

Course Guide

# IBM Cloud Application Performance Management 8.1.4 Fundamentals

Course code TM674 ERC 1.0



## March 2018 edition

### NOTICES

This information was developed for products and services offered in the USA.

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-NC1\_1\_9  
Armonk, NY 1\_0504-1\_785  
United States of America*

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: 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 states 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 supply in any way it believes appropriate without incurring any obligation to you.

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.

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 the names and addresses used by an actual business enterprise is entirely coincidental.

### TRADEMARKS

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., 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 [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

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 Trade Mark of AXELOS Limited.

ITIL is a Registered Trade Mark of AXELOS Limited.

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 other countries.

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.

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

**© Copyright International Business Machines Corporation 2017.**

**This document may not be reproduced in whole or in part without the prior written permission of IBM.**

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

|  |             |
|--|-------------|
| <b>About this course .....</b>   | <b>0-xv</b> |
| About the student .....  | 0-xvi       |
| Learning objectives .....  | 0-xvii      |
| Course agenda .....  | 0-xviii     |
| <br>   |             |
| <b>Unit 1 Introduction to IBM Cloud Application Performance Management .....</b> | <b>1-1</b>  |
| Learning objectives .....  | 1-2         |
| Unit outline .....   | 1-3         |
| Lesson 1 Overview and architecture .....   | 1-4         |
| The Cloud landscape .....  | 1-5         |
| IBM Cloud Application Performance Management .....                               | 1-6         |
| Why IBM Cloud Application Performance Management?<br>.....                       | 1-8         |
| IBM Cloud APM Portfolio: V8.1.4 offerings .....                                  | 1-9         |
| IBM Cloud APM further offerings .....  | 1-10        |
| Bundled product list .....   | 1-12        |
| IBM Cloud APM architecture .....   | 1-13        |
| Lesson 2 Monitoring agents and categories .....                                  | 1-14        |
| Monitoring agents by product and platform (1 of 5) .....                         | 1-15        |
| Monitoring agents by product and platform (2 of 5) .....                         | 1-16        |
| Monitoring agents by product and platform (3 of 5) .....                         | 1-17        |
| Monitoring agents by product and platform (4 of 5) .....                         | 1-18        |
| Monitoring agents by product and platform (5 of 5) .....                         | 1-19        |
| Create custom agents with IBM Agent Builder .....                                | 1-20        |
| Lesson 3 Application-based monitoring .....                                      | 1-21        |
| Application-based monitoring overview (1 of 2) .....                             | 1-22        |
| Application-based monitoring overview (2 of 2) .....                             | 1-23        |
| Application summary .....  | 1-24        |
| Current component status .....   | 1-25        |
| Navigate from a widget to an underlying cause .....                              | 1-26        |
| View component details .....   | 1-27        |
| Identify root causes with deep-dive diagnostics .....                            | 1-28        |
| Monitor user experience .....  | 1-29        |
| Locate problems with transaction tracking .....                                  | 1-30        |
| Viewing historical data .....  | 1-31        |
| Opening reports from the Application Dashboard .....                             | 1-32        |
| Lesson 4 Monitoring agent examples .....   | 1-33        |
| The Application Dashboard navigator .....  | 1-34        |
| My Components: A summary of events and agents .....                              | 1-35        |
| Monitoring agents for Linux OS, UNIX OS, and Windows OS .....                    | 1-36        |

|  |            |
|--|------------|
| Example of Windows OS agent details (1 of 2) .....                                       | 1-37       |
| Example of Windows OS agent details (2 of 2) .....                                       | 1-38       |
| Example of Events tab .....  | 1-39       |
| Monitoring agent for IBM HTTP Server: Summary dashboard .....                            | 1-40       |
| IBM HTTP Web Server: Detail dashboard with website list .....                            | 1-41       |
| Lesson 5 Integrating with Cloud APM .....  | 1-42       |
| Hybrid Gateway overview .....  | 1-43       |
| Adding in the Hybrid Gateway .....   | 1-44       |
| Viewing hybrid agents in the dashboard .....   | 1-45       |
| Benefit of integrating IBM Tivoli Monitoring events .....                                | 1-46       |
| Coexistence of v6 and v7 agents with v8 agents .....                                     | 1-47       |
| Integrating APM v8 agents with IBM Tivoli Monitoring V6 Tivoli Data Warehouse .....      | 1-48       |
| Integrating IBM Cloud and APM on-premises .....  | 1-49       |
| On-premises example of an IBM Cloud Liberty Application .....                            | 1-50       |
| Integrating with Netcool/OMNIbus .....   | 1-51       |
| Integrating with IBM Operations Analytics Log Analysis .....                             | 1-52       |
| Integrating with IBM Operations Analytics Predictive Insights .....                      | 1-53       |
| Integrating with IBM Alert Notification .....  | 1-54       |
| Integrating with IBM Control Desk (Cloud) .....  | 1-55       |
| Integrating with Dashboard Application Services Hub .....                                | 1-56       |
| Creating a custom dashboard page and widgets .....                                       | 1-57       |
| Lesson 6 The Cloud APM lab environment .....   | 1-58       |
| The VMware lab environment .....   | 1-59       |
| Example of an application to monitor: DayTrader .....                                    | 1-60       |
| Lab architecture .....   | 1-61       |
| Lab solution: Simple application with five monitoring agents .....                       | 1-62       |
| Instructor demonstration .....   | 1-63       |
| Student exercises .....  | 1-64       |
| Summary .....  | 1-65       |
| .....  | 1-65       |
| <b>Unit 2 Cloud APM server installation .....</b>  | <b>2-1</b> |
| Learning objectives .....  | 2-2        |
| Unit outline .....   | 2-3        |
| Lesson 1 Overview of Installation .....  | 2-4        |
| Installable content .....  | 2-5        |
| On-Cloud implementation process .....  | 2-6        |
| On-premises implementation process .....   | 2-7        |
| Lesson 2 Prerequisites and the prerequisite checker .....                                | 2-8        |
| Server requirements .....  | 2-9        |
| Server prerequisites: Ports .....  | 2-10       |
| Ports that are used for internal communications between server components (1 of 2) ..... | 2-11       |
| Ports that are used for internal communications between server components (2 of 2) ..... | 2-12       |
| Software requirements for the Cloud APM server .....                                     | 2-13       |
| Consistent time settings .....   | 2-14       |
| Browser support .....  | 2-15       |
| DB2 installation on a remote server .....  | 2-16       |
| MongoDB installation on a remote server .....  | 2-17       |

|  |      |
|--|------|
| Server installation application . . . . .  | 2-18 |
| Lesson 3 Installing the Cloud APM server . . . . .                                   | 2-19 |
| Server installation flow . . . . .   | 2-20 |
| User input: Server installation directory, license agreement, and password . . . . . | 2-21 |
| User input: Configuring the agent images (1 of 2) . . . . .                          | 2-22 |
| User input: Configuring the agent images (2 of 2) . . . . .                          | 2-23 |
| Server installation prerequisite checker . . . . .                                   | 2-24 |
| Server installation process . . . . .  | 2-25 |
| Main components . . . . .  | 2-26 |
| Managing JVM heap size . . . . .   | 2-27 |
| Managing DB2 buffer pool . . . . .   | 2-28 |
| Uninstalling the Cloud APM server . . . . .  | 2-29 |
| Instructor demonstration . . . . .   | 2-30 |
| Student exercises . . . . .  | 2-31 |
| Summary . . . . .  | 2-32 |

|   |            |
|---|------------|
| <b>Unit 3 Installing, configuring, and managing Cloud APM agents.....</b>   | <b>3-1</b> |
| Learning objectives . . . . .   | 3-2        |
| Unit outline . . . . .  | 3-3        |
| Lesson 1 Installing Cloud APM agents . . . . .                              | 3-4        |
| Agent image preconfiguration . . . . .                                      | 3-5        |
| Agent image preconfiguration outside server installation (1 of 2) . . . . . | 3-6        |
| Agent image preconfiguration outside server installation (2 of 2) . . . . . | 3-7        |
| Installing an agent (1 of 2) . . . . .                                      | 3-8        |
| Installing an agent (2 of 2) . . . . .                                      | 3-9        |
| Configuring an agent . . . . .  | 3-10       |
| Lesson 2 Starting and stopping Cloud APM agents . . . . .                   | 3-11       |
| Determining which agents are installed and running on a server . . . . .    | 3-12       |
| Starting and stopping the Monitoring Agent for Linux OS . . . . .           | 3-13       |
| Starting and stopping the Monitoring Agent for DB2 . . . . .                | 3-14       |
| Lesson 3 Accessing data from a Cloud agent . . . . .                        | 3-15       |
| Logging in to the Performance Management Console for on-premises . . . . .  | 3-16       |
| Logging in to the Performance Management Console on Cloud . . . . .         | 3-17       |
| Successful login (1 of 2) . . . . .   | 3-18       |
| Successful login (2 of 2) . . . . .   | 3-19       |
| Accessing data from an agent by using the summary boxes . . . . .           | 3-20       |
| Accessing data from an agent by using the status overview . . . . .         | 3-21       |
| Accessing data from an agent by using the navigator . . . . .               | 3-22       |
| Lesson 4 Configuring and using the log file agent . . . . .                 | 3-23       |
| Configuring log file monitoring (1 of 2) . . . . .                          | 3-24       |
| Configuring log file monitoring (2 of 2) . . . . .                          | 3-25       |
| A simple log file configuration sample . . . . .                            | 3-26       |
| Log file Configurations List page . . . . .                                 | 3-27       |
| Creating a log file configuration . . . . .                                 | 3-28       |
| Distributing a log file configuration . . . . .                             | 3-29       |
| Undistributing a log file configuration . . . . .                           | 3-30       |
| Deleting a log file configuration . . . . .                                 | 3-31       |
| Displaying a log file in the Cloud APM console (1 of 3) . . . . .           | 3-32       |

|   |            |
|---|------------|
| Displaying a log file in the Cloud APM console (2 of 3) .....       | 3-33       |
| Displaying a log file in the Cloud APM console (3 of 3) .....       | 3-34       |
| Student exercises .....   | 3-35       |
| Summary .....   | 3-36       |
| <b>Unit 4 Administration .....</b>                                  | <b>4-1</b> |
| Learning objectives .....   | 4-2        |
| Unit outline .....  | 4-3        |
| Lesson 1 Starting and stopping the Cloud APM server .....           | 4-4        |
| List of Cloud APM services (1 of 3) .....                           | 4-5        |
| List of Cloud APM services (2 of 3) .....                           | 4-6        |
| List of Cloud APM services (3 of 3) .....                           | 4-7        |
| APM command .....   | 4-8        |
| Managing the Monitoring Infrastructure Node (MIN) service .....     | 4-9        |
| Managing the Cloud APM console .....                                | 4-10       |
| Lesson 2 Managing applications .....                                | 4-11       |
| Cloud APM console .....   | 4-12       |
| Defining an application .....                                       | 4-13       |
| Adding an application manually (1 of 2) .....                       | 4-14       |
| Adding an application manually (2 of 2) .....                       | 4-15       |
| Discovering applications (1 of 2) .....                             | 4-16       |
| Discovering applications (2 of 2) .....                             | 4-17       |
| Using templates (1 of 2) .....                                      | 4-18       |
| Using templates (2 of 2) .....                                      | 4-19       |
| Editing an application .....  | 4-20       |
| Deleting an application .....                                       | 4-21       |
| Example: Simple application of Linux operating systems .....        | 4-22       |
| Example: Simple application with six agents .....                   | 4-23       |
| Examining data from an application .....                            | 4-24       |
| Monitoring agent for WebSphere Application Server .....             | 4-25       |
| Lesson 3 Creating custom views .....                                | 4-26       |
| Dashboard viewer in Custom Views .....                              | 4-27       |
| Maximized chart .....   | 4-28       |
| Viewing other pages and setting a default .....                     | 4-29       |
| Page management options .....                                       | 4-30       |
| Select a page template .....  | 4-31       |
| Dashboard page editor .....   | 4-32       |
| Edit template .....   | 4-33       |
| Set chart properties .....  | 4-34       |
| Set chart metric (1 of 2) .....                                     | 4-35       |
| Set chart metric (2 of 2) .....                                     | 4-36       |
| Save and preview the page .....                                     | 4-37       |
| Context-specific dashboards: Application (1 of 2) .....             | 4-38       |
| Context-specific dashboards: Application (2 of 2) .....             | 4-39       |
| Context-specific dashboards: Component .....                        | 4-40       |
| Context-specific dashboards: Instance * .....                       | 4-41       |
| Lesson 4 Using attribute details to access data from an agent ..... | 4-42       |
| Viewing attribute details (1 of 2) .....                            | 4-43       |

|  |      |
|--|------|
| Viewing attribute details (2 of 2) .....                           | 4-44 |
| Line charts with the attribute details .....                       | 4-45 |
| Saving Attribute detail tables and charts (1 of 2) .....           | 4-46 |
| Saving Attribute detail tables and charts (2 of 2) .....           | 4-47 |
| Deleting saved tables and charts .....                             | 4-48 |
| Lesson 5 Managing users in the Cloud APM console .....             | 4-49 |
| Integrating LDAP with Cloud APM (1 of 3) .....                     | 4-50 |
| Integrating LDAP with Cloud APM (2 of 3) .....                     | 4-51 |
| Integrating LDAP with Cloud APM (3 of 3) .....                     | 4-52 |
| basicRegistry.xml .....  | 4-53 |
| Role-based access control (1 of 2) .....                           | 4-54 |
| Role-based access control (2 of 2) .....                           | 4-55 |
| Default policy structure (1 of 2) .....                            | 4-56 |
| Default policy structure (2 of 2) .....                            | 4-57 |
| Roles .....  | 4-58 |
| Individual users .....   | 4-59 |
| User groups .....  | 4-60 |
| New role creation and configuration .....                          | 4-61 |
| New role creation and configuration: Resource permissions .....    | 4-62 |
| Example: A user with full permissions on a small test system ..... | 4-63 |
| Example: A user with no permissions .....                          | 4-64 |
| Example: A user with no administrative permissions .....           | 4-65 |
| Example: A user with restricted application access .....           | 4-66 |
| Instructor demonstration .....                                     | 4-67 |
| Student exercises .....  | 4-68 |
| Summary .....  | 4-69 |

|   |            |
|---|------------|
| <b>Unit 5 Monitoring events.....</b>                              | <b>5-1</b> |
| Learning objectives .....   | 5-2        |
| Unit outline .....  | 5-3        |
| Lesson 1 Understanding events .....                               | 5-4        |
| Event indicators .....  | 5-5        |
| Applications show the most severe status .....                    | 5-6        |
| Viewing all events for all components .....                       | 5-7        |
| Viewing all events for a single application .....                 | 5-8        |
| Open events by severity .....                                     | 5-9        |
| Threshold-generated events .....                                  | 5-10       |
| Drill-down to affected resource .....                             | 5-11       |
| Using the Event Status widget .....                               | 5-12       |
| Lesson 2 Creating thresholds by using the Threshold Manager ..... | 5-13       |
| Selecting the data type .....                                     | 5-14       |
| Modifying the fields (1 of 2) .....                               | 5-15       |
| Modifying the fields (2 of 2) .....                               | 5-16       |
| Threshold fields (1 of 2) .....                                   | 5-17       |
| Threshold fields (2 of 2) .....                                   | 5-18       |
| The resulting event .....   | 5-19       |
| Special operators that are supported in Edit Conditions .....     | 5-20       |
| Execute command example that uses the Missing comparison .....    | 5-21       |

|   |             |
|---|-------------|
| Display item example .....  | 5-22        |
| Adding multiple conditions .....  | 5-23        |
| Deleting thresholds .....   | 5-24        |
| Thresholds enablement .....   | 5-25        |
| <b>Lesson 3 Managing Resource Groups .....</b>                          | <b>5-26</b> |
| Resource Group Manager .....  | 5-27        |
| Creating a resource group (1 of 2) .....                                | 5-28        |
| Creating a resource group (2 of 2) .....                                | 5-29        |
| Instructor demonstration .....  | 5-30        |
| Student exercises .....   | 5-31        |
| Summary .....   | 5-32        |
| <b>Unit 6 Monitoring the user experience of applications .....</b>      | <b>6-1</b>  |
| Learning objectives .....   | 6-2         |
| Unit outline .....  | 6-3         |
| Lesson 1 What is user experience monitoring? .....                      | 6-4         |
| Lesson 2 Introduction to the Response Time Monitoring agent .....       | 6-5         |
| Requests and Response Time .....  | 6-6         |
| End User Transaction Status Overview .....                              | 6-7         |
| Viewing individual transaction details .....                            | 6-8         |
| Viewing user activity .....   | 6-9         |
| Monitoring mobile device user transactions .....                        | 6-10        |
| User activity by device (operating system) .....                        | 6-11        |
| Session details by device (operating system) .....                      | 6-12        |
| Lesson 3 Introduction to the HTTP Server agent .....                    | 6-13        |
| Component status .....  | 6-14        |
| Web server detail .....   | 6-15        |
| Web Site Detail page .....  | 6-16        |
| Lesson 4 Introduction to JavaScript injection .....                     | 6-17        |
| Data from JavaScript injection .....                                    | 6-18        |
| Lesson 5 Deploying end user monitoring components .....                 | 6-19        |
| Supported transaction features .....                                    | 6-20        |
| Supported software .....  | 6-21        |
| If integrating Response Time and HTTP server agents .....               | 6-22        |
| If not integrating Response Time and HTTP server agents .....           | 6-23        |
| Incorporating the Response Time agent in applications .....             | 6-25        |
| Student exercises .....   | 6-26        |
| Summary .....   | 6-27        |
| <b>Unit 7 Monitoring applications with synthetic transactions .....</b> | <b>7-1</b>  |
| Learning objectives .....   | 7-2         |
| Unit outline .....  | 7-3         |
| Lesson 1 Introduction to synthetic transaction monitoring .....         | 7-4         |
| Two versions .....  | 7-5         |
| Points of presence .....  | 7-6         |
| Lesson 2 Monitoring synthetic transactions .....                        | 7-7         |
| Monitoring synthetic transactions (2 of 4) .....                        | 7-8         |
| Monitoring synthetic transactions (3 of 4) .....                        | 7-9         |

|   |            |
|---|------------|
| Monitoring synthetic transactions (4 of 4) .....                                  | 7-10       |
| Synthetic transaction monitoring reports .....                                    | 7-11       |
| Lesson 3 Deploying synthetic transaction monitoring .....                         | 7-12       |
| Creating custom playback points of presence .....                                 | 7-13       |
| Managing synthetic transactions .....   | 7-14       |
| Creating synthetic transactions that use a URL .....                              | 7-15       |
| Recording Selenium IDE scripts .....  | 7-16       |
| Creating synthetic transactions that use a script (1 of 2) .....                  | 7-17       |
| Creating synthetic transactions that use a script (2 of 2) .....                  | 7-18       |
| Student exercises .....   | 7-19       |
| Summary .....   | 7-20       |
| <b>Unit 8 Monitoring resources.....</b>   | <b>8-1</b> |
| Learning objectives .....   | 8-2        |
| Unit outline .....  | 8-3        |
| Lesson 1 Overview of resource monitoring .....                                    | 8-4        |
| Application-centric dashboards showing resource status at a glance (review) ..... | 8-5        |
| Drill down from the instance to resource details (review) .....                   | 8-6        |
| Lesson 2 Deployment planning .....  | 8-7        |
| Supported data collector domains .....  | 8-8        |
| Comparative advantages of agents .....  | 8-9        |
| Comparative advantages to installing data collectors .....                        | 8-10       |
| DB2 agent deployment planning .....   | 8-11       |
| WebSphere agent deployment planning .....   | 8-12       |
| Lesson 3 Configuration .....  | 8-13       |
| Configuration summary (1 of 5) .....  | 8-14       |
| Configuration summary (2 of 5) .....  | 8-15       |
| Configuration summary (3 of 5) .....  | 8-16       |
| Configuration summary (4 of 5) .....  | 8-17       |
| Configuration summary (5 of 5) .....  | 8-18       |
| Configuring multi-instance agents .....   | 8-19       |
| Configuring an agent with a silent configuration file .....                       | 8-20       |
| Configuring an agent with a postinstallation script (1 of 2) .....                | 8-21       |
| Configuring an agent with a postinstallation script (2 of 2) .....                | 8-22       |
| WebSphere agent default configuration .....                                       | 8-23       |
| Configuring the Node.js agent .....   | 8-24       |
| Configuring the Node.js data collector for an on-premises installation .....      | 8-25       |
| Student exercises .....   | 8-26       |
| Summary .....   | 8-27       |
| .....   | 8-28       |
| <b>Unit 9 Tracking transactions through application components .....</b>          | <b>9-1</b> |
| Learning objectives .....   | 9-2        |
| Unit outline .....  | 9-3        |
| Lesson 1 Transaction tracking overview .....                                      | 9-4        |
| Agents supporting transaction tracking .....                                      | 9-5        |
| Agents: End-to-end correlation support .....                                      | 9-6        |
| Elements of transaction topologies .....  | 9-8        |

|  |      |
|--|------|
| Uninstrumented service tracking .....                  | 9-9  |
| Known uninstrumented services .....                    | 9-10 |
| Topology tooltip .....                                 | 9-11 |
| Navigating transaction tracking (1 of 2) .....         | 9-12 |
| Navigating transaction tracking (2 of 2) .....         | 9-13 |
| Lesson 2 Using transaction topologies .....            | 9-14 |
| Example: IBM Integration Bus in a critical state ..... | 9-15 |
| Access IIB Component widget .....                      | 9-16 |
| IIB transaction volume .....                           | 9-17 |
| Middleware transaction dashboard .....                 | 9-18 |
| Service dependency details .....                       | 9-19 |
| Middleware transaction details .....                   | 9-20 |
| Transaction dependency details .....                   | 9-21 |
| Middleware transaction details (continued) .....       | 9-22 |
| Middleware transaction instances (1 of 2) .....        | 9-23 |
| Middleware transaction instances (2 of 2) .....        | 9-24 |
| Lesson 3 Configuring transaction tracking .....        | 9-25 |
| Agent configuration dashboards .....                   | 9-26 |
| Selecting the agent to be disabled/enabled .....       | 9-27 |
| Student exercises .....                                | 9-28 |
| Summary .....  | 9-29 |

|   |             |
|---|-------------|
| <b>Unit 10 Introduction to deep-dive diagnosis.</b> .....         | <b>10-1</b> |
| Learning objectives .....   | 10-2        |
| Unit outline .....  | 10-3        |
| Lesson 1 Deep-dive resource monitoring overview .....             | 10-4        |
| Supported agents for deep-dive diagnosis .....                    | 10-5        |
| Lesson 2 Code-level monitoring features of supported agents ..... | 10-6        |
| Viewing code-level data (1 of 2) .....                            | 10-8        |
| Viewing code-level data (2 of 2) .....                            | 10-9        |
| Understanding the request stack trace .....                       | 10-10       |
| Understanding the request context .....                           | 10-11       |
| Understanding the method summary (WebSphere only) .....           | 10-12       |
| Lesson 3 More diagnostic features of certain agents .....         | 10-14       |
| Understanding in-flight requests .....                            | 10-15       |
| In-flight requests (1 of 2) .....                                 | 10-16       |
| In-flight requests (2 of 2) .....                                 | 10-17       |
| Value of a heap dump analysis .....                               | 10-18       |
| Heap dump .....   | 10-20       |
| Comparing heap snapshots .....                                    | 10-21       |
| Data that the Memory Analysis feature provides .....              | 10-22       |
| Memory analysis (1 of 2) .....                                    | 10-23       |
| Memory analysis (2 of 2) .....                                    | 10-24       |
| Lesson 4 Deployment planning .....                                | 10-25       |
| Assessing your monitoring needs .....                             | 10-26       |
| Carefully prepare for deployment .....                            | 10-27       |
| Deciding access level .....                                       | 10-28       |
| Managing the amount of data you collect. ....                     | 10-29       |

|   |             |
|---|-------------|
| Lesson 5 Configuration .....  | 10-30       |
| Example 1: WebSphere agent default configuration (review) .....                           | 10-31       |
| Key WebSphere advanced data-collection settings .....                                     | 10-32       |
| Example 2: Node.js agent .....  | 10-33       |
| Student exercises .....   | 10-34       |
| Summary .....   | 10-35       |
| <b>Unit 11 Integrating Cloud APM with other products .....</b>                            | <b>11-1</b> |
| Learning objectives .....   | 11-2        |
| Unit outline .....  | 11-3        |
| Lesson 1 Overview of Cloud APM integration .....  | 11-4        |
| Products that Integrate with Cloud APM .....  | 11-5        |
| OMEGAMON overview .....   | 11-6        |
| z Systems Extension Pack .....  | 11-7        |
| z/OS LPAR (1 of 2) .....  | 11-8        |
| z/OS LPAR (2 of 2) .....  | 11-9        |
| IBM Operations Analytics – Log Analysis .....   | 11-10       |
| Integrate IBM Operations Analytics – Log Analysis .....                                   | 11-11       |
| IBM Operations: Log Analysis integration scenario (1 of 5) .....                          | 11-12       |
| IBM Operations Analytics – Log Analysis integration scenario (2 of 5) .....               | 11-13       |
| IBM Operations Analytics – Log Analysis integration scenario (3 of 5) .....               | 11-14       |
| IBM Operations Analytics – Log Analysis integration scenario (4 of 5) .....               | 11-15       |
| IBM Operations Analytics – Log Analysis integration scenario (5 of 5) .....               | 11-16       |
| Integrate IBM Operations Analytics – Predictive Insights .....                            | 11-17       |
| Early warning .....   | 11-18       |
| Anomaly events .....  | 11-19       |
| Cloud APM integrates with IBM Operations Analytics – Predictive Insights .....            | 11-20       |
| Event hover help: IBM Operations Analytics – Predictive Insights .....                    | 11-21       |
| Detailed analysis .....   | 11-22       |
| Integrate with IBM Alert Management .....   | 11-23       |
| IBM IT Alert Notification email example (Cloud only) .....                                | 11-24       |
| Alert Viewer (1 of 3) .....   | 11-25       |
| Alert Viewer (2 of 3) .....   | 11-26       |
| Alert Viewer (3 of 3) .....   | 11-27       |
| Integration with IBM Control Desk (Cloud only) .....                                      | 11-28       |
| Events in the APM user interface (Cloud only) .....                                       | 11-29       |
| Tickets in IBM Control Desk (Cloud only) .....  | 11-30       |
| Lesson 2 Integrate IBM Tivoli Monitoring .....  | 11-31       |
| Coexistence of v6 and v7 agents with v8 agents .....                                      | 11-32       |
| Hybrid Gateway overview .....   | 11-33       |
| Viewing hybrid agents in the dashboard .....  | 11-34       |
| Benefit of integrating IBM Tivoli Monitoring events .....                                 | 11-35       |
| Integrating with IBM Tivoli Monitoring by using the Hybrid Gateway .....                  | 11-37       |
| From IBM Tivoli Monitoring .....  | 11-38       |
| From Cloud APM .....  | 11-39       |
| Integrating Cloud APM v8 agents with IBM Tivoli Monitoring V6 Tivoli Data Warehouse ..... | 11-40       |
| Tivoli Common Reporting on IBM APM agent example .....                                    | 11-41       |
| Cloud APM v8 agent data flow to IBM Tivoli Monitoring V6 Tivoli Data Warehouse .....      | 11-42       |

|   |             |
|---|-------------|
| Configuration overview .....  | 11-43       |
| History configuration file contents .....   | 11-44       |
| History configuration file and log file .....                                       | 11-45       |
| Lesson 3 Integrate Netcool/OMNibus .....  | 11-46       |
| Events in the Application Performance Manager user interface .....                  | 11-47       |
| Events in Netcool/OMNibus .....   | 11-48       |
| Lesson 4 Integrate IBM Cloud .....  | 11-49       |
| Hybrid application monitoring: IBM Cloud to IBM Cloud APM Private integration ..... | 11-50       |
| IBM Cloud Python Application (1 of 2) .....   | 11-51       |
| IBM Cloud Python Application (2 of 2) .....   | 11-52       |
| IBM Cloud Liberty application .....   | 11-53       |
| Lesson 5 Integrate IBM Cloud Private .....  | 11-54       |
| IBM Cloud Private container monitoring example .....                                | 11-55       |
| IBM Cloud Private application monitoring example .....                              | 11-56       |
| Monitoring IBM Cloud Private containers .....                                       | 11-57       |
| Monitoring IBM Cloud Private applications .....                                     | 11-58       |
| Lesson 6 Monitor IBM API Connect .....  | 11-59       |
| Monitoring API Connect (1 of 2) .....   | 11-60       |
| Monitoring API Connect (2 of 2) .....   | 11-61       |
| IBM APM manages your IBM API Connect environment (1 of 2) .....                     | 11-62       |
| IBM APM manages your IBM API Connect environment (2 of 2) .....                     | 11-63       |
| API Connect (APIs) .....  | 11-64       |
| API Connect: Response Time details .....  | 11-65       |
| API Connect: Transaction Availability Over Time .....                               | 11-66       |
| API Connect: Node.js stack trace .....  | 11-67       |
| API Connect: DataPower Appliance .....  | 11-68       |
| Lesson 7 Populate Dashboard Application Services Hub with Cloud APM data .....      | 11-69       |
| Custom dashboards in DASH with IBM Cloud APM agent data .....                       | 11-70       |
| Creating widgets on a dashboard page to see monitoring information .....            | 11-71       |
| Connector from the Jazz server to the data provider server .....                    | 11-72       |
| Instructor demonstration .....  | 11-73       |
| Student exercises .....   | 11-74       |
| Summary .....   | 11-75       |
| <b>Unit 12 Reporting and 7-day comparison .....</b>                                 | <b>12-1</b> |
| Learning objectives .....   | 12-2        |
| Unit outline .....  | 12-3        |
| Lesson 1 Introduction to historical 7-day comparison .....                          | 12-4        |
| Historical 7-day comparison example of making compare selections .....              | 12-5        |
| Historical 7-day comparison example with Memory .....                               | 12-6        |
| Historical 7-day comparison example with an application .....                       | 12-7        |
| Lesson 2 Reporting using Tivoli Common Reporting .....                              | 12-8        |
| Reporting .....   | 12-9        |
| Running a report from Tivoli Common Reporting .....                                 | 12-10       |
| Running a report from the Cloud APM console .....                                   | 12-11       |
| Top applications with slowest response time across servers report .....             | 12-12       |
| GC Usage of Application Server report .....   | 12-13       |
| Application Web Response Time report .....  | 12-14       |

|   |       |
|---|-------|
| Thread Pools report .....                             | 12-15 |
| Report images are based on the product offering ..... | 12-16 |
| Configuring Cloud APM reports .....                   | 12-17 |
| Configuring ODBC connections .....                    | 12-18 |
| Installing Cloud APM reports .....                    | 12-19 |
| Student exercises .....                               | 12-20 |
| Summary .....   | 12-21 |



# About this course

IBM Training



IBM Cloud Application Performance Management 8.1.4 Fundamentals

© Copyright IBM Corporation 2018  
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

IBM Cloud Application Performance Management v8.1.4 monitors the performance and availability of computer operating systems and applications. In this 3-day classroom course, you learn about the IBM Cloud Application Performance Management architecture and how to install and configure the product. You learn how to navigate the Cloud APM console. You also learn how to manage events and manage user authorities, and how to integrate with other products, including Netcool/OMNIbus, IBM Tivoli Monitoring, and Dashboard Application Services Hub. This course is designed for users, administrators, and implementers. It is intended to help new users of Application Performance Management v8.1.4 to use the tools to effectively manage their enterprise monitoring.

The course duration is 3 days.

The course has 12 units.

1. ["Introduction to IBM Cloud Application Performance Management "](#)
2. ["Cloud APM server installation "](#)

3. [Installing, configuring, and managing Cloud APM agents](#)
4. [Administration](#)
5. [Monitoring events](#)
6. [Monitoring the user experience of applications](#)
7. [Monitoring applications with synthetic transactions](#)
8. [Monitoring resources](#)
9. [Tracking transactions through application components](#)
10. [Introduction to deep-dive diagnosis](#)
11. [Integrating Cloud APM with other products](#)
12. [Reporting and 7-day comparison](#)

The lab environment for this course uses two platforms:

- Red Hat Enterprise Linux 7.3
- Windows Server 2012

For information about other related courses, see the Cloud & Smarter Infrastructure education training paths website:

[ibm.com/software/software/tivoli/education/](http://ibm.com/software/software/tivoli/education/)

| Details                    |  |
|----------------------------|--|
| <b>Delivery method</b>     | Classroom or instructor-led online (ILO)           |
| <b>Course level</b>        | ERC 1.0  |
|                            | This course is a new course.                       |
| <b>Product and version</b> | IBM Cloud Application Performance Management 8.1.4 |
| <b>Duration</b>            | 3.0 days   |
| <b>Skill level</b>         | Basic / Intermediate                               |

## About the student

This course is designed for users, administrators, and implementers.

Before taking this course, make sure that you have the following skills:

- The ability to navigate Linux and Windows applications
- A working knowledge of an internet browser

# Learning objectives

IBM Training



## Learning objectives (1 of 2)

After completing this course, you should be able to do the following tasks:

- Describe the overall solution
- Install and configure the Cloud APM server
- Install, configure, and manage operating system agents
- Administer Cloud APM, including:
  - Applications
  - Users
  - Groups
  - Custom views
  - LDAP integration

# Course agenda

The course contains the following units:

1. [Introduction to IBM Cloud Application Performance Management](#)

This unit starts with an overview and introduction to IBM Cloud Application Performance Management with a description of the architecture. The agents that are available with IBM Cloud Application Performance Management are explained. The products that IBM Cloud Application Performance Management integrates with are presented.

In these exercises, you start and verify the lab environment. You also learn how to access the DayTrader application and make a simple stock trade.

2. [Cloud APM server installation](#)

This unit covers installation of the Cloud APM server. You learn about packaging, prerequisites, and the step-by-step instructions on how to install the Cloud APM server.

The exercises guide you through the installation of the Cloud APM server and several operating system monitoring agents.

3. [Installing, configuring, and managing Cloud APM agents](#)

This unit covers installation of the Cloud APM monitoring agents on both the Windows and Linux environments. You also learn how to install and preconfigure monitoring agents, how to stop and start an agent, and how to access data from an agent. You also learn how to configure and use the log file agent capabilities of the monitoring agent for Linux OS.

In these exercises, you install several operating system monitoring agents. You manage those operating system agents. You access data from the operating system agents. Finally, you configure and access log file data from the operating system agents.

4. [Administration](#)

This unit teaches how to manage the components of the Cloud APM server, and also teaches how to use and administer the Cloud APM console.

In these exercises, you learn how to manage the Cloud APM server. You create applications that are composed of the data from the monitoring agents. You create several custom views. You also explore the Attribute details of various agents and save customized charts with other users. Additionally, you create new users and assign capabilities to those users. Optionally, you set up the Cloud APM server to connect to LDAP.

5. [Monitoring events](#)

This unit covers how to create, update, and delete thresholds, which in turn create events. You explore the Threshold Manager, where you create and modify thresholds that in turn create events when the thresholds defined are met. You also learn how to use the resource group manager. The resource group manager determines which agents that run on specific servers evaluate the thresholds that are defined.

In these exercises, you learn the relationship between thresholds and events. You create thresholds that test for simple and multiple conditions. You create thresholds that run commands to solve the issue that is detected. You adjust resource groups and learn the impact of these adjustments on thresholds and events.

6. [Monitoring the user experience of applications](#)

In this unit, you learn to monitor the user's experience of your application by monitoring the HTTP requests made by the user to your application.

In the exercises for this unit, you deploy front-end transactional monitoring with the Response Time and HTTP Server agents.

7. [Monitoring applications with synthetic transactions](#)

In this unit, you learn to monitor an application by using synthetic transactions.

In these exercises, you create a synthetic transaction for playback and monitoring. By completing these tasks, you enable periodic monitoring of the website that the script accesses.

8. [Monitoring resources](#)

This unit covers installation and configuration of monitoring agents on both the Windows and Linux environments. You learn about agent installation, configuration, and resource-monitoring features of monitoring agents.

The exercises first guide you through the installation of the WebSphere and DB2 monitoring agents on the Linux system.

9. [Tracking transactions through application components](#)

In this unit, you learn to describe the transaction tracking features of IBM Cloud Application Performance Management, Advanced.

This unit covers transaction tracking exercises. You learn to access the information that transaction tracking collects, and how to interpret this data. In addition, you learn how to turn transaction tracking off.

10. [Introduction to deep-dive diagnosis](#)

This presentation is a technical overview of the code-level monitoring features of IBM Cloud Application Performance Management, Advanced.

In addition to resource monitoring, Cloud Application Performance Management Advanced supports deep-dive diagnosis.

11. [Integrating Cloud APM with other products](#)

This unit describes how to integrate the products IBM Tivoli Monitoring, Netcool/OMNIbus, IBM Operations Analytics Log Analysis, Dashboard Application Services Hub, and other products with IBM Cloud APM.

In these exercises, you integrate Cloud APM with IBM Tivoli Monitoring, IBM Netcool/OMNIbus, and IBM Dashboard Application Services. You also configure email notification and examine other advanced configuration options.

## 12. [Reporting and 7-day comparison](#)

In this unit, you display 7-day comparison reports and learn how to install and run Tivoli Common Reporting reports.

In Cloud APM, certain widgets that display information are compared against the same time frames from other days. This feature is known as Historical 7-day comparison.

---

# **Unit 1 Introduction to IBM Cloud Application Performance Management**

IBM Training



## **Introduction to IBM Cloud Application Performance Management**

© Copyright IBM Corporation 2018  
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

This unit starts with an overview and introduction to IBM Cloud Application Performance Management with a description of the architecture. The agents that are available with IBM Cloud Application Performance Management are explained. The products that IBM Cloud Application Performance Management integrates with are presented.

## Learning objectives

After completing this unit, you should be able to:

- Describe IBM Cloud APM and its architecture
- List some monitoring agents and categories of monitoring agents
- Describe application-based monitoring
- Describe some examples of monitoring agent output
- Explain integration with other products
- Describe the classroom lab environment

## Unit outline

- Lesson 1: Overview and architecture
- Lesson 2: Monitoring agents and categories
- Lesson 3: Application-based monitoring
- Lesson 4: Monitoring agent examples
- Lesson 5: Integrating with Cloud APM
- Lesson 6: Introduction to the lab environment

### *Unit outline*

This slide shows the lessons for this unit.

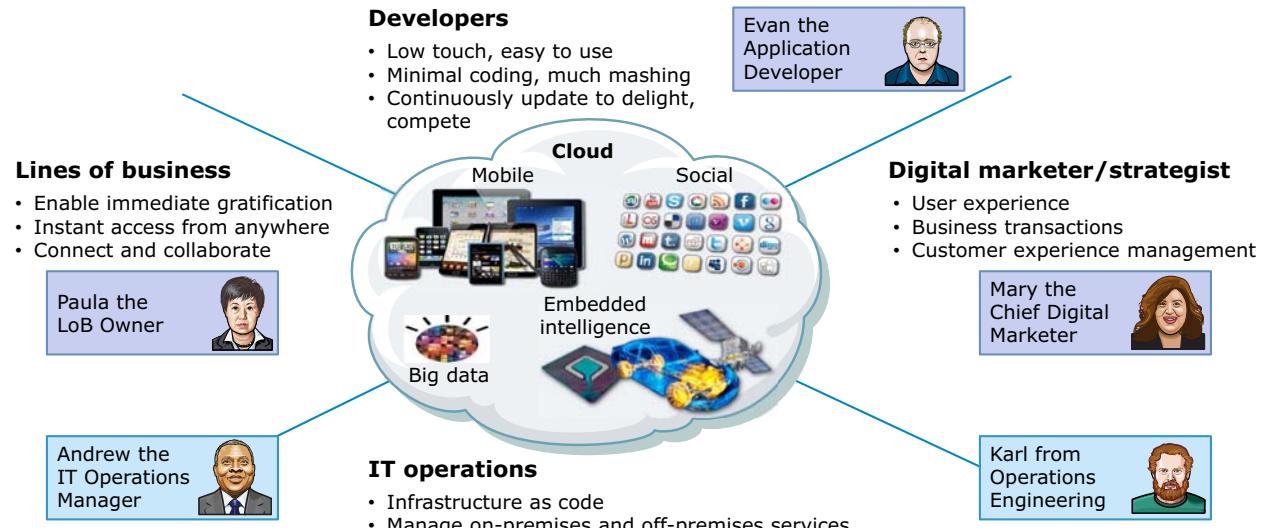
# Lesson 1 Overview and architecture

IBM Training



## Lesson 1: Overview and architecture

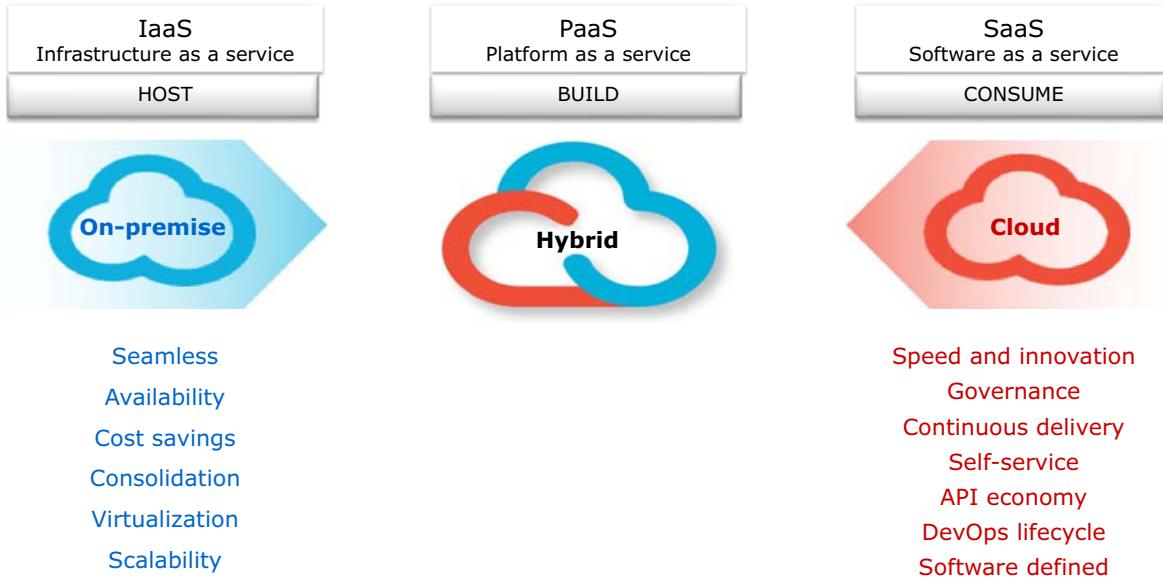
Consumer expectations are driving disruption in application teams



In this lesson, you learn how to describe the IBM Cloud Application Performance Management solution and architecture.

Consumer expectations are driving disruption in application teams. Business applications are the core of business strategies, revenue generation, and service offerings. The stakeholders in the health and performance of business applications are from the traditional IT departments to developers, line-of-business operators, marketers, and strategists. A need exists for application-centric monitoring that all stakeholders can use.

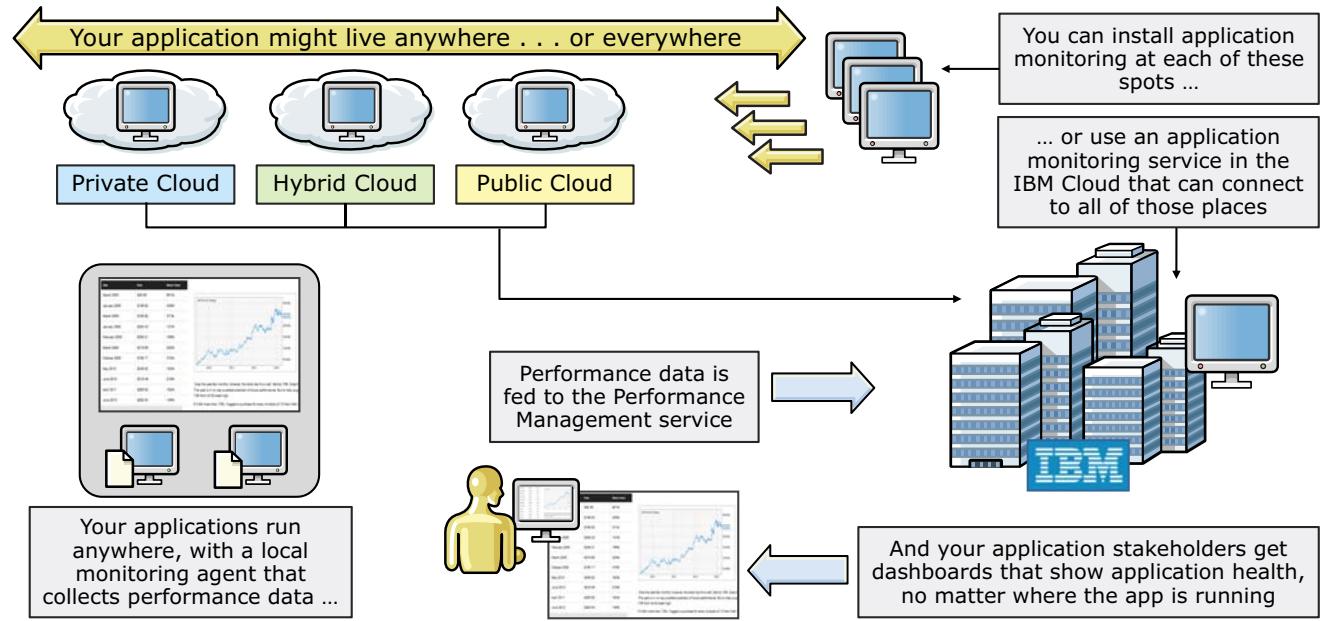
## The Cloud landscape



### The Cloud landscape

The Cloud landscape alters where and how applications are built, deployed, and used. Platforms and software are moving from the traditional on-premises deployment to Cloud-based services for various reasons. With this change comes the need to monitor and manage the existing and new deployment models together with one solution.

## IBM Cloud Application Performance Management



Introduction to IBM Cloud Application Performance Management

6

© Copyright IBM Corporation 2018

### IBM Cloud Application Performance Management

Application performance management (APM) is the practice of detecting and addressing software application issues. The solutions monitor and manage application performance, availability, and security throughout the application lifecycle. They do that by measuring the response times of users, application components, and specific transactions.

IBM Cloud Application Performance Management is a comprehensive solution that helps manage the performance and availability for complex applications that might run in a data center, public Cloud, or hybrid combination. This solution provides you with visibility of your applications to ensure optimal performance and efficient use of resources.

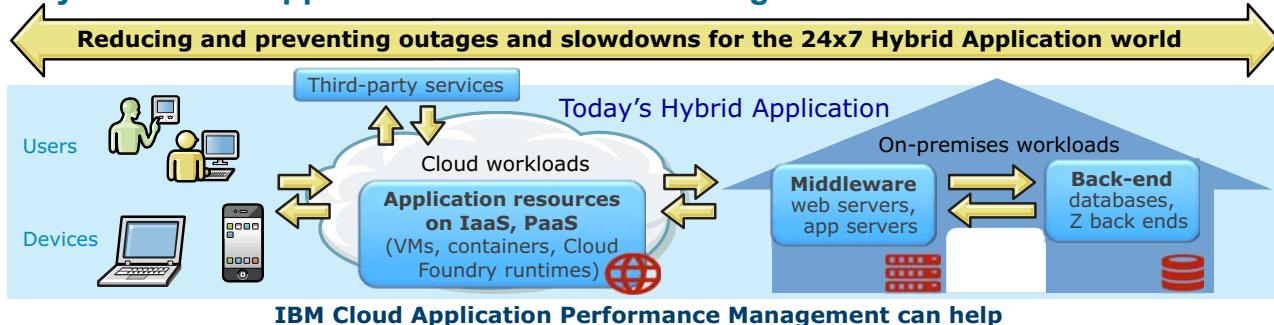
The IBM Cloud Application Performance Management solution collects data from both Cloud APM agents and IBM Tivoli Monitoring agents. Data is displayed in the Cloud APM console for both Cloud APM agents and their hybridized IBM Tivoli Monitoring counterparts.

The installation of your monitoring infrastructure is done in under an hour. The installation of your agents is done in minutes. You can immediately log on to the Cloud APM console to add applications that consist of the managed systems, and view in the Application Performance Dashboard for a status check.

The Application Performance Dashboard navigator is hierarchical, giving a status overview of your applications, the health of their components, and the quality of the user experience. For more details about your monitored resource, you can click a navigator item or a link in the Status Overview tab.

Consider, for example, that your application has slow response time. The issue is revealed in the dashboard. Starting from your dashboard, you can follow the problem to the source by clicking links to discover the cause: high CPU utilization on a system due to an out-of-control process.

## Why IBM Cloud Application Performance Management?

**1****Identify** performance issues before they affect users or the business

- ✓ **Broadest monitoring coverage** of application environments
- ✓ **Simplified problem identification** that uses cognitive analytics to predict potential outages

**2****Isolate** where the problem is occurring

- ✓ **Visibility of user experience** of application, identifying problems before SLAs are impacted
- ✓ **Quickly isolate bottlenecks** that affect performance of an application

**3****Diagnose** for quicker problem resolution

- ✓ **Identify the source of performance issues** with diagnostics down to the line of code that identifies the exact moment of an issue
- ✓ **Quickly resolve issues** that use integrated Log Analytics to search across all of your IT operational data

### IBM Cloud Application Performance Management on IBM Marketplace

Introduction to IBM Cloud Application Performance Management

7

© Copyright IBM Corporation 2018

#### Why IBM Cloud Application Performance Management?

IBM Cloud Application Performance Management is a comprehensive solution that helps you manage the performance and availability of applications that are deployed on-premises (private), in a public Cloud, or as a hybrid combination. This solution provides you with visibility, control, and automation of your applications, ensuring optimal performance and efficient use of resources.

By using this solution, you manage your data center, Cloud infrastructure, and workloads with cognitive intelligence. You can reduce and prevent outages and slowdowns around the clock in a hybrid application world because Cloud APM assists you. It helps in moving from identifying performance issues to isolating where the problem is occurring and diagnosing issues before your business is affected.

Use the key features, which vary by offering, to work with data that the Cloud APM agents and data collectors collect. More features are available through integration with other products and components.

## IBM Cloud APM Portfolio: V8.1.4 offerings

**Single platform available as SaaS, on-premises, hybrid**

### IBM Cloud APM – Core offerings

#### IBM Cloud Application Performance Management, Base

Application-aware infrastructure monitoring for a huge array of infrastructure and resources



#### IBM Cloud Application Performance Management, Advanced

Application-aware infrastructure monitoring, user experience, end-to-end transaction tracking, application resource monitoring, and deep-dive diagnostics



IT Ops

LoB Owner

Developer

#### IBM Cloud APM: Add-ons

#### Extension Packs

For specialized domains

#### IBM Operations Analytics Predictive Insights

Automatic thresholding and anomaly identification with multi-variate analytics

#### IBM Cloud APM, Availability Monitoring

Application availability from around the world with synthetics

#### Extended capabilities: Add-ons

#### IBM Alert Notification

Get alert notifications and manage escalations of application or service issues

#### IBM Runbook Automation

Create and run runbooks and automated tasks

#### IBM Customer Experience Analytics

Business insights on omnichannel customer behavior

### IBM Cloud APM Portfolio: V8.1.4 offerings

The illustration presents the IBM Cloud Application Performance Management offerings and add-ons for SaaS environments and on-premises environments.

#### IBM Cloud Application Performance Management, Advanced

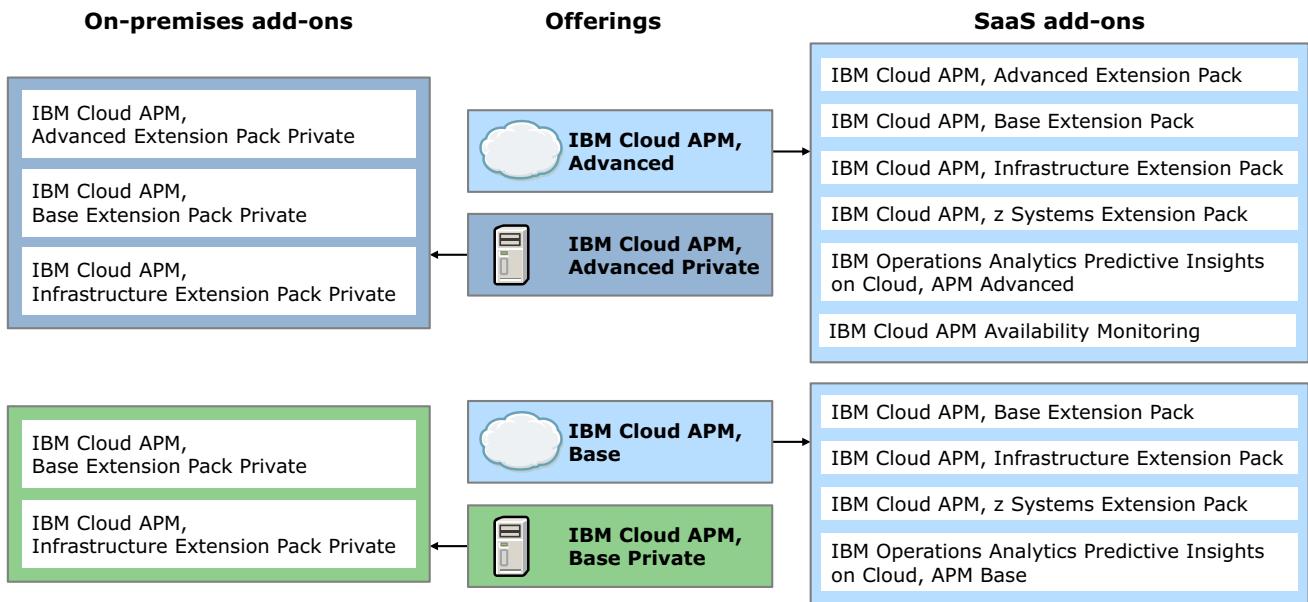
This offering is for user experience, transaction tracking, and resource monitoring of all your application components. You have code-level visibility into your applications and the health of your application servers. Use the diagnostics dashboards to find performance bottlenecks in the application code and for managing your critical applications in production. The offering includes IBM Cloud Application Performance Management, Base, and contains agents and data collectors that you use to monitor applications, transactions, and other resources that are installed in your enterprise.

With this offering, DevOps has a complete solution that provides full visibility and control over your applications and infrastructure. Line-of-business owners can manage critical applications and user experience in production. Application developers can view transaction details and diagnose application problems.

#### IBM Cloud Application Performance Management, Base

This offering is for resource monitoring of infrastructure, application components, and Cloud workloads. Resource monitoring helps you identify and address slow transactions, capacity issues, and outages. The offering contains agents and data collectors that you use to monitor applications and other resources that are installed in your enterprise. With this offering, IT operators can deal with slow transactions, capacity issues, and outages.

## IBM Cloud APM further offerings



Introduction to IBM Cloud Application Performance Management

9

© Copyright IBM Corporation 2018

### IBM Cloud APM further offerings

You can purchase more offerings for the base products that bring added value.

#### Advanced Extension Pack

This extension pack contains the Monitoring Agent for SAP HANA database, the SAP NetWeaver Java Stack agent, and the Monitoring Agent for RabbitMQ. If you have the IBM Cloud Application Performance Management, Advanced offering, this extension pack is available.

#### Base Extension Pack

This extension pack contains the Monitoring Agent for Cassandra, the Monitoring Agent for Hadoop, and the Monitoring Agent for Microsoft Office 365. If you have either of the Cloud APM offerings, this extension pack is available.

#### Infrastructure Extension Pack

This extension pack contains the Monitoring Agent for Amazon EC2 and the Monitoring Agent for Citrix Virtual Desktop Infrastructure. If you have either of the Cloud APM offerings, this extension pack is available.

#### z Systems Extension Pack (Cloud only)

You can use the z Systems Extension Pack to view monitoring data and events for your OMEGAMON application components in the Cloud APM console. If you have either of the Cloud APM offerings, this extension pack is available.

#### Operations Analytics – Predictive Insights

This add-on is for analyzing the metric data that Cloud APM collects, and generating alarms when anomalies are detected. If you have either of the Cloud APM offerings, the add-on is available.

### **Availability Monitoring (Cloud only)**

This add-on is for monitoring the availability and performance of your web applications from multiple, geographically distributed points of presence. This add-on does not function as a stand-alone offering, but is available if you have the IBM Cloud Application Performance Management, Advanced offering.

