leak - Computer N
10.100.85.136	WIN2KSRV-GOLD	Information Leak - Computer N
10.100.85.116	REDHAT8	2005-2666 - OpenSSH - Inform
10.100.85.125	UBUNTU-8-10	2011-1678 - Samba - Security F
10.100.85.120	UBUNTU-6-06-1	Information Leak - Computer N
10.100.85.111	10.100.85.111	2011-5000 - OpenSSH - Denia
10.100.85.115	MANDRIVA-ENTERP	2011-1678 - Samba - Security F
10.100.85.59	10.100.85.59	2012-0814 - OpenSSH - Inform

QVM High Level Architecture

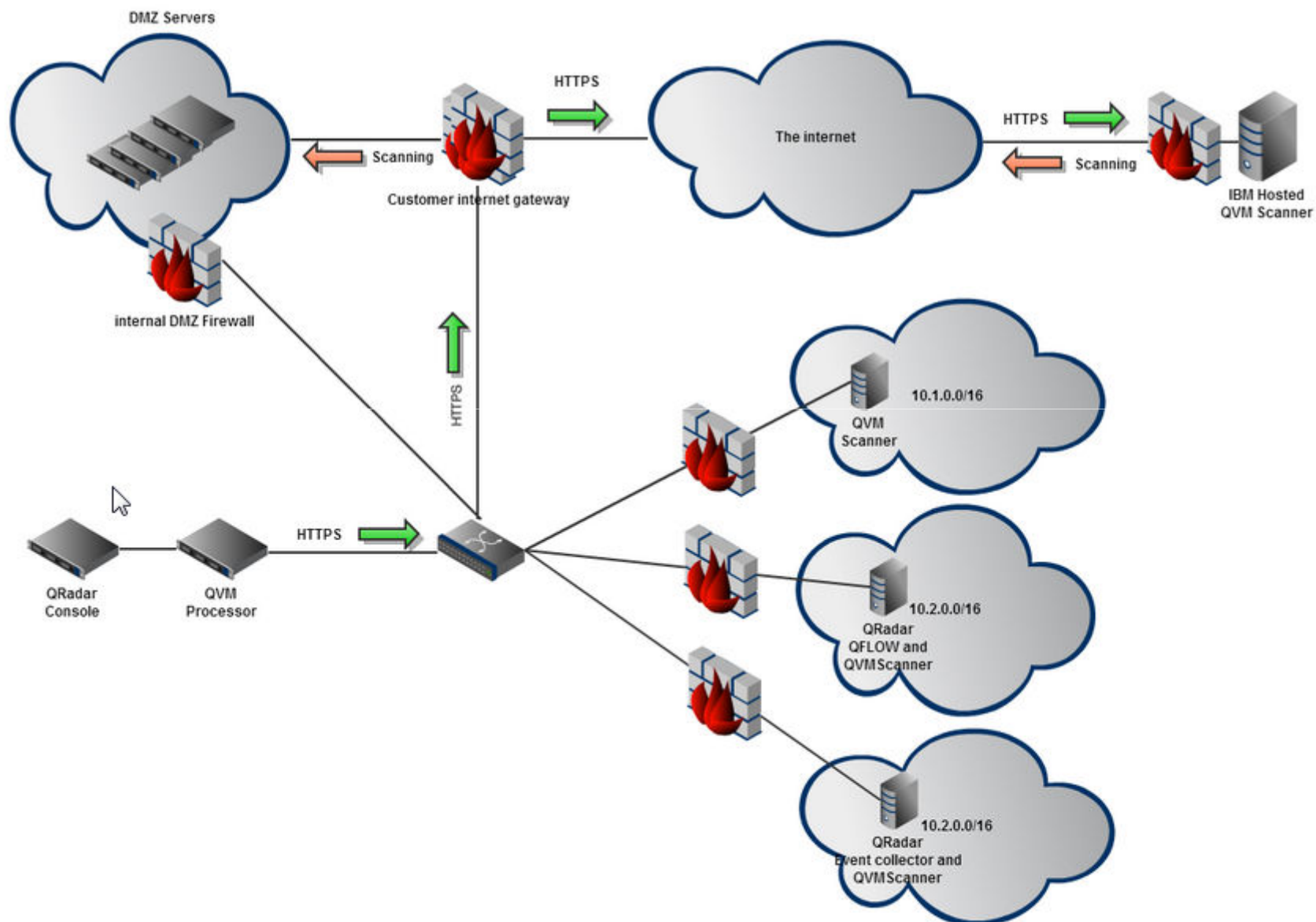


Deployment Scenario – Simple

- All in one
 - QRadar Console
 - QVM Processor
 - QVM Scanner
- Zero software install
- License key enablement
- Simple evaluation process for existing customers



Fully Distributed



Summary

- Enable zero install Vulnerability Management for QRadar customers
 - Included in the QRadar ISO
 - Present in all 7.2+ customer installs
- Supports fully distributed internal and external vulnerability scanning
- Single UI Configured via deployment editor
- Manage vulnerabilities functionality for 3rd party scanners
- All communication between components is encrypted



ibm.com/security

© **Copyright IBM Corporation 2013. All rights reserved.** The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.