## Bundled product list

| Title on Passport Advantage  |   |
|--|---|
| IBM Operations Analytics Log Analysis <i>for offering name</i>   | IBM Tivoli Composite Application Manager for Transactions <i>for offering name</i>  |
| IBM SmartCloud Application Performance Management Standard and Non-Prod V7.7 <i>for offering name</i>    | IBM Tivoli Composite Application Manager Transactions V7.4 Response Time and Internet Service Monitoring <i>for offering name</i>                       |
| IBM SmartCloud Application Performance Management Entry Edition for IBM Monitoring                       | IBM Tivoli Monitoring <i>for offering name</i>  |
| IBM Rational 8.6 for IBM Tivoli Composite Application Manager Transactions V7.4 <i>for offering name</i> | IBM Tivoli Composite Application Manager Transactions V7.4 Transaction Tracking <i>for offering name</i>  |
| IBM Tivoli Composite Application Manager for Applications <i>for offering name</i>                       | IBM Tivoli Monitoring for Virtual Environments <i>for offering name</i>   |
| IBM Tivoli Composite Application Manager for Application Diagnostics 7.1.0.4 <i>for offering name</i>    | IBM DB2 Enterprise Server Edition 10.1 for IBM Tivoli Composite Application Manager for Application Diagnostics V7.1.0.4                                |
| IBM Tivoli Composite Application Manager for Microsoft Applications <i>for offering name</i>             | IBM WebSphere Application Server 8.5.5 for IBM Tivoli Composite Application Manager for Application Diagnostics v7.1.0.4 for Multiplatform Multilingual |

### Bundled product list

IBM Cloud Application Performance Management Private includes and bundling and licensing for many other products.

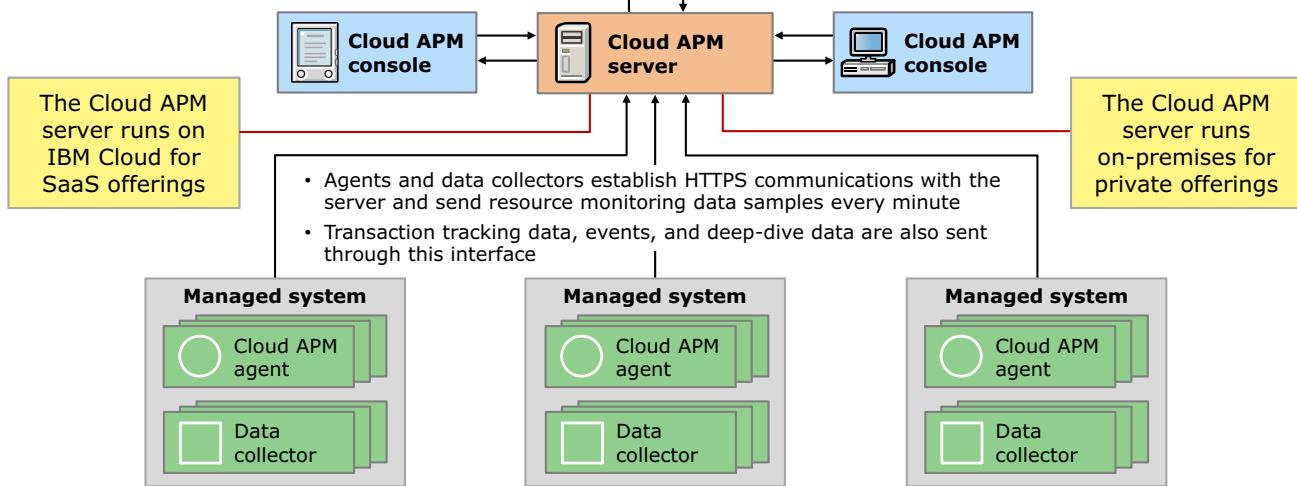
Consult your IBM Sales team for details.

## IBM Cloud APM architecture

- Users log in to the server from a web browser
- The server delivers metrics and events from the agents to the dashboards



IBM Cloud Application Performance Management integrates with other products and components to broaden your perspective with enhanced analytics, reporting, and event handling



### IBM Cloud APM architecture

IBM Cloud Application Performance Management uses agents and data collectors to collect data on the monitored hosts. Agents and data collectors pass the data to the Cloud APM server, which collates it into the Cloud APM console.

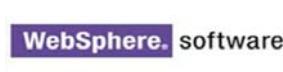
# Lesson 2 Monitoring agents and categories

IBM Training



## Lesson 2: Monitoring agents and categories

- Cloud APM has a huge breadth of coverage that delivers a long list of custom agents and data collectors
- Some agents are delivered only with Cloud APM Advanced, and some agents are delivered with both offerings
- Some agents are delivered only with add-ons
- Some agents support only resource monitoring, and others support deep-dive diagnostics and transaction tracking in addition to resource monitoring



ORACLE  
SIEBEL



Custom Agents  
Using Agent Builder

In this lesson, you learn how to describe Cloud APM agents and data collectors, and how they are categorized.

## Monitoring agents by product and platform (1 of 5)

| Agent and data collectors                     | Cloud APM, Advanced | Cloud APM, Base | Add-ons                       | Linux | AIX | Windows |
|---|---------------------|-----------------|-------------------------------|-------|-----|---------|
| Amazon EC2 agent *                            | RM                  | RM              | Infrastructure Extension Pack | Yes   | Yes | Yes     |
| Cassandra agent *                             | RM                  | RM              | Base Extension Pack           | Yes   | Yes | Yes     |
| Cisco UCS agent                               | RM                  | RM              | No                            | Yes   | No  | Yes     |
| Citrix Virtual Desktop Infrastructure agent * | RM                  | RM              | Infrastructure Extension Pack | Yes   | No  | Yes     |
| DB2 agent *                                   | RM                  | RM              | No                            | Yes   | Yes | Yes     |
| DataPower agent                               | RM, TT              | RM              | No                            | Yes   | Yes | No      |
| Hadoop agent *                                | RM                  | RM              | Base Extension Pack           | Yes   | Yes | Yes     |
| HMC Base agent                                | RM                  | RM              | No                            | No    | Yes | No      |
| HTTP Server agent                             | RM, TT              | RM              | No                            | Yes   | Yes | No      |
| IBM Integration Bus agent *                   | RM, TT              | —               | No                            | Yes   | Yes | Yes     |
| J2SE data collector *                         | RM, TT              | —               |                               | Yes   | Yes | Yes     |

LEGEND: RM = Resource monitoring; TT = Transaction Tracking; DD = Deep-dive diagnostics

### Monitoring agents by product and platform (1 of 5)

This slide and the four slides that follow it are a list of monitoring agents that are included with each product at the time this presentation was created.

For descriptions of the agents, open this URL:

[https://www.ibm.com/support/knowledgecenter/SSHLNR\\_8.1.4/com.ibm.pm.doc/install/overview\\_agent\\_capabilities.htm](https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/install/overview_agent_capabilities.htm)

## Monitoring agents by product and platform (2 of 5)

| Agent and data collectors   | Cloud APM, Advanced | Cloud APM, Base | Add-ons | Linux | AIX | Windows |
|---|---------------------|-----------------|---------|-------|-----|---------|
| JBoss agent *   | RM, TT, DD          | RM              | No      | Yes   | No  | Yes     |
| Liberty data collector for IBM Cloud and on-premises applications * | RM, TT, DD          | -               |         | Yes   | Yes | Yes     |
| Linux KVM agent *   | RM                  | RM              | No      | Yes   | No  | No      |
| Linux OS agent *  | RM                  | RM              | No      | Yes   | No  | No      |
| Microsoft Active Directory agent *                                  | RM                  | RM              |         | No    | No  | Yes     |
| Microsoft Cluster Server agent                                      | RM                  | RM              | No      | No    | No  | Yes     |
| Microsoft Exchange Server agent *                                   | RM                  | RM              | No      | No    | No  | Yes     |
| Microsoft Hyper-V Server agent                                      | RM                  | RM              | No      | No    | No  | Yes     |
| Microsoft Internet Information Services agent *                     | RM                  | RM              | No      | No    | No  | Yes     |
| Microsoft Lync Server agent *                                       | RM                  | RM              | No      | No    | No  | Yes     |
| Microsoft .NET agent *  | RM, TT, DD          | RM              | No      | No    | No  | Yes     |

LEGEND: RM = Resource monitoring; TT = Transaction Tracking; DD = Deep-dive diagnostics

### Monitoring agents by product and platform (2 of 5)

For descriptions of the agents, open this URL:

[https://www.ibm.com/support/knowledgecenter/SSHLNR\\_8.1.4/com.ibm.pm.doc/install/overview\\_agent\\_capabilities.htm](https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/install/overview_agent_capabilities.htm)

## Monitoring agents by product and platform (3 of 5)

| Agent and data collectors   | Cloud APM, Advanced | Cloud APM, Base | Add-ons             | Linux | AIX | Windows |
|---|---------------------|-----------------|---------------------|-------|-----|---------|
| Microsoft Office 365 agent *  | RM                  | RM              | Base Extension Pack | No    | No  | Yes     |
| Microsoft SharePoint Server agent                                   | RM                  | RM              | No                  | No    | No  | Yes     |
| Microsoft SQL Server agent *  | RM                  | RM              | No                  | No    | No  | Yes     |
| MongoDB agent *   | RM                  | RM              | No                  | Yes   | No  | No      |
| MySQL agent *   | RM                  | RM              | No                  | Yes   | No  | Yes     |
| NetApp Storage agent *  | RM                  | RM              | No                  | Yes   | No  | Yes     |
| Node.js agent *   | RM, DD              | RM              | No                  | Yes   | No  | No      |
| Node.js data collector for IBM Cloud and on-premises applications * | RM, DD, TT          | –               | No                  | Yes   | No  | No      |
| OpenStack agent *   | RM                  | RM              | No                  | Yes   | No  | No      |
| Oracle Database agent   | RM                  | RM              | No                  | Yes   | Yes | Yes     |
| PHP agent   | RM                  | RM              | No                  | Yes   | Yes | No      |

LEGEND: RM = Resource monitoring; TT = Transaction Tracking; DD = Deep-dive diagnostics

### Monitoring agents by product and platform (3 of 5)

For descriptions of the agents, open this URL:

[https://www.ibm.com/support/knowledgecenter/SSHLNR\\_8.1.4/com.ibm.pm.doc/install/overview\\_agent\\_capabilities.htm](https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/install/overview_agent_capabilities.htm)

## Monitoring agents by product and platform (4 of 5)

| Agent and data collectors  | Cloud APM, Advanced | Cloud APM, Base | Add-ons                 | Linux | AIX | Windows |
|--|---------------------|-----------------|-------------------------|-------|-----|---------|
| PostgreSQL agent *   | RM                  | RM              | No                      | Yes   | No  | Yes     |
| Python data collector for IBM Cloud and on-premises applications * | RM, DD              | —               | No                      | Yes   | No  | No      |
| RabbitMQ agent *   | RM                  | —               | Advanced Extension Pack | Yes   | No  | Yes     |
| Response Time Monitoring Agent                                     | RM, TT              | RM              |                         |       |     |         |
| Ruby agent   | RM, DD              | RM              | No                      | Yes   | No  | No      |
| Ruby data collector for IBM Cloud applications *                   | RM, DD              | —               | No                      | Yes   | No  | No      |
| SAP agent  | RM                  | —               | No                      | Yes   | Yes | Yes     |
| SAP HANA Database agent *  | RM                  | —               | Advanced Extension Pack | Yes   | Yes | Yes     |
| SAP NetWeaver Java Stack agent *                                   | RM, TT, DD          | —               | Advanced Extension Pack | Yes   | Yes | Yes     |

LEGEND: RM = Resource monitoring; TT = Transaction Tracking; DD = Deep-dive diagnostics

### Monitoring agents by product and platform (4 of 5)

For descriptions of the agents, open this URL:

[https://www.ibm.com/support/knowledgecenter/SSHLNR\\_8.1.4/com.ibm.pm.doc/install/overview\\_agent\\_capabilities.htm](https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/install/overview_agent_capabilities.htm)

## Monitoring agents by product and platform (5 of 5)

| Agent and data collectors              | Cloud APM, Advanced | Cloud APM, Base | Add-ons | Linux | AIX | Windows |
|--|---------------------|-----------------|---------|-------|-----|---------|
| Siebel agent *                         | RM                  | RM              | No      | Yes   | Yes | Yes     |
| Synthetic Playback agent *             | RM                  | –               | No      | Yes   | No  | No      |
| Tomcat agent *                         | RM, TT              | RM              | No      | Yes   | No  | Yes     |
| UNIX OS agent                          | RM                  | RM              | No      | No    | Yes | No      |
| VMware VI agent *                      | RM                  | RM              | No      | Yes   | No  | Yes     |
| WebLogic agent *                       | RM, TT, DD          | RM              | No      | Yes   | No  | Yes     |
| WebSphere Applications agent *         | RM, TT, DD          | RM              | No      | Yes   | Yes | Yes     |
| WebSphere Infrastructure Manager agent | RM                  | RM              | No      | Yes   | No  | No      |
| WebSphere MQ agent *                   | RM, TT              | –               | No      | Yes   | Yes | Yes     |
| Windows OS agent                       | RM                  | RM              | No      | No    | No  | Yes     |

LEGEND: RM = Resource monitoring; TT = Transaction Tracking; DD = Deep-dive diagnostics

### Monitoring agents by product and platform (5 of 5)

For descriptions of the agents, open this URL:

[https://www.ibm.com/support/knowledgecenter/SSHLNR\\_8.1.4/com.ibm.pm.doc/install/overview\\_agent\\_capabilities.htm](https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/install/overview_agent_capabilities.htm)

## Create custom agents with IBM Agent Builder

- Integrates with Cloud APM on-premises or SaaS

| Name                               | Status   | Page Fa... | Working... |
|------------------------------------|----------|------------|------------|
| DB2                                | DOWN     | 0          | 0          |
| DB2DAS00                           | UP       | 0          | 14         |
| DB2GOVERNOR_DB2COPY1               | DOWN     | 0          | 0          |
| DB2LICD_DB2COPY1                   | DOWN     | 0          | 0          |
| DB2MGMTSVC_DB2COPY1                | UP       | 0          | 9          |
| DB2REMOTECMD_DB2COPY1              | DOWN     | 0          | 0          |
| DSRDBM01                           | DOWN     | 0          | 0          |
| IHSforTivoliEnterprisePortalSer... | UNKNO... | 0          | 0          |

- Summary and details dashboards for selected attributes are packaged and installed with agent
- Existing Cloud APM agent must be installed on the agent host

Introduction to IBM Cloud Application Performance Management

18

© Copyright IBM Corporation 2018

### Create custom agents with IBM Agent Builder

IBM Agent Builder agents can be deployed within a Cloud APM private or Cloud environment. With Agent Builder, you create web user interface definitions for the Cloud APM console in a Cloud APM environment. The Additional Attributes view provides access to all monitored attributes.

# Lesson 3 Application-based monitoring

IBM Training



## Lesson 3: Application-based monitoring

- A fundamental difference from IBM Tivoli Monitoring and Cloud APM is the focus on managing applications
- This lesson covers the basics of managing applications versus managing resources

In this lesson, you learn how to describe the basics of application-based monitoring.

## Application-based monitoring overview (1 of 2)

• You can use Cloud APM to manage applications that are made up of resources

• You are able to easily create applications that are made up of agents that are installed and connected to the Cloud APM server

• The Cloud APM console is the web-based user interface into the product

### Application-based monitoring overview (1 of 2)

The Cloud APM console is the user interface for Performance Management. This unified user interface provides a single view across hybrid applications. You use the console to view the status of your applications and quickly assess and fix performance and availability issues.

The dashboards in the console simplify problem identification so you can isolate bottlenecks that affect application performance. With simple dashboard navigation, you move from a view of application status to code-level detail. You have visibility into source code problems at the exact moment of an issue. You can search and diagnose problems by using integrated search analytics.

## Application-based monitoring overview (2 of 2)

The screenshot shows the 'Application Dashboard' interface. On the left, there's a sidebar with sections for 'Applications', 'Groups', and 'Instances'. The main area is titled 'All My Applications' and lists 'DayTrader' and 'My Components'. Each application has a summary bar with status indicators (red, yellow, green) and a 'Details' link. Below the applications are three summary cards: 'Components' (red), 'Transactions' (green), and 'Events' (red). A callout box contains the following text:

- Application status is solely determined by monitoring events
  - Events come from the monitoring agents of the components and transactions
  - The status of the component (summary widgets) does not affect the status of the application
- Component status is determined by agents that monitor the technology domains that the application is composed of, such as HTTP server, application server, database, WebSphere Message Broker
- Transaction health is determined by the status of the requests that come into the application and then flow back through the application components

### Application-based monitoring overview (2 of 2)

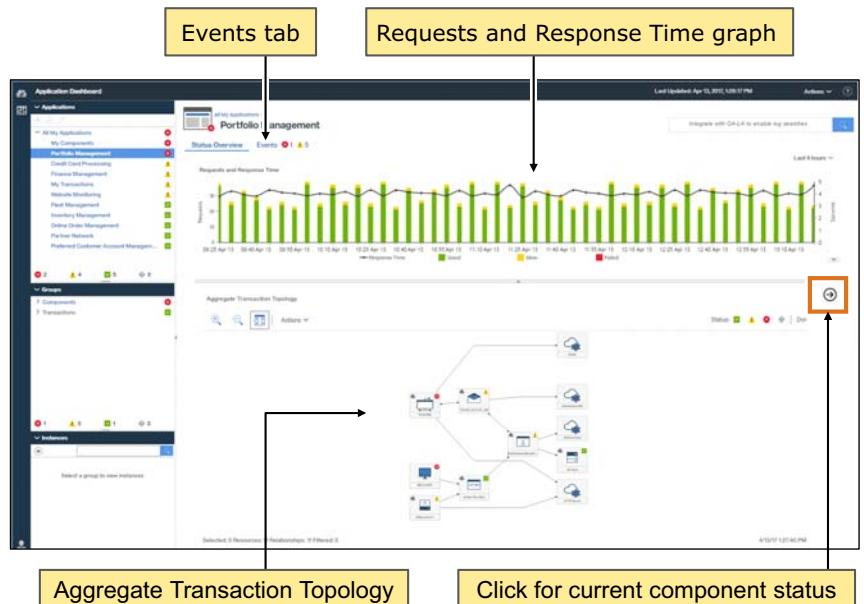
An application is composed of multiple parts. It can have web servers, databases, and operating systems all supporting a single application. The component health indicates to the user how these components are behaving as a unit.

Transactions also must be considered. A web server, database, and operating system might be active, but if the transaction throughput is slow, you want to know about it.

Events are used to indicate when components or transactions need attention. An event is triggered as a result of a threshold that is met. Events affect the status of both the component and the application.

## Application summary

- Requests and Response Time:  
Identifies slow and failed user requests to the applications
- Aggregate Transaction Topology:  
Shows the relationship of application components and identifies where problems are located
- Events: Identifies the number of Critical and Warning events
- Current component status:  
Identifies components with problems
  - Health of each component:  
Normal, Warning, Critical, Unknown



### Application summary

When using the Cloud APM console to drill down into an application, you encounter multiple graphs and tables.

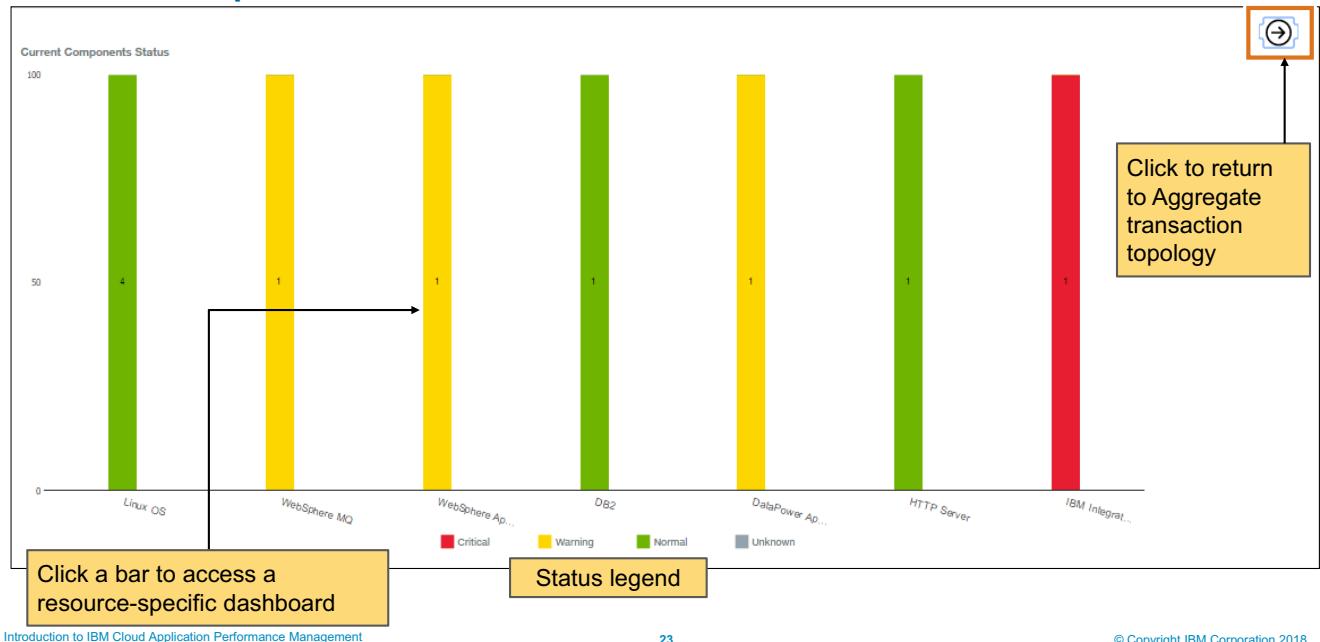
The Event tab shows the events.

The Requests and Response Time graph identifies slow and failed user requests to the applications. It shows the number of transactions, average response time of transactions, percentage of transactions that are good, slow, or failing.

The Aggregate Transaction Topology shows the relationship of application components and identifies where problems are located by monitoring the performance and availability of transactions as they flow through the application components.

The current component status is revealed by clicking the arrow indicated on the slide.

## Current component status



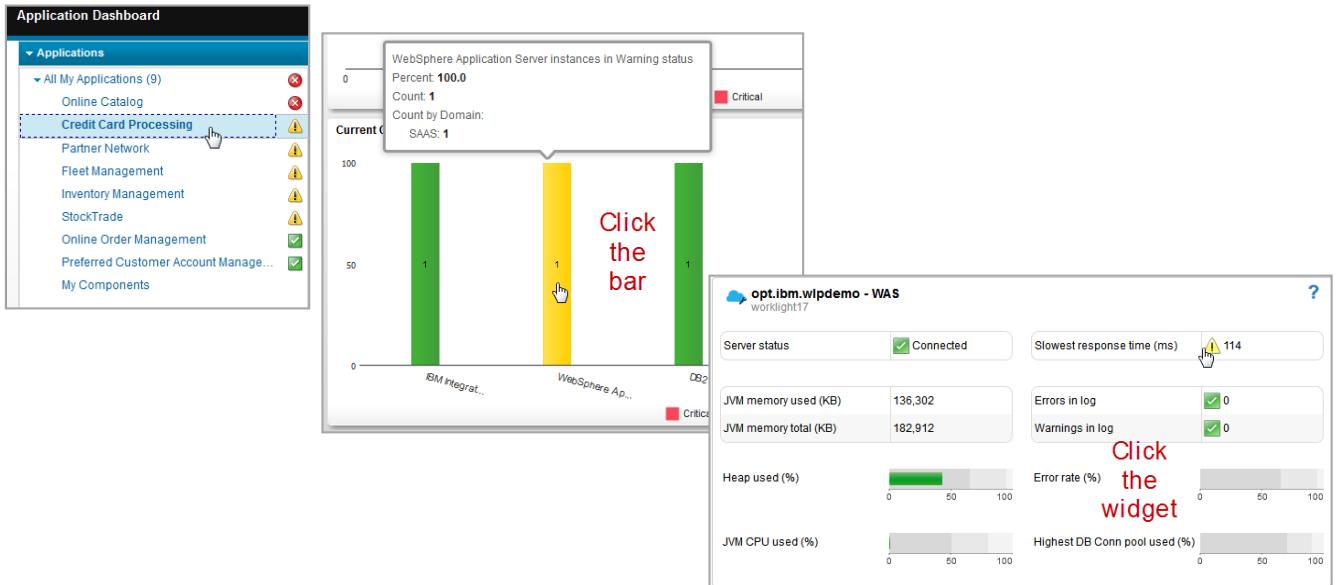
Introduction to IBM Cloud Application Performance Management

23

© Copyright IBM Corporation 2018

Current component status

## Navigate from a widget to an underlying cause



### *Navigate from a widget to an underlying cause*

The Cloud APM console is hierarchical, giving a status overview of your applications, the health of their components, and the quality of the user experience.

For more details about your monitored resource, you can click a navigator item or a link in the Status Overview tab. Consider, for example, that your application has a slow response time. The issue is revealed in the dashboard from a threshold event. Starting from your dashboard, you can follow the problem to the source by clicking links to discover the cause: a WebSphere problem.

Identify a red or yellow component. Click the component bar to navigate to the component summary. Click the summary to view the component details.

## View component details



*View component details*

Click a resource instance widget to access resource detail dashboards.

## Identify root causes with deep-dive diagnostics

**Requests with Slowest Response Time**

| URL  | Request Name                             | Average Response Time (ms) | Error Rate (%) |
|--|--|----------------------------|----------------|
| http://10.62.56.193:80/PlantsByWebSphereAjax/servlet/IRPCAd... | /PlantsByWebSphereAjax/servlet/IRPCAd... | 114                        |                |

**WebSphere Applications**

| Application Name      | Average Response Time | Throughput |
|-----------------------|-----------------------|------------|
| PlantsByWebSphereAjax | 5                     |            |
| PlantsByWebSphereAjax | 1                     |            |
| commsvc.ws.sample     | 0                     |            |
| commsvc.pbx           | 0                     |            |
| DefaultApplication    | 0                     |            |
| lvApp                 | 0                     |            |
| query                 | 0                     |            |

**Request Summary**

| Request name                | Average response time | Minimum response time | Maximum response time | Sampled requests | Request count | CPU time (ms) | Request type | Action                             |
|-----------------------------|-----------------------|-----------------------|-----------------------|------------------|---------------|---------------|--------------|------------------------------------|
| /ITCAM/testware/ejbStateful | 12500                 | 12500                 | 12500                 | 1                | 1             | 612           | Servlet      | <a href="#">View instance data</a> |
| /PlantsByWebSphereAjax/...  | 9744                  | 9744                  | 9744                  | 1                | 1             | 39            | Servlet      | <a href="#">View instance data</a> |
| /PlantsByWebSphereAjax/...  | 1024                  | 1024                  | 1024                  | 1                | 1             | 24            | Servlet      | <a href="#">View instance data</a> |
| /PlantsByWebSphereAjax/...  | 122                   | 122                   | 122                   | 1                | 1             | 30            | Servlet      | <a href="#">View instance data</a> |
| /PlantsByWebSphereAjax/...  | 20                    | 20                    | 20                    | 1                | 9             | 422           | Servlet      | <a href="#">View instance data</a> |
| /PlantsByWebSphereAjax/...  | 10                    | 10                    | 10                    | 1                | 14            | 612           | Servlet      | <a href="#">View instance data</a> |

**Response Time Breakdown**

**Response Time Distribution**

### Identify root causes with deep-dive diagnostics

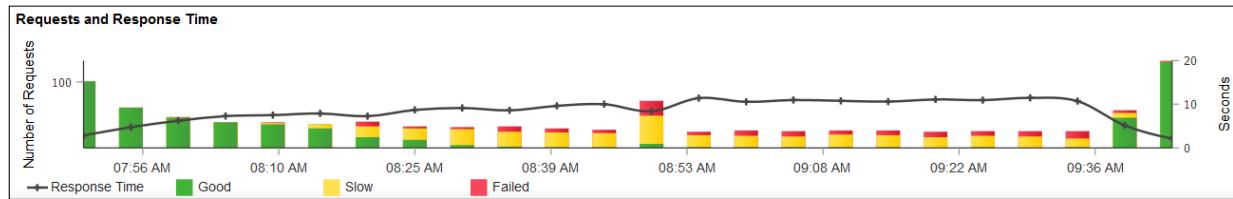
When diagnostic mode is enabled, a Diagnose option is available for slow requests on the Status Overview dashboard.

On the next dashboard, several widgets display response-time data, including a table at the top of the Request Summary table.

To see request-instance data, click the link in the Action column.

## Monitor user experience

- Monitors the performance and availability of HTTP requests from users to your application
- Includes these monitoring components:
  - Response Time agent for monitoring incoming HTTP transactions
  - HTTP Server agent
  - JavaScript injection for monitoring browser activity



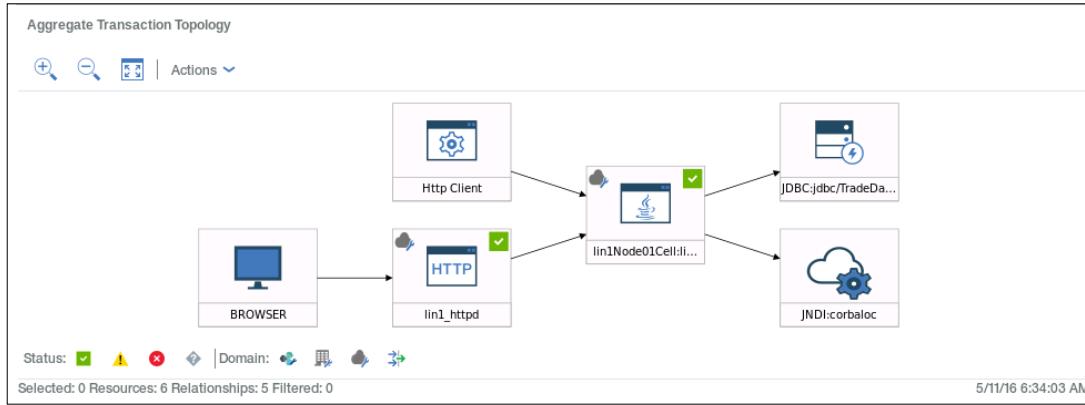
### Monitor user experience

End User Transactions dashboards now include user and device information, which was previously displayed in the Authenticated Users and Mobile Devices Users dashboards in the Users group.

User, session, and device information is now sorted by location (country, state, and city) based on the IP address of the user. The updated dashboards help administrators to understand user volumes and whether issues are isolated to specific sets of users.

## Locate problems with transaction tracking

- Monitors availability and performance of middle and back-end transactions
  - For current, live transactions and transactions over time (trend analysis)
- Creates topology diagrams that show transaction paths through application components
  - Identifies where transactions and applications are failing or slow
    - Helps identify root cause of problems
    - Helps determine problem ownership



### Locate problems with transaction tracking

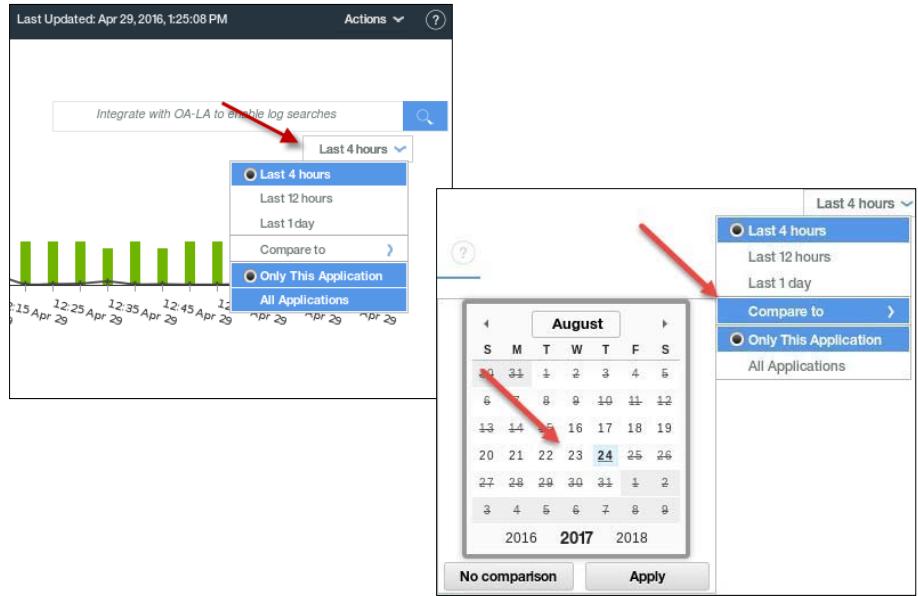
Each node represents the transaction data within a monitored domain. The two types of topologies are aggregate and instance. An aggregate topology is a topology of aggregated transaction data, which is the average performance of a transaction over the aggregate interval. An instance topology is a topology based on a single transaction instance and shows actual time values.

The node image is unique for each monitored domain. Lines between nodes show transactions that are flowing between nodes. Lines with one arrowhead indicate that the transaction requests flow in one direction only. Lines with two arrowheads indicate bidirectional transactions. A status indicator for good, slow, or failed is placed on the upper right of each node.

Roll over a node for details on that node.

## Viewing historical data

- Plot charts, bar charts
- Default last 4 hours
- Options for other time spans
  - Last 12 hours
  - Last 1 day
  - Last 1 week
    - Some limitations
  - Only this application or all applications
- Applies to all widgets on a dashboard



### Viewing historical data

The dashboard user can determine the time span for certain widgets that show data that is plotted over time. The default behavior is to show the past 4 hours. The other available options are last 12 hours, last day, and last week. Certain history widgets, such as in the WebSphere monitor, are limited to a maximum of 1 day to avoid excessive load on the Monitoring Infrastructure Node server.

You can choose to apply the time span change to only the current application or all applications. You should keep in mind that increasing the time span increases the load on the Monitoring Infrastructure Node server and can slow your response time, possibly by a significant amount.

## Opening reports from the Application Dashboard

You can access available reports from the Actions menu

Last Updated: May 4, 2016, 6:48:52 PM

All My Applications

EJB Performance

DB Connection Pools

Available reports

Last Updated: May 4, 2016, 6:48:52 PM

All My Applications

Compare Performance of Multiple Applications

Application Performance and Usage

Compare Application Performance over Two Time Periods

Application Request Performance

DB Connection Pools

EJB Performance

GC Usage of Application Server

JVM Usage for Application Server

Threadpools

WebApplication Performance

Application Request Performance for Cluster

JVM and GC Usage for Cluster

Top applications with slowest response time across servers

### Opening reports from the Application Dashboard

The reports can be launched in context from the dashboard. When you are positioned on the All My Applications dashboard, you can run the All My Applications report. When you are viewing application details, and that application has transactions, you can run the other three reports in the context of the currently selected application.

Select an application from **Application Dashboard > Applications**. The slide shows an example of selecting the DayTrader application. From the Actions menu, select **Launch To Reports**. From the next drop-down menu, more choices might be available, depending on which application is initially selected.

# Lesson 4 Monitoring agent examples

IBM Training



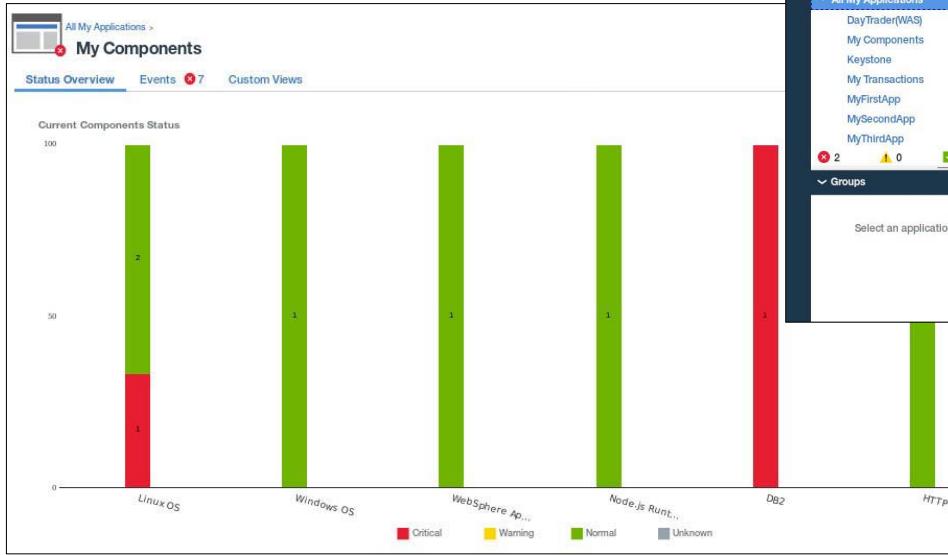
## Lesson 4: Monitoring agent examples

- Given the number of agents that Cloud APM supports, you review a subset of the agents during this class
- It is useful to get some examples of the output that you see as you explore the agent
- It has a common appearance, behavior, and drill-down capability regardless of which agent you are using

This lesson presents examples of monitoring agent output.

## The Application Dashboard navigator

- Application Dashboard is the starting navigator



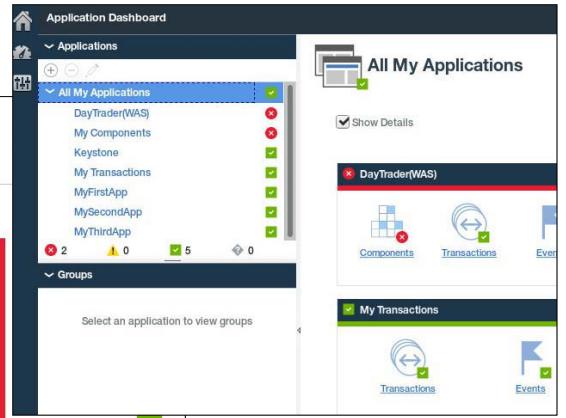
Introduction to IBM Cloud Application Performance Management

32

© Copyright IBM Corporation 2018

### The Application Dashboard navigator

- More navigators can be clicked to see more agent information



After logging in to the Cloud APm console and selecting **Performance > Application Performance Dashboard**, the Application Dashboard opens. This navigator is the beginning of steps that drill down to display more information.

## My Components: A summary of events and agents



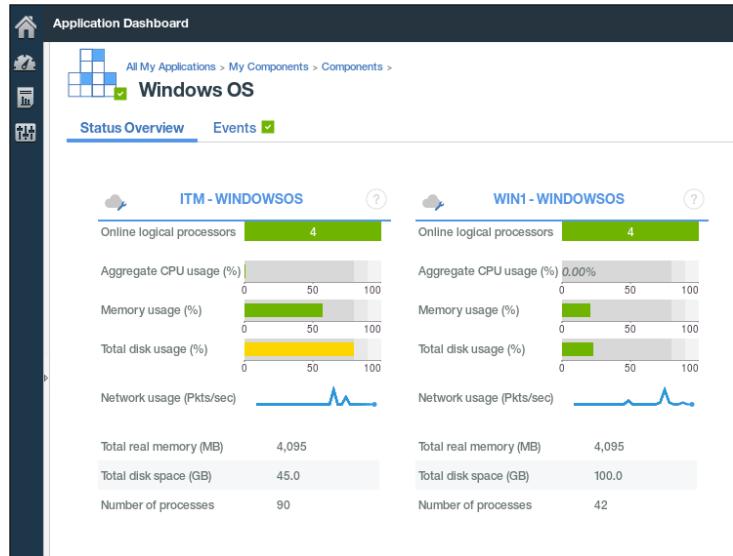
*My Components: A summary of events and agents*

Clicking any of the bars' open widgets with more information about the events or agents. The colors of the bars are listed in the legend. Green bars indicate that the agent is active.

## Monitoring agents for Linux OS, UNIX OS, and Windows OS

- Basic operating system statistics
  - CPU
  - Memory
  - Disk
  - Network

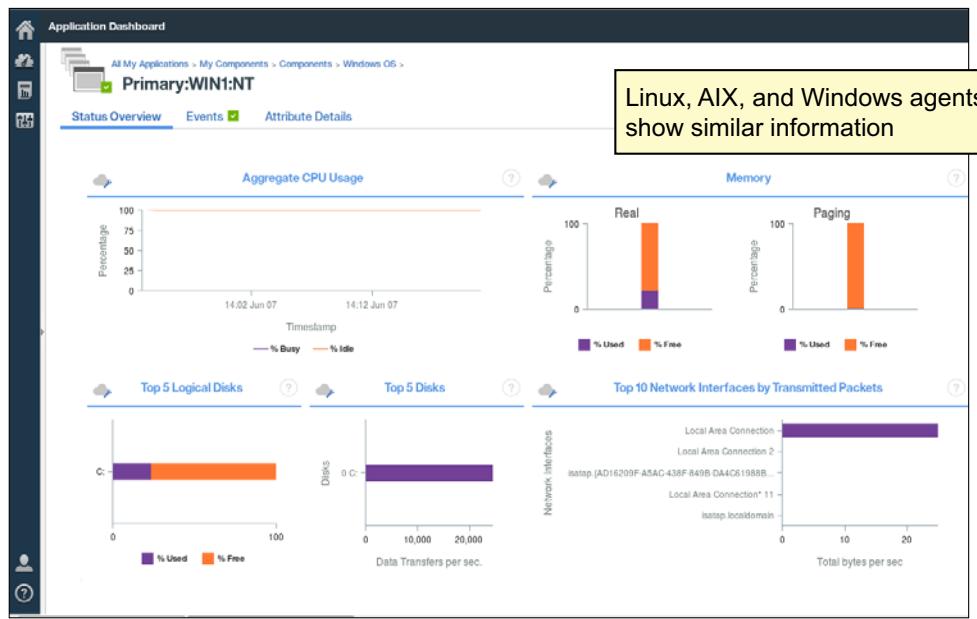
**Note:** Linux OS, UNIX OS, and Windows OS agents are configured and started automatically



### Monitoring agents for Linux OS, UNIX OS, and Windows OS

The operating system monitoring agents provide the basic operating system metrics such as CPU, memory, disk, and network. The status overview shows you the server's health at a glance. The entire widget is a hyperlink that you can use to gather more details.

## Example of Windows OS agent details (1 of 2)



### Example of Windows OS agent details (1 of 2)

The instance details show you information about the Aggregate CPU Usage, Memory, Top 5 Logical Disks, and the Top 10 Network Interfaces over the past 2 hours.

The screen capture is an example of the Windows OS monitoring agent, but the UNIX OS and Linux OS monitoring agents show you the same information in the same views.

## Example of Windows OS agent details (2 of 2)

The screenshot shows the Application Dashboard for a Windows OS agent named 'Primary:WIN1:NT'. The dashboard includes sections for Status Overview, Events, and Attribute Details. The Status Overview section displays real-time metrics like Data Transfers per sec. and Total bytes per sec. The Processes Information section lists various system statistics such as the number of processes (42), threads (605), semaphores (1,045), mutexes (1,033), events (3,343), and sections (1,340). The Log Files section shows no items to display. The System Information section provides details about the operating system (Windows\_2008\_R2 - 6.1), FQDN (win1.ibm.edu), computer name (VMware Virtual Platform), host addresses (192.168.1.103 - ::1), system uptime (3 days), and hyper-threading status (Disabled). Below these, the System, Application and Security Logs section lists logs for Security, Application, and System types, showing their last modified date, usage percentage, number of events, and log size.

| Log name    | Log type    | Date time last modified | Usage | Number of events | Log size |
|-------------|-------------|-------------------------|-------|------------------|----------|
| Security    | Security    | Jun 3, 2016 9:22:14 PM  | 0.10% | 2,966            | 2,116 KB |
| Application | Application | Jun 3, 2016 9:22:14 PM  | 0.05% | 934              | 1,092 KB |
| System      | System      | Jun 3, 2016 9:22:12 PM  | 0.05% | 2,945            | 1,092 KB |

Example of Windows OS agent details (2 of 2)

Scrolling further down the page shows you processes information, log files, system information, and log details.

## Example of Events tab

The screenshot shows the 'My Components' dashboard. At the top, there are tabs for 'Status Overview', 'Events (7)', and 'Custom Views'. A progress bar at the top indicates 100.00% completion. Below the tabs, it says 'Total Events: 7 Critical Events: 7 Warning Events: 0 Normal Events: 0'. The main area is a table with the following columns: Threshold Name, Status, Severity, Display Item, Source, Timestamp, and Description. The table lists seven critical events, all of which are 'Open' and have a severity of 'Critical'. The descriptions for these events mention various system components like 'gnome-clocks', 'TRADEDDB', and 'db2inst1'. The timestamp for all events is Dec 20, 2017.

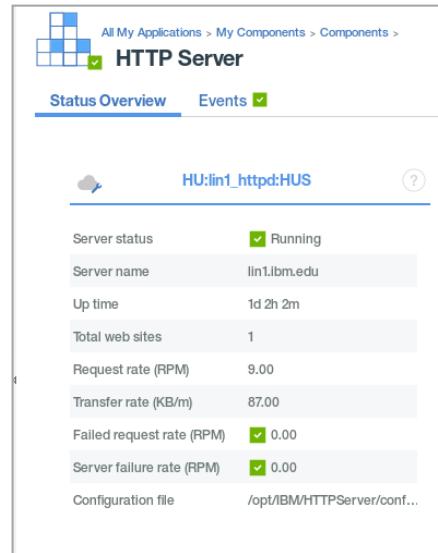
| Threshold Name                 | Status | Severity | Display Item | Source          | Timestamp                 | Description |
|--------------------------------|--------|----------|--------------|-----------------|---------------------------|-------------|
| Linux_Missing_Process          | Open   | Critical | gnome-clocks | apm:LZ          | Dec 20, 2017, 5:04:39 PM  |             |
| UDB_Appl_PkgCache_Hit_Low_2    | Open   | Critical | TRADEDDB     | db2inst1:in1:UD | Dec 20, 2017, 2:53:08 PM  | An applic   |
| UDB_DB_BP_Hit_Ratio_Low_2      | Open   | Critical | TRADEDDB     | db2inst1:in1:UD | Dec 20, 2017, 2:50:11 PM  | A databa    |
| UDB_DB_Pool_Hit_Idx_Pct_Crit_2 | Open   | Critical | TRADEDDB     | db2inst1:in1:UD | Dec 20, 2017, 11:07:25 AM | The perc    |
| UDB_DB_Pool_Hit_Rat_Pct_Crit_2 | Open   | Critical | TRADEDDB     | db2inst1:in1:UD | Dec 20, 2017, 11:07:25 AM | The perc    |
| UDB_Buff_Max_Used_Pct_Crit_2   | Open   | Critical | db2inst1     | db2inst1:in1:UD | Dec 20, 2017, 10:07:10 AM | The perc    |
| UDB_Buff_Used_Pct_Crit_2       | Open   | Critical | db2inst1     | db2inst1:in1:UD | Dec 20, 2017, 10:07:10 AM | The perc    |

### Example of Events tab

This slide is an example of the Events tab.

## Monitoring agent for IBM HTTP Server: Summary dashboard

- The IBM HTTP Server can be installed in one or multiple directories (copy, instance) in an operating system
- A web server has one or multiple websites configured
- Each website has its unique port



### Monitoring agent for IBM HTTP Server: Summary dashboard

The monitoring agent for HTTP helps you monitor availability, performance, and activity of your web server and associated websites.

On the highest-level dashboard, a summary widget is displayed, which returns data for these items:

- Server name
- Status
- Up time

In addition, data is displayed for these items:

- Total websites that are configured on this server instance
- Request rate per minute
- Transfer rate in KB per minute, and per-minute statistics for other rates:
  - Failed requests rate
  - Server failure rate
  - Failed login rate

The location of the configuration file is also provided.

## IBM HTTP Web Server: Detail dashboard with website list

The Web Server Details dashboard provides this information:

- List of websites on this web server
- Historical graphs:
  - Request Rate
  - Transfer Rate
  - Failed Rate
  - Successful and Failed Login Rate
- Website-specific data when you select a website in the list for review

The screenshot shows a dashboard titled "HU:nc9098036112\_httpd:HUS". It includes tabs for "Status Overview", "Events", and "Attribute Details". Below these tabs is a "Web Site List" table with the following data:

| Web Site Name                      | Status  | Web Server Name                    | Failed Request Rate | Failed Page Rate | Server Failure Rate | Failed Login Rate | Successful Logins | Successful Requests |
|------------------------------------|---------|------------------------------------|---------------------|------------------|---------------------|-------------------|-------------------|---------------------|
| 9.98.36.112(80)                    | Running | 9.98.36.112                        | 12                  | 12               | 0                   | 0                 | 0                 | 12                  |
| nc9098036112.tivlab.austin.ibm.com | Running | nc9098036112.tivlab.austin.ibm.com | 0                   | 0                | 0                   | 0                 | 0                 | 0                   |

### IBM HTTP Web Server: Detail dashboard with website list

With the Web Server Detail dashboard, you determine the successful and failed requests to the web server, and to the websites on this server. In addition, you can determine the number of KB that are sent to the web server and the number of failed and successful logins to the website.

# Lesson 5 Integrating with Cloud APM

IBM Training



## Lesson 5: Integrating with Cloud APM

- Integrating with IBM Tivoli Monitoring
  - Hybrid gateway
  - Agent coexistence
  - ITM Data Warehouse
- Integrating with IBM Cloud
- Integrating with Netcool/OMNIbus
- Integrating with IBM Operations Analytics Log Analysis
- Integrating with IBM Operations Analytics – Predictive Insights
- Integrating with IBM Alert Notification
- Integrating with IBM Control Desk
- Integrating with DASH



This section describes how Cloud APM can integrate with other IBM products to expand your monitoring solution.

## Hybrid Gateway overview

- Customers need to manage both IBM Tivoli Monitoring 6 On Premises and Cloud APM agents
  - In an environment that includes both IBM Tivoli Monitoring and Cloud APM products, you can install the Hybrid Gateway to provide a consolidated view of managed systems from both domains
- The Hybrid Gateway can help customers migrate from Tivoli Monitoring 6 to Cloud APM
- The Hybrid Gateway must be installed in your Tivoli Monitoring environment on a system with Red Hat Enterprise Linux Server 6 Update 2 or higher
- The Hybrid Gateway can support in the range of 1500 – 2000 Tivoli Monitoring on-premises agents

### Hybrid Gateway overview

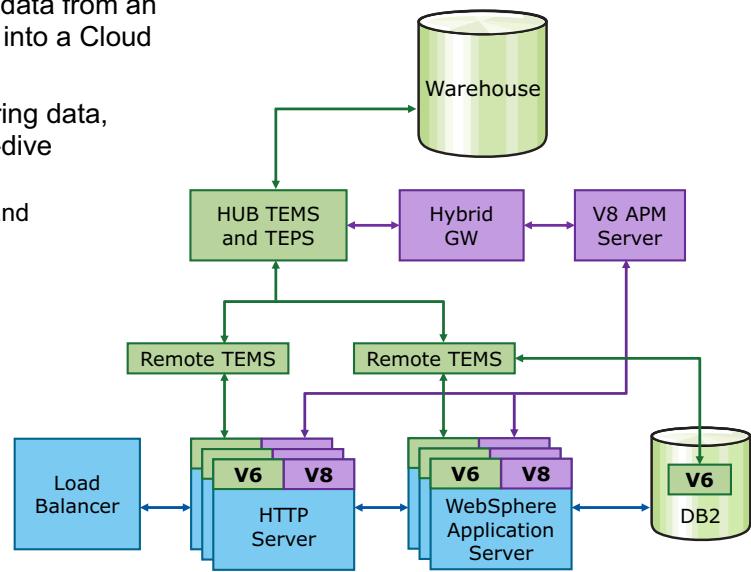
When your monitored environment includes both IBM Tivoli Monitoring and IBM Cloud APM, you can install the Hybrid Gateway to get a consolidated view of managed systems from both domains.

When the Performance Management Hybrid Gateway is installed and configured, you can view managed systems from a Tivoli Monitoring domain in the Performance Management console. This gateway must be installed on systems with Red Hat Enterprise Linux Server 6 Update 2 or later.

Having more than 2000 managed systems can degrade performance. You can view a limit of 2000 managed systems.

## Adding in the Hybrid Gateway

- You can use Hybrid Gateway to bring data from an IBM Tivoli Monitoring V6 environment into a Cloud APM V8 environment
- Hybrid GW supports resource monitoring data, but not transaction tracking and deep-dive diagnostic data
  - Use v8 agents for transaction tracking and deep-dive diagnostic data
- Both metric data and events can be visualized in IPM V8
- Uses a single web-based console
- Suggest an extra Tivoli Enterprise Portal Server for the hybrid gateway
- 8.1.4 adds the ability to have multiple hybrid gateways



### Adding in the Hybrid Gateway

This simplified application topology gives you an idea of what the process would look like adding APM capabilities for .NET, IIB/Broker, or MQ. The business application components are in blue. IBM Tivoli Monitoring V6 and V7 components are in green, and APM V8 components are in purple.

## Viewing hybrid agents in the dashboard

The screenshot shows the Cloud APM dashboard with two main views:

- ITM - WINDOWSOS:** This view displays performance metrics for an IBM Tivoli Monitoring (ITM) agent running on a Windows OS. It includes:
  - Online logical processors: 4
  - Aggregate CPU usage (%): 0.00%
  - Memory usage (%): ~40%
  - Total disk usage (%): ~100%
  - Network usage (Pkts/sec): Line chart showing fluctuating traffic.
  - Total real memory (MB): 4,095
  - Total disk space (GB): 35.0
  - Number of processes: 95
- WIN1 - WINDOWSOS:** This view displays performance metrics for a Cloud APM agent (WIN1) running on a Windows OS. It includes:
  - Online logical processors: 4
  - Aggregate CPU usage (%): 0.00%
  - Memory usage (%): ~40%
  - Total disk usage (%): ~100%
  - Network usage (Pkts/sec): Line chart showing fluctuating traffic.
  - Total real memory (MB): 4,095
  - Total disk space (GB): 100.0
  - Number of processes: 45

Both views include a "Status Overview" tab and an "Events" tab. The top navigation bar shows "All My Applications > My Components > Components > Windows OS". The bottom of the page includes copyright information: "Introduction to IBM Cloud Application Performance Management" and "© Copyright IBM Corporation 2018".

- ITM is an IBM Tivoli Monitoring agent
- WIN1 is a Cloud APM agent



### Viewing hybrid agents in the dashboard

Hybrid agents can be viewed in the Cloud APM console. In a hybrid environment, you can see information that represents agents from traditional monitoring systems and from Cloud APM. In the example, views display the IBM Tivoli Monitoring Linux agents, and counts of agents from Tivoli Monitoring and from Cloud APM.

Notice the icon on the view that represents the Status Overview and the Details that are in the upper-left corner of each view. It looks like a building with a wrench on it. This icon indicates agents from a traditional Tivoli Monitoring environment or domain that are displayed in Cloud APM by using the hybrid agent.

## Benefit of integrating IBM Tivoli Monitoring events

The screenshot displays two interfaces side-by-side. On the left is the 'Enterprise Status - localhost - SYSADMIN' window from the Tivoli Monitoring interface, showing a tree view of 'Enterprise', 'Linux Systems', and various hosts like 'nc9037034031'. On the right is the 'IBMSmartCloud Application Dashboard' from Cloud APM, showing the 'Event Dashboard' with a chart titled 'Open Situation Counts - Last 24 Hours' and a table of 'Event Severity Summary (Total: 2)'. A yellow callout box on the right states: 'Customers can now see situation events that are opened by the IBM Tivoli Monitoring agents and are integrated into APM'.

| Situation Name | Status | Severity | Display Item    | Source       | Timestamp  |
|----------------|--------|----------|-----------------|--------------|------------|
| HG_EIF_Sit     | Open   | Critical | nc9037034031.LZ | nc9037034031 | 2015-10-20 |
| HG_EIF_Sit     | Open   | Critical | nc9037034211.LZ | nc9037034211 | 2015-10-20 |

Benefit of integrating IBM Tivoli Monitoring events

No new components are necessary to install in the Advanced configuration for the Hybrid Gateway. The Hybrid Gateway still requires a Managed System Group name that corresponds to the IBM Tivoli Monitoring Managed System List name. The Hybrid Gateway also still requires a Tivoli Enterprise Portal Server host name, Portal Server Port, Portal Server Protocol, Portal Server user name, and any applicable pass-through proxy port and protocol.

The EIF Port in the Hybrid Gateway configuration affects the integration. The Hybrid Gateway listens for events on the same port as the MIN event.

In the Hub Tivoli Enterprise Monitoring Server configuration in IBM Tivoli Monitoring, The Tivoli Event Integration Facility (EIF) must be activated. The location of the Hybrid Gateway and its EIF listener port must be provided. If events are already being emitted to another destination (for example, OMNIbus), further destinations can be defined by using the `tacmd createeventdest` command.

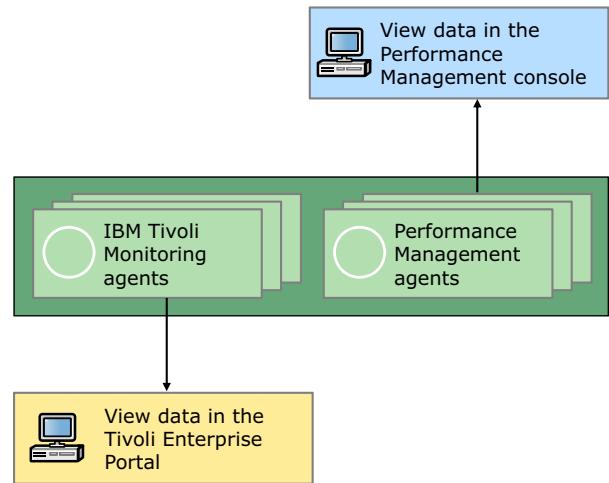
From IBM Tivoli Monitoring in the Situation Editor, edit a situation whose events should be forwarded to APM. On the EIF tab:

- Select the **Forward Events to an EIF Receiver** check box.
- Select the new **Hybrid Gateway Receiver**.
- Repeat these steps for each situation.

As a result, for each situation that was modified to specify the Hybrid Gateway destination, the Hub Tivoli Enterprise Monitoring Server forwards all events from any IBM Tivoli Monitoring agent to which the situation is distributed.

## Coexistence of v6 and v7 agents with v8 agents

- You can install Cloud APM agents (version 8) on the same computer where IBM Tivoli Monitoring agents (versions 6 or 7) are installed
- Both agent types cannot be installed in the same directory
- When agents coexist on the same computer, data from version 8 agents is available in the Performance Management console and data from versions 6 or 7 agents is available in the Tivoli Enterprise Portal
- Version 6 or 7 agents can coexist on the same computer as version 8 agents and monitor different resources
  - When they are integrated with the Hybrid Gateway, data from both agents is available in the Performance Management console



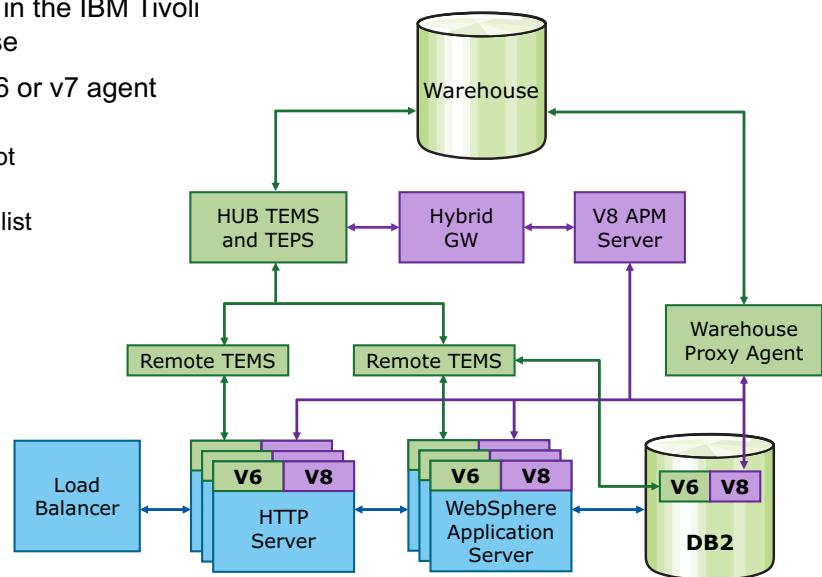
### Coexistence of v6 and v7 agents with v8 agents

The goal is to provide users with the ability to install both IBM Tivoli Monitoring and APM agents on the same system. Areas of conflict are resolved in the implementation, such as file system locations and registry settings. If coexisting agents are monitoring the same resources, the following scenarios are not supported:

- Both agents store data in the same IBM Tivoli Data Warehouse. For example, if both agents send data to the same Tivoli Data Warehouse, do not use the version 8 WebSphere MQ agent and version 6 or 7 WebSphere MQ agent to monitor the same queue manager on your system. This scenario also applies to multi-instance agents. For more information, see Tivoli Data Warehouse for historical reporting.
- Version 6 or 7 agents are integrated with the Hybrid Gateway to display data from both agents in the Performance Management console. For example, version 6 or 7 agents might be connected to the same Cloud APM server through the Hybrid Gateway. If so, do not use the version 8 IBM Integration Bus agent and the version 6 or 7 ITCAM Agent for WebSphere Message Broker to monitor the same broker on your system.
- A Tivoli Monitoring agent that is integrated with the Hybrid Gateway to display data in the Cloud APM console might be monitoring a resource, and you might want your Performance Management agent to monitor that resource. In that case, complete the following steps:
  - Remove the Tivoli Monitoring agent from any applications that include it.
  - Remove the Tivoli Monitoring agent from the Tivoli Monitoring managed system group that Cloud APM is configured to use.
  - Wait at least 24 hours, then install the Cloud APM agent, and add it to an application.

## Integrating APM V8 agents with IBM Tivoli Monitoring V6 Tivoli Data Warehouse

- Customers can store historical data in the IBM Tivoli Monitoring V6 Tivoli Data Warehouse
- Only agents with a corresponding v6 or v7 agent are supported
  - New metrics unique to APM V8 are not warehoused
  - See the documentation for a detailed list
- Data is sent from the Application Performance Management V8 agents to the warehouse proxy and then inserted into the Tivoli Data Warehouse
- Allows for enterprise-wide reporting

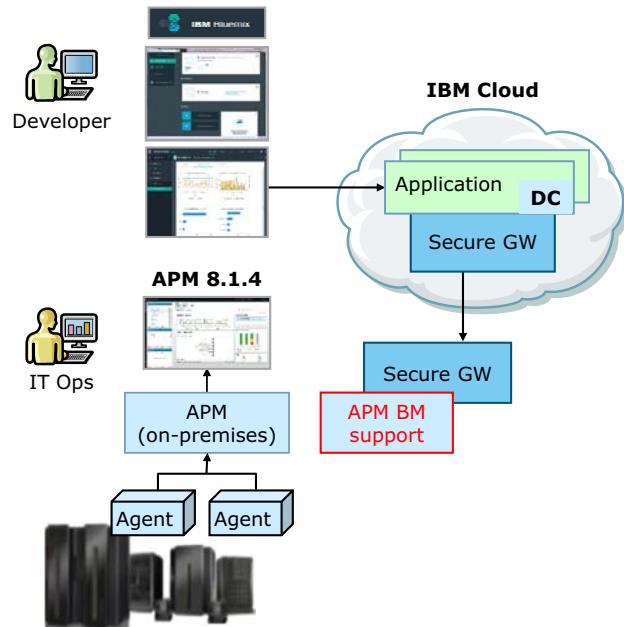


### Integrating APM v8 agents with IBM Tivoli Monitoring V6 Tivoli Data Warehouse

Sample history files for agents are available on your Cloud APM server. Use the sample file for your agent as the basis for creating the history configuration XML file on the Cloud APM server. The server propagates the configuration to all agents of this type. The history file specifies the warehouse proxy agent address, the data sets to collect samples from, the frequency of data collection, and how long to keep the data locally.

## Integrating IBM Cloud and APM on-premises

- Enable the monitoring of the IBM Cloud application to be fed into the private Cloud APM server
  - Data that is fed by using the IBM Secure Gateway
- Integrates Monitoring and deep-dive data
  - Availability Monitoring and Log Analysis are not integrated

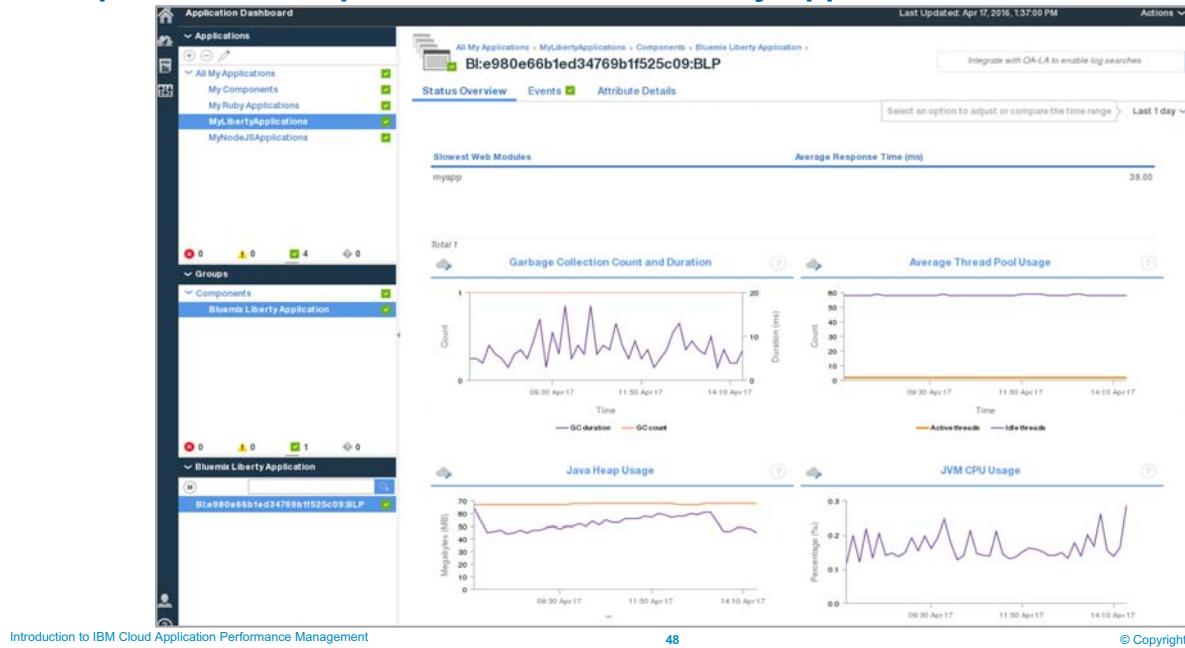


### Integrating IBM Cloud and APM on-premises

The Hybrid feature allows an IBM Cloud application to send its data to Cloud APM. It provides only resource and deep-dive data, not availability or log.

Data is passed from the IBM Cloud application to the private APM server by using the IBM Cloud Secure Gateway service, which provides an encrypted tunnel that allows data to reach through firewalls.

## On-premises example of an IBM Cloud Liberty Application



### On-premises example of an IBM Cloud Liberty Application

This slide shows the IBM Cloud data from a Liberty application that is shown in an on-premises Cloud APM console.

## Integrating with Netcool/OMNIbus

- Alerts, generated in Cloud APM, can be forwarded to the customer's on-premises OMNIbus, providing one method for doing event management
- Integration supports:
  - Forwarding alerts the customer's firewall from APM to the customer's on-premises OMNIbus
  - Coexists with firewalls, uses HTTPS that is initiated from the customer's environment
  - Queues alerts in case OMNIbus is temporally not available
  - Alerts follow the standard EIF format that is used in existing Tivoli Monitoring
- When you have event forwarding that is configured, you can customize:
  - Base EIF slot message
  - Custom EIF slots for events that are sent to a receiver such as Netcool/OMNIbus
- The Threshold Editor has a new Forward EIF Event field and EIF Slot Customization button for customizing how events are mapped to forwarded events

### Integrating with Netcool/OMNIbus

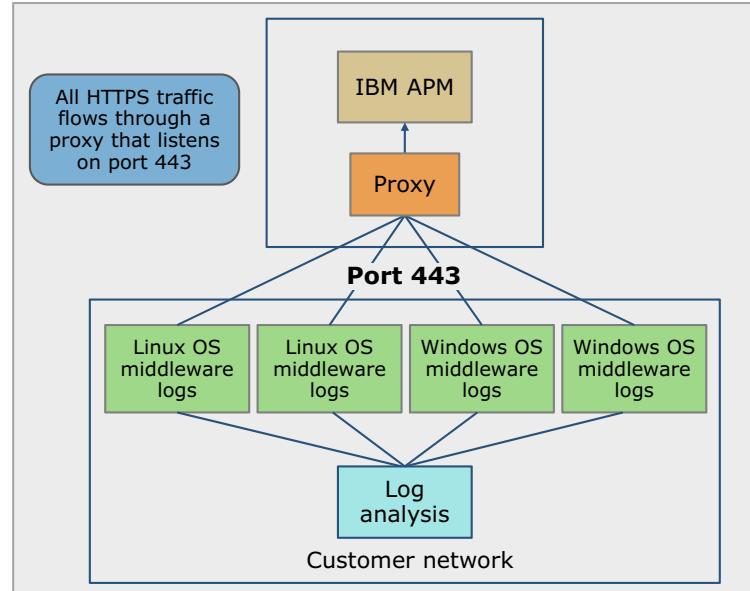
The Integration agent forwards alerts that were generated in Cloud APM to the customer's on-premises OMNIBUS. Customers use this feature to integrate their Cloud APM alerts with their on-premises alerts, providing one method for event management.

Cloud APM on Private can forward alerts directly to a customer's on-premises OMNIBUS.

## Integrating with IBM Operations Analytics Log Analysis

Integration features:

- APM Cloud search, enter error information from events into the search field
- Search starts an on-premises version of IBM Operations Analytics Log Analysis
- IBM Operations Analytics Log Analysis provides insight by analyzing error patterns in log files
  - It also provides expert advice for errors



### Integrating with IBM Operations Analytics Log Analysis

You can integrate Cloud APM with IBM Operations Analytics Log Analysis. With this integration, you search for error messages from various locations in the customer environment. IBM Operations Analytics Log Analysis supports expert advice, which improves the usability of the messages that are issued by indicating what actions to take to address the errors that are detected.

## Integrating with IBM Operations Analytics Predictive Insights

- IBM Operations Analytics Predictive Insights on Cloud
  - This new component extends the capabilities of Cloud APM by providing early detection of service and application issues to help avoid service disruptions and outages that affect your business
  - Predictive Insights automatically learn the normal operational behavior of complex infrastructures, such as a cloud, and is designed to identify problems before you know to look for them
- IBM Operations Analytics Predictive Insights
  - Provides real-time performance analysis for business services
  - Analyzes monitoring data to learn the normal behavior of a business service and create a performance model
  - Generates an alarm when behavior outside normal behavior is detected (anomaly)



### Integrating with IBM Operations Analytics Predictive Insights

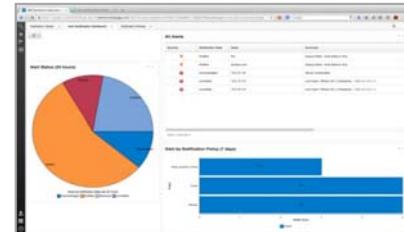
IBM Operations Analytics Predictive Insights on Cloud provides real-time performance analysis for business services. Earlier detection of service and application issues helps you avoid service disruptions and outages that affect your business.

The Predictive Insights product automatically learns the normal operational behavior of complex infrastructures, such as a cloud. The product is designed to identify problems before you know to look for the anomaly.

The Predictive Insights User Interface provides dynamic views of identified anomalies and all relevant metrics. The normalized view supports metric comparison and trend identification.

## Integrating with IBM Alert Notification

- The product IBM Alert Notification is a notification system
  - It meets increasing demands for agility and efficient collaboration among IT operations team members
- You can use IBM Alert Notification to provide email notification of alerts when application performance exceeds thresholds
- IBM Alert Notification is offered with Cloud APM
  - When subscribed for Cloud APM, IBM Alert Notification is made available automatically
- The situations from Cloud APM can be forwarded to IBM Alert Notification to send email notifications
  - The source for the alert data is from on-premises monitoring agents
- Another version of IBM Alert Notification is available as part of the Collaborative Operations offering, with the following results:
  - Integrating with IBM Operations Control Desk to open a ticket as a service request
  - Adding REST API for integrating with other event sources



### Integrating with IBM Alert Notification

IBM IT Alert Notification is a simple notification system. It meets the increasing demand for agility and efficient collaboration among IT operations team members that use multiple monitoring tools. It gives IT staff instant notification of alerts for any issues in your IT operations environment, optimizing your business performance, increasing customer satisfaction, and protecting revenue.

Because IBM IT Alert Notification is provided as a service, IBM installs and manages the required server infrastructure, reducing your time-to-value and offering low-maintenance ownership. IBM IT Alert Notification is offered with Cloud APM on Cloud. You can activate IBM IT Alert Notification with your IBM ID and password on IBM Marketplace:

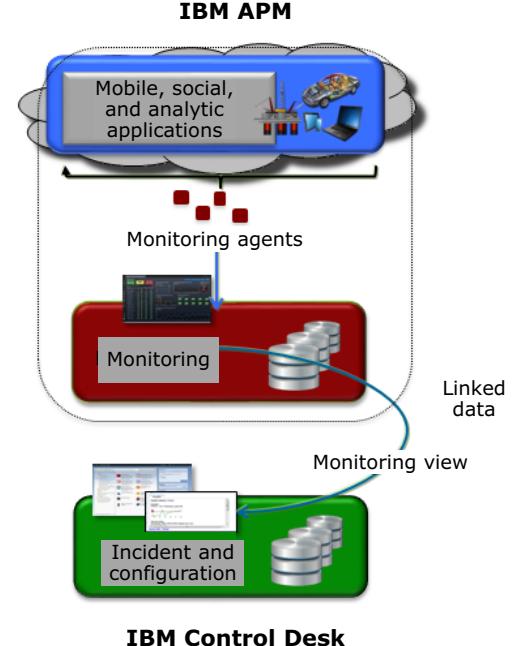
<https://www.ibm.com/marketplace/cloud/us/en-us>

IBM IT Alert Notification can be integrated with Cloud APM in a few clicks. The data from the on-premises monitoring agents is the source for the alert data. Cloud APM can also be integrated with an existing physical on-premises installation of Tivoli Netcool/OMNIbus.

When the Collaborative Operations product is available, an integration with IBM Control Desk becomes available. With this integration, a ticket can be opened as a service request.

## Integrating with IBM Control Desk (Cloud)

- When Cloud APM detects an issue with your application, it can automatically open a service request in IBM Control Desk
- Your specialists can fix problems in your applications before users have time to report them
- Your help desk spends more time on solving application issues and less time on answering support calls



### Integrating with IBM Control Desk (Cloud)

The integration of Cloud APM and IBM Control Desk provides business value by making your help desk more efficient. When Cloud APM detects an issue with your application, it can automatically open a service request in IBM Control Desk. With this automation, your specialists can fix problems in your applications before users have time to report them. Your help desk spends more time on solving application issues and less time on answering support calls.

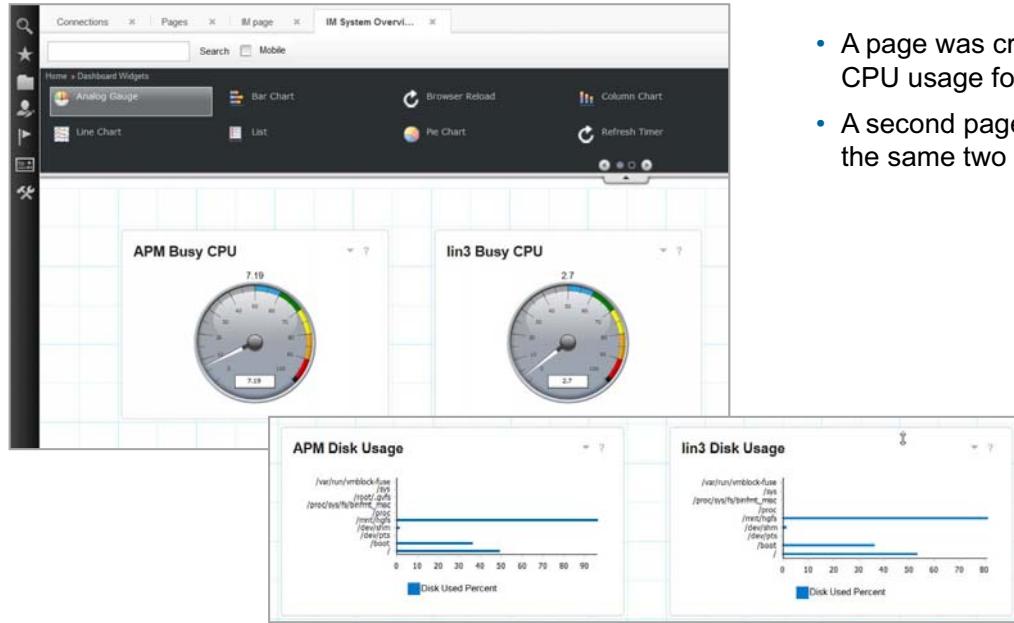
## Integrating with Dashboard Application Services Hub

- The Dashboard Application Services Hub integrates with Cloud APM
- IBM Dashboard Application Services Hub provides a single console for administering IBM products and related applications
- Dashboard Application Services Hub is the user interface for Jazz for Service Management
- You can integrate these products, for example:
  - Cloud APM with DASH to view monitoring agent data
  - Netcool/Impact with DASH to view the Netcool/Impact GUI
  - Netcool/OMNibus with DASH to view the OMNibus alerts
- The IBM Dashboard Application Services Hub provides a set of features to customize the console and build custom dashboards
- Pages are created that contain widgets, which you use to build charts, gauges, and tables that contain monitoring data

### *Integrating with Dashboard Application Services Hub*

The Dashboard Application Services Hub is used to create pages of customized Cloud APM agent data.

## Creating a custom dashboard page and widgets



Introduction to IBM Cloud Application Performance Management

55

© Copyright IBM Corporation 2018

### Creating a custom dashboard page and widgets

This slide shows parts of two dashboard pages that are created to show data from Cloud APM agents.

The gauge widgets are used with the KLZ\_CPU data set to show CPU usage on two servers.

The bar chart widgets use the KLZ\_Disk data set and show the disk usage by mount point for the same two servers.

# Lesson 6 The Cloud APM lab environment

IBM Training

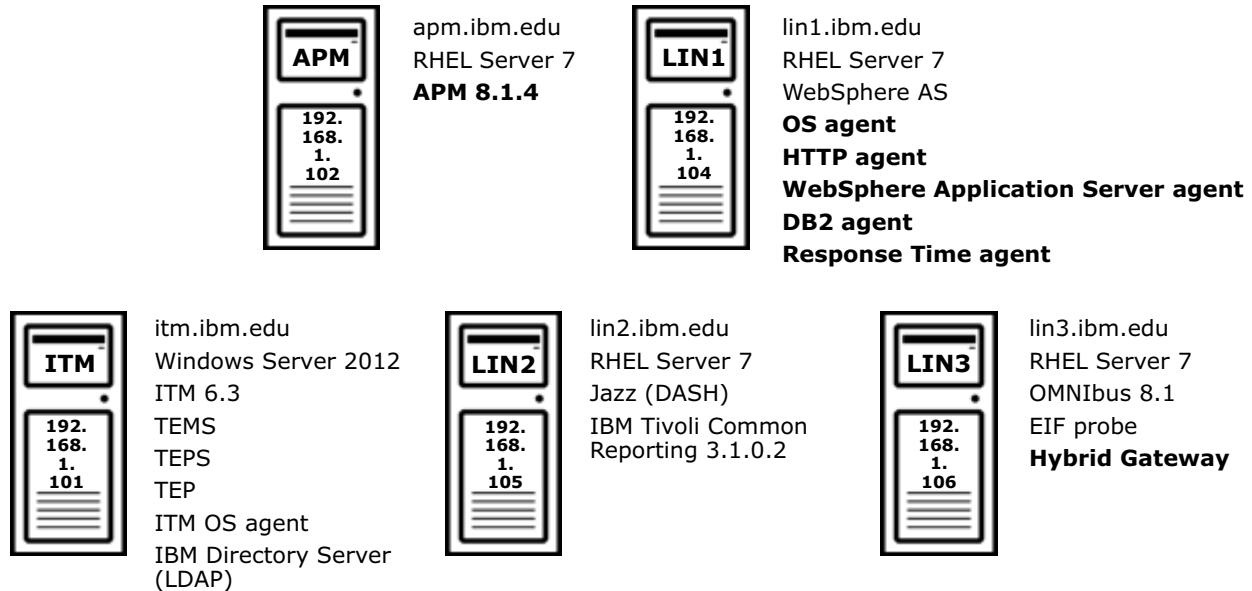


## Lesson 6: The Cloud APM lab environment

- A Linux server exists for installing the Cloud APM Private software
- These Cloud APM Private components are installed during the exercises:
  - Management Information Node
  - Operating system agents
  - HTTP, WebSphere Application Server, and DB2 agents
- Multiple applications are built on the Cloud APM server to manage agents and components
- Products are integrated with Cloud APM
  - The environment has preexisting IBM Tivoli Monitoring, Tivoli Common Reporting, and Netcool/OMNIbus

This slide shows what you work with and what you accomplish in the lab environment.

## The VMware lab environment



### The VMware lab environment

The bold items on the slide are installed during the lab exercises.

## Example of an application to monitor: DayTrader

### DayTrader

- DayTrader is benchmark application
- DayTrader is built around the paradigm of an online stock trading system
- With this application, users can log in, view their portfolio, look up stock quotes, and buy or sell stock shares
- In addition to the full workload, the application also contains a set of primitives that are used for functional and performance testing of various Java EE components and common design patterns

The screenshot shows the DayTrader application running in Mozilla Firefox. The browser title bar reads "Welcome to DayTrader - Mozilla Firefox". The address bar shows the URL "http://localhost/daytrader/scenario". The DayTrader interface has a red header bar with "DayTrader Home", "Account", "Portfolio", "Quotes/Trade", and "Logoff" buttons. The main content area displays "Welcome uid:10509." and "User Statistics" including account ID (10510), account created (Tue May 05 02:58:11 GMT 2015), total logins (5), and session created (Tue Aug 18 18:21:08 GMT 2015). It also shows "Market Summary" for 2015-08-18, listing the DayTrader Stock Index (TSIA) at 98.14 (-4.00%). Below this are sections for "Account Summary" and "Top Gainers" and "Top Losers" stocks.

| Symbol | Price  | Change |
|--------|--------|--------|
| s:100  | 62.19  | -26.81 |
| s:101  | 64.55  | -32.45 |
| s:102  | 97.45  | -17.55 |
| s:103  | 165.73 | 11.73  |
| s:104  | 199.14 | 48.14  |

| Symbol | Price  | Change |
|--------|--------|--------|
| s:150  | 154.03 | -42.97 |
| s:158  | 10.41  | 3.41   |
| s:197  | 94.66  | 17.68  |
| s:198  | 115.24 | -48.76 |
| s:199  | 114.67 | -26.33 |

Introduction to IBM Cloud Application Performance Management

58

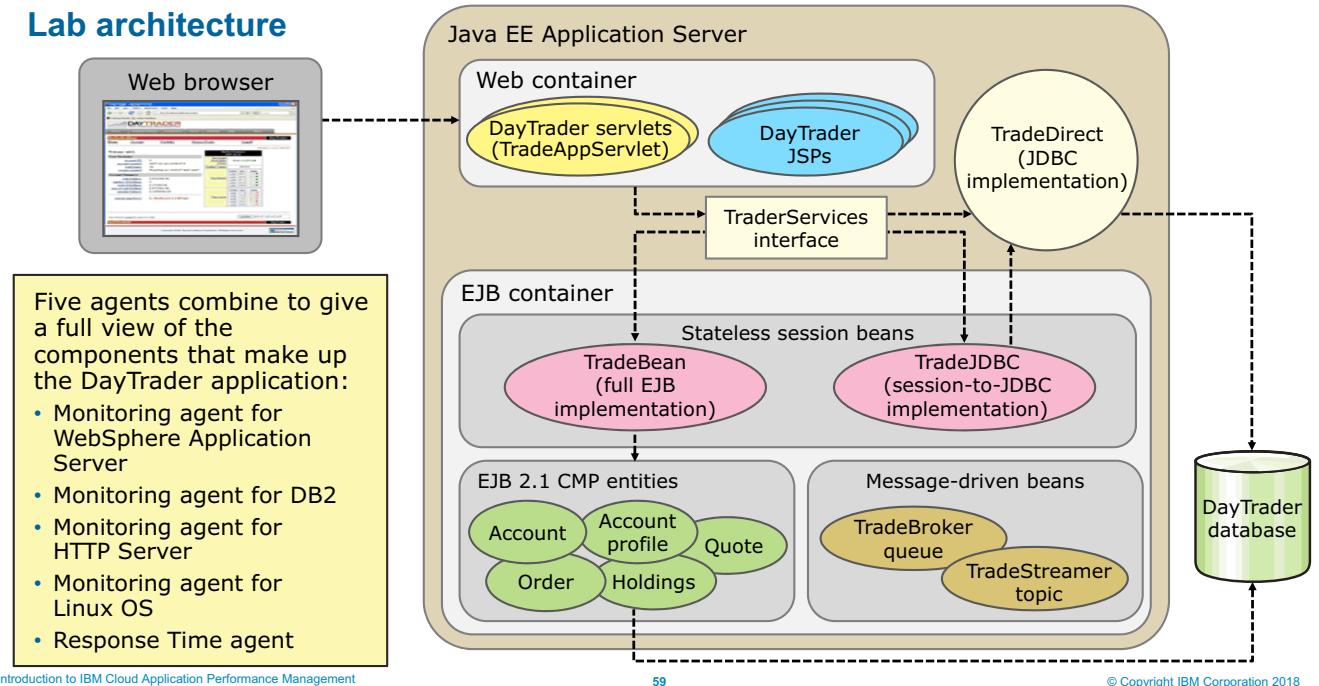
quotes s.0, s.1, s.2, s.3, s.4

© Copyright IBM Corporation 2018

### Example of an application to monitor: DayTrader

DayTrader is commonly used benchmark application that is built around the example of an online stock trading system. It is installed and configured, and you use it for the exercises for this class.

## Lab architecture



Introduction to IBM Cloud Application Performance Management

59

© Copyright IBM Corporation 2018

### Lab architecture

Multiple monitoring agents in this class monitor the DayTrader application. You install and configure the monitoring agents to provide insight into the availability and performance of the components of the application.

## Lab solution: Simple application with five monitoring agents



Introduction to IBM Cloud Application Performance Management

60

© Copyright IBM Corporation 2018

*Lab solution: Simple application with five monitoring agents*

On completion of the lab exercises, you see the data for all of the monitoring agents in a single dashboard.

## Instructor demonstration



## Student exercises



Complete the exercises for this unit in the Course Exercises Guide.

## Summary

Now that you have completed this unit, you should be able to:

- Describe IBM Cloud APM and its architecture
- List some monitoring agents and categories of monitoring agents
- Describe application-based monitoring
- Describe some examples of monitoring agent output
- Explain integration with other products
- Describe the classroom lab environment



# **Unit 2 Cloud APM server installation**

IBM Training



## **Cloud APM server installation**

© Copyright IBM Corporation 2018  
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

This unit covers installation of the Cloud APM server. You learn about packaging, prerequisites, and the step-by-step instructions on how to install the Cloud APM server.

## Learning objectives

After completing this unit, you should be able to:

- Describe the installation process for Cloud APM
- Explain the prerequisites and the prerequisite checker
- Install and configure the Cloud APM server

## Unit outline

- Lesson 1: Overview of installation
- Lesson 2: Prerequisites and the prerequisite checker
- Lesson 3: Installing the Cloud APM server

# Lesson 1 Overview of installation

IBM Training



## Lesson 1: Overview of installation

Installation and configuration impacts: on Cloud versus on-premises

For IBM Cloud Application Performance Management on Cloud:

- Because IBM hosts the Cloud APM server in IBM Marketplace, you do not install or configure it
- You download Cloud APM agents from packages on IBM Marketplace, and they are preconfigured to connect to your unique Cloud APM server

For IBM Cloud Application Performance Management Private:

- You install the Cloud APM server on your local hardware
- You create the preconfigured agent packages, and they are stored on your Cloud APM server depot

For IBM Cloud Application Performance Management (both Cloud and Private):

- You install the agents on the targets
- The only difference from the agent installation and configuration is where you obtain the software:
  - For on Cloud, download the agent software from the IBM Marketplace instance
  - For on-premises, download the agent software from the Cloud APM server

### Overview of installation

In this lesson, you learn to describe the similarities and the differences of the installation process on-premises and in a SaaS environment.

## Installable content

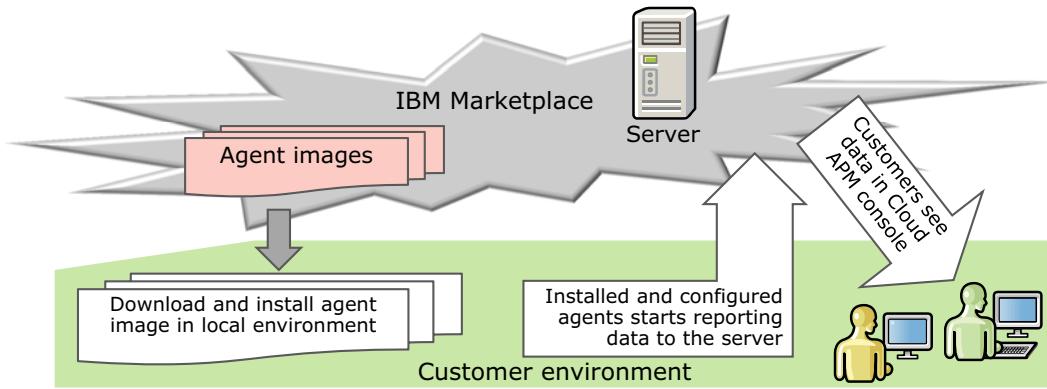
- For IBM Cloud Application Performance Management, user can choose offerings:
  - IBM Cloud Application Performance Management, Base
  - IBM Cloud Application Performance Management, Advanced
- Add-ons:
  - Base Extension Pack
  - Advanced Extension Pack
  - Infrastructure Extension Pack
  - z Systems Extension Pack (CO)
  - Availability Monitoring (CO)
  - Operations Analytics – Predictive Insights

### *Installable content*

With IBM Cloud Application Performance Management, the customer purchases one of these offerings and add-ons. The customer can then download the needed installation software and integration components. This slide lists the various software components that the customer can download.

## On-Cloud implementation process

- User requests new Performance Management service
- Monitoring server is installed and runs in Cloud on IBM Marketplace (IBM site)
- Users download the agents that are preconfigured to connect a Cloud APM server that runs on IBM Marketplace
- Users install agents in their environment (customer site: Cloud or on-premises)

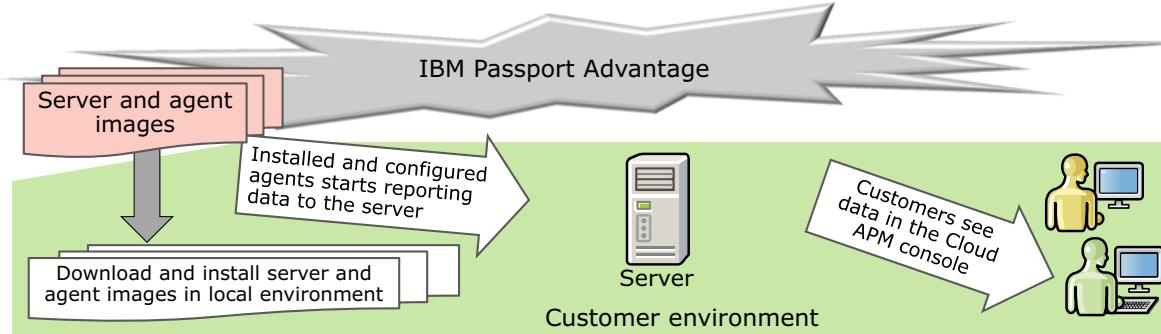


### On-Cloud implementation process

This slide shows the deployment process for IBM Cloud Application Performance Management on Cloud. The customer requests a new Performance Management service from IBM Marketplace. The Performance Management is deployed and runs in the Cloud on the IBM Marketplace servers. The customer downloads the agents, which are preconfigured to connect to a Cloud APM server that runs on IBM Marketplace. Customers install the agents in their environments, which can be on a server, in the Cloud, or on-premises.

## On-premises implementation process

1. User downloads and installs monitoring server in local environment (customer site)
2. User downloads and preconfigures agent images to connect to locally installed server
  - Agent image preconfiguration process can be done at these times:
    - During server installation
    - As a separate step after the server installation
3. User installs agents in local environment (customer site)



### On-premises implementation process

This slide shows the deployment process for Cloud APM on-premises. Customers purchase Cloud APM and can then download the software from IBM Passport Advantage. Customers download and install Cloud APM server in their local environments. They also download and preconfigure agent images to connect to locally installed servers. This preconfiguration process can be done either during the server installation or as a separate step after the server installation. Customers can then install agents in their local environments.

# Lesson 2 Prerequisites and the prerequisite checker

IBM Training



## Lesson 2: Prerequisites and the prerequisite checker

Prerequisite checking is the first step of the installation flow

- If the prerequisite checker fails, installation stops
- Prerequisite checking is skipped when `SKIP_PRECHECK=1` is set in environment
  - Use: `export SKIP_PRECHECK=1`
- Use caution when skipping the prerequisite checker
  - The prerequisites are there for a reason
- When all of the user input is collected, the installer runs IBM Prerequisite Scanner (PRS) to ensure that the server meets the requirements

PRS can return one of three values:

- PASS: The server meets all of the prerequisites
- WARNING: The user must decide whether the installation should be continued on the server
- ERROR: At least one of the prerequisites is not met
  - The installation stops

In this lesson, you learn how to research the prerequisites for a successful installation.

The server installer first checks for prerequisites. If the prerequisite checker fails, the installation stops. You can skip the prerequisites checker by setting the `SKIP_PRECHECK` variable to 1. When the prerequisites checker finishes, it displays a list of found and expected prerequisites properties.

## Server requirements

- The Cloud APM server requires a Red Hat Enterprise Linux Server Version 6 or 7 operating system

| Processor, memory, and disk requirements based on a single system configuration |                      |              |                |
|---|----------------------|--------------|----------------|
| Hardware component  | Minimum requirements |              |                |
|   | Small configuration  | Medium       | Large          |
| Free memory   | 24 GB                | 32 GB        | 40 GB          |
| Number of processors  | 6                    | 8            | 16             |
| Available disk space  | 30 GB                | 30 – 1000 GB | 1000 – 3000 GB |
| Number of agents  | Fewer than 100       | 100 – 2000   | 2000 – 10000   |

### Server requirements

This slide lists the platform prerequisites for the Cloud APM server, including supported operating system, RAM, processors, and disk space. If the minimum requirements for a small configuration are not met, notice that the prerequisite checker fails.

## Server prerequisites: Ports

- The Cloud APM server requires several ports to be available for the prerequisite checker to allow an installation:

| Port  | Description   |
|-------|---|
| 80    | HTTP port for the Agent Subscription Facility (ASF) and Central Configuration Server  |
| 443   | HTTPS port for the Agent Subscription Facility (ASF) and Central Configuration Server |
| 8080  | HTTP port for the Performance Management console user interface                       |
| 9443  | HTTPS port for the Performance Management console user interface                      |
| 13245 | Port 1 for role-based access control  |
| 13246 | Port 2 for role-based access control  |
| 13247 | Port 3 for role-based access control  |
| 13248 | Port 4 for role-based access control  |
| 50000 | Port for DB2  |

### Server prerequisites: Ports

Ports that are used by the Cloud APM server are listed on this slide.

## Ports that are used for internal communications between server components (1 of 2)

- The Cloud APM server requires several ports to be open for internal communications:

| Port  | Description   |
|-------|---|
| 1527  | Port for Service Component Registry database: The port is labeled <code>SCRDERBYDB</code> in the prerequisite scanner output                          |
| 2181  | Port for Zookeeper process of Kafka Message Broker: The port is labeled <code>ZOOKEEPER</code> in the prerequisite scanner output                     |
| 6066  | Port for Spark applications: The port is labeled <code>SPARKAAPPS2</code> in the prerequisite scanner output  |
| 6414  | Port for Gaian database: The port is labeled <code>FNGAIANDB</code> in the prerequisite scanner output  |
| 7077  | The port is labeled <code>SPARKAAPPS1</code> in the prerequisite scanner output   |
| 18080 | The port is labeled <code>SPARKMASTER</code> in the prerequisite scanner output   |
| 18085 | The port is labeled <code>SPARKWORKER</code> in the prerequisite scanner output   |
| 8090  | Port for Performance Management consoles back-end connection: The port is labeled <code>SERVER1HTTP</code> in the prerequisite scanner output         |
| 8091  | Port for secure Performance Management consoles back-end connection: The port is labeled <code>SERVER1HTTPS</code> in the prerequisite scanner output |

### *Ports that are used for internal communications between server components (1 of 2)*

This slide lists the ports that the Cloud APM server firewall must open to be available for remote connections.

## Ports that are used for internal communications between server components (2 of 2)

- The Cloud APM server requires several ports to be open for internal communications:

| Port  | Description   |
|-------|---|
| 8099  | The port is labeled <code>OIDCHTTPS</code> in the prerequisite scanner output   |
| 9092  | Port for Kafka Message Broker: The port is labeled <code>KAFKA1</code> in the prerequisite scanner output                                       |
| 9989  | Port for Kafka Message Broker: The port is labeled <code>KAFKA2</code> in the prerequisite scanner output                                       |
| 9998  | Port for EIF receiver: The port is labeled <code>FNEIFRCVR</code> in the prerequisite scanner output  |
| 10001 | Port for Open Services for Lifecycle Collaboration service provider: The port is labeled <code>OSLCPM</code> in the prerequisite scanner output |
| 12315 | Port for Service Component Registry Java back end: The port is labeled <code>SCRJAVABKEND</code> in the prerequisite scanner output             |
| 27000 | Port for MongoDB document store database: The port is labeled <code>MONGODB</code> in the prerequisite scanner output                           |
| 32105 | Port for internal messaging: The port is labeled <code>FNINTMSG</code> in the prerequisite scanner output                                       |

### *Ports that are used for internal communications between server components (2 of 2)*

This slide lists the ports that the Cloud APM server firewall must open to be available for internal connections.

## Software requirements for the Cloud APM server

Software: Red Hat Enterprise Linux Server 6

- Update 2 or later
- Hardware: x86-64
- Bit value: 64-Exploit

Dependencies:

- Checked by the prerequisite scanner
- Notable dependencies include:
  - Maximum number of user processes  
`os.ulimit=[type:maxprocesseslimit]4096+`
  - Maximum number of open files  
`os.ulimit=[type:filedescriptorlimit]32768+`

Library dependencies:

- `os.lib.libc_64=regex{libc\.so.*}`
- `os.lib.libgcc_64=regex{libgcc.*\.so.*}`
- `os.lib.libstdc++_64=regex{libstdc++\.so\.5}`
- `os.lib.libstdc++_64=regex{libstdc++\.so\.6}`
- `os.lib.libstdc++_32=regex{libstdc++\.so\.6}`
- `os.lib.pam_64=regex{libpam\.so.*}`
- `os.lib.pam_32=regex{libpam\.so.*}`
- `os.package.sg3_utils=sg3_utils`
- `bash`
- `ksh`

## Consistent time settings

To ensure a consistent time setting, use NTP (Network Time Protocol):

- NTP still requires setting a consistent and appropriate time zone
- NTP is supported on all platforms where Cloud APM runs
- Enabling NTP varies by operating system

For Red Hat Enterprise Linux 6:

- Examine `/etc/ntp.conf` to be sure that it contains a list of public NTP servers

```
# Use public servers from the pool.ntp.org project.  
# Please consider joining the pool (http://www.pool.ntp.org/join.html).  
server 0.rhel.pool.ntp.org iburst  
server 1.rhel.pool.ntp.org iburst ←  
server 2.rhel.pool.ntp.org iburst  
server 3.rhel.pool.ntp.org iburst
```

- Make sure `/etc/ntp.conf` has proper file permissions
- Restart (or start) the NTP daemon:
  - `service ntpd restart`
- Make sure that the NTP daemon starts at boot time:
  - `chkconfig ntpd on`

### Consistent time settings

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

## Browser support

| Browser                         | Version   |
|---------------------------------|---|
| Apple Safari (desktop only)     | 8.0 and future fix packs<br>10.1 and future fix packs |
| Apple Safari on iOS (iPad only) | 9.x and future fix packs                              |
| Google Chrome                   | 59 and future fix packs<br>60 and future fix packs    |
| Microsoft Internet Explorer     | 11.0 and future fix packs                             |
| Mozilla Firefox ESR             | 52 and future fix packs                               |

## DB2 installation on a remote server

- DB2 can be installed on a local machine by the Cloud APM server installer
- You can alternatively connect to a DB2 server on a remote machine
- You must create the DB2 database on the remote machine before you start the installation of the Cloud APM server
  - DB2 Version 10.5 fix pack 6 must be installed and licensed
  - DB2 user `db2apm` must be created and in the `db2iadm1` group
  - DB2 user `itmuser` must be created and in the `dasadm1` group
- Scripts and configuration details are in the documentation
- At installation time, you are prompted for the DB2 connection details to the remote DB2 database

### *DB2 installation on a remote server*

You might want to connect to a remote DB2 server to adhere to your organization's database server administration policies. Connecting to a remote DB2 server also reduces the load on the Cloud APM server, which improves performance. Consider a remote DB2 setup when the necessary disk I/O performance cannot be achieved on the hardware that is allocated for your Cloud APM server.

## MongoDB installation on a remote server

- MongoDB is always installed on a local machine without prompting the user
- MongoDB is configured and started for each type of offering
- Users can decide to disable the local installation of MongoDB, install MongoDB on a remote server, and configure the monitoring server to use the remote installation

### *MongoDB installation on a remote server*

MongoDB is a NoSQL open source database that is installed with the Cloud APM server. The MongoDB stores data for the transaction tracking feature that is available with the IBM Cloud Application Performance Management offering, and threshold event data. You can install and configure the MongoDB on a remote system from the server. In large-scale environments, an external MongoDB can be used to reduce load at the server.

## Server installation application

| Default user ID                        | Purpose  | Default password         | Directory and script that can be used to change the default password after the installation |
|--|--|--------------------------|---|
| <b>gaiandb</b>                         | Is used to access the Performance Management embedded Derby configuration database | <b>g1an08pW0rd</b>       | None  |
| <b>apmadmin</b>                        | Is used to log in to the Performance Management console                            | <b>apmpass</b>           | <b>/opt/ibm/ccm/apmpasswd.sh</b>  |
| <b>smadmin</b>                         | Is used to authenticate with server1 Liberty process                               | <b>apmpass</b>           | <b>/opt/ibm/ccm/tools/smapasswd.sh</b>  |
| <b>itmuser</b>                         | Is used to access the Prefetch data store and SCR database                         | <b>db2Usrpasswd@08</b>   | <b>/opt/ibm/ccm/db2_users_passwd.sh</b>   |
| <b>db2apm<br/>db2fenc1<br/>dasusr1</b> | DB2 instance users   | <b>db2Usrpasswd@08</b>   | <b>/opt/ibm/ccm/db2_users_passwd.sh</b>   |
| <b>admin user</b>                      | Is used to access the MongoDB, which stores Transaction Tracking data              | <b>mongoUsrpasswd@08</b> | <b>/opt/ibm/ccm/tools/mongopasswd.sh</b>  |

### Server installation application

This slide describes the users that are set up by default and their respective passwords.

# Lesson 3 Installing the Cloud APM server

IBM Training



## Lesson 3: Installing the Cloud APM server

- Download server image
- Unpack on local system and run the installation program:  
`install.sh`
  - Server is installed to any directory (default):  
`/opt/ibm`  
Note: Installation path is customizable
  - In 8.1.4 release, CLI installation is supported only
  - Use `root` to install

```
root@apm:/downloads/APM814/server
File Edit View Search Terminal Help
[root@apm ~]# cd /downloads/APM814/
[root@apm APM814]# ls
agents reports server
[root@apm APM814]# cd server
[root@apm server]# ls
apm_advanced_8.1.4.0.tar
[root@apm server]# tar -xvf apm_advanced_8.1.4.0.tar
```

In this lesson, you learn how to install the Cloud APM server.

This slide discusses how to start the Cloud APM server installer, some of the requirements to run the installer, and some of the results. The installer is in the `apm_advanced_8.1.4.0.tar` file. Copy and extract it onto the target system and run the `install.sh` command. In the 8.1.4 release, only the CLI installer is supported, and you must be `root` to do the installation. The server installs into the `/opt/ibm` directory by default, but you can change this directory.

The installer creates the four users that are shown in the slide with the default password previously shown, but you can change it by setting the passwords in the `install.properties` file before running the installer. The installer does not support the use of an existing DB2 installation, and if DB2 users exist, the user must provide valid passwords in the `install.properties` file.

## Server installation flow

- Collecting user input
  - Upgrading or new installation
  - Change installation directory
  - License agreement
  - Set APM administrator password
  - Preconfigure agent packages (optional)
  - Install database or use existing DB2
- Running prerequisite scanner (optional)
- Installation process runs
  - Installing DB2
  - Installing Server components
  - Installing Support
  - Creating the Metric Cache database (Prefetch database)
  - Creating the Topology database (SCR database)
- Installation process runs
  - Finalizing database creation
  - Configuring Summarization and Pruning agent
  - Configuring Messaging Broker (configuring Kafka)
  - Starting server components of Cloud APM
  - Configuring server components of Cloud APM
  - Configuring agent installation images (optional)
  - Install summary

### Server installation flow

This slide shows the basic actions of the server installer that is divided into three phases: user input, prereq scanner, and installation process. The following slides cover each of these phases in more detail.

## User input: Server installation directory, license agreement, and password

- Users must:
  - Indicate whether they are doing an upgrade or not
  - Select an installation directory
  - Accept the license agreement

```
packages/AgentFrameworks/zlinux/misc/.apm_config/keyfiles/keyfile.rdb
packages/AgentFrameworks/zlinux/misc/.apm_config/keyfiles/keyfile.sth
packages/AgentFrameworks/zlinux/misc/.apm_config/omnibus.environment
offerings/ipm_apm_advanced 8.1.4.0.offering
[root@apm server]# ./install.sh

Do you want to upgrade from an existing installation of the IBM Cloud Application Performance Management server [ 1-yes or 2-no; "no" is default ]?

This script will install IBM Cloud Application Performance Management, Advanced Private (8.1.4.0).

Do you want to continue [ 1-yes or 2-no; "yes" is default ]?1

Do you want to change the default installation directory ( /opt/ibm ) [ 1-yes or 2-no; "no" is default ]?

Do you accept the license agreement(s) found in the /downloads/APM814/server/licenses/ipm_apm_advanced directory [ 1-accept or 2-decline ]?1
```

### User input: Server installation directory, license agreement, and password

This slide shows the first required customer input: determining where to install the software, accepting the license agreement, and optionally setting the password for the administrator user ID (**apmadmin**). The default password is **apmpass**.

## User input: Configuring the agent images (1 of 2)

- The user must:
  - Accept the default password or provide a new one
- The user can preconfigure the agent images:
  - Provide the location of the source packages
  - Provide the location of where the preconfigured package is to be placed (`/opt/ibm/ccm/depot`)

```
License agreement was accepted, installation will proceed...

Do you want to change the default password for the administrator account [ 1-yes or 2-no; "no" is default ]?1
Enter the password:
Confirm the password:
The password was accepted and will be used for the administrator account.

Agent installation images must be configured to connect to this server. If you have downloaded the agent images to the same system as the server, you can configure the agent images now.

Do you want to configure the compressed (*.zip or *.tar) agent installation files now [ 1-yes or 2-no; "yes" is default ]?1
Enter the path to the directory where you downloaded the agent, Hybrid Gateway, and/or data collector installation images (e.g. /opt/agents):/downloads/APM814/agents/
Enter the path to the directory where configured agent installation images can be stored or accept the default [/opt/ibm/ccm/depot]:
```

### User input: Configuring the agent images (1 of 2)

Users also have an opportunity to preconfigure the agent packages. If a user chooses to preconfigure the agent package, that user must provide the location of the packages (the packages must all be in one directory). The agents should use that host name or IP address to communicate with the Cloud APM server.

## User input: Configuring the agent images (2 of 2)

- The user must:
  - Provide the address of the Cloud APM server
  - Confirm that the installation is to continue

Enter the IP address/hostname that will be used by agents to communicate with the server.

Enter the IP address/hostname or accept the default [192.168.1.102]:

Enter the hostname and IP address of the server that will be used in a web browser to log in to the IBM Cloud Application Performance Management console. Accept the default values or provide your own.

Default values:

Fully qualified domain name: `apm.ibm.edu`  
Short hostname: `apm`  
IP address: `192.168.1.102`

Do you want to use these values [ 1-yes or 2-no; "yes" is default ]?

- Indicate whether you are installing a new DB2 or connecting to an existing one

Do you want to install the DB2 database or connect to an existing DB2? [ 1-install database or 2-connect to existing database; "1-install database" is default ]? 1

Running Prerequisite Scanner. This may take a few minutes depending on the number of checked components and machine's performance.

Setting Prerequisite Scanner output directory to user defined directory: /opt/ibm/ccm/logs/apm-prs\_20171002\_152411

### User input: Configuring the agent images (2 of 2)

Users also have an opportunity to preconfigure the agent packages. If a user chooses to preconfigure the agent package, that user must provide the location of the packages (the packages must all be in one directory). The agents should use that host name or IP address to communicate with the Cloud APM server.

## Server installation prerequisite checker

- When all of the user input is collected, the installer runs the IBM Prerequisite Scanner (PRS) to ensure that the machine meets the server requirements
  - If the prerequisite checker fails, installation stops
  - Prerequisite checking is skipped when SKIP\_PRECHECK=1 is set in the environment
  - Use: export SKIP\_PRECHECK=1
- The PRS can return:
  - PASS: The machine meets all of the prerequisites
  - WARNING: The user must decide whether the installation should be continued on the machine
  - ERROR: At least one of the prerequisites is not met and the installation is stopped
- Note:
  - New in 8.1.4 is a warning about LDAP
  - This warning can be ignored

```
root@apm:/downloads/APM814/server
File Edit View Search Terminal Help
Machine Information
Machine name: apm.ibm.edu
Serial number: VMware-56 4d 1b 05 97 50 70 99-9e b3 3b df 49 46 54 eb

Scenario: Prerequisite Scan
PRS execution is in progress, it may take some time ...
IPDB2 - IBM Cloud Application Performance Management and IBM DB2 Server [version 08010300]:
Property          Result    Found      Expected
=====
os.isLDAPConfigured    WARN     True       False

Overall result: WARNING
Detailed results are also available in /opt/ibm/ccm/logs/apm-prs_20171012_085724/result.txt
The prerequisite check returned warnings. Installation can be continued, however is recommended
to meet all above requirements.
Continue with this installation [ 1-yes or 2-no; "no" is default ]?1
```

### Server installation prerequisite checker

The server installer checks for prerequisites before proceeding with the installation. If the prerequisite checker fails the installation stops, you can skip the prerequisites checker by setting the `SKIP_PRECHECK` variable to 1. When the prerequisites checker finishes, it displays a list of found and expected prerequisites properties.

## Server installation process

- The installation should take 45 – 90 minutes, depending on the hardware
- The installer indicates whether the installation was successful, where the installation images are for the agents, and the installed server size based on the CPUs, memory, and free disk space

```
root@apm:/downloads/APM814/server
File Edit View Search Terminal Help
No further user input is required. The installation and configuration of components is now starting and may take up to one hour to complete. The installation log is available at "/opt/ibm/ccm/logs/apm-server-install_20171002_152411.log".
Installing DB2. Please wait...
Installing the IBM Cloud Application Performance Management server. Please wait...
DB05105 Verification of /var/lib/rpm/Packages succeeded.
Starting components of the IBM Cloud Application Performance Management server...
.....
Configuring components of the IBM Cloud Application Performance Management server...

All components are configured successfully.
Configuring agent installation images...
Pre-configured agent installation images are available in the following directory: /opt/ibm/ccm/depot.
The configuration of agent installation images can also be done manually.
To do this manual configuration, first create configuration packages by using the following script: /opt/ibm/ccm/make_configuration_packages.sh. Then, use the output packages from the first script and run the following one: /opt/ibm/ccm/configure_agent_images.sh.
Finalizing the installation...
The server size has been configured as 'small' based on the number of CPUs and amount of memory .
To reconfigure the server size, run script /opt/ibm/ccm/server_size.sh with the desired size as a parameter. Valid sizes are: small, medium, large.
Please review the documentation at http://ibm.biz/mon_doc for more information.
To begin using the product, copy the configured agent images to the systems running the applications you want to monitor and install the agents. Log in to the IBM Cloud Application Performance Management console using https://apm.ibm.edu:9443 and review the topics on the "Getting Started" page.
[root@apm server]#
```

Cloud APM server installation

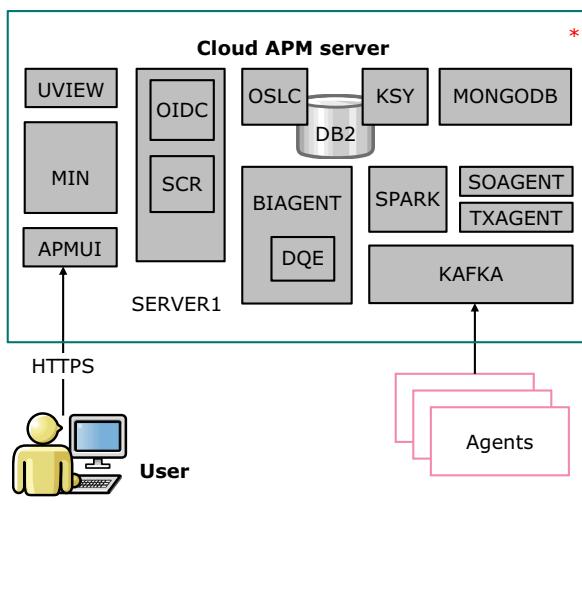
25

© Copyright IBM Corporation 2018

### Server installation process

This slide shows the final steps of the installation process.

## Main components



- **APMUI:** Performance Management console features \*
- **BIAGENT:** Bluemix integration agent (BMI)
- **DB2:** Prefetch database
- **DQE:** Service for Bluemix integration (BMI)
- **KAFKA:** KAFKA message broker
- **KSY:** Summarization and pruning
- **MIN:** Monitoring Infrastructure Node component that maintains the list of connected agents, advanced configuration data, and threshold events
- **MONGODB:** Database that stores threshold events and transaction tracking for APM offering
- **OIDC:** OpenID Connect (OIDC) is a simple identity protocol over OAuth 2.0
- **OSLC:** Open Services for Lifecycle Collaboration service provider for establishing application relationships
- **SCR:** Service Component Repository for resource, attribute, and relationship information
- **SERVER1:** Server1 application server, which runs the dashboard data provider and some Service Component Repository components
- **SOAGENT:** Agent that aggregates transaction data from multiple playback agents and generates events according to threshold definitions
- **SPARK:** Spark infrastructure and applications such as the AAR Aggregator and Instance Analyzer
- **TXAGENT:** Transactions Event agent, which sets the thresholds that are used to classify middleware transactions
- **UVIEW:** Universal View service for defining dashboard pages in the Custom Views tab of the Application Performance Dashboard

### Main components

This slide lists and describes each of the main services of the Cloud APM server. Users access the Cloud APM console through the APMUI service.

This slide is accurate for APM 8.1.4, which does not manage these components in a Cloud environment.

## Managing JVM heap size

- To change the server size, run the `server_size.sh` command followed by the specified size
  - For example: `server_size.sh small`
  - Note: this command restarts all of the Liberty servers
- The JVM heap size is adjusted according to the values in the following table:

| Component                        | Large   | Medium  | Small   |
|----------------------------------|---------|---------|---------|
| Server1 application server       | 3072 MB | 2048 MB | 1536 MB |
| APMUI service                    | 4096 MB | 3072 MB | 1536 MB |
| Uviews (Liberty server instance) | 1024 MB | 1024 MB | 1024 MB |
| MIN (Liberty server instance)    | 2048 MB | 1536 MB | 512 MB  |
| OIDC                             | 256 MB  | 128 MB  | 128 MB  |
| Kafka                            | 512 MB  | 512 MB  | 256 MB  |
| Zookeeper                        | 256 MB  | 256 MB  | 256 MB  |
| MongoDB Cache                    | 4096 MB | 2048 MB | 1024 MB |

## Managing DB2 buffer pool

- To change the DB2 buffer pool, run the `server_size.sh` command followed by the specified size
  - For example: `server_size.sh small`
  - Note: this command restarts all of the Liberty servers
- The buffer pool is adjusted according to these values:

| Database | Buffer pool  | Medium | Small  | Extra small |
|----------|--------------|--------|--------|-------------|
| DATAMART | IBMDFAULTBP  | 300000 | 200000 | 100000      |
| WAREHOUS | IBMDFAULTBP  | 200000 | 100000 | 50000       |
| SCR32    | TBSMSCR16KBP | 100000 | 50000  | 30000       |
| SCR32    | TBSMCFG16KBP | 10000  | 5000   | 1000        |

## Uninstalling the Cloud APM server

- On the system where the Cloud APM server is installed, open the command line
- Run the following command in the `/opt/ibm/ccm` directory (or `/custom_path/ccm` if you installed the server in a different path):
  - `uninstall.sh`
  - The uninstaller checks for the Performance Management offerings that are installed and a message prompts you to select which offering or offerings to uninstall
- Review the list of installed Performance Management offerings and enter the number of the offering (or offerings) to uninstall or enter `q` (quit) to cancel the uninstallation

### *Uninstalling the Cloud APM server*

If you no longer want the Cloud APM server on your system, you can uninstall it. The procedure does not remove the monitoring agents other than the Summarization and Pruning agent that was installed with the server. If multiple IBM Cloud APM offerings are installed, you can select to uninstall a subset if you do not want to uninstall all offerings.

## Instructor demonstration



## Student exercises



Complete the exercises for this unit in the Course Exercises Guide.

## Summary

Now that you have completed this unit, you should be able to:

- Describe the installation process for Cloud APM
- Explain the prerequisites and the prerequisite checker
- Install and configure the Cloud APM server

# **Unit 3 Installing, configuring, and managing Cloud APM agents**

IBM Training



## **Installing, configuring, and managing Cloud APM agents**

© Copyright IBM Corporation 2018  
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

This unit covers installation of the Cloud APM monitoring agents on both the Windows and Linux environments. You also learn how to install and preconfigure monitoring agents, how to stop and start an agent, and how to access data from an agent. You also learn how to configure and use the log file agent capabilities of the monitoring agent for Linux OS.

## Learning objectives

After completing this unit, you should be able to:

- Install and preconfigure the various types of Cloud APM agents
- Start and stop the Cloud APM agents
- Access data from a Cloud APM agent
- Configure and use the log file agent

## Unit outline

- Lesson 1: Installing Cloud APM agents
- Lesson 2: Starting and stopping Cloud APM agents
- Lesson 3: Accessing data from a Cloud APM agent
- Lesson 4: Configuring and using the log file agent

### *Unit outline*

This slide shows the lessons for this unit.

# Lesson 1 Installing Cloud APM agents

IBM Training

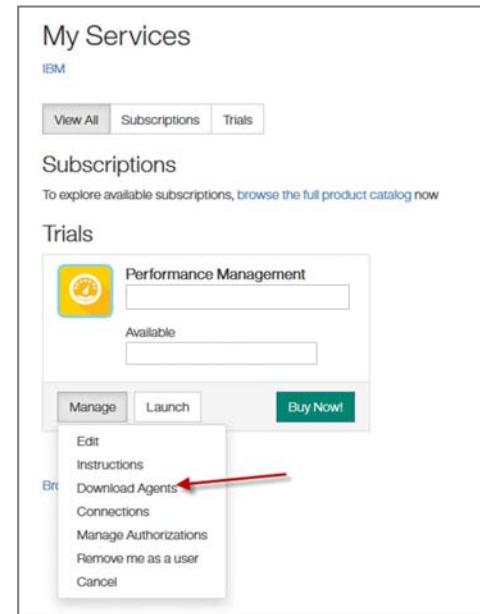


## Lesson 1: Installing Cloud APM agents

### Installation and configuration impact of Cloud versus on premises

For IBM Cloud APM (both Cloud and Private):

- You install the agents on the targets
- The only difference from the agent installation and configuration is where you obtain the software:
  - For Cloud, download the agent software from the IBM Marketplace instance
  - For on premises, download the agent software from the Performance Management Server (by default the `/opt/ibm/ccm/depot` directory)



In this lesson, you learn how to install Cloud APM agents.

Some common tasks must be performed on the installation whether you are installing in a Cloud environment or on-premises.

## Agent image preconfiguration

Agent images that are downloaded from Passport Advantage are not preconfigured to connect to any particular server

- Agent packages that are not preconfigured cannot connect to the Performance Management Server

Preconfiguration process updates agent image:

- Information about server component location (host name or IP address)
- GSKit encryption keys
- Secure communication certificates (optional) when agent-server communication is configured to HTTPS

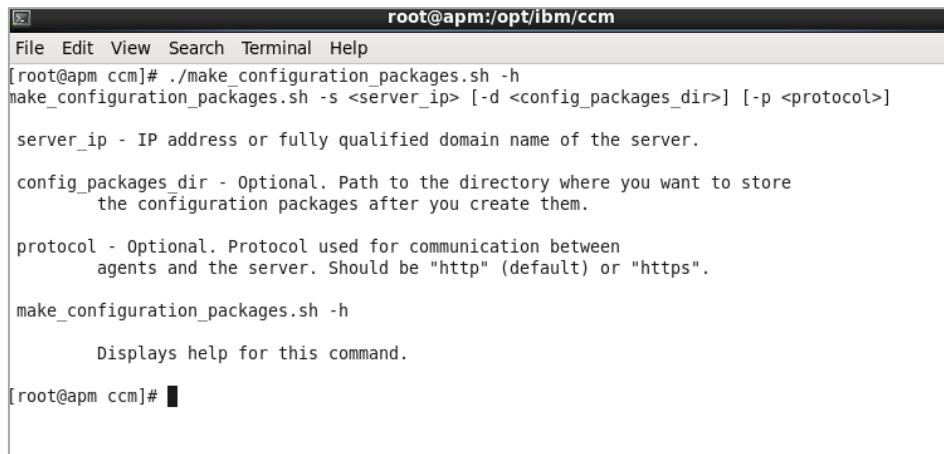
Users can preconfigure agent images:

- During server installation
- After server installation by using:
  - `/opt/ibm/ccm/make_configuration_packages.sh`  
and then on Performance Management server, by using:  
`configure_agent_images.sh`
  - Note: After agent installation, the user cannot reconfigure installed agents to start reporting to a different server

### Agent image preconfiguration

Agent images that are downloaded from Passport Advantage are not preconfigured to connect to any particular server and are not functional until they are preconfigured. The second bullet lists how the agent image is modified during the preconfiguration process. As stated earlier, you can preconfigure during or after the server installation. You use the `make_configuration_packages.sh` script to preconfigure the agent packages.

## Agent image preconfiguration outside server installation (1 of 2)



The screenshot shows a terminal window titled "root@apm:/opt/ibm/ccm". The window contains the help text for the `make_configuration_packages.sh` script. The text describes the command usage and parameters:

```
File Edit View Search Terminal Help
[root@apm ccm]# ./make_configuration_packages.sh -h
make_configuration_packages.sh -s <server_ip> [-d <config_packages_dir>] [-p <protocol>]
server_ip - IP address or fully qualified domain name of the server.
config_packages_dir - Optional. Path to the directory where you want to store
                      the configuration packages after you create them.
protocol - Optional. Protocol used for communication between
           agents and the server. Should be "http" (default) or "https".
make_configuration_packages.sh -h
                                Displays help for this command.

[root@apm ccm]#
```

### Agent image preconfiguration outside server installation (1 of 2)

This slide shows the help screen for the `make_configuration_packages.sh` script. The screen shows that you can run the command with all parameters for a silent installation. Otherwise, you can run the command by itself, and then answer the prompts for each parameter. As was shown during the server installation, for preconfiguration you must enter the path to the unpreconfigured packages, the IP address of host name of the Cloud APM server, and the protocol to be used: HTTP or HTTPS.

## Agent image preconfiguration outside server installation (2 of 2)

```
[root@apm ccm]# ./configure_agent_images.sh -h
configure_agent_images.sh -p <configuration_package_dir> -s <agent_images_dir> [-a <agent_frameworks_dir>] [-d <pre-configured_images_dir>] [-t]

configuration_package_dir - Path to the directory where
                           the configuration packages that contain
                           the parameters for connecting the agents to
                           the server are stored. The packages are in
                           *.zip format for Windows systems or *.tar
                           format for Linux or AIX systems.

agent_images_dir - Path to the directory where the agent images
                   and/or the Hybrid Gateway image are stored.

agent_frameworks_dir - Optional. Path to the directory where agent
                      offering framework packages are stored. By default it is
                      <installation directory>/ccm/AgentFrameworks

pre-configured_images_dir - Optional. Path to directory where you want
                           the pre-configured images to be stored. If
                           you do not specify a directory and you
                           extracted the images then the
                           pre-configuration is done to the extracted
                           images. Otherwise, the pre-configured
                           images are stored in <installation directory>/ccm/depot by
                           default.

configure_agent_images.sh -h

Displays help for this command.
```

### Agent image preconfiguration outside server installation (2 of 2)

This slide shows the help screen for the `configuration_agent_images.sh` script. As was shown during the server installation, for preconfiguration you must enter the path to the unpreconfigured packages, the IP address of host name of the Cloud APM server, and the protocol to be used: HTTP or HTTPS.

## Installing an agent (1 of 2)

- Copy the appropriate package to the server and extract its contents
- Change into the installation directory and run installer script
  - On premises: `./installAPMAgents.sh`
  - Cloud: `./installAPMaaSAgents.sh`

```

lin1:/tmp/linagents/APMADV_Agent_Install_8.1.4.0 # ./installAPMAgents.sh

The following products are available for installation:

1) Monitoring Agent for Cisco UCS
2) Monitoring Agent for DataPower
3) Monitoring Agent for DB2
4) Monitoring Agent for HTTP Server
5) Monitoring Agent for IBM Integration Bus
6) Monitoring Agent for JBoss
7) Monitoring Agent for Linux KVM
8) Monitoring Agent for MongoDB
9) Monitoring Agent for WebSphere MQ
10) Monitoring Agent for MySQL
11) Monitoring Agent for NetApp Storage
12) Monitoring Agent for Nodejs
13) Monitoring Agent for OpenStack
14) Monitoring Agent for Oracle Database
15) Monitoring Agent for Linux OS
16) Monitoring Agent for PHP
17) Monitoring Agent for PostgreSQL
18) Response Time Monitoring Agent
19) Monitoring Agent for Ruby
20) Monitoring Agent for SAP Applications
21) Monitoring Agent for Siebel
22) Monitoring Agent for Synthetic Playback
23) Monitoring Agent for Tomcat
24) Monitoring Agent for VMware VI
25) Monitoring Agent for WebSphere Applications
26) Monitoring Agent for WebLogic
27) Monitoring Agent for WebSphere Infrastructure Manager
28) all of the above

Type the numbers that correspond to the products that you want to install. Type
'a' to quit selection.
If you enter more than one number, separate the numbers by a space or comma.

Type your selections here (For example: 1,2): 
```

Installing, configuring, and managing Cloud APM agents

8

© Copyright IBM Corporation 2018

### Installing an agent (1 of 2)

To install an agent, copy the appropriate preconfigured package to the target server, extract the contents, and run the `installAPMAgents` script. The slide shows the first part of the installation flow.

## Installing an agent (2 of 2)

```

root@apm:/agents/APMADV_Agent_Install_8.1.4.0
File Edit View Search Terminal Help
If you enter more than one number, separate the numbers by a space or comma.
Type your selections here (For example: 1,2): 15
The following agents will be installed:
Monitoring Agent for Linux OS
Are your selections correct [ 1-Yes, 2-No; default is 1 ]? 1
Please specify the agent home (default: /opt/ibm/apm/agent):
The agent will be installed in /opt/ibm/apm/agent
Do you accept the license agreement(s) found in the directory /agents/APMADV_Agent_Install_8.1.4.0/licenses?
Please enter [ 1-to accept the agreement, 2-to decline the agreement ] : 1
User has accepted the license agreement(s).
Monitoring Agent for Linux OS will be installed.
Installing Monitoring Agent for Linux OS.

root@apm:/agents/APMADV_Agent_Install_8.1.4.0#

```

```

root@apm:/agents/APMADV_Agent_Install_8.1.4.0
File Edit View Search Terminal Help
#####
The following agents were installed successfully into the /opt/ibm/apm/agent directory:
Monitoring Agent for Linux OS
Agent status:
Agent is running. Process ID is 25803
Server connection status: Unknown
The installation log file is /opt/ibm/apm/agent/logs/APMAgents_install.log.
For any agent that is running, the agent is configured with the default settings.
To configure your agents, use the following detailed instructions:
For IBM Cloud Application Performance Management SaaS:
http://ibm.biz/kc-ipmcloud-configagent
For IBM Cloud Application Performance Management On Premises:
http://ibm.biz/kc-ipm-configagent
As part of the configuration instructions, you will use the following commands to configure and manage each installed agent:
Monitoring Agent for Linux OS          /opt/ibm/apm/bi
n/os-agent.sh start or stop or status or uninstall
#####
[root@apm APMADV_Agent_Install_8.1.4.0]#

```

### Installing an agent (2 of 2)

This slide shows the rest of the agent installation flow. In this case, further configuration is required to a data collector, as indicated in the messages.

## Configuring an agent

Operating system agents require no configuration

- Monitoring Agent for Linux OS
- Monitoring Agent for UNIX OS
- Monitoring Agent for Windows OS
- Because all agents are preconfigured to connect to the Performance Management Server, any required configuration is about connecting to what is being monitored, not how to connect to the Performance Management Server

The required configuration tasks vary by agent:

- Some agents require prerequisite tasks to be completed before a successful installation
- Many agents require a simple configuration command that either is interactive or points to a text file
- Other agents require more commands or updates to configuration files, such as these examples:
  - Adding include statements to drive plug-ins
  - Running commands to add discovered configurations into the target software that is monitored
  - Running commands to discover the application to be monitored

### Configuring an agent

Some agents require no special configuration, but some agents require configuration. Some domains might be able to run multiple instances on the same server, such as DB2, WebSphere, and WebSphere MQ. The agent must be configured for each instance, even if only one instance is running. Some agents require that a data collector is added to the monitored domain. Consult the product documentation for specific instructions for each agent.

# Lesson 2 Starting and stopping Cloud APM agents

IBM Training



## Lesson 2: Starting and stopping Cloud APM agents

### Commands for managing the monitoring agents

- On Linux
  - cd /opt/ibm/apm/agent/bin
  - ./<agent-type>-agent.sh status<instance\_name>
  - ./<agent-type>-agent.sh start <instance\_name>
  - ./<agent-type>-agent.sh stop <instance\_name>
  - ./<agent-type>-agent.sh config <instance\_name>
  - ./<agent-type>-agent.sh uninstall <instance\_name>
  - For example: ./mongodb-agent.sh start mongo1 where mongo1 is the instance name
- On Windows
  - cd C:\IBM\APM\
  - <agent-type>-agent.bat status<instance\_name>
  - <agent-type>-agent.bat start <instance\_name>
  - <agent-type>-agent.bat stop <instance\_name>
  - <agent-type>-agent.bat config <instance\_name>
  - <agent-type>-agent.bat uninstall<instance\_name>
  - For example: mysql-agent.bat start mysql1 where mysql1 is the instance name

**Note:** Operating system agents start when the server starts

In this lesson, you learn how to start and stop Cloud APM agents.

You can manage these agents from the command line, whether you are running on Windows or on Linux. Each agent type has start, stop, and status options. Because most agents can have multiple instances, you provide the instance name in the command.

You must be in administrator mode to run the commands on Windows operating systems.

## Determining which agents are installed and running on a server

Use the `cinfo` command to determine which agents are installed or running

The screenshot shows a terminal window titled "Terminal". The user has run the command `./cinfo`. The output displays system information and a product inventory. The product inventory section lists various monitoring agents with their names, shared libraries, and versions.

```
***** Thu Jun 9 13:19:13 UTC 2016 *****
User: root Groups: root db2iadml
Host name : lin1 Installer Lvl:08.13.00.00
Home: /opt/ibm/apm/agent
*****
-- CINFO Menu --
1) Show installed products
2) Show which products are currently running
3) Exit CINFO

***** Thu Jun 9 13:24:16 UTC 2016 *****
User: root Groups: root db2iadml
Host name : lin1 Installer Lvl:08.13.00.00
Home: /opt/ibm/apm/agent
*****
Host Prod PID Owner Start ID ..Status
lin1 hu 6180 root Jun08 None ...running
lin1 yn 16741 root Jun08 None ...running
lin1 lz 25830 root Jun08 None ...running
lin1 ud 24662 root Jun08 db2inst1 ...running
lin1 t5 49251 root Jun08 None ...running

***** Thu Jun 9 13:21:03 UTC 2016 *****
User: root Groups: root db2iadml
Host name : lin1 Installer Lvl:08.13.00.00
Home: /opt/ibm/apm/agent
*****
...Product inventory (/opt/ibm/apm/agent)
ax IBM Monitoring Shared Libraries
lx8266 Version: 06.35.11.00
gs IBM GSKit Security Interface
lx8266 Version: 08.00.50.56
hu Monitoring Agent for HTTP Server
lx8266 Version: 01.00.04.00
jr IBM Monitoring JRE
lx8266 Version: 08.02.00.00
lz Monitoring Agent for Linux OS
lx8266 Version: 06.35.11.00
t5 Response Time Monitoring Agent
lx8266 Version: 08.13.00.00
ud Monitoring Agent for DB2
lx8266 Version: 07.10.05.00
yn Monitoring Agent for WebSphere Applications
lx8266 Version: 07.30.11.00
```

Installing, configuring, and managing Cloud APM agents

12

© Copyright IBM Corporation 2018

### Determining which agents are installed and running on a server

This slide shows the agent commands that are installed on this server. The agent commands can vary on each server.

## Starting and stopping the Monitoring Agent for Linux OS

- Each agent has a shell script or `.bat` file for starting, stopping, or showing the status of the agent

```
[root@lin1 /]# cd /opt/ibm/apm/agent/bin/←  
[root@lin1 bin]# ./os-agent.sh status←  
Agent status:  
Agent is running. Process ID is 9952  
Server connection status: Connected  
For more information, see the following file: /opt/ibm/apm/agent/logs/lz_ServerConnectionStatus.txt  
[root@lin1 bin]# ./os-agent.sh stop←  
Processing. Please wait...  
Stopping Monitoring Agent for Linux OS ...  
Monitoring Agent for Linux OS was stopped gracefully.  
[root@lin1 bin]# ./os-agent.sh status←  
Agent status:  
Agent is not running  
[root@lin1 bin]# ./os-agent.sh start←  
Processing. Please wait...  
Starting the Monitoring Agent for Linux OS...  
Monitoring Agent for Linux OS started  
[root@lin1 bin]# ./os-agent.sh status←  
Agent status:  
Agent is running. Process ID is 1103  
Server connection status: Connected  
For more information, see the following file: /opt/ibm/apm/agent/logs/lz_ServerConnectionStatus.txt  
[root@lin1 bin]#
```

### Starting and stopping the Monitoring Agent for Linux OS

This slide shows the Monitoring Agent for Linux OS being stopped gracefully and restarted.

## Starting and stopping the Monitoring Agent for DB2

- The `db2-agent.sh` command controls the Monitoring Agent for DB2

```
[root@lin1 ~]# cd /opt/ibm/apm/agent/bin/  
[root@lin1 bin]# ./db2-agent.sh status db2inst1 ←  
Agent instance status:  
db2inst1 is running, PID 68200  
Server connection status: Connected  
For more information, see the following file: /opt/ibm/apm/agent/logs/ud_db2inst1_ServerConnectionStatus.txt  
[root@lin1 bin]# ./db2-agent.sh stop db2inst1 ←  
Sourcing db2profile for user db2inst1 ←  
Processing. Please wait...  
Stopping Monitoring Agent for DB2...  
Monitoring Agent for DB2 was stopped gracefully.  
[root@lin1 bin]# ./db2-agent.sh status db2inst1 ←  
Agent instance status:  
db2inst1 is not running  
[root@lin1 bin]# ./db2-agent.sh start db2inst1 ←  
Sourcing db2profile for user db2inst1  
Processing. Please wait...  
Starting the Monitoring Agent for DB2...  
Monitoring Agent for DB2 started  
[root@lin1 bin]# ./db2-agent.sh status db2inst1 ←  
Agent instance status:  
db2inst1 is running, PID 103886  
Server connection status: Connected  
For more information, see the following file: /opt/ibm/apm/agent/logs/ud_db2inst1_ServerConnectionStatus.txt  
[root@lin1 bin]#
```

### Starting and stopping the Monitoring Agent for DB2

This slide shows that the Monitoring Agent for DB2 stopped gracefully and restarted.

# Lesson 3 Accessing data from a Cloud agent

IBM Training



## Lesson 3: Accessing data from a Cloud agent

### Before starting the Cloud APM console:

- Determine the IP address of the Performance Management server
- To ensure that the user interface is not truncated, use a minimum resolution of 1280 x 1024
- Use one of the following browsers:

| Browser           | Version   |
|-------------------|---|
| Internet Explorer | 11 (11.0.44) and above                            |
| Chrome version    | 59.0.3071.115 (Official Build) (64-bit) and above |
| Firefox           | ESR 52.x and above                                |
| Safari            | Version 10.1.1 and above                          |

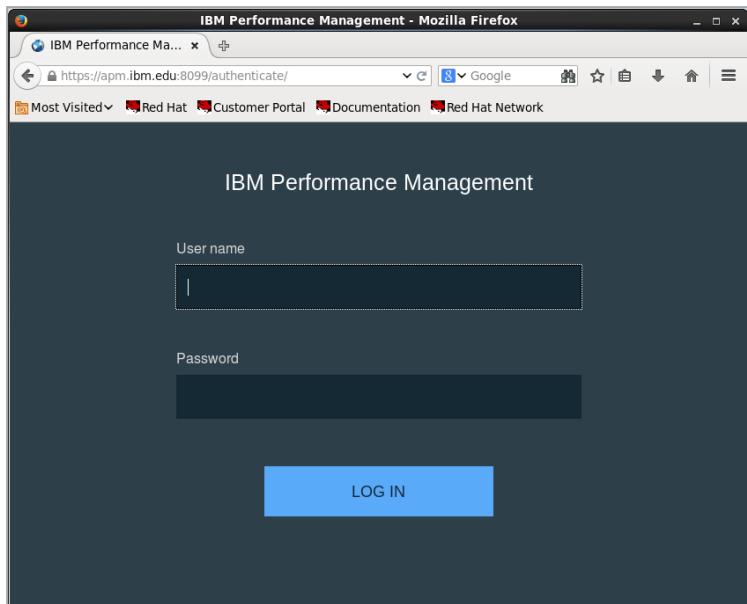
In this lesson, you learn how to access data from a Cloud agent.

## Logging in to the Performance Management Console for on-premises

- To log in to the Performance Management Console, open a supported browser and navigate to this URL:

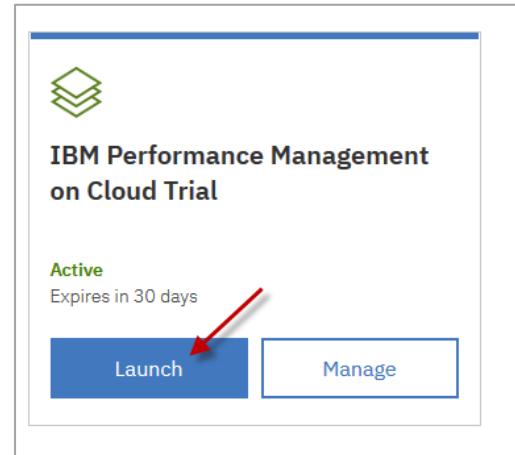
<https://server host:9443>

- After you are prompted for a logon ID, enter the following credentials for the default user:
  - User name: **apmadmin**
  - Password: **apmpass** (by default)
  - Note: For this course, you use the password **object00** in the exercises



## Logging in to the Performance Management Console on Cloud

- To log in to the Cloud APM console, open a supported browser and navigate to the URL that is provided to you from IBM Marketplace
- Log in with the user name and password that you used to register for the service
- In the IBM Performance Management on Cloud Trial row, click **Launch**



## Successful login (1 of 2)

- After you log in, the Getting Started page is displayed with learning options for User Tasks and Administrator Tasks and links to Community Resources

The screenshot shows the 'Getting started' page of the IBM Cloud Application Performance Management interface. At the top, there's a navigation bar with icons for home, user profile, and help, followed by the URL https://df30a9361d77718cd7fcb25be8fb736d.customers.na.apm.ibmserviceengage.com and a 'Most Visited' link. The main content area has a dark header 'Getting started' and a sub-header 'Thank you for using IBM Cloud Application Performance Management.' Below this, a paragraph explains the service's purpose: 'IBM Cloud Application Performance Management is a comprehensive solution that helps you manage the performance of your applications. It provides you with visibility, control, and automation of your applications, ensuring optimal performance and efficient usage.' Two links are provided: 'Watch the getting started video' and 'Take a tour of the performance management dashboard.' A section titled 'User Tasks' follows, with a sub-header 'Learn about these common tasks.' It features three circular icons with icons: a document for 'View application status', a clock for 'View end user application response time', and a transaction symbol for 'View transaction details'. To the right, there's a vertical sidebar with sections for 'Line of Business Owner' and 'Application Dev'.

Installing, configuring, and managing Cloud APM agents

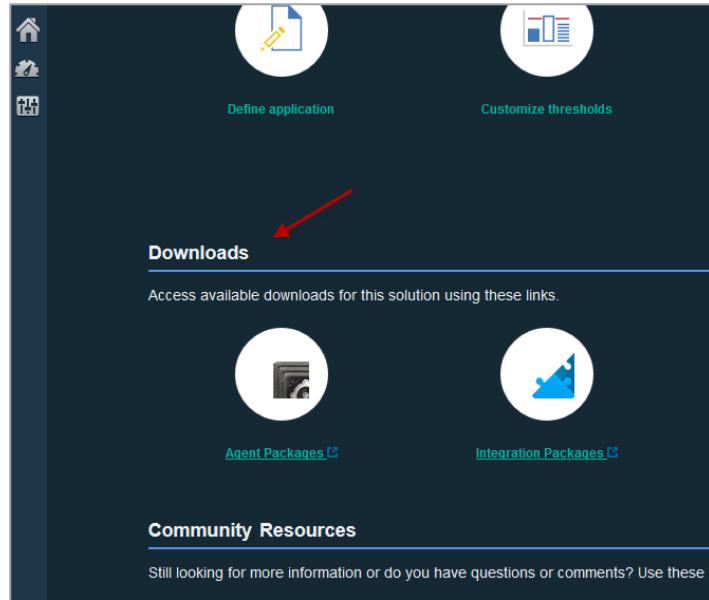
18

© Copyright IBM Corporation 2018

Successful login (1 of 2)

## Successful login (2 of 2)

- On Cloud, you have an extra section for downloads

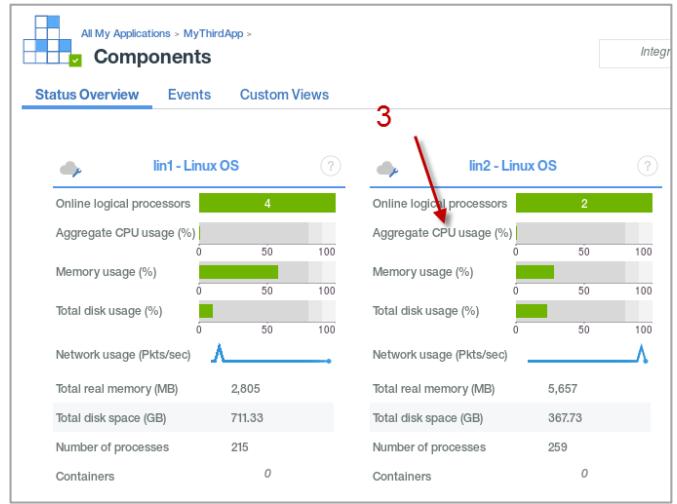


## Accessing data from an agent by using the summary boxes



- 1) Click the Performance Management Dashboard in the navigation bar
- 2) Select the **Components** link in the summary box of an application
- 3) Select the instance

A screenshot of the Application Dashboard. On the left, there's a sidebar with 'Applications' and 'Groups'. Under 'Applications', 'All My Applications' is selected. A red arrow labeled '2' points to this selection. In the center, there's a summary box titled 'All My Applications' with a 'Components' link. Another red arrow labeled '3' points to this 'Components' link. At the bottom, there's a footer with the text 'Installing, configuring, and managing Cloud APM agents'.



### Accessing data from an agent by using the summary boxes

Data for an IBM Cloud agent can be accessed in many ways.

You can use summary boxes to locate data for an IBM Cloud agent.

## Accessing data from an agent by using the status overview

The figure consists of three screenshots of the IBM Cloud Application Performance Management interface:

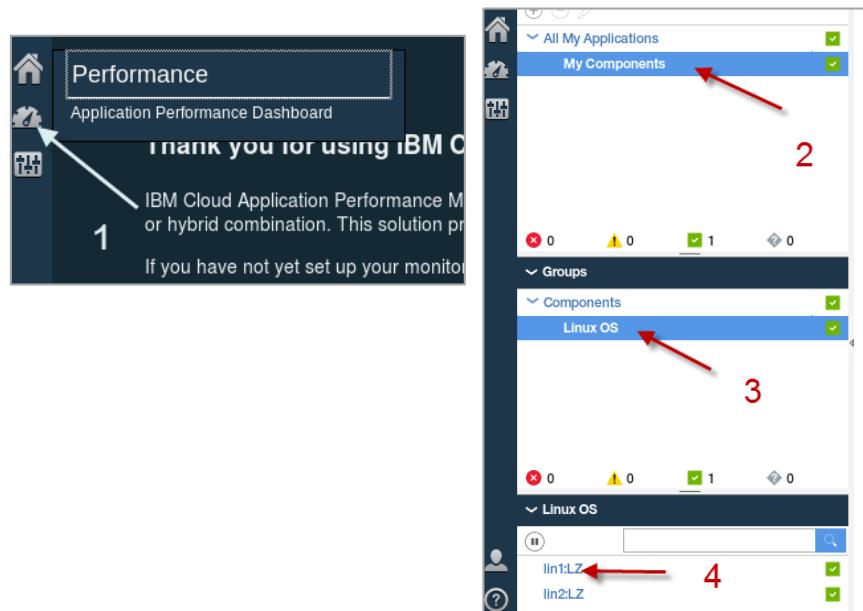
- Screenshot 1:** Shows the "Performance" dashboard. A red arrow labeled "1" points to the "Performance Management Dashboard" link in the top navigation bar.
- Screenshot 2:** Shows the "My Components" page under "All My Applications". A red arrow labeled "2" points to the "My Components" link in the left sidebar.
- Screenshot 3:** Shows the "Components" page for the application "MyThirdApp". A red arrow labeled "3" points to the "Status Overview" tab. The page displays two Linux OS components: "lin1 - Linux OS" and "lin2 - Linux OS", each with various performance metrics like Online logical processors, Aggregate CPU usage (%), Memory usage (%), Total disk usage (%), Network usage (Pkts/sec), Total real memory (MB), Total disk space (GB), Number of processes, and Containers.
- Screenshot 4:** Shows a close-up of the "Status Overview" section for the "lin1 - Linux OS" component. A red arrow labeled "4" points to the "Status Overview" tab. The page displays metrics for "lin1 - Linux OS" including Online logical processors (4), Aggregate CPU usage (%), Memory usage (%), Total disk usage (%), Network usage (Pkts/sec), Total real memory (MB), Total disk space (GB), Number of processes, and Containers.

Accessing data from an agent by using the status overview

You can use the status overview widget to locate data for an IBM Cloud agent.

## Accessing data from an agent by using the navigator

- 1) Click the Performance Management Dashboard in the navigation bar
- 2) Select an application in the Navigator
- 3) Expand Components, and select a group or subgroup
- 4) Select the instance



### Accessing data from an agent by using the navigator

You can use the navigator to locate data for an IBM Cloud agent.

# Lesson 4 Configuring and using the log file agent

IBM Training



## Lesson 4: Configuring and using the log file agent

### Log file overview

The operating system agents support monitoring log files

- Monitors text-based log files
- Regular expressions can be used for parsing the logs
- For compatibility, the OS agent consumes the following information and formats from:
  - IBM Tivoli Monitoring 6.x Log File Agent
  - Tivoli Event Console Log File Adapter
- These format strings allow the agent to filter the log data according to patterns in the format file and submit only the relevant data to an event consumer
  - The OS Agent sends data to the Performance Management server or through the Event Integration Facility (EIF) to any EIF receiver, such as the OMNIbus EIF probe or IBM Operations Analytics – Log Analysis
  - Agent provides configurable log file monitoring capability

In this lesson, you learn how to configure and use the log file agent component of the Monitoring agent for Linux OS.

Log files are a common tool for detecting application issues. The ability to display logs and parse logs from the operating system agent reduces the number of agents that are required to manage your enterprise.

## Configuring log file monitoring (1 of 2)

In the Cloud APM console, access the Agent configuration task

- Configuration tabs for all OS types are displayed when any one OS agent is installed
- The only managed systems that are listed on the tab are the ones that the user has permission to see

Create a configuration definition

- The log file agent requires a pair of files to read and forward log messages from one or more files
  - `<useful-name>.conf`: Defines what log to read, when to read, and where to forward it to
  - `<useful-name>.fmt`: For parsing and reformatting the messages that you read from the log file
- The configuration name must be unique
- The configuration can be distributed to multiple managed systems

### Configuring log file monitoring (1 of 2)

Centrally configuring logs from the Performance Management console simplifies the administrator's task.

## Configuring log file monitoring (2 of 2)

Distribute a configuration

- Request to distribute or undistribute one configuration to one or more managed systems
- Central Configuration Service does the distribution
- The files sent to the managed systems use the configuration name

Begin monitoring

- After the configuration is distributed to the agent, access the Application Performance Management UI and drill down to the managed system to see the log file monitoring information
- Click in the log file monitoring summary to see the details page for log monitoring

## A simple log file configuration sample

This example pulls all the messages from a WebSphere Application Server log:

- Configuration file:

```
LogSources=/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/server1/SystemOut.log
UnmatchLog=/tmp/WAS.unmatched
IncludeEIFEventAttr=yes
ConfigFilesAreUTF8=Y
```

- Format file:

```
REGEX ALLLINE
(.*)
msg $1
END
```

### *A simple log file configuration sample*

The configuration file points to the file to be parsed.

The format file determines what messages are shown in the user interface.

## Log file Configurations List page

The screenshot shows the 'Log file Configurations List page' for the 'Linux OS' tab. On the left, a sidebar menu includes 'System Configuration' (highlighted with a red arrow), 'Advanced Configuration', 'Agent Configuration', 'Role Based Access Control', 'Threshold Manager', 'Synthetic Script Manager', and 'Resource Group Manager'. Below the sidebar is a table with columns: Configuration Name, Configuration Description, Configuration File Name, Distributions, Status, and Managed system name. A message at the top states: 'Use this page to configure monitoring of log files on Linux machines.' At the bottom of the table area, there is a note: 'No items to display.'

• All OS types use this same initial page layout  
• **System Configuration > Agent Configuration > Linux OS**  
• Click the **New** icon above the left table to create a log file configuration

The screenshot shows the 'Agent Configuration' page under 'Agent Configuration'. It has tabs for WebSphere, Ruby, IBM Integration Bus, WebSphere MQ, and Unix OS. A message says: 'Use this page to configure monitoring of log files on Linux machines.' Below it is a table with columns: Configuration Name, Configuration Description, and a note: 'No items to display.' A red arrow points to the green '+' icon in the top toolbar, which is used to create a new configuration.

### Log file Configurations List page

As soon as you have an FMT and CFG file, you can load it into APM to prepare for distribution of those definitions.

## Creating a log file configuration

New Log File Configuration

Configuration Name \* WAS

Configuration Description Display the WebSphere Application Server Log

Select Conf File WAS.conf View

Select FMT File WAS.fmt View

Done Cancel

Conf file content

```
LogSources=/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/server1/SystemOut.log
UnmatchLog=/tmp/WAS.unmatched
IncludeElfEventAttr=yes
ConfigFilesAreUTF8=Y
ConfigFilesAreUTF8=Y
```

Close

### Creating a log file configuration

1. Enter the required Configuration Name (it must be unique).
2. Enter an optional description for the configuration.
3. Click **Select a Conf File** to open the file selector and select a **.conf** file.
4. Click **Select an FMT File** to open the file selector and select a **.fmt** file.
5. Optionally, use the **View** buttons to view the uploaded file contents.
6. Click **Done** to save this definition and return to the Configuration List page.

Required inputs are validated and as you enter values.

Input is validated when **Done** is clicked. If something needs to change, a message appears and the entry field is highlighted.

## Distributing a log file configuration

The screenshot shows the 'Agent Configuration' page for Linux OS. A configuration named 'WAS' is selected, monitoring the 'Display the WebSphere Application Server Log' with the file name 'WAS.conf'. A modal dialog titled 'Information' displays the message 'Request to deploy the Log Configuration received by server' with a 'Close' button. Below the configuration list, a table shows distribution status for one managed system, 'In1:L2', which is checked and has a green status indicator.

| Distributions | Status                              | Managed system name | Version  |
|---------------|-------------------------------------|---------------------|----------|
| 0             | <input checked="" type="checkbox"/> | In1:L2              | 06.35.11 |

Installing, configuring, and managing Cloud APM agents

29

© Copyright IBM Corporation 2018

### Distributing a log file configuration

Your configuration definition is in the list.

If no managed systems are listed on the Configurations List page, click the reset button above the distributions table.

To distribute a configuration, first select the configuration then select one or more managed systems and click **Apply Changes**. Central Config Services are requested to distribute the configuration.

## Undistributing a log file configuration

The screenshot shows the 'Agent Configuration' page for 'Linux OS'. A red arrow points to the 'WAS' configuration entry in the list. Another red arrow points to the 'Apply Changes' button at the bottom of the configuration details panel. A third red arrow points to the 'lin1LZ' managed system entry in the distribution table, which has a checked status indicator.

Configuration Name: WAS  
Configuration Description: Display the WebSphere Application Server Log  
Configuration File Name: WAS.conf

| Managed systems          | Status                              | Managed system name | Version  |
|--------------------------|-------------------------------------|---------------------|----------|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | lin1LZ              | 06.35.11 |

Total Selected: 0

Installing, configuring, and managing Cloud APM agents

30

© Copyright IBM Corporation 2018

### Undistributing a log file configuration

Select the log file configuration to be undistributed.

The managed systems that are already distributed are automatically selected in the distributions list table.

To undistribute a configuration, clear the managed systems where the configuration should be undistributed and click **Apply Changes**. Central Config Services are requested to undistribute the configuration.

## Deleting a log file configuration

The screenshot shows the 'Agent Configuration' interface for the 'Linux OS' tab. It displays a table of log configurations. One row is selected for 'WAS' with the configuration description 'Display the WebSphere Application Server Log' and the file name 'WAS.conf'. Above the table, there are buttons for adding (+), editing (pencil), and deleting (-). A red arrow points to the delete button. To the right, a confirmation dialog box is open with the title 'Confirmation' and the message 'Do you want to remove selected log configurations?'. It has 'OK' and 'Cancel' buttons, with a red arrow pointing to the 'OK' button.

### Deleting a log file configuration

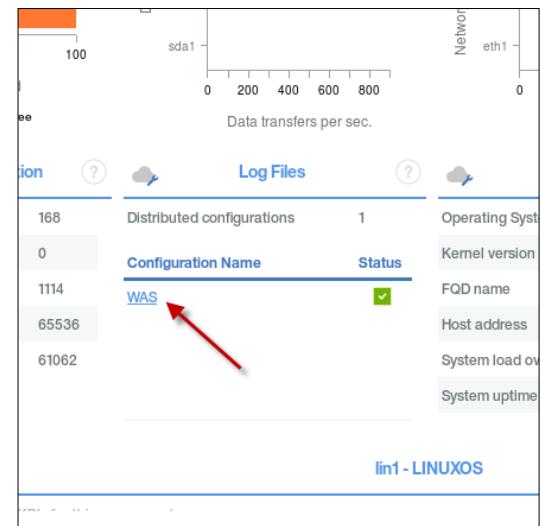
Select the logfile configuration to be deleted.

Click the “Delete” button above the left table.

The configuration is deleted on Central Config Services and on the OS agents where it was previously distributed.

## Displaying a log file in the Cloud APM console (1 of 3)

- You can view the log file monitoring configuration for the OS agents that you deployed to monitor log files
- Procedure
  - Open the Application Dashboard and click **My Components**
  - Click **Groups > Components** and select the OS agent, for example, Linux OS agent
  - Click **Linux OS > agent name** where agent name is the system where you deployed the configuration
  - To view the Log Files widget, double-click anywhere on the status widget
  - In the **Status Overview > Log Files** widget, click the profile to view the log monitoring configurations that are distributed and the monitored logs



### Displaying a log file in the Cloud APM console (1 of 3)

Click the log file definitions to display the log files collected. More than one can be possible.

## Displaying a log file in the Cloud APM console (2 of 3)

**Procedure**

- In the Monitored Logs window, you can view the Configuration Details and the Monitored Logs
- The Configuration Details include the configuration name, description, subnode, configuration file, type, status, and error code
- You can also view the log files that are monitored in the configuration
- Click the log file name to view all the log file events that are associated with the log file

The screenshot shows the Application Dashboard with the path: All My Applications > DayTrader > Components > Linux OS > lin1:LZ. Under Status Overview, the Monitored Logs section is selected. It shows a table for Configuration Details with one row for WAS, and another table for Monitored Logs with one row for the file /opt/IBM/WebSphere/App... with status OK.

| Configuration | Description                 | Subnode Name | Configuration File                                       | Type | Status | Error Code |
|---------------|-----------------------------|--------------|--|------|--------|------------|
| WAS           | Display the WebSphere Ap... | LZ:lin1_WAS  | /opt/ibm/apm/agent/localconfig/lz/log_discovery/WAS.conf | log  | ACTIVE | NO_ERROR   |

| File Name                 | File Type    | File Status | Processed Records | Matched Records | File Size | Current Position | Codepage | Last Modification Time  |
|---------------------------|--------------|-------------|-------------------|-----------------|-----------|------------------|----------|-------------------------|
| /opt/IBM/WebSphere/App... | REGULAR_FILE | OK          | 468               | 468             | 77060     | 76904            | UTF-8    | May 12, 2016 7:25:05 AM |

### Displaying a log file in the Cloud APM console (2 of 3)

Click the log file to display the contents.

## Displaying a log file in the Cloud APM console (3 of 3)

All My Applications > DayTrader > Components > Linux OS > lin1:LZ

**Status Overview**   **Events**   **Attribute Details**

Overview > Monitored Logs > Events In Monitored Log

**Monitored Log**

| Configuration | File Name                                       | File Type     | File Status | Processed Records | Matched Records | File Size | Current Position | Codepage | Last Modification Time  |
|---------------|---|---------------|-------------|-------------------|-----------------|-----------|------------------|----------|-------------------------|
| WAS           | /opt/IBM/WebSphere/AppServer/logs/SystemOut.log | REGULAR, F... | OK          | 473               | 473             | 77553     | 77553            | UTF-8    | May 12, 2016 7:25:11 AM |

**Log File Events**

| Timestamp             | Message   |
|-----------------------|---|
| May 12, 2016 07:25:12 | [5/12/16 7:25:09:566 UTC] 00000094 SystemOut O ## Htt... ports: 9060;"HTTP,9043;"HTTPS,9443;"HT...        |
| May 12, 2016 07:25:12 | [5/12/16 7:25:11:091 UTC] 000000a0 ServletWrapp... com.ibm.ws.webcontainer.servlet.ServletWrapper...      |
| May 12, 2016 07:25:12 | [5/12/16 7:25:11:515 UTC] 000000a0 ServletWrapp... com.ibm.ws.webcontainer.servlet.ServletWrapper...      |
| May 12, 2016 07:25:07 | [5/12/16 7:25:05:373 UTC] 00000098 ttpapi4  I Loaded kbb library <span style="color: red;">(arrow)</span> |
| May 12, 2016 07:25:07 | [5/12/16 7:25:05:376 UTC] 00000098 ttpapi4  I Loaded TTAPI library: dc_ttapi                              |
| May 12, 2016 07:25:02 | [5/12/16 7:24:57:367 UTC] 00000062 SharedEJBRunn... I WSR0057: EJB jar started: PlantsByWebSphere...      |
| May 12, 2016 07:25:02 | [5/12/16 7:24:57:368 UTC] 00000062 webapp I com.ibm.ws.webcontainer.webapp.WebGroupImpl! WebC...          |
| May 12, 2016 07:25:02 | [5/12/16 7:24:57:378 UTC] 00000062 WASSessionCor... I SessionContextRegistry getSessionContext SES...     |
| May 12, 2016 07:25:02 | [5/12/16 7:24:57:445 UTC] 00000062 WebContainerL... I WebContainerLifecycle startApplication OpenWe...    |
| May 12, 2016 07:25:02 | [5/12/16 7:24:57:636 UTC] 00000062 BeansDeployer I BeansDeployer validateInjectionPoints All inject...    |
| May 12, 2016 07:25:02 | [5/12/16 7:24:57:640 UTC] 00000062 WebContainerL... I WebContainerLifecycle startApplication OpenWe...    |
| May 12, 2016 07:25:02 | [5/12/16 7:24:57:643 UTC] 00000062 DefaultFacesC... I Reading standard config META-INF/standard-fac...    |

**Procedure (continued)**

- Click the event to view the event details, for example, all the fields that you defined in the Format file

| Event Details    |   |   |
|------------------|---|---|
| Timestamp        | May 12, 2016 7:25:07 AM   | Custom Slot 1   |
| Log Name         | SystemOut.log   | Custom Slot 2   |
| TEC Class        | ALLLINE   | Custom Slot 3   |
| Event Type       | Event   | Custom Slot 4   |
| Occurrence Count | 1   | Custom Slot 5   |
| Remote Host      |   | Custom Slot 6   |
| Message          | [5/12/16 7:25:05:373 UTC] 00000098 ttpapi4  I Loaded kbb library <span style="color: red;">(arrow)</span> | Custom Slot 7   |
| Custom Integer 1 | 0   | [5/12/16 7:25:05:373 UTC] 00000098 ttpapi4  I Loaded kbb library <span style="color: red;">(arrow)</span> |
| Custom Integer 2 | 0   | Custom Slot 9   |
| Custom Integer 3 | 0   | Custom Slot 10  |

Installing, configuring, and managing Cloud APM agents

34

© Copyright IBM Corporation 2018

### Displaying a log file in the Cloud APM console (3 of 3)

Selecting an entry in a log shows the fields that are parsed.

© Copyright IBM Corp. 2018

3-34

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

## Student exercises



Complete the exercises for this unit in the Course Exercises Guide.

## Summary

Now that you have completed this unit, you should be able to:

- Install and preconfigure the various types of Cloud APM agents
- Start and stop the Cloud APM agents
- Access data from a Cloud APM agent
- Configure and use the log file agent

# **Unit 4 Administration**

IBM Training



## **Administration**

© Copyright IBM Corporation 2018  
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

This unit teaches how to manage the components of the Cloud APM server, and also teaches how to use and administer the Cloud APM console.

## Learning objectives

After completing this unit, you should be able to:

- Manage the Cloud APM server components
- Describe the major functions that are involved in managing applications
- Create custom views in the Cloud APM console
- Use attribute details to access data from an agent
- Manage users of the Cloud APM console

## Unit outline

- Lesson 1: Starting and stopping the Cloud APM server
- Lesson 2: Managing applications
- Lesson 3: Creating custom views
- Lesson 4: Using attribute details to access data from an agent
- Lesson 5: Managing users of the Cloud APM console

### *Unit outline*

This slide shows the lessons for this unit.

# Lesson 1 Starting and stopping the Cloud APM server

IBM Training



## Lesson 1: Starting and stopping the Cloud APM server

- The Cloud APM server has multiple components
- These components can be started, stopped, and restarted either as a group or individually
- The command that is used to manage the Cloud APM server is the `apm` command

In this lesson, you learn how to start and stop components of the Cloud APM server.

## List of Cloud APM services (1 of 3)

| Service | Description  |
|---------|--|
| apmui   | Cloud APM console component that handles incoming user interface requests  |
| biagent | Component for Cloud APM data collectors, which is enabled by default   |
| db2     | <ul style="list-style-type: none"><li>DB2 server that is used to persist monitoring data and applications that are displayed in the Cloud APM console</li><li>This component is only used if you install a local DB2 server when you install the Cloud APM server</li></ul>  |
| dqe     | Component for Cloud APM data collectors, which is enabled by default   |
| kafka   | Message bus component for internal communication between components  |
| ksy     | Summarization and Pruning Agent for maintaining database partitions and pruning monitoring data in the DB2 server  |
| min     | <ul style="list-style-type: none"><li>Monitoring Infrastructure Node component that maintains the list of connected agents, advanced configuration data, and threshold events</li><li>The min component is also the agent interface component that includes the agent REST interface and central configuration services HTTP server</li><li>The REST interface is used by agents to send monitoring data that is persisted in the DB2 server and threshold events</li><li>The central configuration service HTTP server handles requests from agents for their configuration files, for example, threshold definitions</li></ul> |

### List of Cloud APM services (1 of 3)

The Cloud APM server is made up of 16 services, which are listed on these slides.

## List of Cloud APM services (2 of 3)

| Service        | Description  |
|----------------|--|
| <b>mongodb</b> | <ul style="list-style-type: none"><li>(Not available with Cloud APM, Base Private) MongoDB NoSQL open source database that stores data for threshold events and for the transaction tracking functionality</li><li>This component is only used if you install a local MongoDB database when you install the Cloud APM server</li></ul>   |
| <b>oidc</b>    | <ul style="list-style-type: none"><li>OpenID Connect (OIDC) is a simple identity protocol over OAuth 2.0</li><li>The OIDC provider in Liberty Profile is implemented as an OAuth 2.0 extension</li></ul>   |
| <b>oslc</b>    | Open Services for Lifecycle Collaboration service provider that registers the computer system, software server, and application resources that are monitored by agents in the service component registry   |
| <b>scr</b>     | Service Component Registry that persists application definitions and their relationships to agent resources in the DB2 server  |
| <b>server1</b> | <ul style="list-style-type: none"><li>Cloud APM console backend component that retrieves monitoring data and applications from the DB2 server and persists threshold definitions, resource group definitions, and role-based access control definitions</li><li>If you restart server1, you must also restart the apmui component after restarting the server1 component</li></ul> |

## List of Cloud APM services (3 of 3)

| Service        | Description  |
|----------------|--|
| <b>spark</b>   | <ul style="list-style-type: none"><li>(Not available with Cloud APM, Base Private) Component that controls the spark infrastructure and the applications such as the AAR Aggregator and Instance Analyzer that run on it</li><li>If you stop this service, you lose function</li></ul> |
| <b>txagent</b> | <ul style="list-style-type: none"><li>(Not available with Cloud APM, Base Private) Transactions Event agent, which sets the thresholds that are used to classify middleware transactions</li><li>If you stop this component, you lose function</li></ul>                               |
| <b>uviews</b>  | Universal View service for defining dashboard pages in the Custom Views tab of the Application Performance Dashboard   |

## APM command

The `apm help` command displays all of the `apm` command options

```
# apm help
```

- Usage: `apm [-f|--force] command service_name`
- `-f` or `--force` option applies only to the `stop`, `stop_all`, `restart`, and `restart_all` commands
- The apm commands are as follows:
  - `status | ss` Show whether service is running or stopped
  - `start | st` Start an apm service by name
  - `start_all | sta` Start all apm services
  - `stop | sp` Stop an apm service by name
  - `stop_all | spa` Stop all apm services
  - `restart | rt` Restart a running apm service by name
- `service_name` is one of the services: `apmui`, `biagent`, `db2`, `dqe`, `kafka`, `ksy`, `min`, `mongodb`, `oidc`, `oslc`, `scr`, `server1`, `soagent`, `spark`, `txagent`, `uvviews`

```
root@apm:~#
File Edit View Search Terminal Help
[root@apm ~]# apm help
Usage: apm [-f|--force] command service_name
-f or --force option only applies to the stop, stop_all, restart, and restart_all commands
The apm commands are:
status | ss Show if service is running or stopped
start | st Start an apm service by name
start_all | sta Start all apm services
stop | sp Stop an apm service by name
stop_all | spa Stop all apm services
restart | rt Restart a running apm service by name
restart_all | rta Restart all apm services
service_name is one of: db2 ksy kafka spark txagent mongodb scr oidc server1 min apmui oslc biagent soagent
```

With the `apm` command, you can stop, start, restart, and see the status of the various components that make up the Cloud APM server. You can stop and start all services with one command, or you can stop, start, or restart each service independently.

## Managing the Monitoring Infrastructure Node (MIN) service

- The Monitoring Infrastructure Node component maintains the list of connected agents, advanced configuration data, and threshold events
- **apm start min** starts the Monitoring Infrastructure Node component
- **apm stop min** stops the Monitoring Infrastructure Node



```
[root@apm ~]# apm stop min
Stopping service min (PID 4405).
Service min stopped.
[root@apm ~]# apm start min
Starting service min
.....
Service min started (PID 19687).
[root@apm ~]#
```

### Managing the Monitoring Infrastructure Node (MIN) service

The Monitoring Infrastructure Node is the key component of the Cloud APM server.

## Managing the Cloud APM console

- The Cloud APM console component handles incoming user interface requests
- **apm start apmui** starts the Cloud APM console component
- **apm stop apmui** stops the Cloud APM console
- When the console stops, the browser connection fails

```
File Edit View Search Terminal Help
[root@apm ~]# apm stop apmui
Stopping service apmui (PID 6856).
Service apmui stopped.
[root@apm ~]# apm start apmui
Starting service apmui
-----
Service apmui started (PID 9028).
[root@apm ~]# apm status apmui
Service apmui started (PID 9028).
[root@apm ~]#
```



### Unable to connect

Firefox can't establish a connection to the server at apm.ibm.edu:9443.

### Managing the Cloud APM console

The apmui component controls access to the Cloud APM console interface.

# Lesson 2 Managing applications

IBM Training



## Lesson 2: Managing applications

### Major functions of managing applications

- Managing applications includes the following tasks:
  - Creating, editing, and deleting applications
  - Accessing data within the applications that are defined

In this lesson, you learn how to manage applications in the Cloud APM console.

## Cloud APM console

- The Cloud APM console is an application-centric user interface that features easy navigation from symptom to cause:
  - Navigate from a widget to an underlying cause
  - Investigate events
  - Diagnose transactions

The Cloud APM console is an application-centric web-based user interface that features easy navigation from symptom to cause.

## Defining an application

- Applications are added, modified, or deleted by using the Application Editor
- To group data from agents in an organized fashion, create applications that are organized by using these methods:
  - Location
  - Function
  - Responsibility
- The Application Editor supports adding applications in three ways:
  - Manually
  - By discovery
  - Using templates
- The Application Editor is also used to edit and delete applications

The following slides explore adding, modifying, and deleting applications in more detail.

## Adding an application manually (1 of 2)

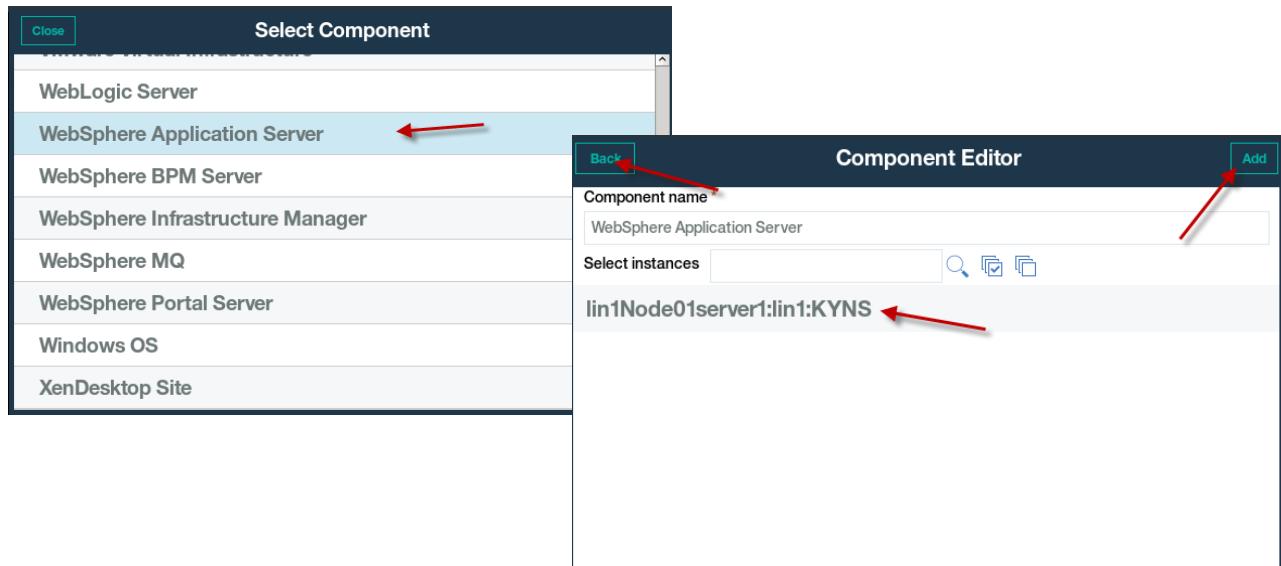
The image consists of two side-by-side screenshots. The left screenshot is the 'Application Dashboard' showing a navigation bar with 'Applications' expanded, revealing 'Add Application'. Below it are 'My Components' and 'My Transactions'. The right screenshot is the 'Add Application' dialog box. It has fields for 'Application name \*' (containing 'MyApplication') and 'Description' (containing 'This is my first application'). At the bottom, there's a section titled 'Application components' with a large empty area and a green button with a plus sign (+) labeled 'Add comp'.

### Adding an application manually (1 of 2)

You can use the Application Editor to add an application manually.

1. Click the plus (+) sign in the Application Dashboard to add components.
2. In the Add Application window, assign your application a name and optional description. Click the highlighted plus sign to add components.

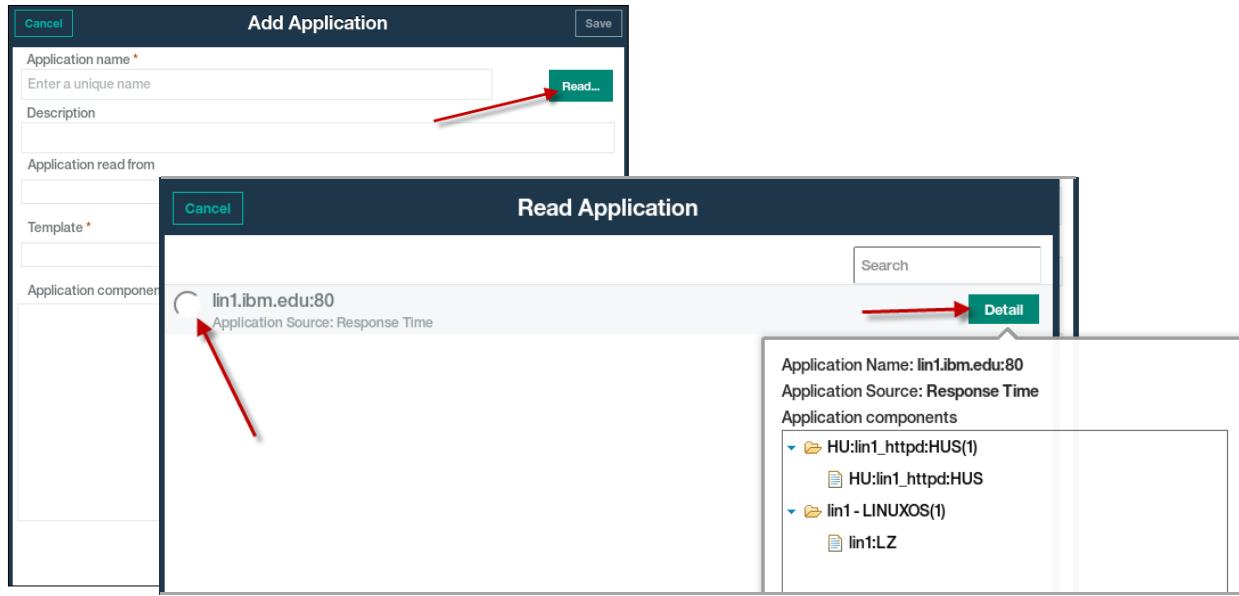
## Adding an application manually (2 of 2)



### Adding an application manually (2 of 2)

3. Click the component type that you want to add. In this example, you are adding an instance of WebSphere Application Server.  
A list of known instances of the resource type is displayed.
4. Select the instance in list, and click **Add**.  
You are returned to the list of resource types.
5. Add any additional components to your application.
6. Click **Close**.
7. Click **Save**.

## Discovering applications (1 of 2)



Administration

16

© Copyright IBM Corporation 2018

### Discovering applications (1 of 2)

You can add application resources that are discovered by the monitoring infrastructure.

1. After opening the Application Editor, give the application a name and optional description. In this example, the application is called Discovered application.
2. Click the **Read** button to view discovered resources.
3. Click **Detail** for more information on the selected resource.
4. Click a radio button to select the discovered application that you want to incorporate.

## Discovering applications (2 of 2)

The screenshot shows the IBM Application Dashboard interface. On the left, a modal window titled 'Add Application' is open. It contains fields for 'Application name \*' (set to 'Discovered Application'), 'Description' (set to 'This is a discovered application'), and other optional fields like 'Template \*' (set to 'Custom Application'). Two red arrows point to the 'Application name' field and the 'Description' field. A red arrow also points to the 'Save' button at the top right of the modal. On the right, the main dashboard shows a list of applications under 'All My Applications'. The 'Discovered Application' is listed there with a status icon. Below the application list are sections for 'Groups' (Components, Transactions) and 'Instances'. To the right of the dashboard is a 'Status Overview' section with a chart titled 'Requests and Response Time' showing request counts over time, and a 'Aggregate Transaction Topology' section with a diagram showing a connection from a 'BROWSER' to a system icon.

Discovering applications (2 of 2)

5. Click **Save** to complete application creation.
6. Observe the new application added to the list of All\_My\_Applications.

Bear in mind that the resource and associated monitoring agent existed. You are making the application visible in the UI.

## Using templates (1 of 2)

The figure consists of three screenshots of an application editor interface. The first screenshot shows the 'Add Application' window with the 'Application name' field containing 'Application From Template' and the 'Template' dropdown set to 'Custom Application'. A red arrow points to the 'Custom Application' option. The second screenshot shows a 'Select Template' dialog with a list of options including 'Hadoop', 'WebSphere MQ', 'IBM Integration Bus', 'KV1 Application', 'Oracle WebLogic', and 'CISCO UCS Infrastructure'. A red arrow points to 'IBM Integration Bus'. The third screenshot shows the 'Add Application' window again, but now with 'IBM Integration Bus' selected in the 'Template' dropdown and listed under 'Application components'. A red arrow points to the 'IBM Integration Bus' entry. A callout box contains the text: 'Repeat the process for the remaining IIB components to complete application configuration'.

Administration

18

© Copyright IBM Corporation 2018

### Using templates (1 of 2)

You can use the Application Editor to add applications by using templates.

1. After opening the Application Editor, click the highlighted arrow to see the list of available templates. In this example, an IBM Integration Bus is selected.
2. In the Add Application window, assign your application a name and optional description. Click the highlighted plus sign to add components.

## Using templates (2 of 2)

The screenshot illustrates the process of creating an application from a template in the IBM Integration Bus (IIB) environment.

**Component Editor:** On the left, the "Component Editor" window shows a list of selected instances: "WLBRK9000::KQIB" and "TRADEBK::KQIB". A red arrow points to the "Add" button at the top right of this window. Another red arrow points to the "Select instances" search bar.

**Application Dashboard:** On the right, the "Application Dashboard" shows the "All My Applications" section. It lists several applications: "Application From Template" (selected), "My Components", "SimpleTrade", and "My Transactions". A red arrow points to the "Application From Template" entry.

**Instructions:** A yellow callout box contains the text: "Repeat the process for the remaining IIB components to complete application configuration".

**Progress Bar:** At the bottom center, a progress bar indicates the status of component addition. It shows two completed steps (blue icons) and one step in progress (grey icon). A green checkmark icon is positioned next to the progress bar.

**Page Navigation:** The bottom left shows "Administration" and page numbers "4" and "19". The bottom right includes the copyright notice "© Copyright IBM Corporation 2018".

### Using templates (2 of 2)

A list of two available IIB components is displayed.

3. Select the instance that you want; then, click **Add** to add it to the application.
4. Select Back and repeat the process for any other IIB components you want in the application.
5. When finished, click **Save**.

The application appears in the Application Dashboard after a few moments.

## Editing an application

The screenshot shows the IBM Application Dashboard interface. On the left, there's a sidebar with sections for Applications, Groups, and Components. In the main area, there's a 'Status Overview' chart showing 'Requests and Response Time' over time. A specific application, 'DayTrader', is selected in the list, highlighted with a blue border. An 'Edit Application' button is located next to it. On the right, a detailed 'Edit Application' dialog box is open. It has tabs for 'Cancel', 'Edit Application', and 'Save'. Under 'Edit Application', there are fields for 'Application name' (set to 'DayTrader'), 'Description', and 'Template' (set to 'Custom Application'). The 'Application components' section contains a hierarchical tree view of resources. Red arrows in the image point to the edit icon in the dashboard sidebar, the 'Edit Application' button for 'DayTrader', and the edit icons next to the resource names in the component list.

Administration

20

© Copyright IBM Corporation 2018

### Editing an application

You can use the Application Editor to edit an application.

1. Select the application in the list
2. Click the pencil icon.
3. In the Edit Application window, select the component that you want to modify in the Application Components list.
4. To delete the resource instance, click the minus sign.
5. Confirm the deletion and save the modified application definition.
6. To change or modify instances, click the pencil icon.
7. Make your changes and save the application definition.

## Deleting an application

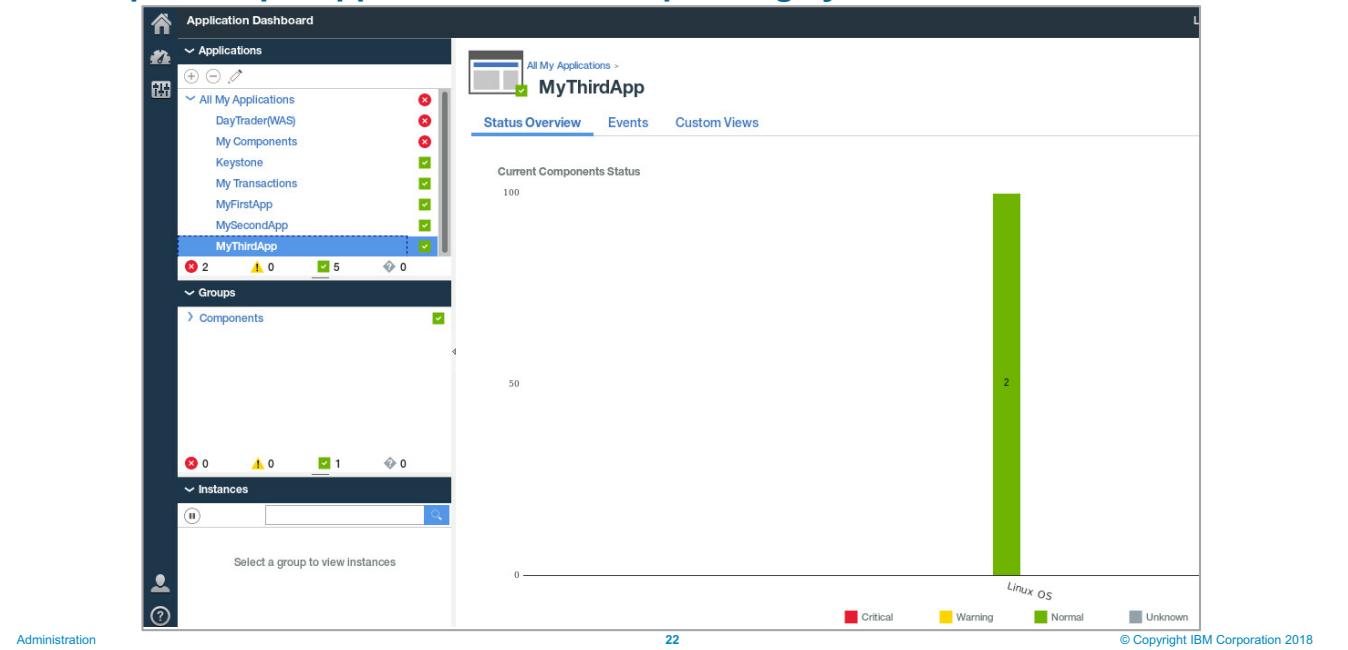
The screenshot shows the Application Dashboard interface. On the left, under 'Applications', there is a list with 'Discovered Application' selected. A red arrow points to the minus sign icon next to 'Remove Application'. Another red arrow points to the 'Discover Application' entry in the list. To the right, the 'Discovered Application' details page is shown with a status overview and a bar chart titled 'Requests and Response Time'. Below the chart is an alert message: 'Do you want to delete application Discovered Application ?' with 'Yes' and 'No' buttons. A red arrow points to the 'Yes' button.

### Deleting an application

You can use the Application Editor to delete an application.

1. Select the application in the list. Click the minus sign.
2. Click **Yes** to confirm the deletion or **No** to cancel the operation.

## Example: Simple application of Linux operating systems



Example: Simple application of Linux operating systems

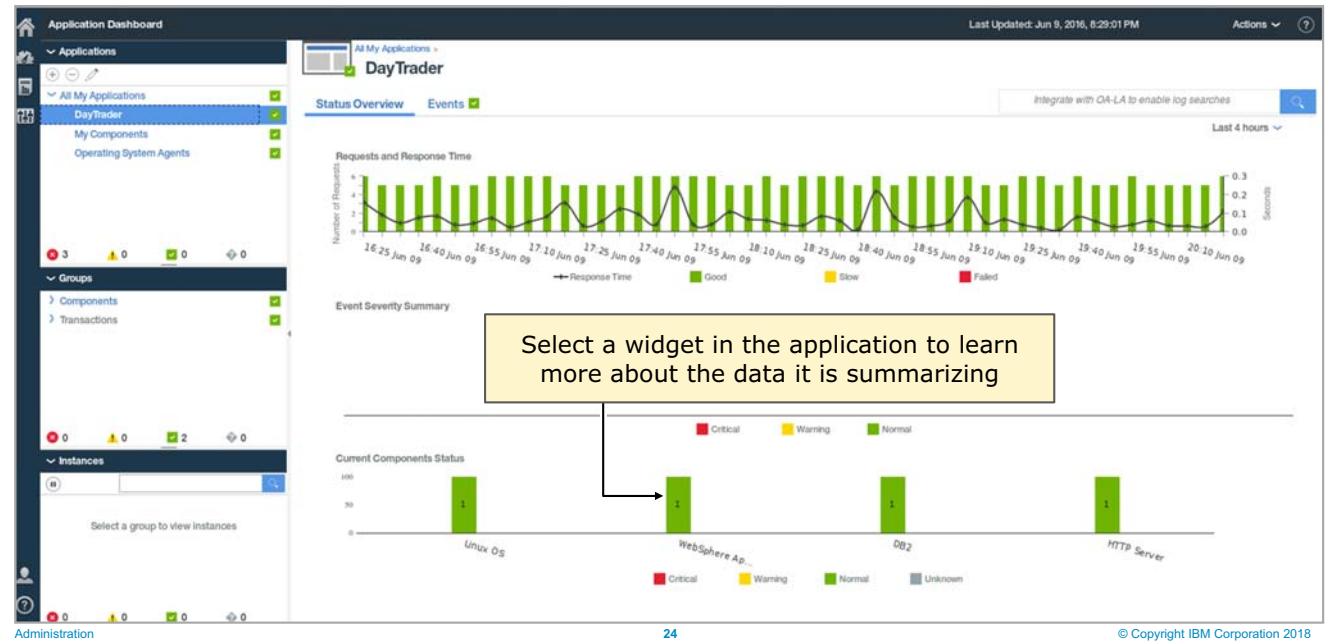
## Example: Simple application with six agents



Example: Simple application with six agents

This screen capture shows the monitoring agents for the DayTrader application from the exercises.

## Examining data from an application



Examining data from an application

Select a widget to learn more details about the resources that it is monitoring.

## Monitoring agent for WebSphere Application Server

The screenshot shows the IBM Monitoring Agent interface for a WebSphere Application Server. The top navigation bar includes 'All My Applications > DayTrader > Components > WebSphere Application Server'. The main area has tabs for 'Status Overview' (selected) and 'Events'. A callout box points to the 'Status Overview' tab with the text: 'Select the widget to learn more about the data that it summarizes'. The 'Status Overview' section displays various metrics for 'lin1Node01server1 - WAS':

| Server status | Connected | Slowest response time (ms) |
|---------------|-----------|----------------------------|
|               | Connected | 44                         |

Below this are four cards:

- JVM memory used (KB): 194,930
- JVM memory total (KB): 223,936
- Heap free after GC(%): 0% to 100%
- JVM CPU used (%): 0.00% to 100%

The 'WAS Information' panel on the right lists server details:

| WAS Information    |                          |
|--------------------|--------------------------|
| Error Rate (%)     | 0.00%                    |
| PID                | 16713                    |
| Server name        | server1                  |
| Node name          | linNode01                |
| Cell name          | linNode01Cell            |
| Monitoring modes   | DataCollector Monitoring |
| Server type        | Traditional WebSphere    |
| PM level (runtime) | Extended                 |

Below the WAS Information are three monitoring charts:

- GC (history): Shows GC duration (ms) over time.
- EJB Containers (history): Shows Method Average Response Time (ms).
- Method Invocation Rate (per sec): Shows the rate of method invocations.

At the bottom left is an 'Administration' link, and at the bottom right is the copyright notice: © Copyright IBM Corporation 2018.

Monitoring agent for WebSphere Application Server

Many monitoring agents have multiple levels of data, like the Monitoring Agent for WebSphere Application Server.

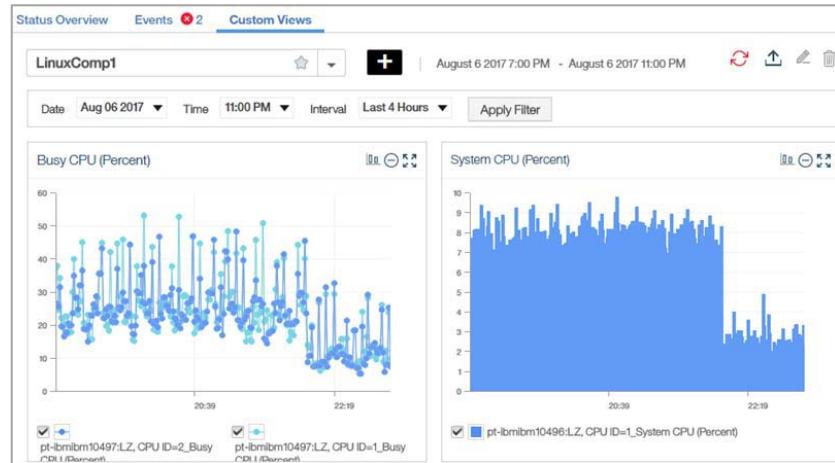
# Lesson 3 Creating custom views

IBM Training



## Lesson 3: Creating custom views

- Create custom pages with custom charts to display performance data of components and resources
- Select Application, Component, and Instance in left navigation and click **Custom Views**
  - Custom Views can have many pages of charts
  - One page is set as default
  - Click + to create new page of charts
- Page editor is used to define pages and charts
  - Page templates are provided
- Add and remove charts to a page
  - Line chart, bar chart, area chart, and grid chart
  - Select one or more metrics
- Context specific: Pages that are created at all three levels in the left navigation (Application, Component, and Instance) are visible on that level only



Administration

26

© Copyright IBM Corporation 2018

In this lesson, you learn how to create custom views.

The Custom Views option provides the provision for the user to create and view the dashboards that have the performance data of the various components and resources available to the user. It can be accessed by selecting any application, component, or instance from the Cloud APM console left navigation and by clicking the **Custom Views** tab on the right window.

Users can modify the dashboard to meet their own requirements by selecting the various charts that are provided by the application such as Line chart, Bar chart, Area chart, and Grid chart. A user can select one or more metrics that have the required data to be shown in these charts.

It provides various templates that can be used to create the dashboard page. The user can create and edit the dashboard in the Dashboard Editor, which provides the facility to add or update charts, metrics, and templates as part of the widgets. The created dashboard can be viewed in the Dashboard Viewer. The user can select a particular dashboard to be the default, and it is shown to the user when Custom View is selected.

Users can also use it to create the context-specific dashboards, where the dashboards can be created at all three levels in the left navigation – that is, application, component, and instance. The dashboard that is created at a level is visible on that level only.

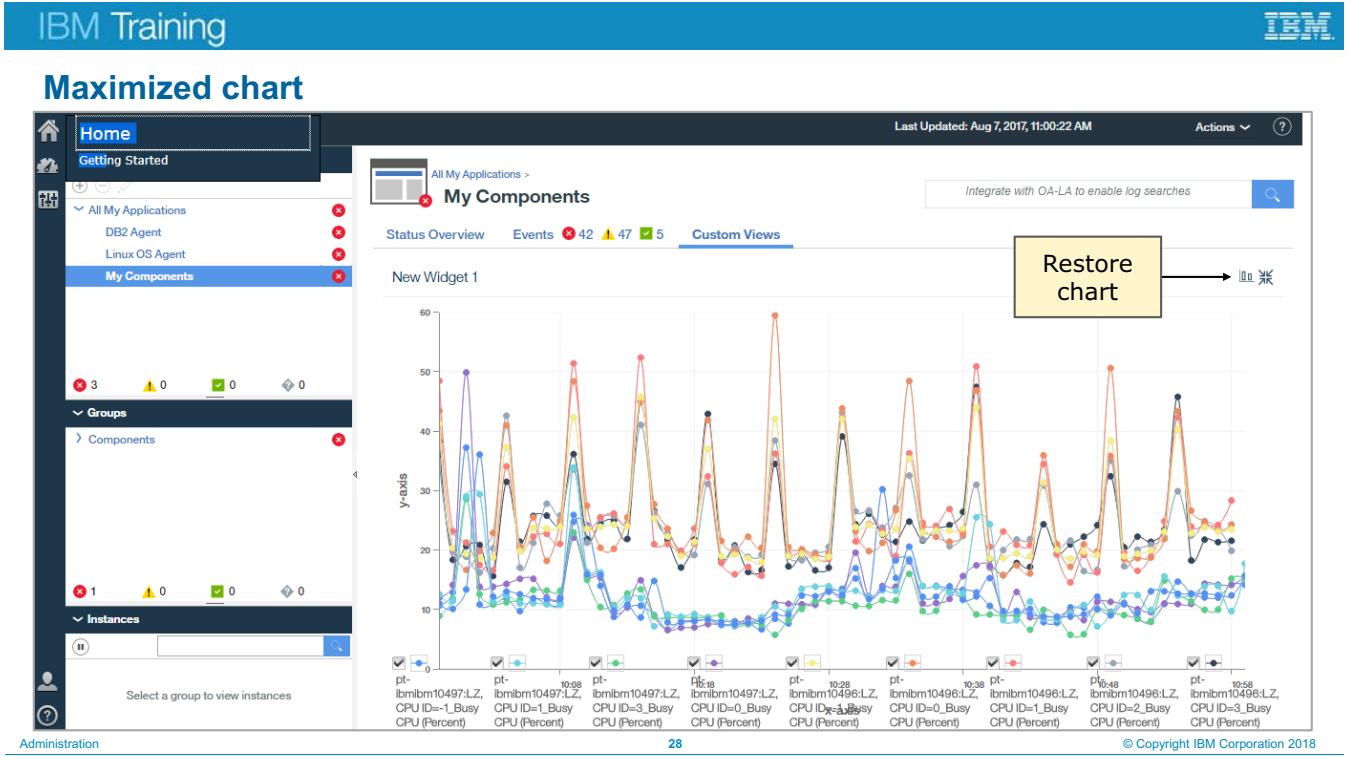
## Dashboard viewer in Custom Views

The screenshot shows the IBM Cloud APM console's 'Custom Views' feature. On the left, there's a navigation sidebar with 'Applications', 'Components', and 'Instances' sections. The main area displays a 'My Components' dashboard named 'LinuxDash5'. This dashboard includes a status overview with counts for red (3), yellow (0), green (0), and blue (0) components. It also features two data visualizations: 'New Widget 1' (a line chart with multiple series) and 'New Widget 2' (a table showing 'Write Time' and 'Instance Name' with corresponding 'Blocks Read' values). At the top right, there are buttons for 'Auto Refresh' and 'Maximize chart'. The bottom right corner includes a copyright notice for IBM Corporation 2018.

Dashboard viewer in Custom Views

Select any application, component, or instance from the Cloud APM console left navigation and click **Custom Views**.

- Dashboard Viewer: Shows the already created custom pages for the item that is selected in the left navigation.
- Apply Filter: View data for a required date, time, or interval by selecting it from the filter section. After selecting the values, click **Apply Filter**. The dashboard is refreshed with the data by the applied filter.
- Auto Refresh: The dashboard can be auto-refreshed by selecting the “Auto Refresh” option, which is off by default. The default interval for refresh is 1 minute
- Maximize: Click the Maximize button to maximize a chart.



Maximized chart

Click the Restore button to go back to the normal size.

## Viewing other pages and setting a default

The screenshot shows the IBM Application Dashboard interface. On the left, there's a sidebar with sections for Applications, Groups, and Instances. The main area is titled 'My Components' and shows a status overview with counts for errors (3), warnings (0), and successes (0). Below this is a 'Custom Views' tab. In the center, there's a dashboard titled 'LinuxDash5' with a line chart titled 'New Widget 1' showing data over time. To the right of the chart is a table titled 'New Widget 2' with columns for Write Time, Instance Name, and Blocks Read. A yellow callout box labeled 'Change page' points to the 'Custom Views' tab. Another yellow callout box labeled 'Set as default' points to a star icon next to the 'LinuxDash5' dashboard name.

### Viewing other pages and setting a default

Changing dashboards: Select a different dashboard from the dashboard menu.

Setting a default dashboard: Set a dashboard as the default by selecting the star icon in front of the dashboard name. Whenever the next user opens the Custom Views tab, the default dashboard is loaded.

## Page management options

The screenshot shows the IBM Application Dashboard interface. On the left, there's a sidebar with sections for Applications, Groups, and Instances. The main area displays a 'My Components' dashboard with a status overview showing 42 events, 53 warnings, and 5 successes. A 'Custom Views' tab is selected. Overlaid on the interface are several yellow callout boxes with arrows pointing to specific UI elements:

- A large yellow box labeled 'Create page' points to a '+' icon at the top right of the dashboard area.
- A yellow box labeled 'Edit page' points to a pencil icon on the right side of the dashboard.
- A yellow box labeled 'Delete page' points to a trashcan icon on the right side of the dashboard.

The central part of the dashboard features a chart titled 'New Widget 1' showing data over time from 09:32 to 10:32. Below the chart is a legend with five entries: pt-ibmibm10497:L..., pt-ibmibm10497:L..., pt-ibmibm10497:L..., pt-ibmibm10497:L..., and pt-ibmibm10497:L... . To the right of the chart is a table titled 'New Widget 2' with the following data:

| Write Time | Instance Name       | Blocks Read |
|------------|---------------------|-------------|
| 09:33      | pt-ibmibm10497:L... | 9,326,818   |
| 09:33      | pt-ibmibm10497:L... | 10,023      |
| 09:33      | pt-ibmibm10497:L... | 9,315,323   |
| 09:33      | pt-ibmibm10497:L... | 153,631,498 |
| 09:33      | pt-ibmibm10497:L... | 153,630,250 |
| 09:33      | pt-ibmibm10497:L... | 9,296,439   |
| 09:33      | pt-ibmibm10497:L... | 8,232       |
| 09:33      | pt-ibmibm10497:L... | 10,052      |
| 09:33      | pt-ibmibm10497:L... | 153,629,226 |

### Page management options

Page management offers the following options:

- Create Dashboard: Create a dashboard page by clicking the + icon.
- Edit Dashboard: Edit the current dashboard by clicking the Edit (pencil) icon.
- Delete Dashboard: Delete a dashboard page by clicking the Delete (trashcan) icon.

## Select a page template

The screenshot shows the IBM Application Dashboard interface. On the left, there's a sidebar with sections for Applications, Groups, and Instances. The 'My Components' section is currently selected. On the right, the main area displays 'All My Applications > My Components'. It shows status metrics: 3 red circles, 0 yellow triangles, 0 green checkmarks, and 0 blue diamonds. Below this, there are tabs for Status Overview, Events (42 errors, 44 warnings, 5 successes), and Custom Views. A search bar at the top right says 'Integrate with OA-LA to enable log searches'. A modal window titled 'Select a Template for your Custom Page' is open, showing five template options: 1X2 Template (2 boxes), 2X2 Template (4 boxes), 2X3 Template (6 boxes), 3X3 Template (9 boxes), and a 3X1 Template (3 boxes). A 'Back' button is in the top right of the modal. At the bottom of the dashboard, there's an 'Administration' link and a copyright notice: '© Copyright IBM Corporation 2018'.

Select a page template

To select a template page, select the preferred template from the page. Each template has a distinct number and layout of chart widgets. Clicking any of the templates opens the new page where a user can set the dashboard properties. A user can go back to the Dashboard page by clicking the “Back” button.

The screenshot shows the 'Dashboard page editor' interface. On the left, a sidebar navigation includes 'Applications' (All My Applications, DB2 Agent, Linux OS Agent), 'Groups' (Components), and 'Instances'. The main content area is titled 'My Components' and contains a chart labeled 'LinuxDash5'. A yellow box highlights the 'Page name' field, which is set to 'LinuxDash5'. Another yellow box highlights the 'Page time frame' button. On the right, there are buttons for 'Save page' and 'Set Default Timeframe for Page' (set to '1 hour'). A table with six rows and five columns is also visible.

### Dashboard page editor

The dashboard opens in the dashboard editor. Edit the page.

- Dashboard page name: Enter a name for the page.
- Page time frame: Set the default time frame for the data in the “Set Default time frame for page” drop-down list.
- Save: Click **Save** to save changes to the page.
- Edit the chart type, metric, widget names, and template from this page.

The screenshot shows the IBM Application Dashboard interface. On the left, there's a sidebar with sections for Applications, Groups, and Instances. The main area is titled 'My Components' and contains a 'Status Overview' section with counts for errors (3), warnings (0), and successes (0). Below this is a 'Custom Views' tab, which is selected. A specific view named 'LinuxDash5' is displayed, featuring a line chart with two data series (red and green) and a table with five columns labeled 'Column Title 1' through 'Column Title 5'. A yellow box highlights the 'Edit template' button at the top right of the view area. The bottom of the screen shows a footer with copyright information.

### Edit template

In the edit template page, edit the template length and width. Save the edited template by clicking the “Edit template” icon again.

## Set chart properties

The screenshot shows the IBM Application Dashboard interface. On the left, there's a sidebar with sections for Applications, Groups, and Instances. The main area is titled 'My Components' and displays a chart with red and green data points. A yellow box highlights the 'Chart name' field. To the right, a modal window titled 'Chart properties' is open, showing options for selecting a chart type (Line, Area, Bar, Grid) and adding X and Y axis labels. There are also checkboxes for 'Show Legend' and 'Show Interpolation'. The status bar at the bottom indicates 'Last Updated: Aug 4, 2017, 6:42:54 PM'.

### Set chart properties

To set chart properties, proceed as follows:

- Chart name: Edit the widget names by clicking the pencil icon on each chart widget.
- Chart properties: Click the Chart properties icon to set its properties.
- Select the chart type to be used for the widget. Available options are Line, Area, Chart, and Grid.
- Add the X-axis and Y-axis labels from this window.
- Select or clear “Show Legend” and “Show Interpolation” options.

## Set chart metric (1 of 2)

The screenshot shows the IBM Application Performance Dashboard interface. On the left, there's a navigation sidebar with sections like 'Performance', 'All My Applications', 'My Components', 'Groups', and 'Instances'. The main area is titled 'My Components' and displays status metrics for various components. A modal window titled 'Select Metric' is open in the center, prompting the user to define a metric group. It includes fields for 'Resource Type' (set to 'Linux OS'), 'Metric Type' (set to 'KLZ\_CPU'), 'Metric' (set to 'Busy CPU (Percent)'), and 'Resource Instance' (set to '\*'). Below these, there's a 'Set Condition for Metric Group' section with a 'WHERE' clause: 'CPU ID = \*'. There are also buttons for 'Actions' and '+ Add Another Metric'.

### Set chart metric (1 of 2)

Select Metric: Select the metric to be shown on the widget from this window.

- Resource Type shows the available resources for the selected application.
- Metric type shows the available metric types for the selected resource type.
- The Metric drop-down list shows the available metric for the selected Resource type and Metric type combination.
- Resource instance shows the available instances for the selected Resource type. If the user selected "\*" in the instance list, then the chart shows the data of all the instances for that particular application and resource type.

## Set chart metric (2 of 2)

The screenshot shows the IBM Application Dashboard interface. On the left, there's a sidebar with 'Applications', 'Groups', and 'Instances'. The main area is titled 'My Components' with tabs for 'Status Overview', 'Events', and 'Custom Views'. A modal window titled 'Select Metric' is open, showing fields for 'Resource Type' (Linux OS), 'Metric Type' (KLZ\_CPU), 'Metric' (Busy CPU (Percent)), 'Resource Instance' (pt-lbmbm10497:1), and a 'Set Condition for Metric Group' section where 'CPU ID = 1' is selected. The 'Actions' row contains icons for edit, save, and delete.

### Set chart metric (2 of 2)

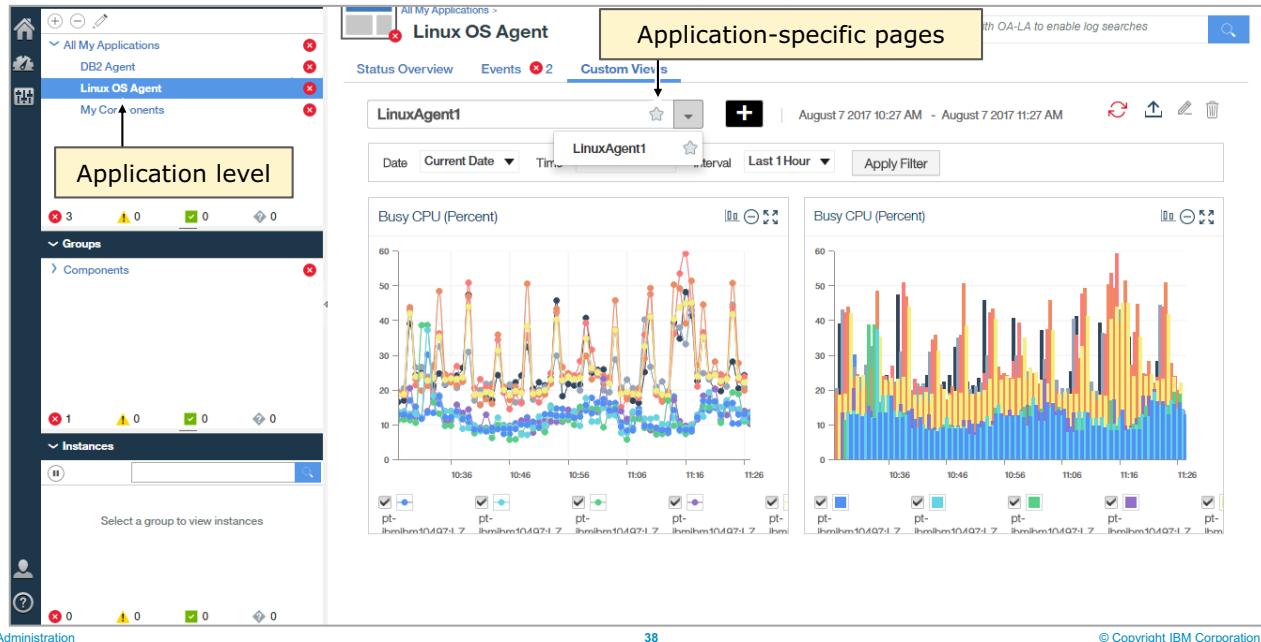
- Resource instance: If any instance is selected in the drop-down list, then the chart shows the data of only that instance.
- Condition: Set the condition for the selected metric for an instance. This option is not available if '\*' is selected as the instance. Save or delete the selected metric by using the icons in the same row. Add more metrics by using the **Add Another Metric** option.

The screenshot shows the IBM Application Dashboard interface. On the left, there's a sidebar with sections for Applications, Groups, and Instances. The main area is titled 'My Components' and contains a status overview with counts for errors (3), warnings (0), successes (0), and pending (0). Below this is a 'Custom Views' tab, which is currently selected. A modal window titled 'LinuxDash5' is open, displaying a green checkmark icon and the message 'LinuxDash5 dashboard saved successfully'. In the background, there's a line chart with red data points showing a downward trend from left to right. To the right of the chart is a table with five columns labeled 'Column Title 1' through 'Column Title 5', each containing six rows of placeholder text.

Save and preview the page

Save the dashboard page before preview. Click the preview button to view the page with the defined charts.

## Context-specific dashboards: Application (1 of 2)



Context-specific dashboards: Application (1 of 2)

Context-specific dashboard listing: A dashboard that is created at the application level from the left navigation for a particular application is visible for only that application. For example, if the user created the dashboard for the Linux OS Agent application, it is not visible for the DB2 agent application or any other application, component, or instance.

## Context-specific dashboards: Application (2 of 2)

The screenshot shows the IBM Monitoring and Analytics interface. On the left, there's a navigation sidebar with sections for Applications, Groups, and Instances. Under Applications, 'DB2 Agent' is selected, highlighted with a blue border. A callout box labeled 'Application level' points to this selection. The main dashboard area has a title 'All My Applications > DB2 Agent' and a sub-section titled 'Application-specific pages'. Below this are tabs for 'Status Overview', 'Events' (with 8 items), and 'Custom Views'. The 'Custom Views' tab is currently active, indicated by a blue underline. A callout box labeled 'Application-specific pages' points to this tab. The dashboard displays two cards: 'Maximum Connection' (a line chart showing values from 0 to 40 over time from 10:39 to 11:19) and a table of 'Maximum Connection' data. The table has columns for 'Write Time', 'Instance Name', and 'Maximum Connection'. The data shows multiple entries for 'db2apm: pt-ibmib...' at various times between 10:30 and 10:32, all with a maximum connection value of 40.

| Write Time | Instance Name       | Maximum Connection |
|------------|---------------------|--------------------|
| 10:30      | db2apm: pt-ibmib... | 40                 |
| 10:30      | db2apm: pt-ibmib... | 40                 |
| 10:30      | db2apm: pt-ibmib... | 40                 |
| 10:31      | db2apm: pt-ibmib... | 40                 |
| 10:31      | db2apm: pt-ibmib... | 40                 |
| 10:31      | db2apm: pt-ibmib... | 40                 |
| 10:32      | db2apm: pt-ibmib... | 40                 |
| 10:32      | db2apm: pt-ibmib... | 40                 |

Context-specific dashboards: Application (2 of 2)

If the user created the dashboard for the DB2 agent application, it is not visible for the Linux OS Agent application or any other application, component, or instance.

## Context-specific dashboards: Component

The screenshot shows the IBM Operations Analytics - Log Analysis interface. On the left, the navigation pane displays 'Applications' (DB2 Agent, Linux OS Agent, My Components), 'Groups' (Components, Linux OS), and instances (pt-ibmibm10497:LZ, pt-ibmibm10496:LZ). A yellow box highlights the 'Component level' under 'Components'. In the center, a dashboard titled 'LinuxComp1' is displayed for the 'Linux OS Agent' component. The dashboard includes a 'Status Overview' section with event counts (0 red, 2 yellow, 0 green, 0 grey) and a 'Custom Views' tab. Below this are two line charts: 'Busy CPU (Percent)' and 'System CPU (Percent)', both showing data from August 7, 2017, 10:34 AM to 11:34 AM. The 'Busy CPU' chart shows spikes reaching up to 60%, while the 'System CPU' chart remains relatively stable around 8%. A legend at the bottom of each chart lists various process names with corresponding colored squares.

Context-specific dashboards: Component

Context-specific dashboard listing continued: The dashboard that is created at the application level is not available for the components or the instance of the same application. The components or instances level shows only the dashboard that is created at that level.

## Context-specific dashboards: Instance \*

The screenshot shows the IBM APM interface. On the left, there's a navigation tree under 'My Components' for the DB2 component, listing various DB2 instances. One instance, 'db2apm:pt-ibmibm10496:UD', is selected. To the right, a detailed dashboard for this instance is displayed. The dashboard has tabs for 'Status Overview', 'Events', 'Custom Views' (which is currently selected), and 'Attribute Details'. The main area of the dashboard is titled 'DB2InstanceDash1'. It includes a chart titled 'Maximum Con...' showing a metric over time, a table for 'Resource Instance' with one entry marked with an orange box, and a table for 'Actions'. A yellow box labeled 'Instance-specific pages' points to the 'Custom Views' tab, and another yellow box labeled 'Instance level' points to the DB2 instance in the navigation tree.

Context-specific dashboards: Instance \*

Context-specific instance \*: A dashboard that is created at the instance level with the “Resource Instance” as \* is visible for all the instances of that application and component combination.

Here “DB2InstanceDash1” was created having \* in the resource instance for the instance **db2apm:pt-ibmibm10496:UD** selected in the left navigation. The DB2InstnaceDash1 dashboard is visible under the instance in the left menu and under the DB2 component and any application that has that instance.

# Lesson 4 Using attribute details to access data from an agent

IBM Training



## Lesson 4: Using attribute details to access data from an agent

- All data that is collected by monitoring agents is available from the attribute details feature
- Not all data that an agent collects is displayed in a widget
- You access the attribute details for a monitoring agent instance by selecting the attribute details tab

In this lesson, you learn how to do the following tasks:

- Access attribute details from a monitoring agent
- Save attribute details customizations for later use
- Share attribute details customizations with other users

## Viewing attribute details (1 of 2)

The screenshot shows the IBM Application Dashboard interface. The top navigation bar includes links for 'All My Applications', 'DayTrader', 'Components', 'WebSphere Application Server', and 'lin1Node01server1:lin1:KYNS'. The main content area has tabs for 'Status Overview', 'Events' (selected), and 'Attribute Details'. Under 'Attribute Details', there is a form with fields for 'Enter title' (set to 'Garbage\_Collection\_Analysis'), 'Choose a type' (radio buttons for 'Real time' and 'Historical' - the latter is selected), 'Choose a chart or table' (with a chart icon), and 'Choose the metrics:' (a list of data sets). A 'Filter' button is also present. To the right, a list of attributes is shown with checkboxes, where most are checked. A red arrow points to the 'Attributes' checkbox at the top of the list.

| Attributes   |
|--|
| <input checked="" type="checkbox"/> ASID                     |
| <input checked="" type="checkbox"/> GC Rate (per min)        |
| <input checked="" type="checkbox"/> Heap Used (%)            |
| <input checked="" type="checkbox"/> Kbytes Free              |
| <input checked="" type="checkbox"/> Kbytes Max Heap          |
| <input checked="" type="checkbox"/> Kbytes Total Freed by GC |
| <input checked="" type="checkbox"/> Kbytes Used              |
| <input checked="" type="checkbox"/> Node Name                |
| <input checked="" type="checkbox"/> Origin Node              |

### Viewing attribute details (1 of 2)

The attributes that are included in the Dashboard widgets cannot be changed. Therefore, if you want to see something that is not already on the dashboard, you can use the Attribute Details feature to view the values.

1. To view attribute details, click a component instance to select it, and click the Attribute Details tab, as shown in this example.
2. Select a type, real-time or historical.
3. Select whether you want a chart or a table.
4. Select the data set, also known as attribute group, that contains the attributes of interest. You can select only one data set at a time. Click each attribute that you want to see. Clicking the box marked Attributes selects them all.
5. Click **Preview Results**. The attributes that are included in the Dashboard widgets cannot be changed. Therefore, if you want to see something that is not already on the dashboard, you can use the Attribute Details to view the values.

## Viewing attribute details (2 of 2)

All My Applications > DayTrader > Components > WebSphere Application Server > lin1Node01server1:lin1:KYNs

Status Overview Events Attribute Details

Last Saved: Save date unknown Last Refresh: May 7, 2016, 9:52:47 PM

Garbage\_Collection\_Analysis ~ Filter

No filter applied

| Kbytes Used | Times Run | Process ID | Real Time (ms) | Real Time (%) | Origin Node                    | Kbytes Max Heap | Kbytes Total Freed by GC | Node Name | GC Rate (per min) | ASID | Summary | Server Name | Kbytes Free |
|-------------|-----------|------------|----------------|---------------|--------------------------------|-----------------|--------------------------|-----------|-------------------|------|---------|-------------|-------------|
| 116913      | 4         | 10182      | 49             | 0.0           | lin1Node01server1:lin1: 262144 | 50828           | 0                        | lin1      | 3,999             | N/A  | No      | server1     | 39459       |
| 116352      | 3         | 10182      | 31             | 0.0           | lin1Node01server1:lin1: 262144 | 42618           | 0                        | lin1      | 2,999             | N/A  | No      | server1     | 39920       |
| 116070      | 2         | 10182      | 13             | 0.0           | lin1Node01server1:lin1: 262144 | 29469           | 0                        | lin1      | 2,000             | N/A  | No      | server1     | 42022       |
| 117842      | 9         | 10182      | 103            | 0.1           | lin1Node01server1:lin1: 262144 | 43205           | 0                        | lin1      | 2,999             | N/A  | No      | server1     | 45494       |
| 117894      | 3         | 10182      | 38             | 0.0           | lin1Node01server1:lin1: 262144 | 42759           | 0                        | lin1      | 3,000             | N/A  | No      | server1     | 40840       |
| 117588      | 4         | 10182      | 32             | 0.0           | lin1Node01server1:lin1: 262144 | 57137           | 0                        | lin1      | 4,000             | N/A  | No      | server1     | 40748       |
| 117220      | 3         | 10182      | 42             | 0.0           | lin1Node01server1:lin1: 262144 | 42968           | 0                        | lin1      | 2,998             | N/A  | No      | server1     | 41115       |
| 117102      | 3         | 10182      | 13             | 0.0           | lin1Node01server1:lin1: 262144 | 42894           | 0                        | lin1      | 2,999             | N/A  | No      | server1     | 41234       |
| 116785      | 3         | 10182      | 19             | 0.0           | lin1Node01server1:lin1: 262144 | 43275           | 0                        | lin1      | 3,001             | N/A  | No      | server1     | 41679       |
| 116857      | 3         | 10182      | 20             | 0.0           | lin1Node01server1:lin1: 262144 | 43370           | 0                        | lin1      | 2,998             | N/A  | No      | server1     | 41857       |
| 116558      | 3         | 10182      | 13             | 0.0           | lin1Node01server1:lin1: 262144 | 43108           | 0                        | lin1      | 2,998             | N/A  | No      | server1     | 41906       |
| 116135      | 3         | 10182      | 12             | 0.0           | lin1Node01server1:lin1: 262144 | 43285           | 0                        | lin1      | 2,999             | N/A  | No      | server1     | 42329       |
| 115935      | 3         | 10182      | 16             | 0.0           | lin1Node01server1:lin1: 262144 | 43447           | 0                        | lin1      | 2,999             | N/A  | No      | server1     | 42529       |
| 115707      | 3         | 10182      | 13             | 0.0           | lin1Node01server1:lin1: 262144 | 43602           | 0                        | lin1      | 3,000             | N/A  | No      | server1     | 42885       |
| 115532      | 2         | 10182      | 12             | 0.0           | lin1Node01server1:lin1: 262144 | 20903           | 0                        | lin1      | 2,000             | N/A  | No      | server1     | 43060       |
| 115507      | 4         | 10182      | 23             | 0.0           | lin1Node01server1:lin1: 262144 | 58276           | 0                        | lin1      | 3,999             | N/A  | No      | server1     | 43085       |
| 115842      | 3         | 10182      | 13             | 0.0           | lin1Node01server1:lin1: 262144 | 43294           | 0                        | lin1      | 2,999             | N/A  | No      | server1     | 43450       |

Administration

44

© Copyright IBM Corporation 2018

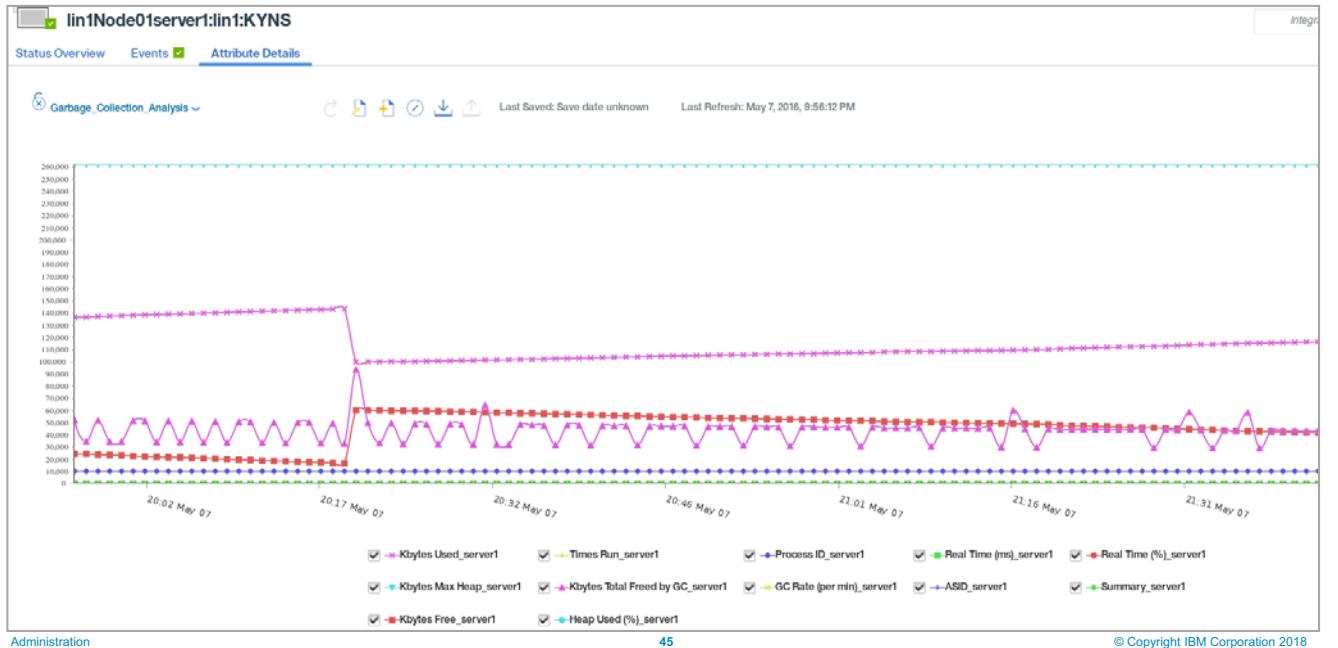
### Viewing attribute details (2 of 2)

This slide shows an example of selected attribute details from the prior slide. This example is of the Monitoring Agent for WebSphere Application Server Garbage Collection Analysis data set.

Depending on how many attributes you selected, you might need to scroll horizontally to see all of them.

Click the Reset tool in the upper-right corner to return to change the time frame for the historical data.

## Line charts with the attribute details



*Line charts with the attribute details*

You can also select a line chart. Only attributes that are collected with historical data are able to be charted with the line chart.

## Saving Attribute detail tables and charts (1 of 2)

The screenshot shows the Application Dashboard interface. On the left, there's a chart titled "Garbage Collection Analysis" with three data series: a purple line, a red line, and a blue line. The purple line has a significant spike around March 17, 2017. On the right, there's a configuration panel for saving the chart. A red arrow points to the "New" button in the top right corner of the chart area. Another red arrow points to the "Enter title" field where "Garbage Collection Analysis over the past 2 hours" is typed. A third red arrow points to the preview window below, which shows the same chart with the new title.

### Saving Attribute detail tables and charts (1 of 2)

You can provide a name of a chart or a table to save the customization.

1. When you are looking at a chart or a table you want to save with a title, select **New**.
2. Type a title that you want to use.
3. Select **Preview Results** again.

## Saving Attribute detail tables and charts (2 of 2)

All My Applications > DayTrader > Components > WebSphere Application Server > lin1Node01server1:lin1:KYNS

Status Overview Events  Attribute Details

Garbage Collection Analysis for last 2 hours

Last Saved: Save date unknown

Attribute Details

Last Saved: Save date unknown

Save for Me

Save to Share

Administration 47 © Copyright IBM Corporation 2018

### Saving Attribute detail tables and charts (2 of 2)

The table or chart is presented.

4. Select Save for Me or Save to Share to save your customization for either yourself or for others also.

## Deleting saved tables and charts



Administration

48

© Copyright IBM Corporation 2018

### Deleting saved tables and charts

When you save a chart, you can delete it by selecting the Delete button.

# Lesson 5 Managing users in the Cloud APM console

IBM Training



## Lesson 5: Managing users in the Cloud APM console

You manage user security with several tools in Cloud APM:

- Lightweight Directory Access Protocol (LDAP) or `basicRegistry.xml`
  - These tools manage users, groups, and passwords
- Role Base Access Control
  - A role is a group of permissions that control the actions you can perform in Cloud APM
  - Use the role-based access control page to manage users and roles
  - This tool manages which users can do which operations

In this lesson, you learn how to do the following tasks:

- Use local files to define users and groups.
- Configure Cloud APM to use Lightweight Directory Access Protocol (LDAP) to define users and groups.
- Manage user authority with Cloud APM by using role-based access control.

## Integrating LDAP with Cloud APM (1 of 3)

1. To configure Cloud APM to use LDAP for user authentication, update the `ldapRegistry.xml` file with your LDAP server information
2. By default, `ldapRegistry.xml` is in this directory on the Cloud APM server:

`/opt/ibm/wlp/usr/shared/config`

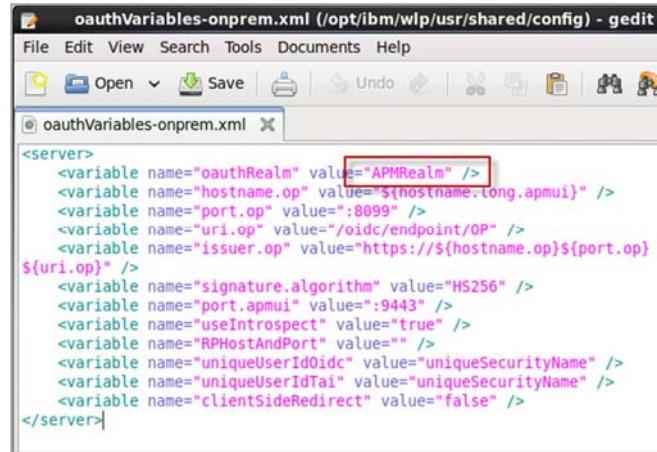
```
<server>
<ldapRegistry id="IBMDirectoryServer1_DAP" realm="APMRealm"
host="192.168.1.101" port="389" ignoreCase="true"
baseDN="cn=APMRealm,ou=admins,o=ibm,c=edu"
ldapTypes="IBM iSeries Directory Server"
searchTimeout="1m"
connectTimeout="2m"
reuseConnection="true"
bindDN="cn=root" bindPassword="{xor}MD010jwrb28="
<idsFilters
  userFilter="(&uid=%v)(objectclass/inetOrgPerson)"
  groupFilter="(&(cn=%v)(|(objectclass/groupOfNames)
  (objectclass/groupOfUniqueNames)(objectclass/groupOfURLs)))"
  userIdMap="*:uid"
  groupIdMap="*:cn"
  groupMemberIdMap="ibm-allGroups:member;ibm-
allGroups:uniqueMember;groupOfNames:member;groupOfUniqueNames:uniqueMember" />
<contextPool enabled="false" initialSize="1" maxSize="0"
timeout="0ms" waitTime="3000ms" preferredSize="3"/>
</ldapRegistry>
</server>
```

### Integrating LDAP with Cloud APM (1 of 3)

This slide shows the key configuration file, `ldapRegistry.xml`, configured to connect to an LDAP on another server.

## Integrating LDAP with Cloud APM (2 of 3)

3. Update the realm name `oauthRealm` value in the `oauthVariables-onprem.xml` file in the `/opt/ibm/wlp/usr/shared/config` directory to match the realm name that is used in LDAP



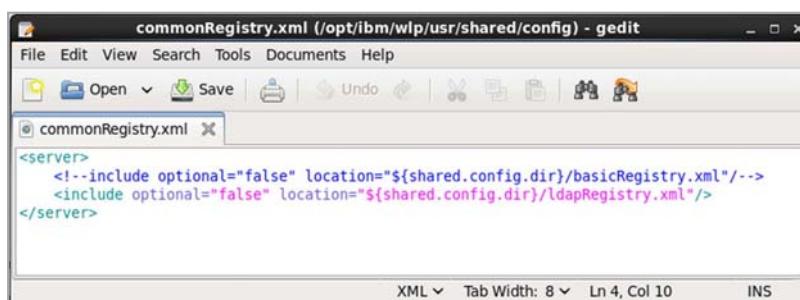
```
<server>
<variable name="oauthRealm" value="APMRealm" />
<variable name="hostname.op" value="${hostname.long.apmui}" />
<variable name="port.op" value=":8099" />
<variable name="uri.op" value="/oidc/endpoint/OP" />
<variable name="issuer.op" value="https://${hostname.op}${port.op}
${uri.op}" />
<variable name="signature.algorithm" value="HS256" />
<variable name="port.apmui" value=":9443" />
<variable name="useIntrospect" value="true" />
<variable name="RPHostAndPort" value="" />
<variable name="uniqueUserId0idc" value="uniqueSecurityName" />
<variable name="uniqueUserIdTai" value="uniqueSecurityName" />
<variable name="clientSideRedirect" value="false" />
</server>
```

### Integrating LDAP with Cloud APM (2 of 3)

This slide shows the configuration file, `oauthVariables-onprem.xml`, configured to connect to the APMRealm on an LDAP server.

## Integrating LDAP with Cloud APM (3 of 3)

4. Update the `commonRegistry.xml` file in the `/opt/ibm/wlp/usr/shared/config` directory to use `ldapRegistry.xml` and save the file
5. Update change the comment lines to use the LDAP registry instead of the common registry

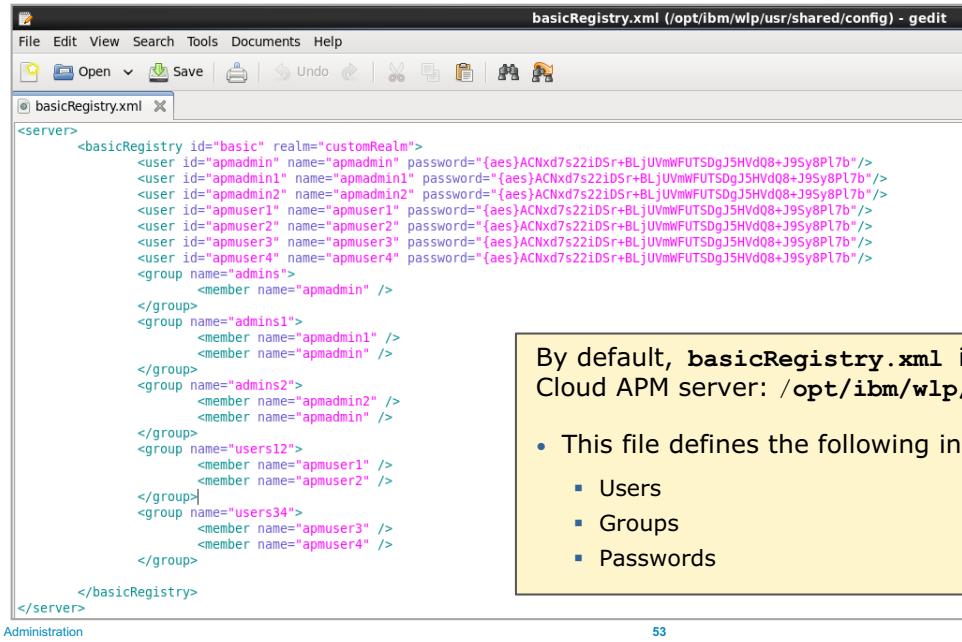


```
commonRegistry.xml (/opt/ibm/wlp/usr/shared/config) - gedit
File Edit View Search Tools Documents Help
Open Save Undo XML
commonRegistry.xml
<server>
    <!--include optional="false" location="${shared.config.dir}/basicRegistry.xml"-->
    <include optional="false" location="${shared.config.dir}/ldapRegistry.xml"/>
</server>

XML Tab Width: 8 Ln 4, Col 10 INS
```

6. Update the `cscsRoleAdmin.new` file with the `apmadmin` information, for example:  
`user:APMRealm/cn=apmadmin,cn=APMRealm,ou=admins,o=ibm,c=edu`
7. Recycle the Cloud APM server

## basicRegistry.xml



```

<server>
  <basicRegistry id="basic" realm="customRealm">
    <user id="apmadmin" name="apmadmin" password="{aes}ACNx7s221D5r+BLjUVMwFUTSDgJ5HvdQ8+J95y8Pl7b"/>
    <user id="apmadmin1" name="apmadmin1" password="{aes}ACNx7s221D5r+BLjUVMwFUTSDgJ5HvdQ8+J95y8Pl7b"/>
    <user id="apmadmin2" name="apmadmin2" password="{aes}ACNx7s221D5r+BLjUVMwFUTSDgJ5HvdQ8+J95y8Pl7b"/>
    <user id="apmuser1" name="apmuser1" password="{aes}ACNx7s221D5r+BLjUVMwFUTSDgJ5HvdQ8+J95y8Pl7b"/>
    <user id="apmuser2" name="apmuser2" password="{aes}ACNx7s221D5r+BLjUVMwFUTSDgJ5HvdQ8+J95y8Pl7b"/>
    <user id="apmuser3" name="apmuser3" password="{aes}ACNx7s221D5r+BLjUVMwFUTSDgJ5HvdQ8+J95y8Pl7b"/>
    <user id="apmuser4" name="apmuser4" password="{aes}ACNx7s221D5r+BLjUVMwFUTSDgJ5HvdQ8+J95y8Pl7b"/>
    <group name="admins">
      <member name="apmadmin" />
    </group>
    <group name="admins1">
      <member name="apmadmin1" />
      <member name="apmadmin" />
    </group>
    <group name="admins2">
      <member name="apmadmin2" />
      <member name="apmadmin" />
    </group>
    <group name="users12">
      <member name="apmuser1" />
      <member name="apmuser2" />
    </group>
    <group name="users34">
      <member name="apmuser3" />
      <member name="apmuser4" />
    </group>
  </basicRegistry>
</server>

```

By default, **basicRegistry.xml** is in this directory on the Cloud APM server: `/opt/ibm/wlp/usr/shared/config`

- This file defines the following information:
  - Users
  - Groups
  - Passwords

*basicRegistry.xml*

This slide shows the **basicRegistry.xml** file that is used for the exercises. You define users and groups in the **basicRegistry.xml** file.

## Role-based access control (1 of 2)

- Role-based access control allows for administrators to manage what actions and resources other administrators and users can perform without service interruption
- Cloud APM has four default roles:
  - Role Administrator
  - Monitoring Administrator
  - System Administrator
  - Monitoring User
- Security policies are applied immediately

### *Role-based access control (1 of 2)*

Role-based access control allows for administrators to manage what actions and resources other administrators and users can do.

## Role-based access control (2 of 2)

Access can be restricted for individual users or user groups:

- By application instance
- By group instance
- By specific agents
  - Building applications
  - Building resource groups
  - Agent configuration
  - Private situations

### User interface

- RBAC component delivers UI page to manage permissions, roles, users, and user groups
- Authorized user can create, update, and delete roles
- Authorized user can assign and unassign permissions to roles
- Authorized user can assign users and user groups to role

## Default policy structure (1 of 2)

|   | Role Administrator |        | Monitoring Administrator |        | System Administrator |        | Monitoring User |        |
|---|--------------------|--------|--------------------------|--------|----------------------|--------|-----------------|--------|
|   | View               | Modify | View                     | Modify | View                 | Modify | View            | Modify |
| <b>System configuration permissions</b> |                    |        |                          |        |                      |        |                 |        |
| Advanced configuration                  | ✓                  | N/A    | —                        | N/A    | ✓                    | N/A    | —               | N/A    |
| Agent configuration                     | ✓                  | N/A    | ✓                        | N/A    | —                    | N/A    | —               | N/A    |
| Informational pages                     | ✓                  | N/A    | ✓                        | N/A    | ✓                    | N/A    | ✓               | N/A    |
| Search provider                         | ✓                  | N/A    | ✓                        | N/A    | —                    | N/A    | —               | N/A    |
| Usage statistics                        | ✓                  | N/A    | ✓                        | N/A    | —                    | N/A    | —               | N/A    |

### Default policy structure (1 of 2)

This slide shows the permissions that are granted to the default policies. A check mark indicates that members of this role have this permission. A dash indicates that members of this role do not have this permission. N/A indicates that this permission does not exist.

## Default policy structure (2 of 2)

|                                   | Role Administrator |   | Monitoring Administrator |        | System Administrator |        | Monitoring User |        |
|-----------------------------------|--------------------|---|--------------------------|--------|----------------------|--------|-----------------|--------|
|                                   | View               | Modify  | View                     | Modify | View                 | Modify | View            | Modify |
| <b>Resource permissions</b>       |                    |   |                          |        |                      |        |                 |        |
| Application Performance Dashboard | ✓                  | ✓   | ✓                        | ✓      | ✓                    | —      | ✓               | —      |
| Applications                      | ✓                  | ✓   | ✓                        | ✓      | —                    | —      | ✓               | —      |
| <i>Individual Application</i>     |                    | <u>Application and resource group permissions</u> |                          |        |                      |        |                 |        |
| Diagnostics Dashboard             | ✓                  | N/A   | ✓                        | N/A    | —                    | N/A    | ✓               | N/A    |
| Resource Group Manager            | ✓                  | N/A   | ✓                        | N/A    | —                    | N/A    | —               | N/A    |
| <i>Individual Resource group</i>  |                    | <u>Application and resource group permissions</u> |                          |        |                      |        |                 |        |
| Resource Groups                   | ✓                  | ✓   | ✓                        | ✓      | —                    | —      | —               | —      |
| Synthetic Script Manager          | ✓                  | N/A   | ✓                        | N/A    | ✓                    | N/A    | —               | N/A    |
| Threshold Manager                 | ✓                  | N/A   | ✓                        | N/A    | —                    | N/A    | —               | N/A    |

The screenshot shows two windows side-by-side. On the left is the 'IBM Training' interface with a sidebar containing icons for Home, Advanced Configuration, Agent Configuration, Role Based Access Control (which has a red arrow pointing to it), Threshold Manager, Synthetic Script Manager, and Resource Group Manager. The main area displays the 'System Configuration' section. On the right is a Firefox browser window titled 'IBM Performance Management - Mozilla Firefox' with the URL <https://apm.ibm.edu:9443/#com.ibm.smai.rbac.ui>. The page is titled 'Role Based Access Control' and describes managing user access using roles. It features three tabs: 'Roles' (which is selected and highlighted with a red arrow), 'User Groups', and 'Individual Users'. Below the tabs is a table with columns 'Role' and 'Description'. The table lists four roles: 'Monitoring Administrator', 'Monitoring User', 'Role Administrator', and 'System Administrator', each with a detailed description. At the top of the table are icons for adding (+), deleting (-), and editing (pencil). A filter box is also present at the top.

## Roles

The Role Based Access Control main page contains three tables:

- Roles table
- User Groups table
- Individual Users table

Use the highlighted icons to add, delete, or edit a role.

Users can navigate between them by using the tabs on the left side. All RBAC pages have a link to the help page in the upper-right corner and a breadcrumb trail in the upper-left corner. Every table provides a filter box for easy search.

## Individual users

The screenshot shows two panels. The left panel is titled 'Individual Users' and lists users: apmadmin, apmadmin2, apmadmin3, apmuser3, apmuser4, apmuser1, and apmuser2. The user 'apmadmin3' is selected and highlighted with a blue border. A red arrow points from the 'Edit' button at the top right of this panel to the 'Edit' button in the second panel. The right panel is titled 'Roles' and lists four roles: Monitoring Administrator, Monitoring User, Role Administrator, and System Administrator. The 'Monitoring Administrator' and 'Role Administrator' checkboxes are checked. Red arrows point from the checked checkboxes in the first panel to the corresponding checked checkboxes in the second panel.

| Role   | Description   |
|--|---|
| <input checked="" type="checkbox"/> Monitoring Administrator | Users whose primary job function is to use Performance Management to monitor systems. Performs tasks such as adding monitoring applications, creating thresholds, adding groups of resources, and distributing the thresholds to these resource groups. |
| <input type="checkbox"/> Monitoring User                     | Users whose primary job function is to configure and maintain the health and state of systems that are monitored by Performance Management.   |
| <input checked="" type="checkbox"/> Role Administrator       | Users whose primary job function is to create access control policies for Performance Management. This role has all permissions.  |
| <input type="checkbox"/> System Administrator                | Users whose primary job function is to perform administration tasks for the Performance Management system. Performs tasks such as configuring the Event Manager, or configuring the Hybrid Gateway.   |

Administration

59

© Copyright IBM Corporation 2018

Individual users

Select the **Individual User** tab and a user. Click **Edit**.

On the next screen, you can select and assign multiple roles to the user.

## User groups

The screenshot shows the 'Role Based Access Control' section of the IBM Cloud APM console. On the left, there's a navigation bar with icons for Home, Applications, and Monitoring. The main area has tabs for 'Roles', 'User Groups' (which is selected and highlighted in blue), and 'Individual Users'. Below these tabs is a 'Filter' input field. The 'User Groups' section lists several groups: 'admins', 'admins1' (which is selected and highlighted with a red box and arrow), 'admins2', 'users12', and 'users34'. On the right, a 'User Group Editor' window is open, showing a table of roles with their descriptions. The 'Monitoring Administrator' role is selected (indicated by a checked checkbox and a red arrow). Other roles listed are 'Monitoring User', 'Role Administrator', and 'System Administrator'. The bottom right corner of the editor window contains the copyright notice: '© Copyright IBM Corporation 2018'.

Administration

60

© Copyright IBM Corporation 2018

### User groups

As with individual users, you can select and edit a group.

## New role creation and configuration

The image consists of two side-by-side screenshots of the IBM Cloud APM Role Editor. Both screenshots show a role named 'All Admins'.

**Left Screenshot (Assign Users to Role):** This section allows you to assign users and user groups to a role. It includes a 'User Groups' tab with a list of groups: 'users12', 'users34', 'admins2', 'admins', and 'admins1'. The 'admins2', 'admins', and 'admins1' entries have red arrows pointing to them, indicating they are selected. There is also a 'Show Only Selected' checkbox.

**Right Screenshot (Assign Permissions to Role):** This section allows you to assign permissions to the role. It has tabs for 'System Configuration Permissions' and 'Resource Permissions'. Under 'System Configuration Permissions', several checkboxes are checked: 'Advanced Configuration' (checked), 'Agent Configuration' (checked), 'Informational Pages' (checked), 'Search Provider' (checked), and 'Usage Statistics' (checked). Red arrows point to each of these checked boxes.

### New role creation and configuration

In Role Editor, you can create a new role, assign it to users and user groups, and configure permissions.

You can create new roles and choose names for them. In this example, the three admin groups are selected for inclusion in the All Admins group.

## New role creation and configuration: Resource permissions

The screenshot shows a user interface for managing resource permissions. On the left, there are two buttons: 'Assign Users to Role' and 'Assign Permissions to Role'. The 'Assign Permissions to Role' button is highlighted with a red arrow. The main area is titled 'Select the permissions you want to assign to the role.' It features a 'System Configuration' section and a 'Resource Permissions' section. The 'Resource Permissions' section is selected, indicated by a red arrow above the tab. Below this, there's a table with columns for 'Permissions' and 'View' and 'Modify' checkboxes. A 'Filter' input field is at the top of the table. Red arrows point to the 'View' and 'Modify' checkboxes for the first few items in the list. At the bottom right of the table are 'Cancel' and 'Save' buttons, with a red arrow pointing to the 'Save' button.

### New role creation and configuration: Resource permissions

You can restrict access to resources such as applications and resource groups.

## Example: A user with full permissions on a small test system

The screenshot shows the Application Dashboard interface. On the left, there's a sidebar with sections for Applications, Groups, and Instances. Under Applications, 'All My Applications' is expanded, listing 'DayTrader(WAS)', 'Keystone', 'My Components', 'My Transactions', 'MyFirstApp', 'MySecondApp', and 'MyThirdApp'. Each application entry includes status indicators (red circles) and a green checkmark icon. The main area is titled 'All My Applications' and displays a grid of application cards. Each card contains the application name, a 'Transactions' icon, a 'Components' icon, and an 'Events' icon. Below each card, there are two more icons: 'Components' and 'Events'. The cards are arranged in three rows: the first row has 'DayTrader(WAS)', 'Keystone', and 'My Components'; the second row has 'My Transactions', 'MyFirstApp', and 'MySecondApp'; the third row has 'MyThirdApp'. At the top right of the main area, there are filter options: 'Show Details' (checked), 'Filter by Status' (with checkboxes for red, yellow, green, and blue), and a button to 'Integrate with OA-LA to enable log searches'. The top right corner also shows 'Last Updated: Jan 16, 2018, 1:44:47 PM' and an 'Actions' dropdown.

*Example: A user with full permissions on a small test system*

The user `apmadmin` can log in with full permissions to access any applications, resources, or folders.

## Example: A user with no permissions



*Example: A user with no permissions*

The user apmuser3 can log in but is not in a group and has no permissions to access any applications, resources, or folders.

## Example: A user with no administrative permissions

The screenshot shows the Application Dashboard interface. On the left, there's a sidebar with sections for Applications, Groups, and Instances. The Applications section lists several applications: DayTrader(WAS), Keystone, My Components, My Transactions, MyFirstApp, MySecondApp, and MyThirdApp. Below this, it says "Select an application to view details". The Groups and Instances sections are empty, with "Select a group to view groups" and "Select a group to view instances" respectively. On the right, there's a main panel titled "All My Applications" showing a grid of application cards. The cards for DayTrader(WAS) and Keystone are highlighted in red, indicating they are in an error state. Other cards for My Transactions, MyFirstApp, and MyThirdApp are green, indicating they are in a healthy state. Each card has icons for Transactions, Components, and Events.

Administration

65

© Copyright IBM Corporation 2018

*Example: A user with no administrative permissions*

The user apmuser1 can log in, but is not in an administrative group and has no permissions to modify any applications, resources, or roles.

Observe that All My Applications shows both DayTrader(WAS) and Keystone applications.

## Example: A user with restricted application access

The screenshot shows the Application Dashboard of the IBM Cloud APM console. On the left, under 'Applications', the 'All My Applications' section is expanded, showing 'My Components' (green checkmark), 'My Transactions' (green checkmark), and 'MyFirstApp' (green checkmark). A red arrow points from the text 'Keystone and DayTrader(WAS) are missing' to the 'MyFirstApp' entry. The 'Groups' and 'Instances' sections below are collapsed. On the right, there are three cards: 'My Components' (Components: 1, Events: 6), 'My Transactions' (Transactions: 0, Events: 3), and 'MyFirstApp' (Components: 0, Events: 0). The top right corner shows 'Last Updated: Jan 16, 2018, 1:57:04 PM'. A red box highlights the 'MyFirstApp' card.

Keystone and DayTrader(WAS) are missing

Example: A user with restricted application access

This user can log in but is not in an administrative group and has no permissions to modify any applications, resources, or roles.

All My Applications shows only the MyFirstApp application. Access to all other applications is removed.

## Instructor demonstration



## Student exercises



Complete the exercises for this unit in the Course Exercises Guide.

## Summary

Now that you have completed this unit, you should be able to:

- Manage the Cloud APM server components
- Describe the major functions that are involved in managing applications
- Create custom views in the Cloud APM console
- Use attribute details to access data from an agent
- Manage users of the Cloud APM console



# Unit 5 Monitoring events

IBM Training



## Monitoring events

© Copyright IBM Corporation 2018  
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

This unit covers how to create, update, and delete thresholds, which in turn create events. You explore the Threshold Manager, where you create and modify thresholds that in turn create events when the thresholds defined are met. You also learn how to use the resource group manager. The resource group manager determines which agents that run on specific servers evaluate the thresholds that are defined.

## Learning objectives

After completing this unit, you should be able to:

- Describe the use of events in Application Performance Management
- Describe how thresholds are used to create events
- Create resource groups to manage the events for managed systems in your enterprise

### *Learning objectives*

This slide lists the objectives for the unit.

## Unit outline

- Lesson 1: Understanding events
- Lesson 2: Creating thresholds by using the Threshold Manager
- Lesson 3: Managing resource groups

### *Unit outline*

This slide lists the unit outline.

# Lesson 1 Understanding events

IBM Training



## Lesson 1: Understanding events

- Event thresholds detect specific application behaviors and conditions based on actively monitored definitions
- Thresholds compare the sampled value of an attribute with the value set in the threshold
  - If the sampled value satisfies the comparison, an event is opened
  - The event closes automatically when the threshold comparison is no longer true
- Predefined thresholds are available for each agent, and you can define new thresholds for monitoring
- In the Application Performance Dashboard, after you select an application, the Events tab is displayed
- The Events tab shows the open events for the current application
- You can drill down to detailed dashboards with performance metrics to help you determine the cause of the event

In this lesson, you learn how to view events in Cloud APM.

## Event indicators

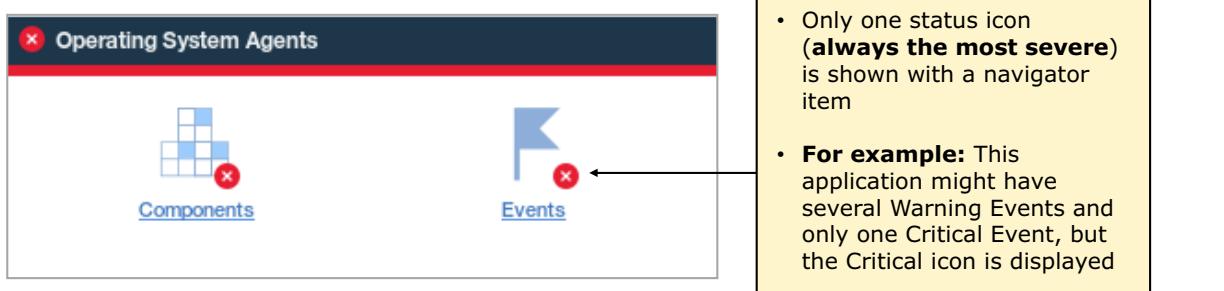
The screenshot shows the Application Dashboard interface. On the left, there's a sidebar with 'Applications' and 'Groups' sections. Under 'Applications', 'All My Applications' is expanded, listing Portfolio Management, My Components, Finance Management, Credit Card Processing, Partner Network, Preferred Customer Account Mana..., and Fleet Management. Below the list are status counts: Red (x) 2, Yellow (⚠) 2, Green (✓) 6, and Grey (diamond) 0. A note says 'Select an application to view groups'. The main area is titled 'All My Applications' and contains a summary box: 'Summary count of Status indicators' with 'Portfolio Management' highlighted. It also includes a 'Filter by Status' section with checkboxes for Red (x), Yellow (⚠), Green (✓), and Grey (diamond). Below this are four application cards: 'Portfolio Management' (red), 'Finance Management' (green), 'Partner Network' (green), and 'Customer Account Mana...' (yellow). Each card has 'Components', 'Transactions', and 'Events' sections with corresponding icons. Callouts explain the colors: 'Red icons indicate Critical Events' points to the red card; 'Green icons indicate condition Normal' points to the green card; 'Yellow icons indicate Warnings' points to the yellow card; and 'Green icons indicate condition Normal' also points to the green card under 'Finance Management'. A note at the bottom states: 'NOTE: The only application with Critical Events in this example is Portfolio Management. My Components in the Applications list displays the most severe status among monitored applications.'

### Event indicators

When a critical event is detected, visual indicators show with the navigators and on the application summary.

- The status indicators consolidate the event severities from the event threshold.
- Critical status indicates all events with a fatal or critical severity.
- Warning status indicates all events with a minor and warning severity.
- Normal status indicates all events with an unknown severity.

## Applications show the most severe status



### *Applications show the most severe status*

Applications can have multiple events and event statuses at any point in time. However, only the most severe status is displayed on the application.

## Viewing all events for all components

The screenshot shows the IBM Application Dashboard interface. On the left, there's a sidebar with 'Applications' and 'Groups'. Under 'Applications', 'My Components' is highlighted with a yellow box and labeled 'Here'. In the main area, there's a section titled 'All My Applications' with a sub-section 'Portfolio Management' which also has 'My Components' highlighted with a yellow box and labeled 'Here'. Another yellow box highlights the 'Events' tab in the 'My Components' section, labeled 'or Here'. To the right, there's a detailed view of the 'Events' tab showing a list of events with columns for Threshold Name, Status, Severity, Display Item, Source, Timestamp, and Description. A legend at the top indicates event types: Critical (red), Warning (yellow), and Normal (green). The status bar at the bottom shows 'Monitoring events' and '7'.

1. Select My Components in the Applications list or on the Dashboard

2. Then, select the Events tab to see a list of Events for all monitored components

| Threshold Name           | Status | Severity | Display Item    | Source          | Timestamp                | Description        |
|--------------------------|--------|----------|-----------------|-----------------|--------------------------|--------------------|
| WMB_Message_Flow_Stopped | Open   | Critical | TRADEBPK_PoC... | TRADEBPK_PoC... | Sep 30, 2017, 4:30:08 AM | IIB message file   |
| BN_Rejected_By_Policy    | Open   | Warning  | BNdatapower2... | BNdatapower2... | Sep 30, 2017, 4:30:08 AM | Client connecti... |
| WAS_Response_Time_High   | Open   | Warning  | f5e0d2ae0afN... | f5e0d2ae0afN... | Sep 30, 2017, 4:30:08 AM | Websphere app...   |
| NET_Memory_High          | Open   | Warning  | TRADERS3-QE     | TRADERS3-QE     | Sep 30, 2017, 4:30:08 AM | .NET memory u...   |
| NET_Memory_High          | Open   | Warning  | TRADERS1-QE     | TRADERS1-QE     | Sep 30, 2017, 4:30:08 AM | .NET memory u...   |

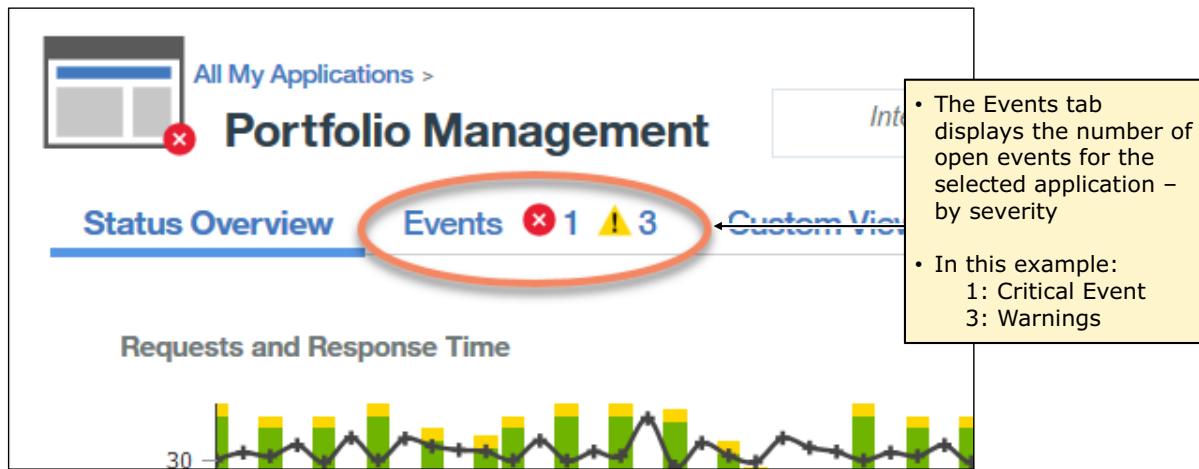
## Viewing all events for a single application

The screenshot shows the IBM Application Dashboard interface. On the left, there's a sidebar with 'Applications' and 'Groups'. Under 'Applications', 'All My Applications' is expanded, showing 'Portfolio Management' (selected), 'My Components', 'Finance Management', 'Credit Card Processing', 'Partner Network', 'Preferred Customer Account Mana...', and 'Fleet Management'. There are also some status indicators: 2 Critical, 2 Warning, 6 Normal, and 0 Unknown. A yellow box labeled 'Here' points to the 'Portfolio Management' item in the list. Another yellow box labeled 'or Here' points to the same item on the main dashboard. The main dashboard has sections for 'Components', 'Transactions', and 'Events'. A yellow box labeled 'Here' points to the 'Events' section. To the right, a detailed view of the 'Portfolio Management' application is shown. It includes a 'Status Overview' with a bar chart (25.00% Critical, 75.00% Normal) and a table of events. The table has columns for 'Threshold Name', 'Status', 'Severity', 'Display Item', and 'Source'. It lists four events: 'WMB\_Message\_Flow\_Stopped' (Open, Critical, TRADEB..., TRADEB...), 'BN\_Rejected\_By\_Policy' (Open, Warning, BN:datap..., BN:datap...), 'WAS\_Response\_Time\_High' (Open, Warning, fBe80d2a..., fBe80d2a...), and 'WAS\_Slow\_Or\_Hung\_Request' (Open, Warning, fBe80d2a..., fBe80d2a...). A yellow box labeled '2. Then, select the Events tab to see a list of Events for the selected application' points to the 'Events' tab in the dashboard.

1. Select your application (example Portfolio Management) in the Applications list or on the Dashboard

2. Then, select the Events tab to see a list of Events for the selected application

## Open events by severity



### Open events by severity

In version 8.1.4, the modified Events tab replaced the Event Severity Summary bar chart.

## Threshold-generated events

Click an event to view details, including:

- Node (with hyperlink to the relevant agent)
- Threshold ID
- Global timestamp
- Type
- Description
- Formula

| Threshold Name           | Status                           | Severity                                      | Display Item                     | Source                           | Timestamp    |
|--------------------------|----------------------------------|---|----------------------------------|----------------------------------|--------------|
| WMB_Message_Flow_Stopped | Open                             | <span style="color: red;">✖ Critical</span>   | TRADEBK:PoC:KQIB                 | TRADEBK:PoC:KQIB                 | Sep 30, 2017 |
| Node                     | <a href="#">TRADEBK:PoC:KQIB</a> |   |                                  |                                  |              |
| Threshold ID             | WMB_Message_Flow_Stopped         |   |                                  |                                  |              |
| Global Timestamp         | Sep 30, 2017, 4:30:08 AM         |   |                                  |                                  |              |
| Type                     | Sampled                          |   |                                  |                                  |              |
| Description              | IIB message flow has stopped     |   |                                  |                                  |              |
| BN_Rejected_By_Policy    | Open                             | <span style="color: yellow;">⚠ Warning</span> | BN:datapower23:DPS               | BN:datapower23:DPS               | Sep 30, 2017 |
| WAS_Response_Time_High   | Open                             | <span style="color: yellow;">⚠ Warning</span> | f8e80d2ae0afNode:docker-was:KYNS | f8e80d2ae0afNode:docker-was:KYNS | Sep 30, 2017 |
| WAS_Slow_Or_Hung_Request | Open                             | <span style="color: yellow;">⚠ Warning</span> | f8e80d2ae0afNode:docker-was:KYNS | f8e80d2ae0afNode:docker-was:KYNS | Sep 30, 2017 |

### Threshold-generated events

Use the Events page to get a summary overview of open events for the selected navigator item and to respond to events with a critical or warning status by drilling down to detailed dashboards.

The status indicators are for events from the thresholds that are running on your managed systems. If the Hybrid Gateway is configured, the events can also be from situations that are running on the managed systems in your IBM Tivoli Monitoring domain. If your environment includes IBM Operations Analytics – Predictive Insights, any detected anomalies are also displayed.

© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

5-10

## Drill-down to affected resource

The screenshot shows the 'Portfolio Management' dashboard under 'All My Applications'. It displays event statistics: Total Events: 4, Critical Events: 1, Warning Events: 3, Normal Events: 0. A legend indicates 25.00% Critical, 75.00% Warning, and 0% Normal. Below this is a table of event details:

| Threshold Name           | Status | Severity | Display Item             | Source           | Timestamp                |
|--------------------------|--------|----------|--------------------------|------------------|--------------------------|
| WMB_Message_Flow_Stopped | Open   | Critical | TRADEBK:PoC:KQIB         | TRADEBK:PoC:KQIB | Sep 30, 2017, 4:30:08 AM |
| Node                     |        |          | TRADEBK:PoC:KQIB         |                  |                          |
| Threshold ID             |        |          | WMB_Message_Flow_Stopped |                  |                          |
| Global Timestamp         |        |          | Sep 30, 2017, 4:30:08 AM |                  |                          |

A callout box points to the 'Display Item' column with the instruction: "Click a link, if present, to navigate to the resource page".

Below this is a 'Message Flow Status' section:

| Message Flow Name          | Status  | Integration Server Name |
|----------------------------|---------|-------------------------|
| TRADEFLOW                  | Stopped | TRADEEG                 |
| TRADEFLOW_DB2              | Started | TRADEEG                 |
| WSHOST_MFP1_WSHOST_....    | Started | TRADEEG                 |
| WSCLIENT_MFP1_WSCLIENT_... | Started | TRADEEG                 |
| MP3_Banking                | Started | TRADEEG                 |

A callout box points to the 'Status' column of the first row with the instruction: "Drill down from this widget to a TRADEFLOW details page". It also lists: "Since the flow is stopped, that page displays no data".

Copyright IBM Corporation 2018

### Drill-down to affected resource

Use the Event Status to get a summary overview of open events for the selected navigator item and to respond to events with a critical or warning status by drilling down to detailed dashboards.

The status indicators are for events from the thresholds that are running on your managed systems. However, if the Hybrid Gateway is configured, the events can also be from situations that are running on the managed systems in your IBM Tivoli Monitoring domain. If your environment includes IBM Operations Analytics – Predictive Insights, any detected anomalies are also displayed in the Events list.

## Using the Event Status widget

- Columns are sortable
  - Nesting sorts are supported
- Columns include:
  - Threshold Name
  - Status
  - Severity
  - Display Item
  - Source
  - Timestamp
  - Description

The screenshot shows the 'Portfolio Management' application interface. At the top, there's a navigation bar with 'All My Applications >' and a search bar that says 'Integrate with OA-LA to enable log searches'. Below the navigation bar, there are three tabs: 'Status Overview', 'Events (1 Critical, 3 Warning)', and 'Custom Views'. The 'Events' tab is selected. A progress bar at the top indicates event distribution: 25.00% Critical (red), 75.00% Warning (yellow). Below the progress bar, it says 'Total Events: 4 Critical Events: 1 Warning Events: 3 Normal Events: 0'. A table follows, with columns: Threshold Name, Status, Severity, Display Item, Source, and Timestamp. The 'Severity' column header has a dropdown arrow, and the 'Description' column header has a note: 'Nested Sort - Do not sort this column'. The table data is as follows:

| Threshold Name           | Status | Severity | Display Item     | Source           | Timestamp                |
|--------------------------|--------|----------|------------------|------------------|--------------------------|
| WMB_Message_Flow_Stopped | Open   | Critical | TRADEBK:PoC:...  | TRADEBK:PoC:...  | Sep 30, 2017, 4:30:00 AM |
| BN_Rejected_By_Policy    | Open   | Warning  | BN:datapower2... | BN:datapower2... | Sep 30, 2017, 4:30:08 AM |
| WAS_Response_Time_High   | Open   | Warning  | f8e80d2ae0afN... | f8e80d2ae0afN... | Sep 30, 2017, 4:30:08 AM |
| WAS_Slow_Or_Hung_Request | Open   | Warning  | f8e80d2ae0afN... | f8e80d2ae0afN... | Sep 30, 2017, 4:30:08 AM |

Using the Event Status widget

# Lesson 2 Creating thresholds by using the Threshold Manager

IBM Training



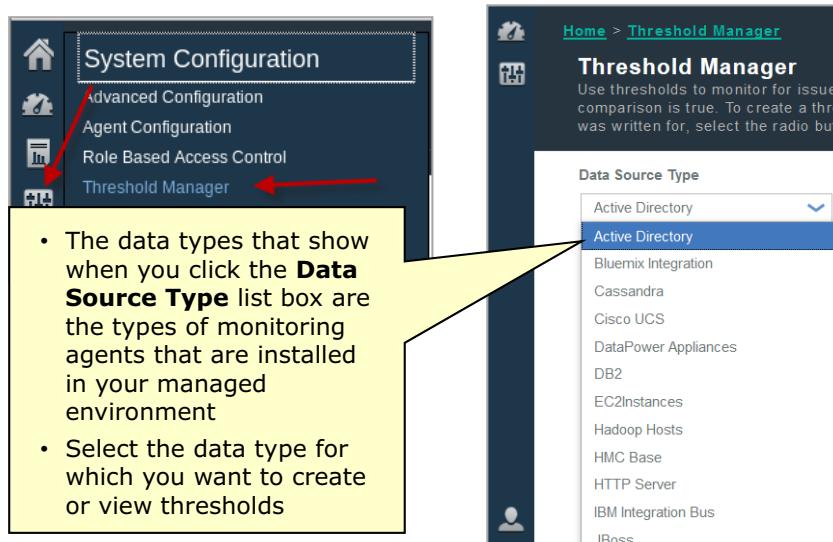
## Lesson 2: Creating thresholds by using the Threshold Manager

- Use thresholds to monitor for issues on your monitored resources
- Thresholds compare current attribute values with given values and open an event when the comparison is true
- To create a threshold, select a data source type from the list and click **New**
- To edit or delete a threshold, select the data source type that it was written for, select the radio button, and click **Edit or Delete**
- To filter the list, type inside the Filter text box

In this lesson, you learn how to create thresholds.

## Selecting the data type

Thresholds sample attributes and compare them with configured values



### Selecting the data type

Threshold Manager installs with predefined thresholds for monitoring agents. You can create new thresholds and edit existing thresholds.

You use thresholds to compare the sampled value of an attribute with the value set in the threshold.

If the sampled value satisfies the comparison, an event is opened. The event closes automatically when the threshold comparison is no longer true.

You access the Threshold Manager from the System Configuration menu.

## Modifying the fields (1 of 2)

| Field Name                   | Description  |
|------------------------------|--|
| Name                         | Unique name fewer than 31 characters. Starts with a letter and no blanks.  |
| Description                  | Optional   |
| Severity                     | Fatal, Critical, Minor, Warning, Unknown   |
| Forward EIF Event            | Specify whether to forward event to EIF receiver or not <ul style="list-style-type: none"> <li>If <b>Yes</b> is selected, you can customize how threshold events are mapped to forwarded EIF events</li> </ul> Click <b>EIF Slot Customization</b> to adjust settings, as required   |
| Interval                     | Select the time interval for testing the threshold <ul style="list-style-type: none"> <li>Allowed values for interval are 000000 (six zeros) for pure-event threshold or at least 000030 (30 seconds) up to 235959 (23 hours, 59 minutes, and 59 seconds) for sampled-event threshold</li> <li>If you select pure event, the attribute group interval is set to 000000 and value change is not possible</li> </ul> |
| Required consecutive samples | Specify how many consecutive threshold samples must evaluate to true before an event is generated (1 - 100)  |
| Data set                     | Select the data that you want to evaluate  |

### Modifying the fields (1 of 2)

A threshold can test for one or more conditions in a data set. Click **Add** to define the comparison for a condition. You can add up to nine conditions in Boolean AND (**&**) comparisons or up to 10 conditions in Boolean OR (**|**) comparisons. After completing the first condition, select the logical operator before clicking **Add** for the next condition.

## Modifying the fields (2 of 2)

| Field Name       | Description   |
|------------------|---|
| Display Item     | Optional. For multiple row data sets. Select a display item attribute when you want the threshold to continue evaluating the remaining rows in the data sampling after an event is opened for a row.  |
| Logical operator | This field is applicable only if the threshold has multiple conditions. After defining the first condition in the Conditions table, select as follows: <ul style="list-style-type: none"> <li>If the previous condition and the next condition must be met, select AND (&amp;)</li> <li>If either of them can be met for the threshold to be breached, select OR ( )</li> </ul>                             |
| Conditions       | The threshold can measure 1 or multiple conditions <ul style="list-style-type: none"> <li>Click <b>New</b> to add a condition</li> <li>Select a condition and click <b>Edit</b> to modify the expression or click <b>Delete</b> to remove the expression</li> <li>To add more conditions to the formula, select AND (&amp;) or OR ( ) in the <b>Logical operator</b> field, and click <b>New</b></li> </ul> |
| Group assignment | Select the check box of the group (or groups) to which the threshold should be assigned.  |
| Execute command  | Optional. The command or script to start when the threshold conditions are true. Supports running the command on the first event, or on every consecutive true interval.  |

## Threshold fields (1 of 2)

The screenshot shows the 'Threshold Editor' page with the following configuration:

- Name:** NT\_Logical\_Disk\_Space\_Critical
- Description:** Opens an event when the unallocated space on a logical disk drive is less than 10%.
- Severity:** Critical
- Forward EIF event:** Yes (selected)
- Interval (HHMMSS):** 00 05 00
- Required consecutive samples:** 1
- Data set:** Active Server Pages (selected)
- Display item:** Disk\_Name
- Logical operator:** And (&)

Annotations highlight specific fields:

- Name field:** The Name field is required. NOTE: Spaces are not allowed.
- Severity, Interval, Samples:** Provide the severity, interval, and required consecutive samples.
- Data set conditions:** Select the data set, display item, and logical operator when multiple conditions are required.

Monitoring events

17

© Copyright IBM Corporation 2018

### Threshold fields (1 of 2)

Give the new threshold a meaningful name.

If necessary, use the Attribute filter field to locate metrics.

Configure the available Severity, Interval, and Consecutive Samples parameters.

Click to add the condition, and complete the configuration. Click **OK**.

## Threshold fields (2 of 2)

The screenshot shows the 'Threshold fields (2 of 2)' configuration page. It includes sections for Logical operator, Conditions, Group assignment, Execute command, and a Save button.

- Logical operator:** Set to 'And (&)'. A callout box says: "Update the condition as necessary".
- Conditions:** Shows two conditions: '%\_Free' (radio button selected) with comparison 'less than or equal to 10' and 'Disk\_Name' with comparison 'not equal to '\_Total'. A callout box says: "The resource group can be a custom group or a System Defined Group."
- Group assignment:** Shows 'Available groups' checked and 'Windows OS' selected. Description: 'System group containing all Windows OS resources.' Type: 'System Defined'. A callout box says: "Optional run a command when the condition is true."
- Execute command:** An empty text area for commands. A callout box says: "Select Save."
- Save:** A green 'Save' button at the bottom right.

### Threshold fields (2 of 2)

Click to add the condition, and then complete configuration. Click **Save**.

## The resulting event

The screenshot shows the IBM Monitoring Events interface. At the top, there's a navigation bar: 'All My Applications > My Components > Components > Windows OS'. Below it is a 'Status Overview' section with tabs for 'Events' (highlighted) and 'Logs'. The 'Events' tab shows 'Events 1 Critical 3 Warning'. A yellow callout box points to this area with the text 'The resulting event from the definitions'.

Below the overview, a summary table provides event counts: 'Total Events: 1 Critical Events: 1 Warning Events: 0 Normal Events: 0'. To the right of the table is a legend: a red bar for 'Critical' and a yellow bar for 'Warning'.

The main table lists a single threshold definition:

| Threshold Name                 | Status | Severity | Display Item |
|--------------------------------|--------|----------|--------------|
| NT_Logical_Disk_Space_Critical | Open   | Critical | C:           |

A detailed view of the threshold row is shown in a modal window:

|                  |   |
|------------------|---|
| Node             | Primary:WIN1:NT   |
| Threshold ID     | NT_Logical_Disk_Space_Critical  |
| Global Timestamp | May 10, 2016, 3:09:35 AM  |
| Type             | Sampled   |
| Description      | Opens an event when the unallocated space on a logical disk drive is less than 10%. |
| Formula          | ( % Free <= 99 AND Logical Disk Name != '_Total' )                                  |

Monitoring events

19

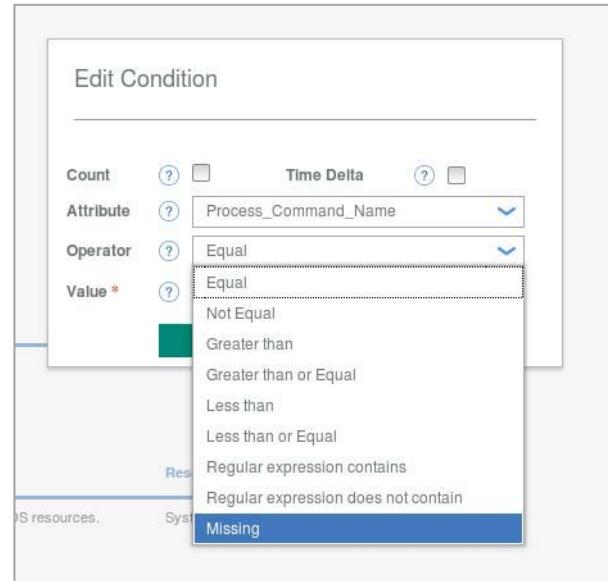
© Copyright IBM Corporation 2018

### The resulting event

This sampled event determines whether you have less than 99% disk space on a Windows disk drive.

## Special operators that are supported in Edit Conditions

- Standard Boolean Operators:
  - Equal
  - Not Equal
  - Greater than
  - Greater than or equal
  - Less than
  - Less than or equal
- Regular expression
  - Equals
  - Not equals
- Missing



### Special operators that are supported in Edit Conditions

The Missing condition is a powerful tool in Cloud APM for monitoring files and processes.

## Execute command example that uses the Missing comparison

The screenshot shows the 'Threshold Manager' configuration window for an 'Execute command' event. The configuration includes:

- Display Item:** Process\_ID
- Logical operator:** And (&)
- Conditions:** Process\_Command\_Name missing xclock
- Group assignment:** Available groups (Linux OS selected), Resource group description: System group containing all Linux OS resources, Resource group type: System Defined
- Execute command:** /usr/bin/xclock; (checkboxes: On first event only, For every consecutive true interval selected)

A yellow callout box points to the 'Execute command' section with the text: "Run this command when the threshold is true".

### Execute command example that uses the Missing comparison

The ability to run commands or scripts to solve issues that are discovered is another powerful tool.

## Display item example

The same threshold, one without Display Item definition and the other with the Disk\_Name attribute provided

**Monitoring events**      22      © Copyright IBM Corporation 2018

### Display item example

The Display Item feature is useful when an attribute can have multiple values that are returned. Examples include process names that are running on a server or disk drives that are available on a Windows server.

## Adding multiple conditions

The screenshot shows the 'Edit Condition' dialog box and the main configuration window for adding multiple conditions.

**Main Configuration Window:**

- Display item: Process\_Command\_Name
- Logical operator: And (&)
- Conditions: Available groups (Process\_Command\_Name) and Linux OS
- A red arrow points to the '+' button in the Conditions section.

**Edit Condition Dialog Box:**

- Count: Time Delta
- Attribute: System\_Name
- Operator: Not Equal
- Value: apm.ibm.edu

**Final Result:**

Conditions:

- Attribute: System\_Name, Comparison: not equal to apm.ibm.edu
- Attribute: Process\_Command\_Name, Comparison: missing xclock

### Adding multiple conditions

The Threshold Manager supports complex Boolean expressions.

## Deleting thresholds

- To delete a threshold, choose it from the list, and select **Delete** (the minus sign)
- Confirm your selection

The screenshot shows the 'Threshold Manager' page with a list of thresholds. A red arrow points to the delete icon (minus sign) next to the 'Linux\_Display\_Item\_Example' threshold. A confirmation dialog box is overlaid on the page, asking 'Are you sure you want to delete Linux\_Display\_Item\_Example?' with 'OK' and 'Cancel' buttons.

| Name                              | Description  |
|-----------------------------------|--|
| Linux_BP_SpaceUsedPct_Critical    | Monitors all mounted file systems for free space used percentage. Once usage is higher than 95%, it triggers a critical alert. |
| Linux_CPU_Utilization_High        | The percentage of CPU utilization is higher than 90%.  |
| Linux_CPU_Utilization_High_Warn   | The percentage of CPU utilization is higher than 80%.  |
| Linux_Disk_Space_Low              | Disk space is low.   |
| <b>Linux_Display_Item_Example</b> | This threshold monitors the display item.  |
| Linux_Fragmented_File_System      | File system fragmentation is high.   |
| Linux_Mem_Utilization_High_Crit   | The memory utilization is higher than 90%.   |
| Linux_Mem_Utilization_High_Warn   | The memory utilization is higher than 80% and lower than 90%.  |

## Thresholds enablement

- Many agents supply thresholds at installation time
- You can decide after installation to enable or disable all of these system defined thresholds
- System Configuration > Advanced Configuration > Thresholds Enablement

**System Configuration**

Advanced Configuration

Agent Configuration

Role Based Access Control

Threshold Manager

Synthetic Script Manager

Resource Group Manager

MongoDB Configuration

Agent Central Configuration

Data Mart

Hybrid Gateway

Kafka Configuration

Tracking Analytics Service

Agent Subscription Facility

Thresholds Enablement

**Parameters**

Configuration for enablement of predefined best practice thresholds.

Choose action to define policy for predefined best practice thresholds

Select option

Enable All

Disable All

This value is required.

*Thresholds enablement*

You can use this feature to quickly enable or disable all product provided thresholds.

# Lesson 3 Managing resource groups

IBM Training



## Lesson 3: Managing resource groups

- Use the Resource Group Manager to organize your monitored systems into named collections that you can assign to eventing thresholds
  - Type of monitored resource
  - Geography
  - Application dependency
  - User responsibility
- You can mix different types of monitoring resources in a group
  - Thresholds are distributed to members of the same resource type
- To create a group, click **New**
- To edit or delete a group, select the radio button for the group and click **Edit** or **Delete**
- To filter the list, type inside the Filter text box

In this lesson, you learn how to perform the following tasks:

- Use the Resource Group Manager to organize your managed resources
- Select which thresholds are evaluated on a resource group

## Resource Group Manager

The screenshot shows two windows side-by-side. The left window is a sidebar titled 'System Configuration' with options like 'Advanced Configuration', 'Agent Configuration', 'Role Based Access Control', 'Threshold Manager', 'Synthetic Script Manager', 'Resource Group Manager' (which has a red arrow pointing to it), and 'Hybrid Gateway Manager'. The right window is titled 'Resource Group Manager' and shows a list of system groups. A red arrow points from the 'Resource Group Manager' button in the sidebar to the 'New' button in the main window. A yellow callout box with a black border and a black arrow points to the 'New' button with the text 'Click the plus sign to create a new resource group'.

| New                              | Resource group name    | Resource group description   |
|----------------------------------|------------------------|--|
| <input checked="" type="radio"/> | DB2                    | System group containing all DB2 resources.   |
| <input type="radio"/>            | HTTP Server            | System group containing all HTTP Server resources.   |
| <input type="radio"/>            | HTTP Server Agent      | System group contains resources of type HTTP Server Agent, but member and containing events displayed in the Performance Management console. |
| <input type="radio"/>            | Linux OS               | System group containing all Linux OS resources.  |
| <input type="radio"/>            | Synthetic Events Agent | System group containing Synthetic Events Agent resources.  |
| <input type="radio"/>            | Synthetic Playback     | System group containing all Synthetic Playback resources.  |
| <input type="radio"/>            | Synthetic Transaction  | System group containing all Synthetic Transaction resources.   |
| <input type="radio"/>            | Transaction Tracking   | System group containing all Transaction Tracking resources.  |
| <input type="radio"/>            | Web Response Time      | System group containing all Web Response Time resources.   |
| <input type="radio"/>            | WebSphere Agent        | This system group contains resources and do not have events displayed in the Performance Management console.                                 |
| <input type="radio"/>            | WebSphere App Server   | System group containing all WebSphere Application Server resources.  |
| <input type="radio"/>            | Windows OS             | System group containing all Windows OS resources.  |

### Resource Group Manager

Resource groups are named collections that you can assign to event thresholds. You can mix different types of monitoring resources in a group; thresholds are distributed to resources of the same type.

1. Click the menu item to open the Resource Group Manager.
2. Click the plus (+) sign to create a new resource group.

## Creating a resource group (1 of 2)

Group name \*

Group description

Resource assignment  Filter

| Available resource                                      | Host name | Type                 | Source Domain |
|---|-----------|----------------------|---------------|
| <input checked="" type="checkbox"/> db2inst1:lin1:UD    | lin1      | DB2                  | On Premises   |
| <input checked="" type="checkbox"/> HU:lin1_httpd:HUS   | lin1      | HTTP Server          | On Premises   |
| <input checked="" type="checkbox"/> KTE-GEN-HOSTNAME:TE | apm       | Transaction Tracking | On Premises   |
| <input checked="" type="checkbox"/> lin1:HU             | lin1      | HTTP Server          | On Premises   |

Show only selected resources

### Creating a resource group (1 of 2)

3. You give the group a name and optional description.
4. Assign resources for your resource assignments from the list of available resources.

## Creating a resource group (2 of 2)

The screenshot shows the 'Resource Group Editor' page. At the top, there are fields for 'Group name' (Linux WAS Servers) and 'Group description' (This resource group is for Linux WAS servers and the software that supports them). Below these are two tables: 'Resource assignment' and 'Threshold assignment'. The 'Resource assignment' table lists four resources: db2inst1.ln1.UD (DB2), HU:ln1\_httpd.HUS (HTTP Server), KTE-GEN-HOSTNAME:TE (Transaction Tracking), and ln1.HU (HTTP Server). The 'Threshold assignment' table lists three thresholds: Interaction\_Avail\_Critical, Interaction\_Avail\_Warning, and Interaction\_Time\_Critical, all of which are Predefined Transaction Tracking thresholds.

| Available resource  | Host name | Type                 | Source Domain |
|---------------------|-----------|----------------------|---------------|
| db2inst1.ln1.UD     | ln1       | DB2                  | On Premises   |
| HU:ln1_httpd.HUS    | ln1       | HTTP Server          | On Premises   |
| KTE-GEN-HOSTNAME:TE | apm       | Transaction Tracking | On Premises   |
| ln1.HU              | ln1       | HTTP Server          | On Premises   |

| Threshold name             | Description   | Type                 | Origin     |
|----------------------------|---|----------------------|------------|
| Interaction_Avail_Critical | A high percentage of interactions have failed.            | Transaction Tracking | Predefined |
| Interaction_Avail_Warning  | A moderate percentage of interactions have failed.        | Transaction Tracking | Predefined |
| Interaction_Time_Critical  | A high percentage of interactions have a slow total time. | Transaction Tracking | Predefined |

Monitoring events

29

© Copyright IBM Corporation 2018

### Creating a resource group (2 of 2)

5. Assign thresholds.
6. If a threshold that you require for the group does not yet exist, save the resource group and create the new threshold.
7. Return to the Resource Group Manager to add the new threshold and complete the configuration of your resource group.

## Instructor demonstration



## Student exercises



Complete the exercises for this unit in the Course Exercises Guide.

## Summary

Now that you have completed this unit, you should be able to:

- Describe the use of events in Application Performance Management
- Describe how thresholds are used to create events
- Create resource groups to manage the events for managed systems in your enterprise

# **Unit 6 Monitoring the user experience of applications**

IBM Training



## **Monitoring the end user experience of applications**

© Copyright IBM Corporation 2018  
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this unit, you learn to monitor the user's experience of your application by monitoring the HTTP requests made by the user to your application.

## Learning objectives

After completing this unit, you should be able to:

- Describe user experience monitoring
- Describe and navigate Response Time and HTTP Server agent data in the Performance Management console
- Deploy the Response Time agent, HTTP Server agent, and JavaScript injection

### *Learning objectives*

This slide lists the objectives for this unit.

## Unit outline

- Lesson 1: What is end user experience monitoring
- Lesson 2: Introduction to the Response Time Monitoring agent
- Lesson 3: Introduction to the HTTP Server agent
- Lesson 4: Introduction to JavaScript injection
- Lesson 4: Deploying end user monitoring components

### *Unit outline*

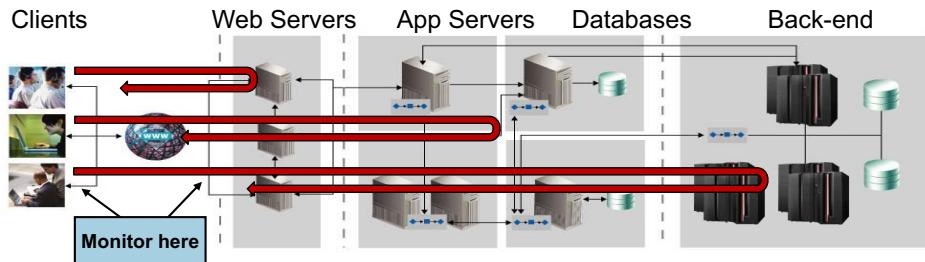
This slide lists the unit outline.

# Lesson 1 What is user experience monitoring?

IBM Training



## Lesson 1: What is end user experience monitoring



- Monitor end user HTTP/HTTPS requests (transactions)
  - Monitors the performance and availability of each request (transaction)
  - Initial, front end requests represent the user experience of the full application
  - Divides into transaction, application, user, device, and session monitoring
- Components
  - Response Time agent for monitoring incoming HTTP transactions
  - JavaScript injection with or without the HTTP Server agent for monitoring user browser activity (ADV)
  - HTTP Server agent for automatic JavaScript injection and overall health of HTTP server

In this lesson, you learn how to describe user experience monitoring.

By monitoring the performance and availability of user requests (transactions), you get an idea of the user's experience and also an overview of how the entire application is performing. This front-end transactional monitoring is done mostly with the Response Time agent, but can integrate with the HTTP Server agent and JavaScript injection into the application HTML pages.

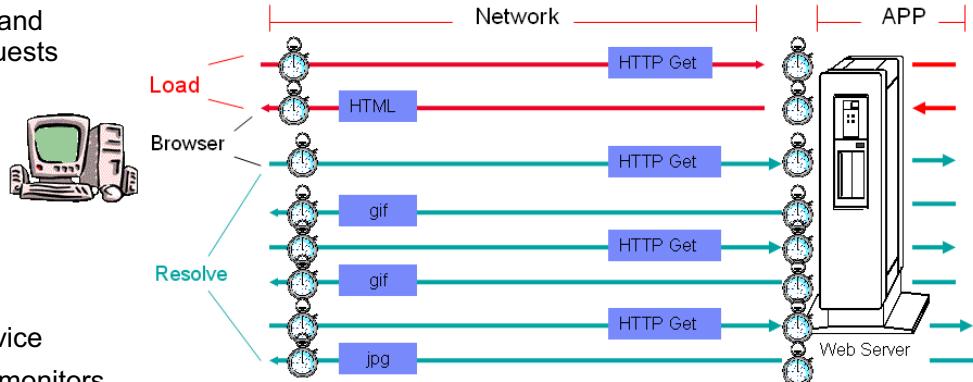
# Lesson 2 Introduction to the Response Time Monitoring agent

IBM Training

IBM

## Lesson 2: Introduction to the Response Time Monitoring agent

- Monitors HTML page and embedded object requests
  - Errors in transaction performance and availability
  - Errors in HTML content and SSL
- Groups data into request components such as application, user, session, and device
- Divides data into and monitors request subcomponents, such as Client Time, Network Time, Server Time, and Load Time
- Integrates with
  - HTTP Server agent
  - JavaScript Injection
  - Transaction tracking



Monitoring the end user experience of applications

5

© Copyright IBM Corporation 2018

In this lesson, you learn how to navigate and understand the Response Time data in the Performance Management console.

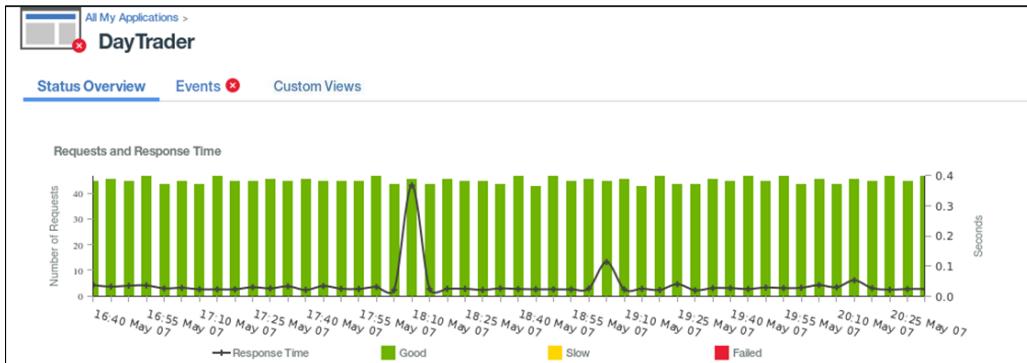
The Response Time Monitoring agent monitors HTML pages and embedded object requests. It looks for errors in transaction performance and availability, and also errors in HTML content and SSL.

The agent groups the transactional data into request components such as application, user, session, and device to monitor the performance and availability of each component. It also divides the transactional data into subcomponents, such as Client Time, Network Time, Server Time, and Load Time to help locate problems.

The agent integrates with the HTTP Server agent, JavaScript injection, and transaction tracking.

## Requests and Response Time

- Transaction or application performance and availability over time
  - Bars are percentage of good, slow, or failed requests
  - Line is average response time
- Roll cursor over a bar for specific counts
- Click widget for more details



### Requests and Response Time

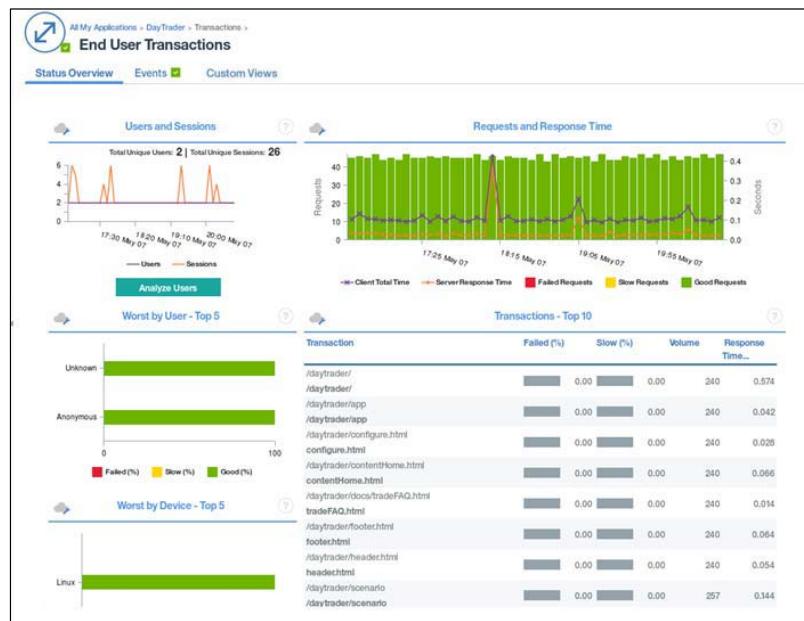
If the application includes the Response Time Monitoring agent (End User Transactions in the Transactions navigator group), the Requests and Response Time stacked bar chart is displayed.

Use this chart to look for trending patterns in performance and availability. Each stacked bar plots the percentage of requests that completed with good response time, slow response time, or failed to complete. The good requests are those requests that finish successfully within the minimum response time threshold, which, by default, is 10 seconds. The slow requests are those requests that finish successfully, but are above the 10-second threshold. The failed requests are those requests that do not finish at all during the sampling interval, or that reported an error. Roll the cursor over a bar for specific counts. The line chart overlay plots the average response time during the 5-minute period.

Use the time selector to change the time range that is displayed, described in “Adjusting and comparing metrics over time.”

## End User Transaction status overview

- Requests and Response Time
  - Same availability data
  - Response time is broken down into subcomponents
- Transactions – Top 10
  - Click a transaction for details
- Users and Sessions
  - Click Analyze Users for details
- Worst by User – Top 5
  - Click widget for details
- Worst by Device – Top 5
  - Click widget for details



Monitoring the end user experience of applications

7

© Copyright IBM Corporation 2018

### End User Transaction status overview

The Status Overview groups the transaction data into different groups and subcomponents to give insight into who and what is available.

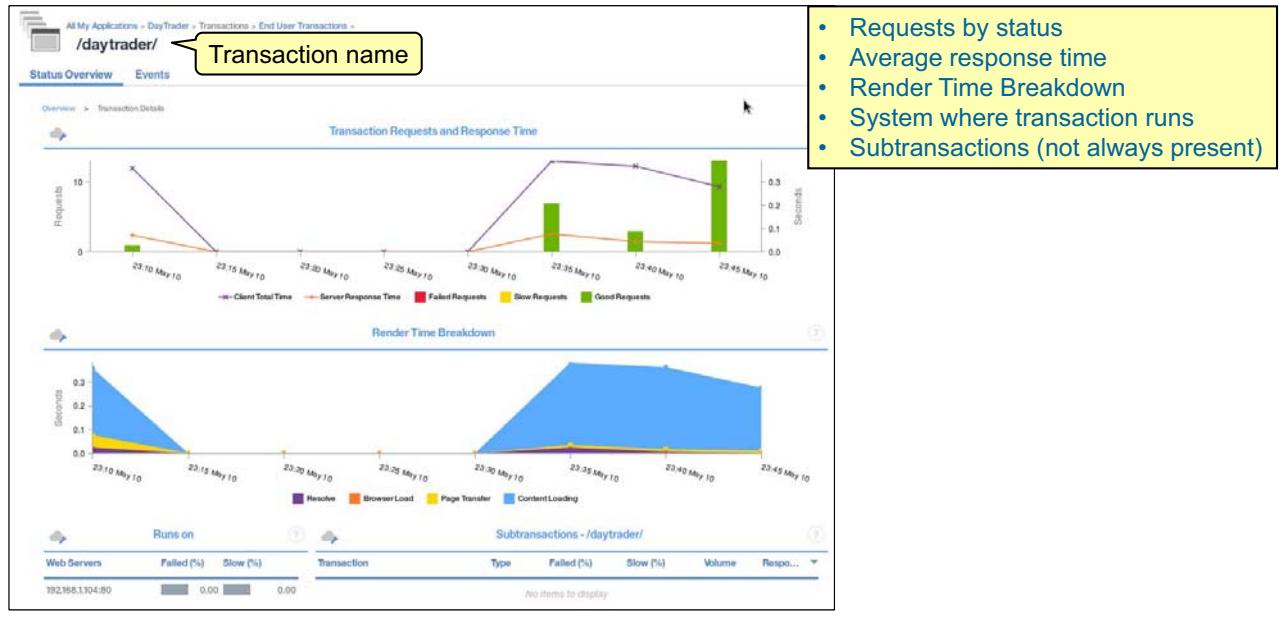
The Request and Response Time widget shows data similar to the parent widget that shows overall performance and availability over time. Each bar represents the average availability of the application transactions that are broken into good, slow, and failed. The average response time is broken into client and server time.

The Transactions – Top 10 widget shows the top 10 worst performing transactions and their summary data. Click a transaction for more details.

The Transactions top 10 view shows the 10 worst performing transactions over the last sampling interval. The response time attribute to the far right shows the average response time by transaction in the sampling interval. The rows in the transactions table are links that you can use to drill down into individual transactions.

You can also see user and session counts, and identify the poorest performing users and devices. Click the widget for more details.

## Viewing individual transaction details



Monitoring the end user experience of applications

8

© Copyright IBM Corporation 2018

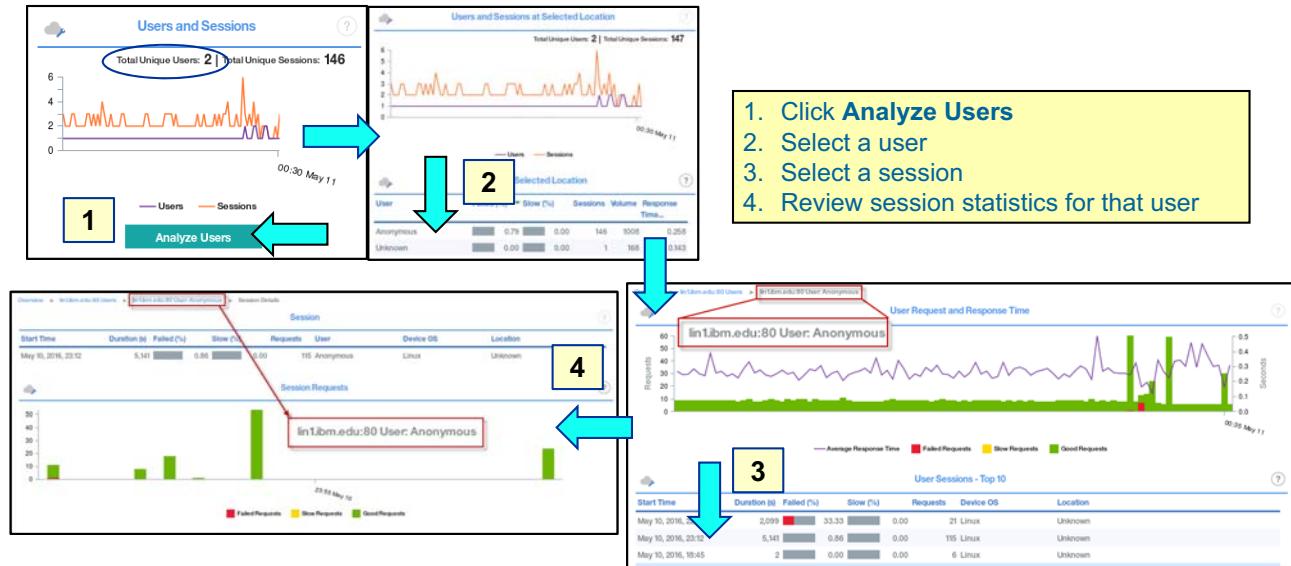
### Viewing individual transaction details

The transaction details window shows requests by status and average response time for an individual transaction. It also shows you the server or servers that the transactions run on.

Also included is a render-time breakdown of requests, including:

- Resolve time
- Browser load
- Page transfer
- Content loading

## Viewing user activity

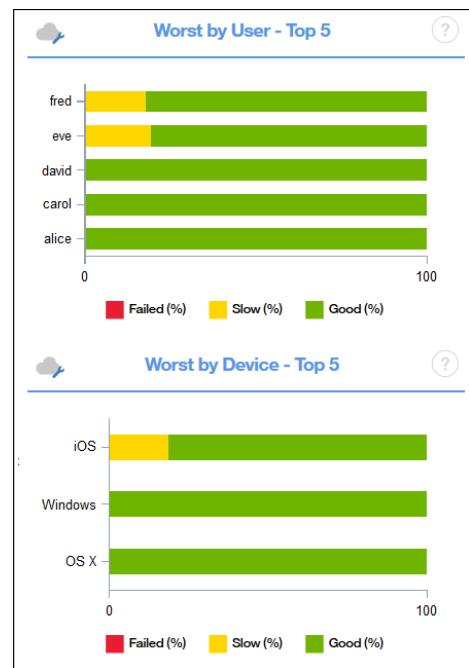
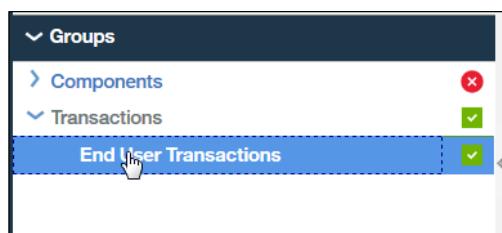


### Viewing user activity

The Users and Sessions widget lists those statistics for the current data collection period. Drill-down is available for individual users down to the session level.

## Monitoring mobile device user transactions

- Response Time Monitoring agent can monitor HTTP and HTTPS for mobile devices
- Access user Transaction activity in the Groups widget
- Drill down by worst-performing users or by device (categorized by OS)

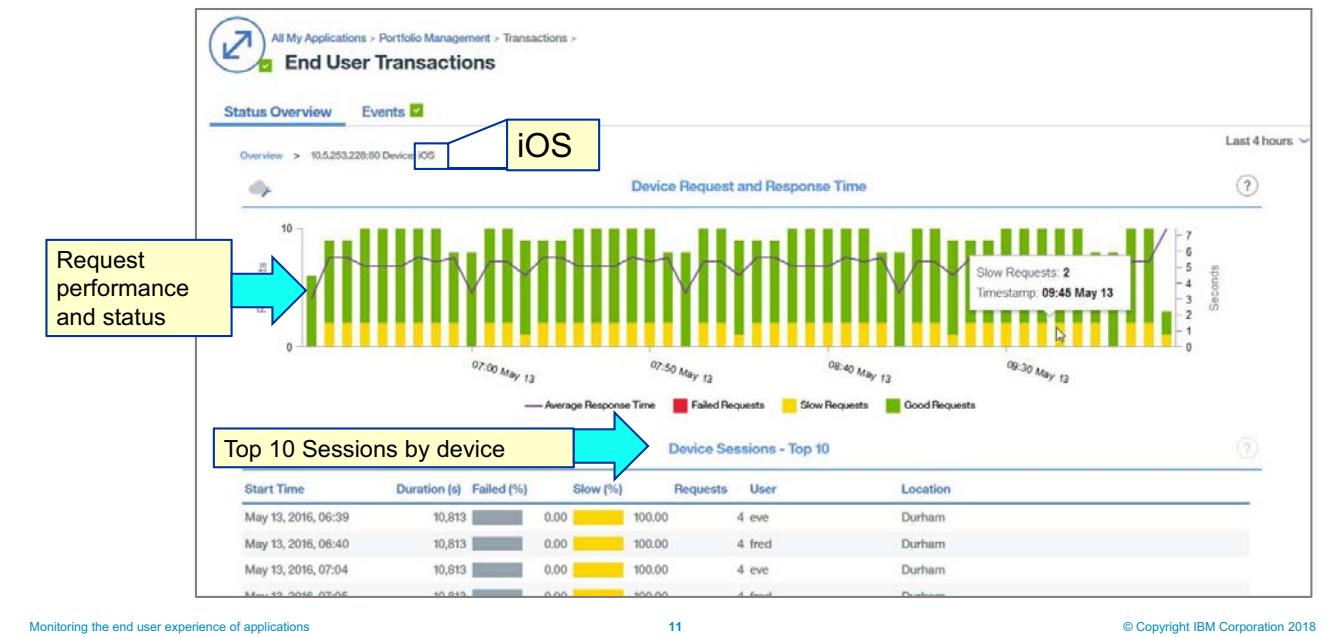


### Monitoring mobile device user transactions

The Response Time Monitoring agent can monitor the performance and availability of HTTP and HTTPS for mobile devices that are accessing your environment.

Track performance by device and by user.

## User activity by device (operating system)



Monitoring the end user experience of applications

11

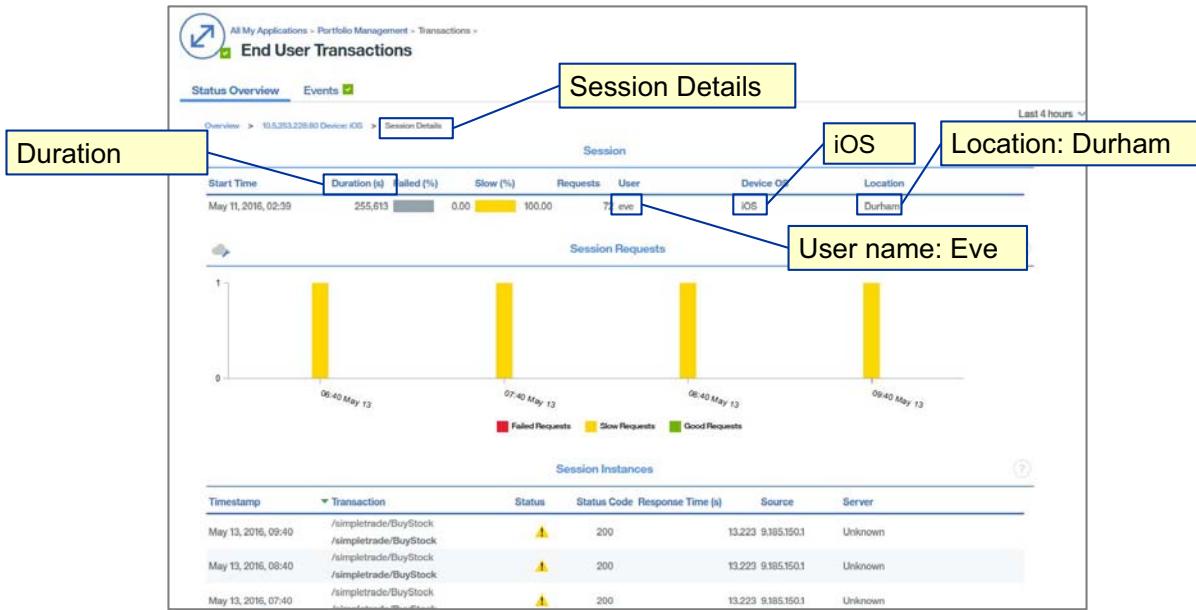
© Copyright IBM Corporation 2018

### User activity by device (operating system)

Monitor user activity by device (read operating system):

- Look at the Mobile Active Sessions graph to see the number of open sessions that served mobile devices on the application server over a recent period. You can use the graph to detect any peak loads.
- Look at the Active Sessions by Mobile OS – Top 5 chart to compare the current number of active sessions per mobile operating system.
- Look at the Session Duration by Mobile OS – Top 5 chart to compare the average session duration, that is, how long a session is running, per mobile operating system. This value is an average for all sessions that are currently open.
- Look at the Requests by Mobile OS – Top 5 chart to compare the number of web requests that are sent from devices that use various mobile operating systems over a recent period.
- Look at the Percentage Failures by Mobile OS – Top 5 chart to see how many requests failed (red), took too long to process (yellow), or were good (green) for each device operating system.
- Click an operating system to open the Mobile Devices Users Details dashboard.

## Session details by device (operating system)



### Session details by device (operating system)

The Session Details level view shows the performance of individual sessions, including the user name, device OS, duration, and location.

# Lesson 3 Introduction to the HTTP Server agent

IBM Training



## Lesson 3: Introduction to the HTTP Server agent

- The Monitoring Agent for HTTP Server is an agent that is designed for both the on-premises and SaaS environments
- The agent:
  - Collects performance data from HTTP Server through IBM HTTP Server module, and
  - Uses the Data Collector of ITCAM for HTTP Server (traditional agent)
- The Monitoring Agent for HTTP Server features product-provided historical data collection, covering:
  - Web server
  - Website
  - Includes virtual host information
- Historical data samples are saved every 5 minutes at the monitored resource
  - Data is retained for 4 hours before the oldest samples are deleted to make room for new data samples

In this lesson, you learn how to navigate and understand HTTP Server agent data in the Performance Management console.

## Component status

The screenshot shows the IBM Application Dashboard interface. On the left, there's a chart titled 'Current Components Status' with four bars: three green and one red. A red arrow points from this chart to the right-hand panel. The right-hand panel is titled 'HTTP Server' and displays detailed status information for the server 'HU:lin1\_httpd:HUS'. The status is listed as 'Running'. Other metrics shown include Up time (0d 22h 16m), Total web sites (1), Request rate (RPM) (42.00), Transfer rate (KB/m) (185.00), Failed request rate (RPM) (2.00 checked), Server failure rate (RPM) (0.00 checked), and Configuration file (/opt/IBM/HTTPServer/conf...). Below the main status table, there's a note: 'Click HTTP Server for component data'.

### Component status

The monitoring agent for HTTP helps you monitor availability, performance, and activity of your web server and associated websites. Access the HTTP Server component data from the application Current Components Status widget or the Components pane.

On the highest-level dashboard, a summary widget is displayed, which returns data for the server name, status, and up time.

In addition, data is displayed for:

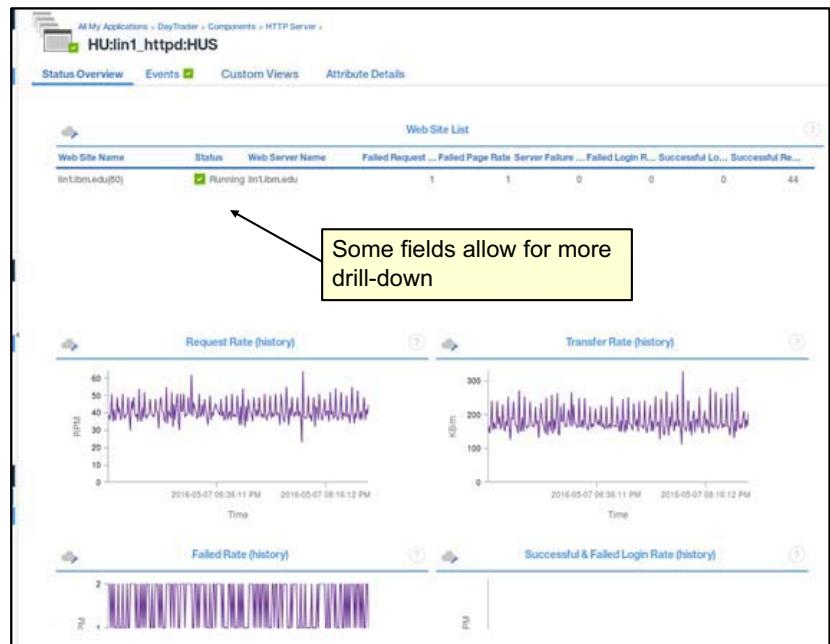
- Total websites that are configured on this server instance
- Request rate per minute
- Transfer rate, in KB per minute, and per-minute statistics for:
  - Failed requests rate
  - Server failure rate
  - Failed login rate

The location of the configuration file is also provided.

Click the widget to drill down for more details.

## Web server detail

- Web Site List
  - List of HTTP servers (ports) monitored by this agent
  - Summary data for each
- Performance over time for all websites that this agent monitors
  - Request rate
  - Transfer rate
  - Failed rate
  - Login rate
- Click a website in the Web Site List for more details



Monitoring the end user experience of applications

15

© Copyright IBM Corporation 2018

### Web server detail

A web server has one or multiple websites that are configured, and each website has its unique port.

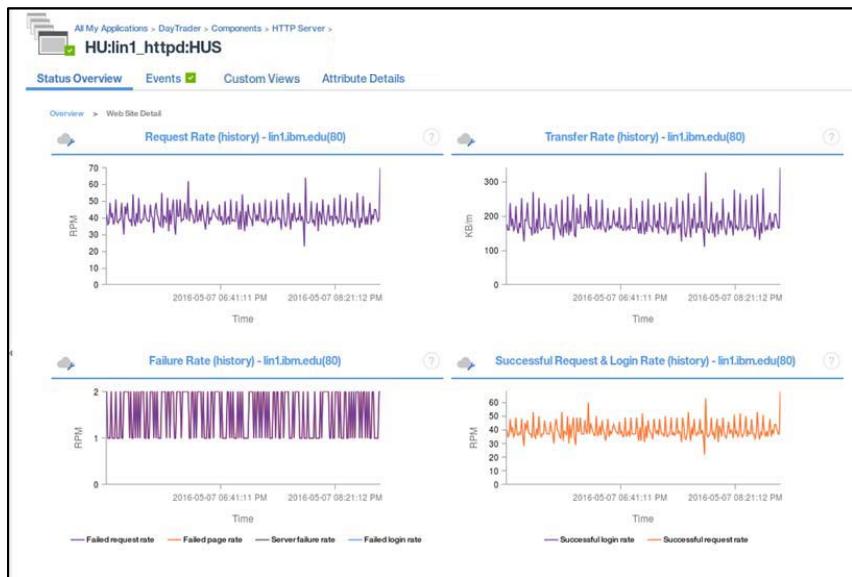
The HTTP Server Status Overview page shows data that is related to all websites (ports) monitored by the agent.

The Web Site List widget lists each website (port) monitored by this agent and summary data about their overall status. Click a website for details on a specific website.

The following widgets show the performance over time for all websites that this agent monitors.

## Web Site Detail page

- Performance over time for a specific website
  - Request rate
  - Transfer rate
  - Failed rate
  - Login rate



### Web Site Detail page

The Web Site Detail page shows the performance over time data for the selected website.

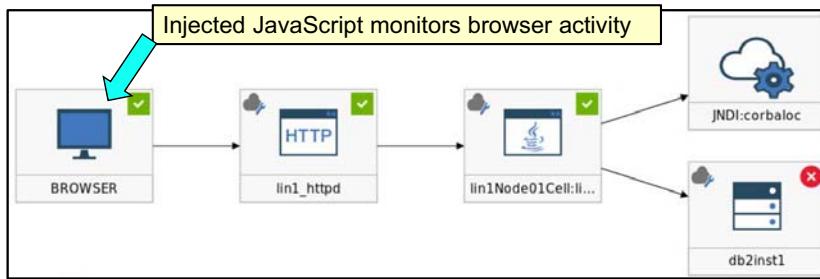
# Lesson 4 Introduction to JavaScript injection

IBM Training



## Lesson 4: Introduction to JavaScript injection

- Monitoring at the browser level
- Inject JavaScript Monitoring Code into the web pages



- For Response Time agents integrated with the HTTP Server agent, JavaScript injection occurs automatically
  - JavaScript injection can be disabled
- For Response Time agent not integrated with the HTTP Server agent, each application must be configured for JavaScript injection

To help you understand the performance of your web pages in a browser and any errors, the Response Time Monitoring agent needs to be able to collect timing data from the browser. With some simple configuration to the application that you want to monitor, monitoring features can collect timing data. This feature is available only in IBM Cloud Application Performance Management.

Using JavaScript, the IBM HTTP Server Response Time module inserts a header into web pages that are served by IBM HTTP Server so that Response Time Monitoring can monitor those pages. To display client-side and network data, monitored web browsers must support JavaScript, and W3C performance and navigation timing. Embedded objects that the page loads are tracked by using cookies. Transaction information from web pages that are served by IBM HTTP Server is then included in End User Transactions dashboards.

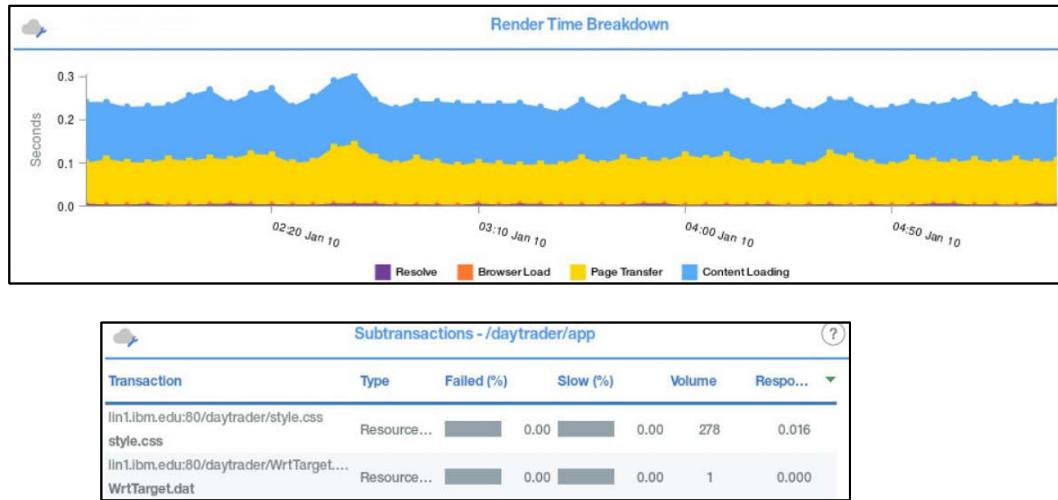
## Limitations

JavaScript to collect browser timings is inserted automatically into a web page only if the page meets the W3C HTML standards. The following conditions must be satisfied:

- Response headers contain Content-Type: text/html.
- Response content includes the <head> element.

## Data from JavaScript injection

- Adds Render Breakdown and Resource Timing data in Subtransaction table



### Data from JavaScript injection

JavaScript injection enables true monitoring of the user experience. It monitors the render time of each page such as resolve, browser load, page transfer, and content loading times. Furthermore, JavaScript injection monitors the performance and availability of page subtransactions (embedded object calls).

# Lesson 5 Deploying end user monitoring components

IBM Training



## Lesson 5: Deploying end user monitoring components

Plan deployment of HTTP Server agent, Response Time agents, and JavaScript injection together

Choose Response Time agent mode

- Integrated with HTTP Server agent
  - Easiest deployment
  - Install both agents at same time
  - Requires Web Response time module be added to HTTP Server
  - Does JavaScript injection (browser monitoring) automatically
- Not integrated with HTTP Server agent (packet analyzer mode)
  - Install Response Time agent before HTTP Server agent
  - Configure Response Time agent for Packet Analyzer mode
  - Manually configure JavaScript injection into web applications (optional)

In this lesson, you learn how to deploy the Response Time agent, HTTP Server agent, and JavaScript injection.

## Supported transaction features

|   | Response Time agent in Packet Analyzer mode | Response Time agent with JavaScript Injection | IBM HTTP Server Response Time module |
|---|---|---|--------------------------------------|
| Transactions Top 10                               | Y   | Y   | Y                                    |
| Server Time                                       | Y   | Y   | Y                                    |
| Render Time Breakdown                             | N   | Y   | Y                                    |
| Ajax Subtransactions                              | Y   | Y   | Y                                    |
| Resource Time data in Subtransactions table       | N   | Y   | Y                                    |
| Transactions Instance (Top 10)                    | Y   | Y   | Y                                    |
| Transaction Instance Topology                     | Y   | Y   | Y                                    |
| Application Topology                              | Y   | Y   | Y                                    |
| Automatic instrumentation of JavaScript Injection | N/A   | N   | Y                                    |

### Supported transaction features

The table shows the features available with the different deployments. The Packet Analyzer mode column shows what you get when you deploy the Response Time agent without JavaScript injection and without integration with the HTTP Server agent. The JavaScript Instrumentation column shows the available features when you deploy the Response Time agent without integration with the HTTP Server agent and manually configure JavaScript injection. The IBM HTTP Server Response Time module column shows the available features when you integrate your Response Time agent with the HTTP Server agent.

## Supported software

- HTTP Server agent
  - IBM HTTP Server
  - Apache server
- Response Time agent
  - Windows: Ensure that Windows Network Monitor is installed before you install the agent
  - Linux
  - AIX
- JavaScript injection
  - JavaScript must be enabled on the browser of the user

### Supported software

This slide shows the supported software for each agent and JavaScript injection.

## If integrating Response Time and HTTP server agents

- Install Response Time and HTTP Server agents on the HTTP server
  - Install agents together or HTTP Server agent before Response Time agent
- Add statement to include HTTP Server Response Time module to each monitored HTTP server
- Restart the HTTP server

```
# GlobalLog logs/cookie-debug.log "%h %l %u %t \"%r\" %>s %b %{User-Agent}i %D %{RH}e %
{WAS}e %{Age}o %{Cache-Control}i exp=%{Expires}o %{Cache-Control}o SC=\"%{Set-Cookie}o
\" C=\"%{Cookie}i\" %{Location}o"
LoadModule was_ap24_module /opt/IBM/WebSphere/Plugins/bin/64bits/mod_was_ap24_http.so
WebSpherePluginConfig /opt/IBM/WebSphere/Plugins/config/webserver1/plugin-cfg.xml
Include "/opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf"]
```

Plain Text ▾ Tab Width: 8 ▾ Ln 877, Col 76 ▾ INS

### If integrating Response Time and HTTP server agents

This slide shows the high-level steps to installing and configuring the Response Time and HTTP Server agents when you integrate the two agents.

## If not integrating Response Time and HTTP server agents

Install and configure Response Time agent alone or before HTTP Server agent on HTTP server

- Configure the Response Time agent for Packet Analyzer mode

Manually configure JavaScript Injection into web pages (optional)

- Add the JavaScript monitoring component to the application
  - For Java EE applications, extract `install_dir/clienttime/ClientTime.war` to a directory accessible to the HTTP server
  - For non-Java EE applications, save `install_dir/clienttime/wrtInstrumentation.js` to a directory accessible to the HTTP server
- Add the following JavaScript to the application header before any other JavaScript:

```
<script language="JavaScript" src="path/wrtInstrumentation.js"
type="text/JavaScript"></script>
```

### *If not integrating Response Time and HTTP Server agents*

This slide shows the high-level steps to installing and configuring the Response Time agent when you want JavaScript injection, but you are not integrating with the HTTP Server agent.

If you want JavaScript injection, complete the following steps. These steps need to be completed only once, unless the application configuration changes.

- Add the JavaScript monitoring component to the application. The procedure that you use depends on the application type:
  - For Java EE applications, extract `install_dir/clienttime/ClientTime.war` from the installation package to a directory accessible to the HTTP server.
  - For non-Java EE applications, such as Ruby, .NET, Python, and Node.js, save `install_dir/clienttime/wrtInstrumentation.js` from the installation package to a directory accessible to the HTTP server.
- Associate the JavaScript monitoring component with the application. This association can normally be done by modifying an application header script. Typically, only one header script needs to be modified for each component or application that is to be monitored.

For both Java EE applications and non-Java EE applications, add the following JavaScript to the application header before any other JavaScript:

```
<script language="JavaScript" src="path/wrtInstrumentation.js"
type="text/JavaScript"></script>
```

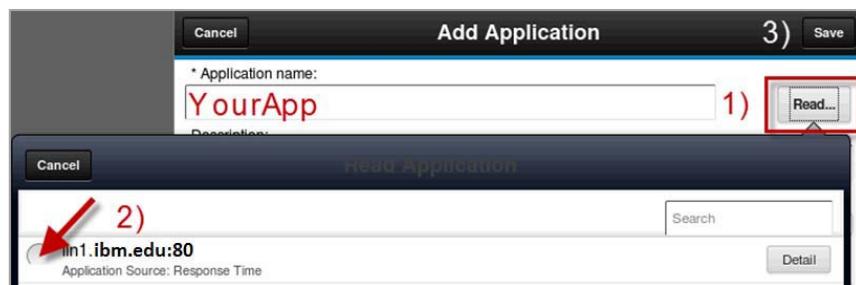
where `path` is the relative path to the JavaScript monitoring component.

For example:

```
<script language="JavaScript" src="/ClientTime/wrtInstrumentation.js"
type="text/JavaScript"></script>Copy
```

## Incorporating the Response Time agent in applications

The Response Time agent must be incorporated in applications with the **Read** feature in the Application Editor



With your application open in the Application Editor, complete these steps:

1. Click **Read**
2. Select the Application Source: Response Time item
3. Click **Save**

### Incorporating the Response Time agent in applications

The Response Time agent must be incorporated in applications with the Read feature in the Application Editor.

With your application open in the Application Editor:

1. Click **Read**.
2. Select the **Application Source: Response Time** item.

Note: Make sure that the fully qualified version is present. In this course, the application server is **lin1.ibm.edu**. If the only available Response Time instance is “lin1:80” (80 is the port number), generate more data until you see the fully qualified version, “**lin1.ibm.edu:80**”.

3. Select the fully qualified host name.
4. Click **Save**.

## Student exercises



Complete the exercises for this unit in the Course Exercises Guide.

## Summary

Now that you have completed this unit, you should be able to:

- Describe user experience monitoring
- Describe and navigate Response Time and HTTP Server agent data in the Performance Management console
- Deploy the Response Time agent, HTTP Server agent, and JavaScript injection



# **Unit 7 Monitoring applications with synthetic transactions**

IBM Training



## **Monitoring applications with synthetic transactions**

© Copyright IBM Corporation 2018  
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this unit, you learn to monitor an application by using synthetic transactions.

## Learning objectives

After completing this unit, you should be able to:

- Describe how to monitor an application with synthetic transactions
- Describe and navigate the synthetic transaction data in the IBM Cloud APM console
- Deploy synthetic transaction monitoring in an IBM Cloud APM, Advanced Private environment

### *Learning objectives*

This slide lists the objectives for the unit.

## Unit outline

- Lesson 1: Introduction to synthetic transaction monitoring
- Lesson 2: Monitoring synthetic transactions
- Lesson 3: Deploying synthetic transaction monitoring

### *Unit outline*

This slide lists the unit outline.

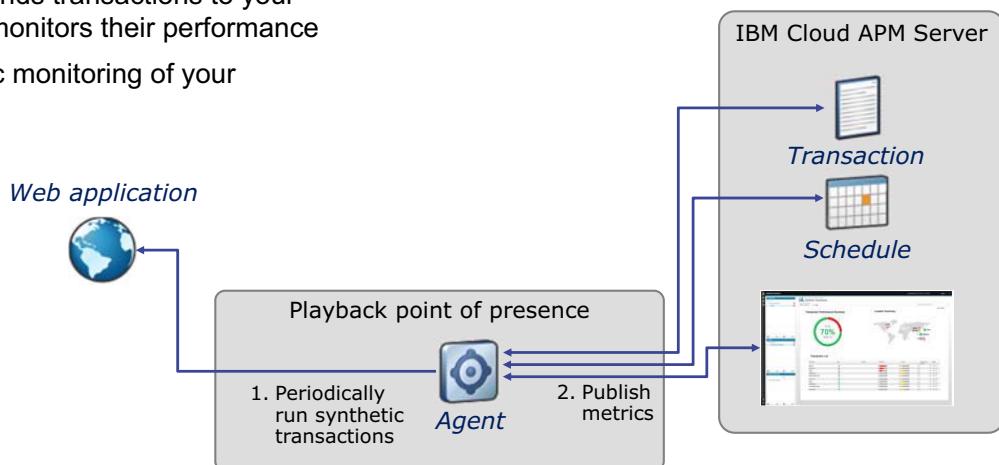
# Lesson 1 Introduction to synthetic transaction monitoring

IBM Training

IBM

## Lesson 1: Introduction to synthetic transaction monitoring

- Monitors the availability and performance of your websites
- Robotic agent sends transactions to your application and monitors their performance
- Provides periodic monitoring of your application



In this lesson, you learn how to describe monitoring an application with synthetic transactions.

- Create synthetic transactions that monitor the performance and availability of private internal-facing web applications.
- Create a synthetic transaction in the Synthetic Script Manager. Generate simple scripts in the Synthetic Script Manager to test the availability of an application, or use Selenium IDE to record synthetic scripts that replicate different user actions with an application. Then, configure a synthetic transaction to play back your script at specific intervals and playback locations.
- Create thresholds and resource groups to raise events and notify stakeholders when your applications are slow or unavailable. View performance data and generate historical reports in the Application Performance Dashboard.

## Two versions

IBM Cloud APM, Advanced Private: Synthetic Monitoring

- Customer deploys Synthetic Playback agent to create own points-of-presence
- Traditional separate interfaces for managing synthetic transactions and viewing data
- Types of transactions
  - Single web page call
  - Scripted user interactions with Selenium IDE

IBM Cloud APM: Availability Monitoring\*

- Provides geographically distributed points of presence that are hosted in IBM Cloud data centers
- New, combined interface for managing synthetic transactions and viewing data
- Types of transaction
  - Single web page or API call
  - Scripted user interactions with Selenium or scripted REST API sequences
- Optionally, user can deploy Synthetic Playback agent to create own points of presence

**\*How to deploy synthetic monitoring in Availability Monitoring is not covered in this course**

### Two versions

Monitoring with synthetic transactions provides periodic monitoring of the performance and availability of your websites from multiple geographically distributed points of presence.

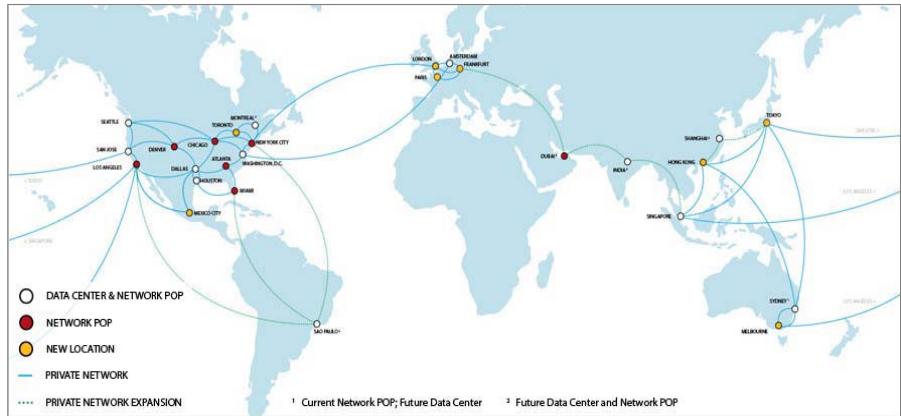
Create a synthetic transaction in the Synthetic Script Manager. Generate simple scripts in the Synthetic Script Manager to test the availability of an application, or use Selenium IDE to record synthetic scripts that replicate different user actions with an application. Then, configure a synthetic transaction to play back your script at specific intervals and playback locations.

Create thresholds and resource groups to raise events and notify stakeholders when your applications are slow or unavailable. View performance data and generate historical reports in the Application Performance Dashboard.

If you monitor user response time for an application with the Response Time agent, you can view KPIs for both user and synthetic transactions in the Application Performance Dashboard. Add synthetic transactions as components to the application that you are monitoring with the Response Time agent.

## Points of presence

- Points of presence are the agents from which synthetic transactions are played and monitored
  - POPs in different locations monitor different access points to your application
- Private: You must deploy your points of presence (Synthetic Playback agent)
- Cloud (Availability Monitoring):  
Use IBM provided points of presence (POP) and deploy own, as needed
  - No work is required on your part to create points of presence
  - Fifteen current locations around the globe



Monitoring applications with synthetic transactions

6

© Copyright IBM Corporation 2018

### Points of presence

IBM Cloud APM (SaaS) is now available as built-in functions in the IBM Cloud APM Advanced offering. You record synthetic transactions for your key business transactions and schedule them to be periodically run from the IBM points of presence.

After a script is uploaded and a corresponding synthetic transaction is defined in the Synthetic Script Manager, the script automatically deploys to the global locations set in the synthetic transaction definition. From there, the transaction is played back periodically based on the defined schedule.

# Lesson 2 Monitoring synthetic transactions

IBM Training



## Lesson 2: Monitoring synthetic transactions

- Dashboards integrate across multiple IBM Cloud APM data sources
- Group scripts together under business applications
- Analyze performance by script, step, and playback location
- Drill into a transaction instance to analyze errors
- Gantt chart visualization helps pinpoint where time is spent



In this lesson, you learn how to navigate and understand the synthetic transaction data in the IBM Cloud APM console.

Use the Application Performance Dashboard to add synthetic transactions as components to a new or existing web application. You can then monitor synthetic transaction data about the availability and performance of your application in the Application Performance Dashboard.

If you are already using the Response Time agent to monitor user response time for an application, you can add a synthetic transaction to this application. You can then view more metrics and KPIs for that application in the Application Performance Dashboard.

## Monitoring synthetic transactions (2 of 4)

The screenshot shows the 'Synthetic Transactions' page in the IBM Application Performance Dashboard. At the top, there's a navigation bar with 'All My Applications > Website Monitoring > Transactions > Synthetic Transactions'. Below the navigation is a 'Status Overview' section with tabs for 'Status Overview' (which is selected) and 'Events'. The main area is divided into two tables: 'Transaction List' and 'Location List'.  
**Transaction List:** This table lists three synthetic transactions: 'splash\_page', 'payments.js', and 'login.js'. Each row includes columns for 'Latest Status' (green checkmark), 'Last Run At' (May 13, 2016, 12:10), 'Response Time Threshold' (15.0, 90.0, 22.0), 'Latest Response Time (Seconds)' (3.33, 118.88, 5.55), 'Average Response Time (Seconds)' (6.08, 85.03, 8.30), 'Unavailable (%)' (0.00, 0.00, 0.00), 'Slow (%)' (12.00, 50.00, 0.00), and 'Runs' (96, 96, 88).  
**Location List:** This table lists two locations: 'Dallas' and 'San Jose'. Each row includes columns for 'Latest Status' (green checkmark), 'Last Run At' (May 13, 2016, 12:10 and 12:05), 'Latest Response Time (Seconds)' (5.55 and 7.62), 'Average Response Time (Seconds)' (42.53 and 25.17), 'Unavailable (%)' (0.00, 0.00), 'Slow (%)' (34.00 and 8.00), and 'Runs' (140, 140).  
**Callout Box:** A yellow callout box is positioned over the Transaction List table, containing the following text:

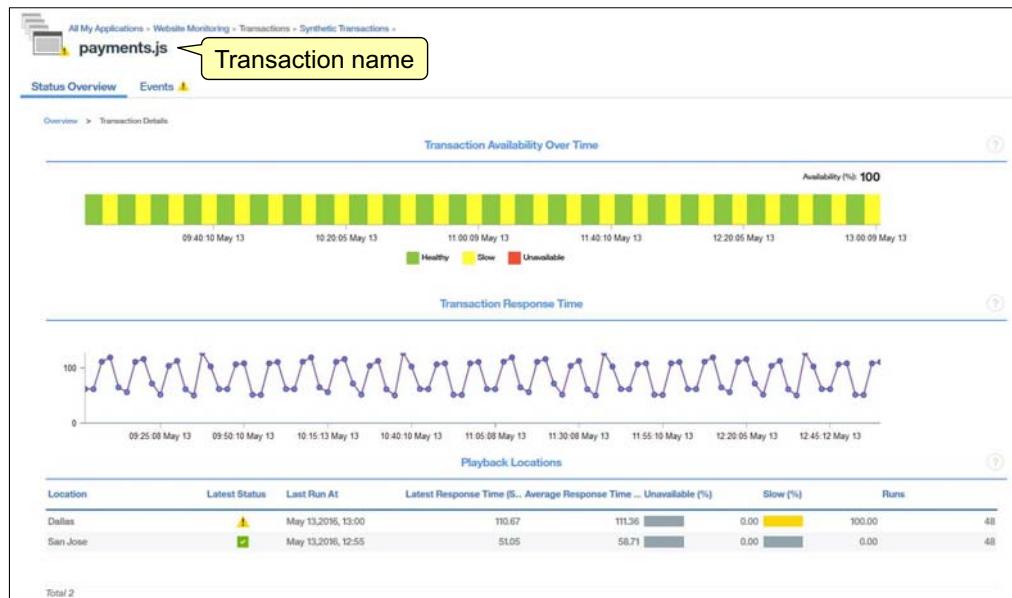
- The **Transaction List** supports drill-down
- No further drill-down is supported for the **Location List**

### Monitoring synthetic transactions (2 of 4)

Use the Application Performance Dashboard to add synthetic transactions as components to a new or existing web application. You can then monitor synthetic transaction data about the availability and performance of your application in the Application Performance Dashboard.

If you are already using the Response Time agent to monitor user response time for an application, you can add a synthetic transaction to this application. You can then view more metrics and KPIs for that application in the Application Performance Dashboard.

## Monitoring synthetic transactions (3 of 4)



## Monitoring synthetic transactions (3 of 4)

Drilling down into a transaction (in this case, payments.js) shows performance over time and by location.

## Monitoring synthetic transactions (4 of 4)

The screenshot shows a monitoring dashboard for synthetic transactions. At the top left, there's a section titled "Playback Locations" with two entries: Dallas (status yellow) and San Jose (status green). A blue arrow points from a callout box labeled "Click a Location to see transaction instances" to the Dallas entry. To the right of this is a "Transaction Instances" table:

| Timestamp          | Status | Response Time (Seconds) |
|--------------------|--------|-------------------------|
| May 13,2016, 13:00 | ⚠️     | 110.67                  |
| May 13,2016, 13:00 | ⚠️     | 108.24                  |
| May 13,2016, 12:50 | ⚠️     | 108.24                  |
| May 13,2016, 12:50 | ⚠️     | 106.45                  |
| May 13,2016, 12:40 | ⚠️     | 102.39                  |
| Total 49           |        |                         |

Below this is a "Subtransaction Instances" table:

| Location | Latest Status | Timestamp          | Status | Response Time (Seconds) | Location |
|----------|---------------|--------------------|--------|-------------------------|----------|
| Dallas   | ⚠️            | May 13,2016, 13:05 | ✓      | 14.63                   | San Jose |
| San Jose | ✓             | May 13,2016, 13:05 | ✓      | 74.48                   | San Jose |
| Total 2  |               | May 13,2016, 13:00 | ⚠️     | 74.63                   | Dallas   |
|          |               | May 13,2016, 13:00 | ⚠️     | 74.46                   | Dallas   |
|          |               | May 13,2016, 12:55 | ✓      | 11.49                   | San Jose |
|          |               | Total 24           |        |                         |          |

A blue arrow points from another callout box labeled "Click a Subtransaction to see instances" to the "check\_out" entry in the subtransaction table. The subtransaction table data is as follows:

| Subtransaction | Latest Status | Timestamp          | Status | Response Time (Seconds) | Location |
|----------------|---------------|--------------------|--------|-------------------------|----------|
| check_out      | ✓             | May 13,2016, 13:00 | ✓      | 15.0                    | 7.48     |
| view_buy       | ✓             | May 13,2016, 13:00 | ✓      | 15.0                    | 3.99     |
| check_part     | ✓             | May 13,2016, 13:00 | ✓      | 15.0                    | 4.52     |
| Total 24       |               |                    |        |                         |          |

### Monitoring synthetic transactions (4 of 4)

The lowest level of drill-down in website monitoring takes administrators to transaction instances by location and subtransaction instances.

## Synthetic transaction monitoring reports

The figure consists of three side-by-side screenshots of a report catalog interface, likely from IBM Application Performance Management (APM) software. Each screenshot shows a hierarchical list of reports under a specific category.

- Screenshot 1:** Shows the top-level "Public Folders" view. A folder named "APM Synthetic" is highlighted with a red box. Other visible categories include "Application Performance", "Common Reporting", "IBM Monitoring 8.1.2 WebSphere Reports", and "IBM Tivoli Monitoring OS Agents Reports".
- Screenshot 2:** Shows the contents of the "APM Synthetic" folder. It contains several report items:
  - "Http Metrics reports"
  - "Transaction Detail by Locations"
  - "Transaction Detail by Subtransactions"
  - "Transactions Overall"
  - "Trend of Subtransactions"
  - "Trend of Transactions"
- Screenshot 3:** Shows the contents of the "Http Metrics reports" folder. It contains:
  - "Http Metrics by Locations of Subtransaction"
  - "Http Metrics by Locations of Transaction"
  - "Http Metrics by Subtransactions"
  - "Http Metrics by Transactions"
  - "Timely Analysis by Locations of Subtransaction"
  - "Timely Analysis by Locations of Transaction"
  - "Timely Analysis by Subtransactions"
  - "Timely Analysis by Transactions"

\*How to run reports is covered in a later unit

### Synthetic transaction monitoring reports

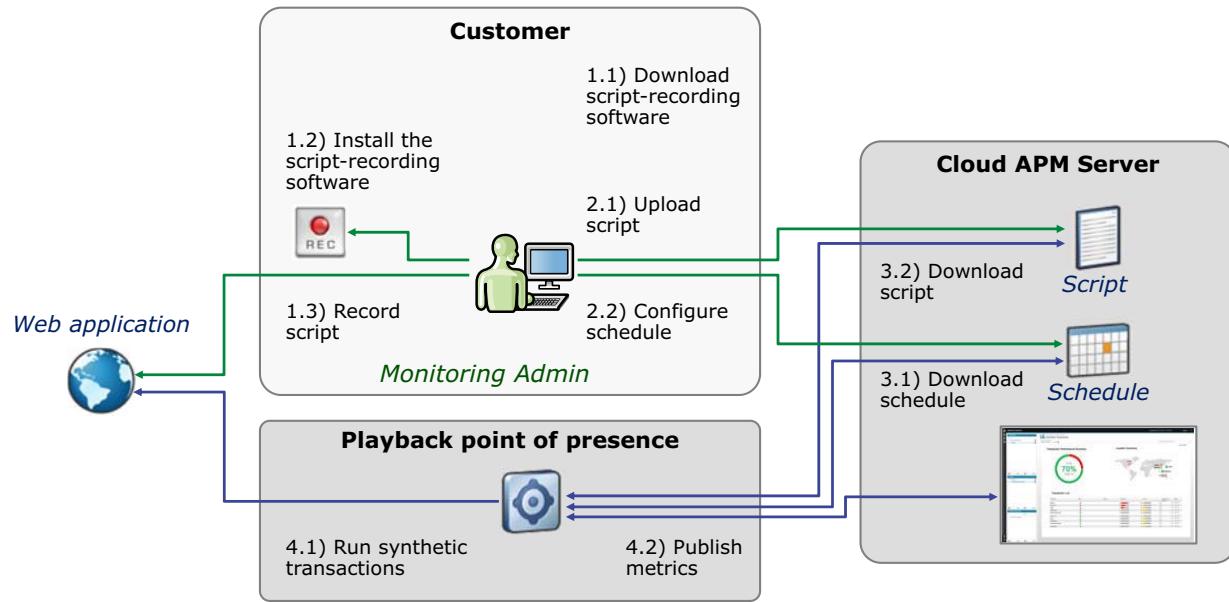
APM provides many prebuilt reports for synthetic transaction monitoring.

# Lesson 3 Deploying synthetic transaction monitoring

IBM Training

IBM

## Lesson 3: Deploying synthetic transaction monitoring



Monitoring applications with synthetic transactions

12

© Copyright IBM Corporation 2018

In this lesson, you learn how to deploy synthetic transaction monitoring in an IBM Cloud APM, Advanced Private environment.

The slide shows the synthetic monitoring workflow. The customer identifies a single URL to monitor or records a script that tests multiple website URLs.

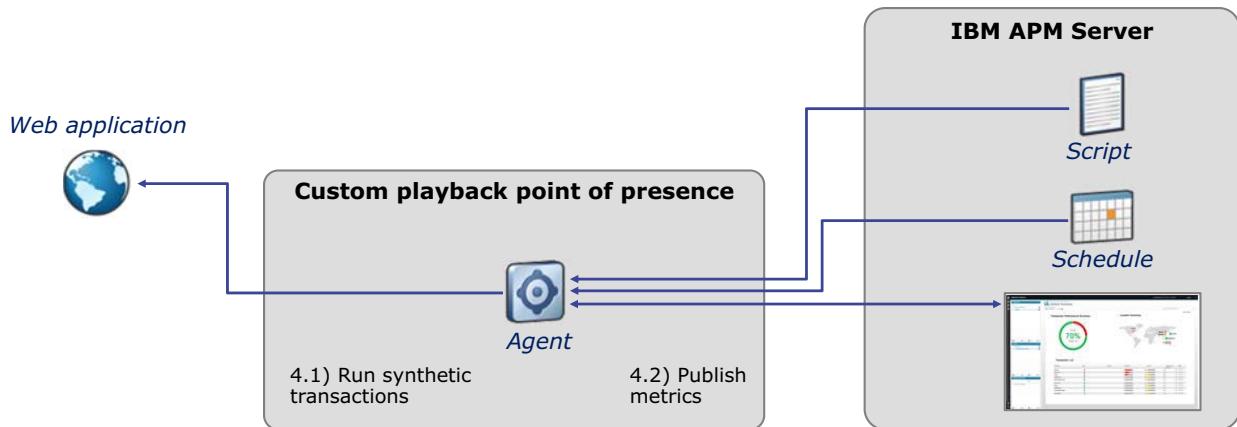
The user then creates the synthetic transaction in the PM Console, entering the single URL or uploading the recorded script. The synthetic transaction has a playback schedule, points of presence, and thresholds.

With the Cloud solution (Availability Monitoring), IBM provides different points of presence around the world. With IBM Cloud APM, users can optionally create their own points of presence by deploying the Synthetic Playback agent. With IBM Cloud APM Private, users must create their own points of presence by deploying the Synthetic Playback agent.

The script plays back on the schedule at the identified points of presence, and the synthetic transactions are monitored.

## Creating custom playback points of presence

- Install the Synthetic Playback agent to create your own playback points of presence
  - Optional for Cloud APM SaaS
  - Required for Cloud APM Private



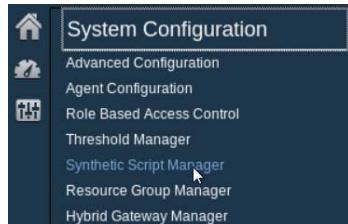
### Creating custom playback points of presence

Create synthetic transactions that monitor the performance and availability of private internal-facing web applications.

Create a synthetic transaction in the Synthetic Script Manager. Generate simple scripts in the Synthetic Script Manager to test the availability of an application, or use Selenium IDE to record synthetic scripts that replicate different user actions with an application. Then, configure a synthetic transaction to play back your script at specific intervals and playback locations.

Create thresholds and resource groups to raise events and notify stakeholders when your applications are slow or unavailable. View performance data and generate historical reports in the Application Performance Dashboard.

## Managing synthetic transactions



- In the System Configuration menu, select the **Synthetic Script Manager**
- View configuration and playback data on existing synthetic transactions
- Add, remove, and edit synthetic transactions

| Transaction Name | Synthetic Script File Name | URL | Description                  | Locations |
|------------------|----------------------------|-----|------------------------------|-----------|
| MyDayTraderApp   | MyDayTraderApp.html        |     | Runs the MyDayTraderApp.html | Austin    |

| Status  | Playback Mode | Interval | Measurements Per Month | Modified Date            | Modified By |
|---------|---------------|----------|------------------------|--------------------------|-------------|
| Started | simultaneous  |          | 5                      | 8,928 Oct 26,2017, 12:18 | apmadmin    |

### Managing synthetic transactions

You manage synthetic transactions in the Synthetic Script Manager. For each synthetic transaction, you can see the transaction name, the URL or script that is run, the locations where it runs, its schedule, and some playback data.

From the Synthetic Script Manager, you can also add, remove, and edit synthetic transactions.

## Creating synthetic transactions that use a URL

The screenshot shows the 'System Configuration' menu with 'Synthetic Script Manager' selected. The main panel displays the 'Upload a Script' tab with fields for 'Transaction Name' (set to 'developerWorks\_blackListAndWriteList') and 'Description'. Below this, there's a section for 'Synthetic Script File' with an 'Upload Script' button and a field containing the URL 'http://www.ibm.com/developerworks/'. At the bottom, there are two sections: 'Blacklist' (containing 'dw\*.s81c.com') and 'Whitelist' (containing 'ibm.com,\*developerworks\*,\*.s81c.com/\*'). A large red box surrounds both the 'Blacklist' and 'Whitelist' sections.

1. In the **System Configuration** menu, select the **Synthetic Script Manager**

2. On the **Upload a Script** tab, assign a transaction name

- The name then appears at the top of the screen

3. Select the URL option:

- Enter any blacklisted addresses \*
- Enter any whitelisted addresses \*

4. Save and activate the transaction

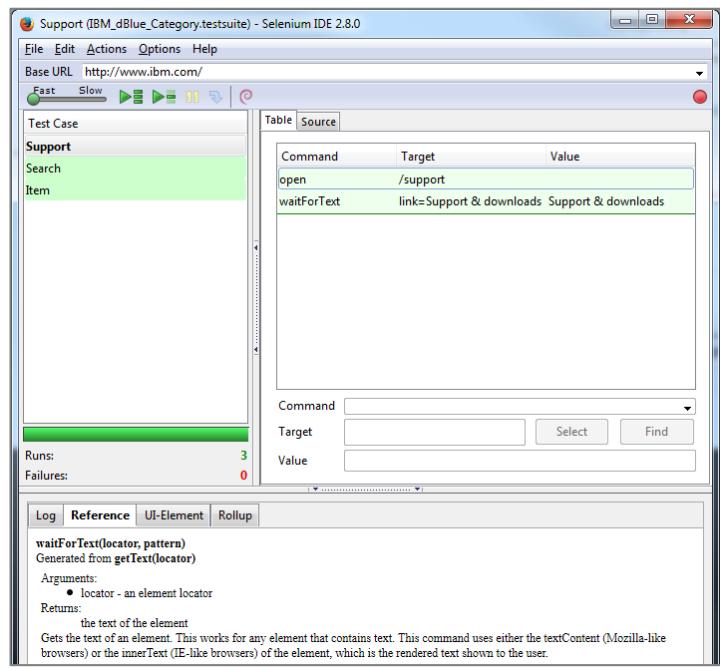
### Creating synthetic transactions that use a URL

Blacklists and whitelists for your synthetic transactions exclude or include requests to specified URLs and domains. Use blacklists and whitelists to filter out or include dependencies that affect the response times for your application, such as third-party metrics.

See documentation for rule details, including wildcards.

## Recording Selenium IDE scripts

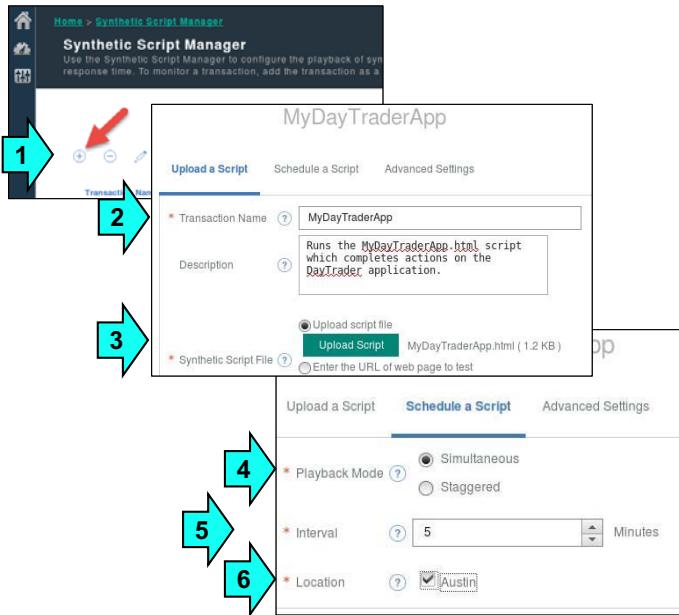
- Record your synthetic transactions visually by using a Firefox browser plug-in
  - Download Selenium IDE from <http://docs.seleniumhq.org/download/>
- Built upon industry-leading Selenium technology
  - Selenese scripting language provides rich capabilities for validating page contents
  - Organize your scripts into multiple test cases to indicate the steps in a business process
- Script recording process
  - Enter base URL
  - Click Start recording button
  - Complete actions in browser
  - Click Stop recording button
  - Save script
- Supported script formats:
  - **.html**
  - **.zip**



### Recording Selenium IDE scripts

Record a script by using the Firefox web browser and the Selenium IDE add-on. With Selenium IDE, you can record user actions on a web page, such as loading a page, clicking a link, or selecting an object. When Selenium IDE is recording, it generates a command for each user action in a script. Then, using Synthetic Script Manager, you can configure scripts to simulate user behavior at your website, at set intervals and at different locations.

## Creating synthetic transactions that use a script (1 of 2)



Monitoring applications with synthetic transactions

17

© Copyright IBM Corporation 2018

### Creating synthetic transactions that use a script (1 of 2)

This slide shows the steps for defining a script-based synthetic transaction.

Note on step 4 to select **Simultaneous** to run the transaction from all locations simultaneously, or select **Staggered** to run the transaction from a different location at each interval.

## Creating synthetic transactions that use a script (2 of 2)

The screenshot shows the 'Advanced Settings' tab of a synthetic transaction configuration. On the left, there's a table for setting thresholds for subtransactions. The first row has 'DayTrader2' as the transaction name and '10' as the response time threshold. The second row has 'open' as the subtransaction name and '2' as the response time threshold. To the right, there's a section for 'Configure variable substitutions for different locations' which currently says 'No Variables defined in this script'. Two blue arrows point to these sections: '7a' points to the subtransaction table, and '7b' points to the variable substitution section.

| Transaction Name | Response Time Threshold (Seconds) |
|------------------|-----------------------------------|
| DayTrader2       | 10                                |
| open             | 2                                 |
| clickAndWait     |                                   |

Configure variable substitutions for different locations  
No Variables defined in this script

7. Where applicable, use the **Advanced Settings** tab to:
  - a) Set thresholds for full script or subtransactions
  - b) Configure variable substitutions
8. Save the transaction

### Creating synthetic transactions that use a script (2 of 2)

Use **Advanced Settings** to configure the response time thresholds and variable substitutions for the transactions. Modify the default response time of 10 seconds for the overall transactions. For Selenium IDE scripts, you can set thresholds for subtransactions.

## Student exercises



Complete the exercises for this unit in the Course Exercises Guide.

## Summary

Now that you have completed this unit, you should be able to:

- Describe how to monitor an application with synthetic transactions
- Describe and navigate the synthetic transaction data in the IBM Cloud APM console
- Deploy synthetic transaction monitoring in an IBM Cloud APM, Advanced Private environment

# **Unit 8 Monitoring resources**

This unit covers installation and configuration of monitoring agents on both the Windows and Linux environments. You learn about agent installation, configuration, and resource-monitoring features of monitoring agents.

IBM Training



## **Monitoring resources**

© Copyright IBM Corporation 2018  
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

## Learning objectives

After completing this unit, you should be able to:

- Describe the features of resource monitoring
- Explain the types of configuration
- Configure monitoring agents for DB2, WebSphere, and Node.js (agent and data collectors)

### *Learning objectives*

This slide lists the objectives for the unit.

## Unit outline

- Lesson 1: Overview of resource monitoring
- Lesson 2: Deployment planning for resource monitoring agents
- Lesson 3: Configuration of resource monitoring agents

# Lesson 1 Overview of resource monitoring

IBM Training



## Lesson 1: Overview of resource monitoring

What resource monitoring includes:

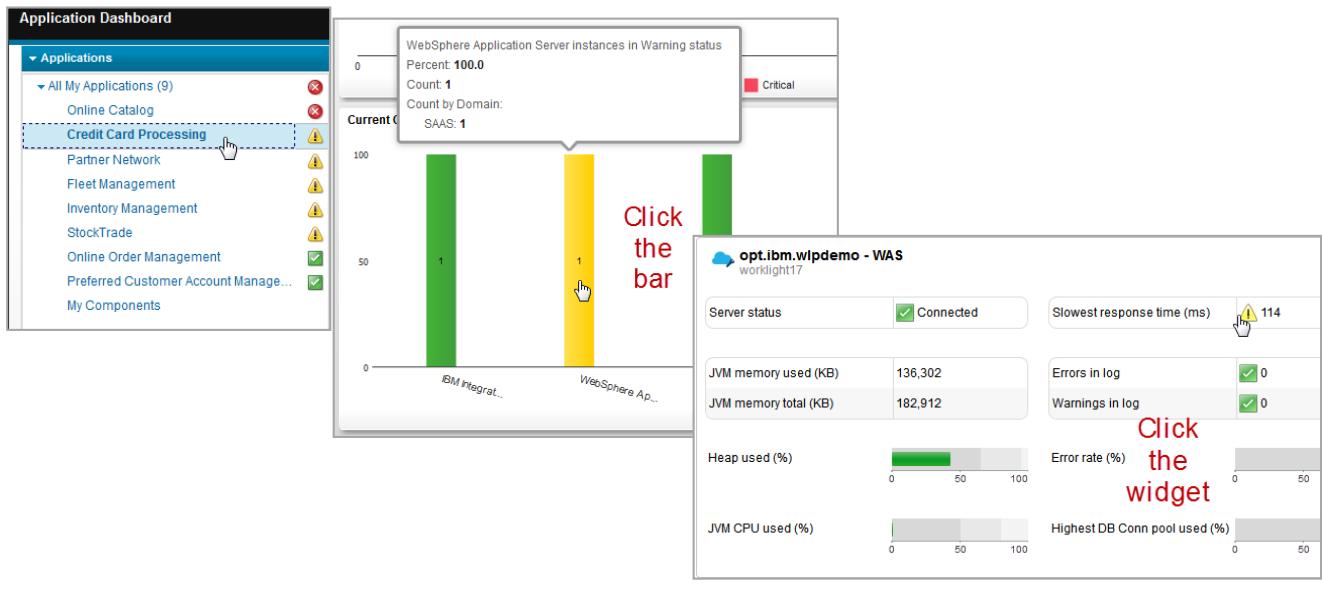
- Application-centric dashboards that show resource status at a glance
- Drill down from the resource instance
- All agents support resource monitoring except for:
  - Response Time Agent
  - Monitoring Agent for Synthetic Transactions
- For a full list of agents, see Unit 1

What resource monitoring does not include:

- Transactional monitoring
  - Response time monitoring (see Unit 6)
  - Synthetic transaction monitoring (see Unit 7)
  - Transaction tracking (see Unit 9)
- Code-level diagnostic data (see Unit 10)
  - Heap dump analysis
  - Memory analysis
  - In-flight request monitoring

Resource monitoring in Cloud APM refers to agents that collect domain-specific data. It supports drill-down, and all functions that are already discussed in this course such as thresholds.

## Application-centric dashboards show resource status at a glance (review)



Monitoring resources

5

© Copyright IBM Corporation 2018

Application-centric dashboards showing resource status at a glance (review)

The Cloud APM console navigator is hierarchical, giving a status overview of your applications, the health of their components, and the quality of the user experience. For more details about your monitored resource, you can click a navigator item or a link in the Status Overview tab. Consider, for example, that your application has a slow response time. The issue is revealed in the dashboard. Starting from your dashboard, you can follow the problem to the source by clicking links to discover the cause: a DB2 problem.

Identify a red or yellow component. Click the component bar to navigate to the component summary. Click the summary to view the component details.

## Drill down from the instance to resource details (review)

**Instance widget**

**Summary Overview Dashboard**

**Requests with Slowest Response Time**

| URI  | Request Name        | Average Response Time (ms) | Count |
|--|---------------------|----------------------------|-------|
| com.ibm.websphere.samples.daytrader....    | getClosedOrders     | 87                         | 0.00% |
| http://lin1.ibm.edu/daytrader/webservic... | /daytrader/scenario | 61                         | 0.00% |
| http://lin1.ibm.edu/daytrader/app          | /daytrader/app      | 16                         | 0.00% |
| com.ibm.websphere.samples.daytrader....    | onMessage           | 5                          | 0.00% |

Click an instance widget (in this case for WebSphere Application Server) to access an overview dashboard, including :

- Slow requests
- In-flight requests
- JVM garbage collection
- EJB containers

Many of these widgets support drill-down to detailed dashboards for the KPIs in question

Drill down from the instance to resource details (review)

Click a resource instance widget to access resource detail dashboards.

# Lesson 2 Deployment planning

IBM Training



## Lesson 2: Deployment planning

### Questions to consider for resource monitoring agents

- Monitored resource on-premises or SaaS?
- Any hardware or software prerequisites?
- User management
- Base or Advanced agent?
  - Resource monitoring only?
  - Deep-dive diagnostics?
  - Transaction tracking?
- Stand-alone agent or data collector?
- Monitored resource remote or local?
- Multi-instance monitored resource?

In this lesson, you learn how to evaluate several factors that affect solution deployment, including:

- On-premises versus SaaS
- Hardware and software prerequisites
- Relative advantages of agents and data collectors
- Remote versus local resource monitoring

## Supported data collector domains

- Domains supporting data collectors:
  - J2SE
  - Liberty
  - Node.js
  - Python
  - Ruby
- Each data collector is configured differently
- See the previous two slides for the configuration procedure for the Node.js data collector:
  - On IBM Cloud
  - On-premises
- Configuration of the other data collectors is not covered in this course

## Comparative advantages of agents

- Install agents when you need:
  - Greater scalability
  - Limited sockets from endpoints to the server
- Maximum flexibility when configuring thresholds:
  - Agents support limiting attributes to the environment that you want to monitor
  - With data collectors, you must choose from the attributes of several data collectors
- Ability to turn on or off diagnostic data collection functions in the Cloud APM console:
  - Diagnostics
  - Transaction tracking
  - Method trace
- On-demand diagnostic data:
  - In-flight requests
  - Heap dump at the current time

## Comparative advantages to installing data collectors

- Install data collectors when you need maximum ease of installation
  - Agents take minutes to install, plus configuration after the installation
  - Data collectors require no installation, only unpacking on the target system, with minimal configuration to follow
- When the responsibility for ownership of monitoring deployment needs to be “shifted left”:
  - Development teams can build data collector installation and configuration into the Continuous Integration / Continuous Deployment process
  - Smaller footprint of the data collector makes it easier for multi-Cloud deployment
  - When applications are installed in containers
- When monitoring applications or platforms that Cloud APM agents do not support:
  - IBM Cloud
  - J2SE
  - Python

## DB2 agent deployment planning

- On-premises or SaaS?
  - On-premises: Configure agent installation package by (and for) Cloud APM Server, then transfer to monitored system
  - SaaS: Download agent installation package from cloud-based Cloud APM server, then transfer to monitored system (see Unit 03)
- Hardware and software prerequisites
  - See the most current Software Product Compatibility Reports
- User management
  - Non-root installation (see product documentation)
  - Configure agent by using same root or non-root user that was used for installing the agent
  - Other user options for configuring and starting agent (see product documentation)
- Remote versus local database monitoring
  - Remote monitoring is enabled during installation (see product documentation)
- Agent instances
  - DB2 agent is multi-instance
  - Same monitoring capabilities in both Advanced and Base agent packages
  - Use naming convention that helps identify instance place in architecture



**Note:** Detailed information is not being provided for non-root installations and remote monitoring since implementing those options is not part of this course.

## WebSphere agent deployment planning

- On-premises or SaaS?
  - On-premises: Configure agent installation package by (and for) Cloud APM server, then transfer to monitored system
  - SaaS: Download agent installation package from the Cloud APM server, then transfer to monitored system (see Unit 3)
- Cloud APM Base or Advanced?
  - Resource monitoring only? (Base and Advanced)
  - Deep-dive diagnostics? (Advanced only)
  - Transaction tracking? (Advanced only)
- WebSphere cluster or single server? (see Notes section)
- User management
- Stand-alone or embedded data collector?
  - WebSphere Liberty on IBM Cloud?
  - WebSphere Application Server?
  - Embedded DC is the deployment option that is used for this course



**Note:** Specific to WebSphere clusters: You can configure the data collector to monitor application server instances in a dynamic cluster. To do this configuration, add some data collector configuration parameters to the server template that is used to create the dynamic cluster server instances. This method is an alternative to configuring dynamic cluster server instances to create the server templates specific for the WebSphere Applications agent.

# Lesson 3 Configuration

IBM Training



## Lesson 3: Configuration

- Manual configuration of a multi-instance agent
- Configuration by using the silent\_config script
- Agent-image preconfiguration
- Run the installation script

See Notes page about agent installation



**Note:** The steps for preconfiguring installation packages and running the initial installation of agents are the same regardless of domain. However, the requisite configuration procedures have differences, which are the focus of this lesson.

## Configuration summary (1 of 5)

| Agent  | More configuration tasks required | Multi-instance |
|--|-----------------------------------|----------------|
| Monitoring Agent for Amazon EC2                            | Yes                               | Yes            |
| IBM Cloud data collectors                                  | Yes                               |                |
| Monitoring Agent for Cassandra                             | Yes                               | Yes            |
| Monitoring Agent for Cisco UCS                             | Yes                               | Yes            |
| Monitoring Agent for Citrix Virtual Desktop Infrastructure | Yes                               | Yes            |
| Monitoring Agent for DataPower                             | Yes                               | Yes            |
| Monitoring Agent for DB2                                   | Yes                               | Yes            |
| Monitoring Agent for Hadoop                                | Yes                               |                |
| Monitoring Agent for HMC Base                              | Yes                               | Yes            |
| Monitoring Agent for HTTP Server                           | Yes                               |                |
| Monitoring Agent for IBM Integration Bus                   | Yes                               | Yes            |
| J2SE data collector  | Yes                               |                |

### Configuration summary (1 of 5)

This table shows which agents require tasks to be completed before the agent can collect data. These tasks include setting up special permissions in the target software to be monitored, installing prerequisite software, or setting up secure connections between the monitoring agent and the target.

## Configuration summary (2 of 5)

| Agent  | More configuration tasks required | Multi-instance |
|--|-----------------------------------|----------------|
| Monitoring Agent for JBoss                                   | Yes                               | Yes            |
| Liberty data collector                                       | Yes                               |                |
| Monitoring Agent for Linux KVM                               | Yes                               | Yes            |
| Monitoring Agent for Linux OS                                |                                   |                |
| Monitoring Agent for Microsoft Active Directory              | Yes                               |                |
| Monitoring Agent for Microsoft Cluster Server                | Yes                               |                |
| Monitoring Agent for Microsoft Exchange Server               | Yes                               |                |
| Monitoring Agent for Microsoft Hyper-V Server                | Yes                               |                |
| Monitoring Agent for Microsoft Internet Information Services | Yes                               |                |
| Monitoring Agent for Microsoft Lync Server                   | Yes                               |                |
| Monitoring Agent for Microsoft Office 365                    | Yes                               |                |

## Configuration summary (3 of 5)

| Agent  | More configuration tasks required | Multi-instance |
|--|-----------------------------------|----------------|
| Monitoring Agent for Microsoft .NET              | Yes                               |                |
| Monitoring Agent for Microsoft SharePoint Server | Yes                               |                |
| Monitoring Agent for Microsoft SQL Server        | Yes                               | Yes            |
| Monitoring Agent for MongoDB                     | Yes                               | Yes            |
| Monitoring Agent for MySQL                       | Yes                               | Yes            |
| Monitoring Agent for NetApp Storage              | Yes                               | Yes            |
| Monitoring Agent for Node.js                     | Yes                               |                |
| Node.js data collector                           | Yes                               |                |
| Monitoring Agent for OpenStack                   | Yes                               | Yes            |
| Monitoring Agent for Oracle Database             | Yes                               | Yes            |
| Monitoring Agent for PHP                         | Yes                               | Yes            |
| Monitoring Agent for PostgreSQL                  | Yes                               | Yes            |
| Python data collector                            | Yes                               |                |

## Configuration summary (4 of 5)

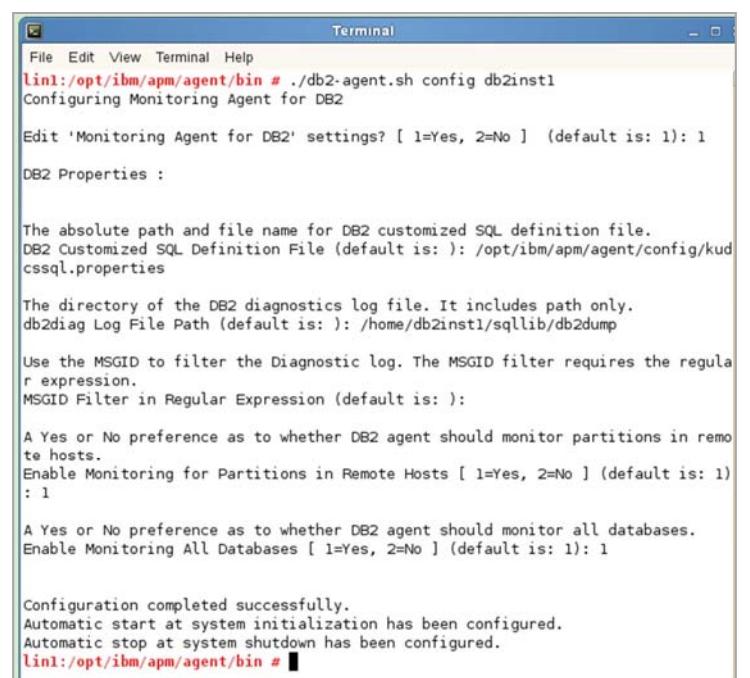
| Agent  | More configuration tasks required | Multi-instance |
|--|-----------------------------------|----------------|
| Monitoring Agent for RabbitMQ                  | Yes                               | Yes            |
| Monitoring Agent for Ruby                      | Yes                               | Yes            |
| Ruby data collector for IBM Cloud applications | Yes                               |                |
| Monitoring Agent for SAP Applications          | Yes                               | Yes            |
| Monitoring Agent for SAP HANA Database         | Yes                               | Yes            |
| Monitoring Agent for SAP NetWeaver Java Stack  | Yes                               | Yes            |
| Monitoring Agent for Siebel                    | Yes                               | Yes            |
| Monitoring Agent for Tomcat                    | Yes                               | Yes            |
| Monitoring Agent for UNIX OS                   |                                   |                |

## Configuration summary (5 of 5)

| Agent   | More configuration tasks required | Multi-instance |
|---|-----------------------------------|----------------|
| Monitoring Agent for VMware VI                        |                                   | Yes            |
| Monitoring Agent for WebLogic                         |                                   | Yes            |
| Monitoring Agent for WebSphere Applications           | Yes                               |                |
| Monitoring Agent for WebSphere Infrastructure Manager |                                   | Yes            |
| Monitoring Agent for WebSphere MQ                     |                                   | Yes            |
| Monitoring Agent for Windows OS                       |                                   |                |

## Configuring multi-instance agents

- Multiple-instance agents
- Run the following command:  
`xxx-agent.sh config instancename`
- Example: Monitoring Agent for DB2  
`db2-agent.sh config db2inst1`



A terminal window titled "Terminal" showing the configuration of the Monitoring Agent for DB2. The command run is `./db2-agent.sh config db2inst1`. The window displays various configuration options and their default values, such as the DB2 properties file path (`/opt/ibm/apm/agent/config/kudssql.properties`) and the db2diag log file path (`/home/db2inst1/sqllib/db2dump`). It also shows the configuration of monitoring for partitions in remote hosts and all databases. The configuration is completed successfully, and automatic start and stop at system initialization and shutdown are configured.

```
File Edit View Terminal Help
lin1:/opt/ibm/apm/agent/bin # ./db2-agent.sh config db2inst1
Configuring Monitoring Agent for DB2

Edit 'Monitoring Agent for DB2' settings? [ 1=Yes, 2=No ] (default is: 1): 1

DB2 Properties :

The absolute path and file name for DB2 customized SQL definition file.
DB2 Customized SQL Definition File (default is: ): /opt/ibm/apm/agent/config/kudssql.properties

The directory of the DB2 diagnostics log file. It includes path only.
db2diag Log File Path (default is: ): /home/db2inst1/sqllib/db2dump

Use the MSGID to filter the Diagnostic log. The MSGID filter requires the regular expression.
MSGID Filter in Regular Expression (default is: )

A Yes or No preference as to whether DB2 agent should monitor partitions in remote hosts.
Enable Monitoring for Partitions in Remote Hosts [ 1=Yes, 2=No ] (default is: 1): 1

A Yes or No preference as to whether DB2 agent should monitor all databases.
Enable Monitoring All Databases [ 1=Yes, 2=No ] (default is: 1): 1

Configuration completed successfully.
Automatic start at system initialization has been configured.
Automatic stop at system shutdown has been configured.
lin1:/opt/ibm/apm/agent/bin #
```

Monitoring resources

19

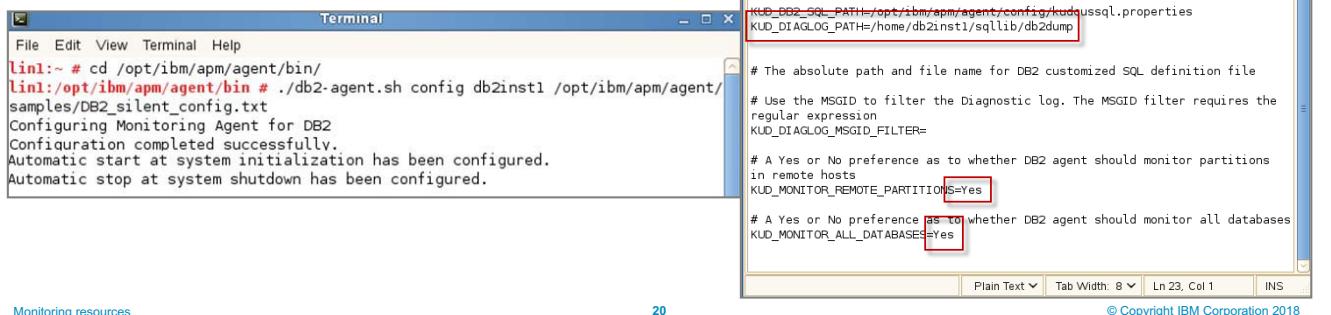
© Copyright IBM Corporation 2018

### Configuring multi-instance agents

This slide shows a simple multi-instance agent configuration command. In this case, no further configuration is required.

## Configuring an agent with a silent configuration file

- You can silently configure agents:
- Update the configuration file:
- Run the following command:  
`xxx.agent.sh config path_to_configfile/  
configfile.txt`
  - Example: Monitoring Agent for DB2  
`db2-agent.sh config /opt/ibm/apm/agent/  
samples/DB2_silent_config.txt`



The screenshot illustrates the configuration process. On the left, a terminal window shows the command being run and its successful execution. On the right, a 'gedit' window shows the 'DB2\_silent\_config.txt' file with several configuration parameters highlighted by red boxes.

Terminal output:

```
lin1:~ # cd /opt/ibm/apm/agent/bin/  
lin1:/opt/ibm/apm/agent/bin # ./db2-agent.sh config db2inst1 /opt/ibm/apm/agent/  
samples/DB2_silent_config.txt  
Configuring Monitoring Agent for DB2  
Configuration completed successfully.  
Automatic start at system initialization has been configured.  
Automatic stop at system shutdown has been configured.
```

gedit window content (highlighted areas):

```
# samples/DB2_silent_config.txt  
#  
# Syntax rules:  
# where <instance_name> is the DB2 instance name you want to monitor  
  
##### PRIMARY CONFIGURATION #####  
OMSCONNECT=NO  
  
##### DB2 PARAMETERS #####  
KUD_DB2_SQL_PATH=/opt/ibm/apm/agent/config/kudussql.properties  
KUD_DIAGLOG_PATH=/home/db2inst1/sqllib/db2dump  
  
# The absolute path and file name for DB2 customized SQL definition file  
# Use the MSGID to filter the Diagnostic log. The MSGID filter requires the  
regular expression  
KUD_DIAGLOG_MSGID_FILTER=  
  
# A Yes or No preference as to whether DB2 agent should monitor partitions  
in remote hosts  
KUD_MONITOR_REMOTE_PARTITIONS=yes  
  
# A Yes or No preference as to whether DB2 agent should monitor all databases  
KUD_MONITOR_ALL_DATABASES=yes
```

Configuring an agent with a silent configuration file

This slide shows an example of using the silent configuration option available to configure an agent. Instead of providing input to the configuration by using multiple prompts, the input is placed in a file and the file is provided as input to the configuration script.

## Configuring an agent with a postinstallation script (1 of 2)

- Example: Monitoring Agent for WebSphere Application Server
- Change to the directory where the config command is located:

```
/opt/ibm/apm/agent/yndchome/7.3.0.14.0/bin
```

- Run the **config.sh** or **simpleconfig.sh** command

```
Terminal
File Edit View Terminal Help
lin1:/opt/ibm/apm/agent/yndchome/7.3.0.11.0/bin # ./simpleconfig.sh
Please note, if you have installed your Monitored WebSphere instance using non-root credentials, Ensure that
this user has read and write access to files under dchome directory. For more information, see the Monitoring
Agent for WebSphere Applications Installation Guide.

-----
- Monitoring Agent for WebSphere Applications
- Data Collector Simple Configuration
```

### Configuring an agent with a postinstallation script (1 of 2)

Some monitoring agents provide custom scripts that are run to configure the external data collectors. The **simpleconfig.sh** command is an example of the script that is provided by the Monitoring Agent for WebSphere Application Server.

## Configuring an agent with a postinstallation script (2 of 2)

- Monitoring Agent for WebSphere Application Server: results
- Select the application server from the list

```
Log file name: /opt/ibm/apm/agent/yndchome/7.3.0.11.0/data/simpleconfig.trace.log.
List of WebSphere Application Server home directories discovered:
Enter a number or enter the full path to a home directory
 1. /opt/IBM/WebSphere/AppServer
Enter a number:
1
Looking for servers under profile AppSrv01
Discovering profile. Please wait...
Configuring. Please wait...

Please ensure the account that was used to run the application server has the read and write privileges to D
CHome/runtime directories.
Configuration completed successfully.
Please restart the WebSphere servers under the selected profile to exploit the full power of Monitoring Agent
for WebSphere Applications Data Collector.
lin1:/opt/ibm/apm/agent/yndchome/7.3.0.11.0/bin #
```

### Configuring an agent with a postinstallation script (2 of 2)

This slide shows the remaining steps of running the `simpleconfig.sh` command.

## WebSphere agent default configuration

Run the `simpleconfig.sh` command to enable:

- All instances in a profile for WebSphere Application Server
- For WebSphere Liberty, single instance or multiple instances in the same directory
  - To monitor more profiles or instances, repeat the configuration
- Data collector that is configured within the server instances, providing maximum monitoring
- For Cloud APM, Base Private:
  - Resource monitoring is enabled
- For Cloud APM, Advanced Private:
  - Resource monitoring
  - Transaction tracking
  - Diagnostic data is enabled
  - Note: Heap Dump and Memory Analysis must be enabled separately

Run `config.sh` under certain conditions

- Refer to notes
- If a non-root user installed WebSphere or Portal server, some additional steps are required

### WebSphere agent default configuration

Reasons to run `config.sh/config.bat` instead of `simpleconfig.sh/simpleconfig.bat`:

- The simpleconfig configuration utility fails.
- You want to configure monitoring for WebSphere Portal Server instances.
- You want to specify a server alias that is displayed in the monitoring user interface during the data collector configuration.
- You want to have more control of what data to be collected. For example, you want to use resource monitoring only and disable diagnostics data and transaction tracking.
- You do not want to configure all application servers within the same profile at one time.
- The data collector is not configured within the application server and you want to reconfigure it.

## Configuring the Node.js agent

1. Open your `[application].js` file in a text editor of your choice and move the cursor to the indicated position:

This example is for the keystone.js application

```
root@apm:~/downloads/node_app/keystone-demo-master
File Edit View Search Terminal Help
// Load .env for development environments
require('dotenv').load();
var Keystone = require('keystone');
/*
 * Application Initialisation
 */
keystone.init({
```

2. Enter a require statement for the specified level of monitoring:

Resource data only:

```
require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm');
```

Be sure to use single quotation marks:  
`'[file location]'`

Resource data plus diagnostic data:

```
require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm/deepdive.js');
```

Resource data, plus diagnostic and method trace data

```
require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm/methodtrace.js');
```

3. Save the application file

4. Recycle the Node.js agent

## Configuring the Node.js data collector for an on-premises installation

From the home directory of your application:

1. Run the following command to extract files from the data collector package:

```
tar -zxf nodejs_datacollector_8.1.4.0.tgz
```

2. Run the following command to install the data collector to your application:

```
npm install nodejs_dc/ibmapm.tgz
```

3. Add the following line to the beginning of the main file of your Node.js application:

```
require('ibmapm');
```

4. Restart your application

If you start your application by running the `node [app.js]` command, “`app.js`” is the main file of your application

### Configuring the Node.js data collector for an on-premises installation

For collective members in the IBM API Connect environment, the main file is defined in the `package.json` file in the home directory or its subfolders.

The collective member automatically restarts after you run this command. If it does not, run the `wlpn-server start collective_member_name` command to restart it manually.



**Hint:** To restart your collective member, run the `wlpn-server stop collective_member_name` command.

For Developer Portal applications in the IBM API Connect environment, you can run the `ps -ef | grep node` command to find the main file.

To restart your Developer Portal applications, first run the `/etc/init.d/restservice stop` command to stop the application, and then the `/etc/init.d/restservice start` command to start it.

## Student exercises



Complete exercises for this unit in the Course Exercises Guide.

## Summary

You now should be able to:

- Describe the features of resource monitoring
- Explain the types of configuration
- Configure monitoring agents for DB2, WebSphere, and Node.js (agent and data collectors)



# **Unit 9 Tracking transactions through application components**

IBM Training



## **Tracking transactions through application components**

© Copyright IBM Corporation 2018  
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this unit, you learn to describe the transaction tracking features of IBM Cloud Application Performance Management, Advanced.

## Learning objectives

After completing this unit, you should be able to:

- Describe the major functions of transaction tracking
- List monitored domains that support transaction tracking
- Explain how to enable and disable transaction tracking

### *Learning objectives*

This slide lists the objectives for this unit.

## Unit outline

- Lesson 1: Overview of transaction tracking
- Lesson 2: Navigating topologies
- Lesson 3: Configuring transaction tracking

### *Unit outline*

This slide lists the outline for this unit.

# Lesson 1 Transaction tracking overview

IBM Training



## Lesson 1: Overview of transaction tracking

- Monitors availability and performance of middle and back-end transactions
  - For current, live transactions and transactions over time (trend analysis)
- Creates topology diagrams that show transaction paths through application components
  - Identifies where transactions and applications are failing or slow
  - Helps identify root cause of problems
  - Helps determine problem ownership
- Because transaction tracking follows a user request through the different domains of your application, you can quickly locate a problem in a multi-domain application

In this lesson, you learn how to describe transaction tracking.

## Agents supporting transaction tracking

| Agent / data collector (Cloud APM Advanced only)                  | Comments  | Requires initial configuration |
|---|---|--------------------------------|
| DataPower agent   | Must be enabled on the Agent Configuration page.  | Yes                            |
| HTTP Server agent   |   |                                |
| IBM Integration Bus agent   | Must be enabled on the Agent Configuration page.<br><br>REST API services are not monitored by the IIB agent  | Yes                            |
| JBoss agent   | Enabling transaction tracking requires changes to:<br>1. Agent instance environment settings file.<br>2. JBoss server startup file.<br>3. DC Runtime Directory agent configuration parameter.<br><br>A script is provided to help you make the changes. | Yes                            |
| Liberty data collector for IBM Cloud and on-premises applications |   |                                |
| Microsoft .NET agent  | You must first register the data collector, <i>then</i> enable transaction tracking on the Agent Configuration page.  | Yes                            |
| Node.js data collector for IBM Cloud and on-premises applications |   |                                |
| Response Time Monitoring Agent                                    |   |                                |
| SAP NetWeaver Java Stack agent                                    | Must be enabled on the Agent Configuration page.<br><br>Requires Advanced Extension Pack  | Yes                            |
| Tomcat agent  |   |                                |
| WebLogic agent  | Transaction tracking on Linux and Windows only  |                                |
| WebSphere Applications agent                                      |   |                                |
| WebSphere MQ agent  | Must be enabled on the Agent Configuration page.  | Yes                            |

### Agents supporting transaction tracking

This slide shows which agents support transaction tracking.

## Agents: End-to-end correlation support

| From / To | IHS | WebSphere  | IIB        | IBM MQ | DataPower | .NET      |
|-----------|-----|------------|------------|--------|-----------|-----------|
| IHS       |     |            |            | N/A    |           |           |
| WebSphere |     | Except SCA | Except JMS |        |           |           |
| IIB       |     | Except JMS |            |        | SOAP only |           |
| IBM MQ    | N/A |            |            |        |           |           |
| DataPower |     |            | SOAP only  |        |           | SOAP only |
| .NET      |     |            |            |        | SOAP only |           |

### Agents: End-to-end correlation support

This slide shows whether transactions can be tracked between the different agents that can do transaction tracking. Green indicates yes. Red indicates no. Yellow indicate yes in limited cases and lists the cases. White indicates that this intersection is not applicable.

Service Component Architecture (SCA) is a specification that describes a model for building applications and systems by using a service-oriented architecture (SOA).

SCA simplifies the creation and integration of business applications that are built by using an SOA. It separates business logic from its implementation so that you can focus on assembling an integrated application without knowing details of its implementation.

SCA divides the steps of building a service-oriented application into two major parts:

- The implementation of components that provide services and use other services.
- The assembly of these service components to build the business application.

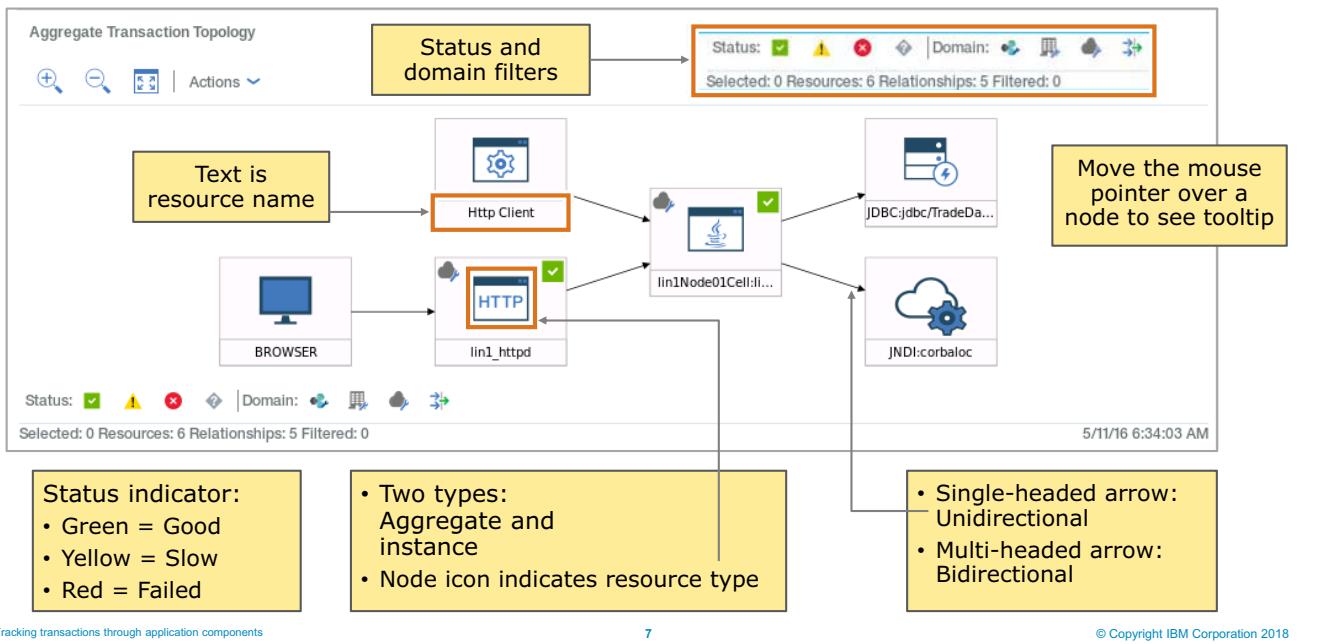
Service components can be assembled graphically by using WebSphere Integration Developer, and the implementation can be added later.

The JMS protocol is based on the Java(TM) Message Service (JMS) and transfers messages through transactional, persistent JMS queues provided by, for example, IBM WebSphere MQ. The JMS protocol supports the following JMS message types:

- StreamMessage (as a byte array)
- BytesMessage (as a byte array)
- TextMessage

In the JMS protocol, one system sends a JMS message to another. After the second system receives the message, it removes it from the queue. From this point forward, the receiving system can process the message asynchronously.

## Elements of transaction topologies



Each node represents the transaction data within a monitored domain. The two types of topologies are aggregate and instance:

- An aggregate topology represents the average performance of a transaction over the aggregate interval.
- An instance topology is a topology based on a single transaction instance and shows actual time values.

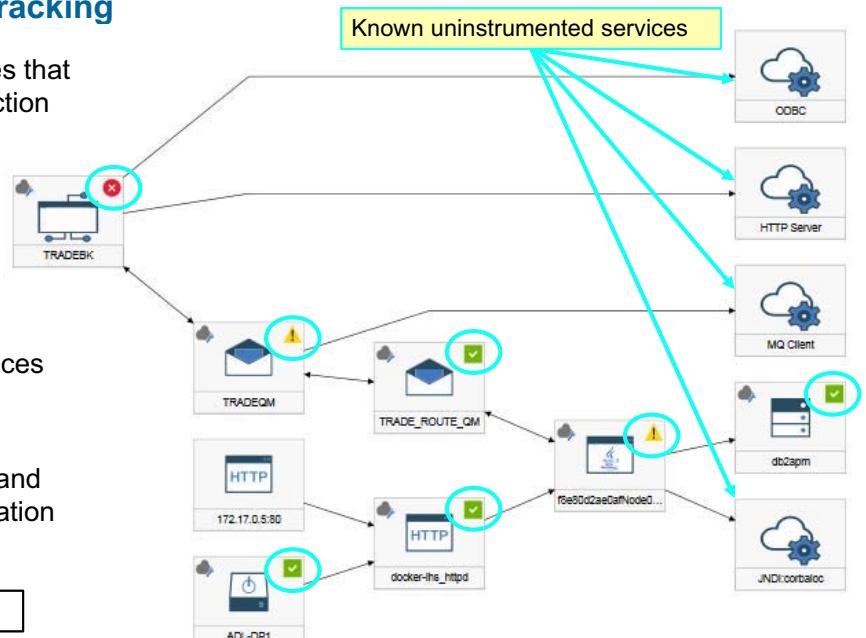
The node image is unique for each monitored domain. Lines between nodes show transactions that flow between nodes. Lines with one arrowhead indicate the transaction requests flow in one direction only. Lines with two arrowheads indicate bidirectional transactions. A status indicator for good, slow, or failed is placed on the upper right of each node.

Roll over a node for details on that node.

## Uninstrumented service tracking

- Mechanism to visualize services that are not tracked through transaction tracking, but interact with tracked domains
  - Referred to as pseudo nodes
- Known uninstrumented services
- Get service-specific icon
- Unknown uninstrumented services
  - Get generic icon
  - Do not get a status icon
- Display in topology is enabled and disabled in Advanced Configuration
  - Disabled by default

 = Instrumented services



### Uninstrumented service tracking

Uninstrumented Service Tracking provides a mechanism for users to visualize services that are used by an application that is not tracked by transaction tracking data collectors. Uninstrumented services are services that are not monitored directly by a transaction tracking agent, but either call or are called by a monitored domain.

Each distinct uninstrumented service is represented as a node in both the Instance Topology and Application Topology diagrams. These diagrams show the relationships between the various tracked and uninstrumented nodes in the application.

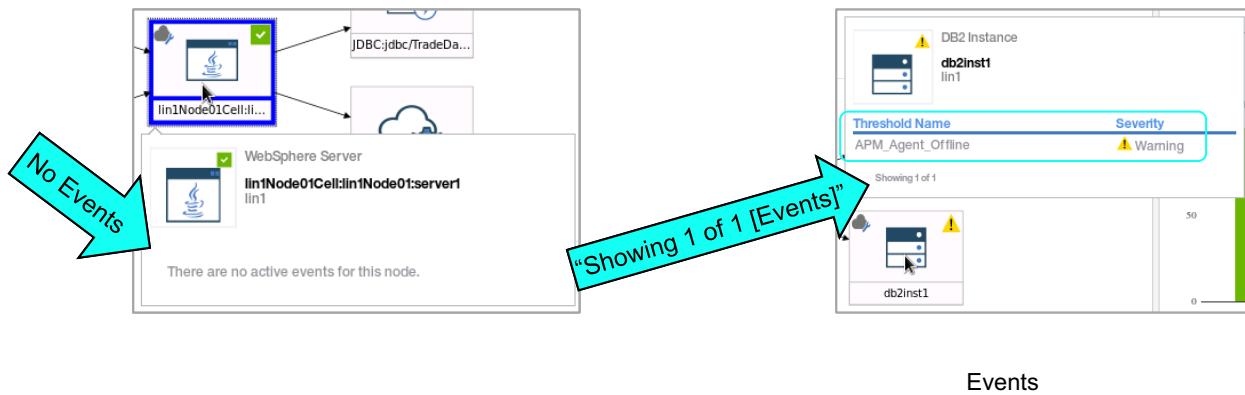
These nodes that are referred to as “pseudo nodes” are annotated with properties that describe the uninstrumented service that is used in the application.

By default, pseudo nodes are disabled in the Performance Management console advanced configuration; enable pseudo nodes to see uninstrumented services in instance and application topologies.

## Known uninstrumented services

- WebSphere
  - Apache HTTP Client
  - JAX-RPC Client
  - JAX-WS Client
  - EJB Client
  - JMS Put and Get
  - MQ Put and Get
  - JDBC Client
- .NET
  - HTTP Client
  - ASMX Client
  - WCF Client
  - Active Directory authentication
- IBM Integration Bus
  - Database and compute nodes where an ODBC data source is specified
  - TCP/IP nodes
  - File nodes for remote FTP or FTPS servers
  - IBM MQ nodes, unless already instrumented
  - SOAP
  - HTTP

## Topology tooltip



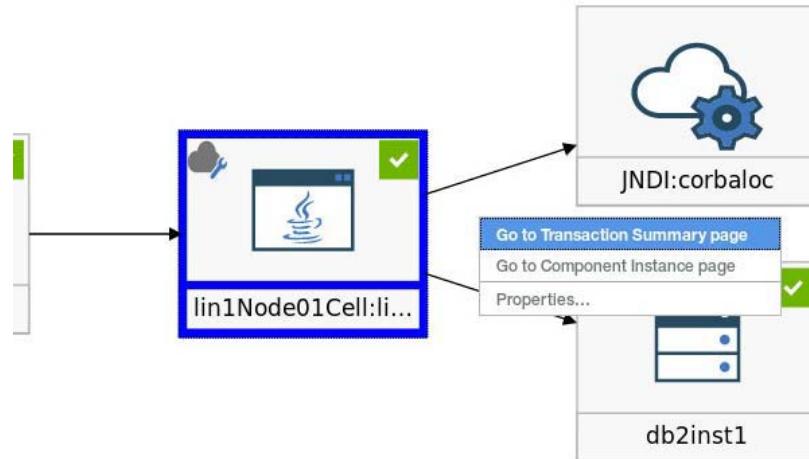
### Topology tooltip

Roll over a topology node to see the tooltip.

The tooltip shows resource:

- Name
- Status
- Type
- Host name
- Events, if any, or a message that indicates that no events exist
- Number of events that are displayed and the total number of events

## Navigating transaction tracking (1 of 2)



12/18/17 3:38:4

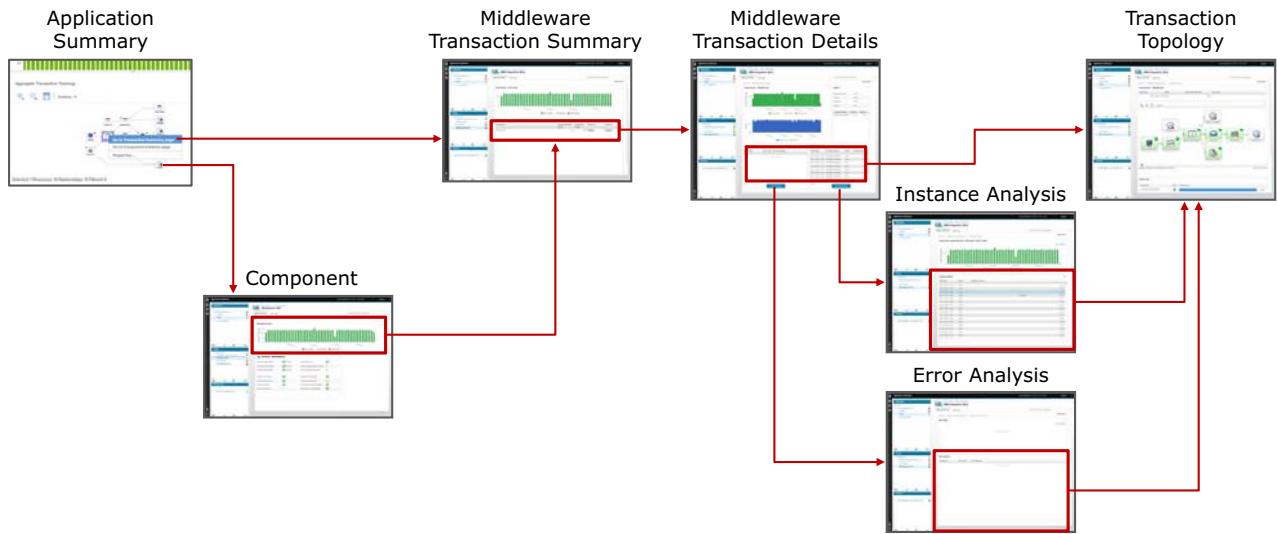
### Navigating transaction tracking (1 of 2)

Click a node to open its component instance page.

Right-click a node to select more navigation options.

Most nodes have a transaction summary and a component instance link.

## Navigating transaction tracking (2 of 2)



### Navigating transaction tracking (2 of 2)

To drill down from Aggregate Transaction topology, right-click a middleware node and select **Go to Transaction Summary page**.

To drill down from the Component page, click the **Transactions** widget.

To drill down to an instance topology page, click the instance in the Middleware Transaction Details, Instance Analysis, or Error Analysis page.

To drill down to the analysis pages, click the appropriate analyze button on the Middleware Transaction Details page.

# Lesson 2 Using transaction topologies

IBM Training



## Lesson 2: Using transaction topologies

Aggregate topologies:

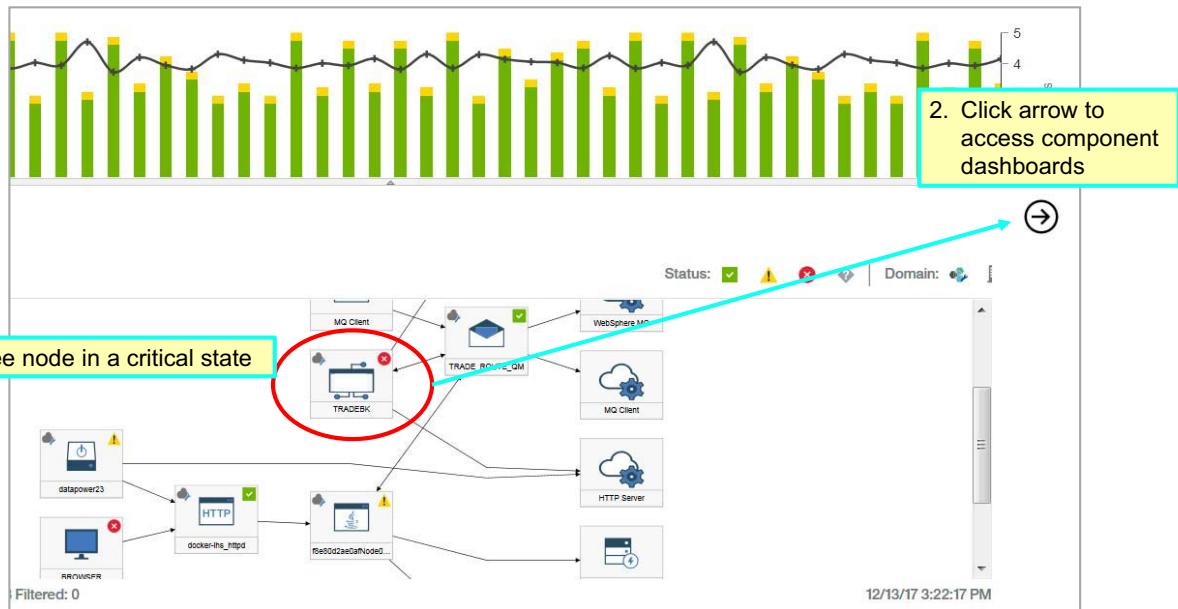
- Provide a birds-eye view of how transaction components interact
- Status indicators show at a glance where issues might be occurring
- Starting point for transaction analysis
  - Show component domain (cloud versus on-premises, for example)
  - Represent the average performance of a transaction over the aggregate interval

Instance:

- Represents a single transaction instance and shows actual time values
- Most useful when the time of suspected issues is known

In this lesson, you discover how to use and interpret transaction topologies.

## Example: IBM Integration Bus in a critical state



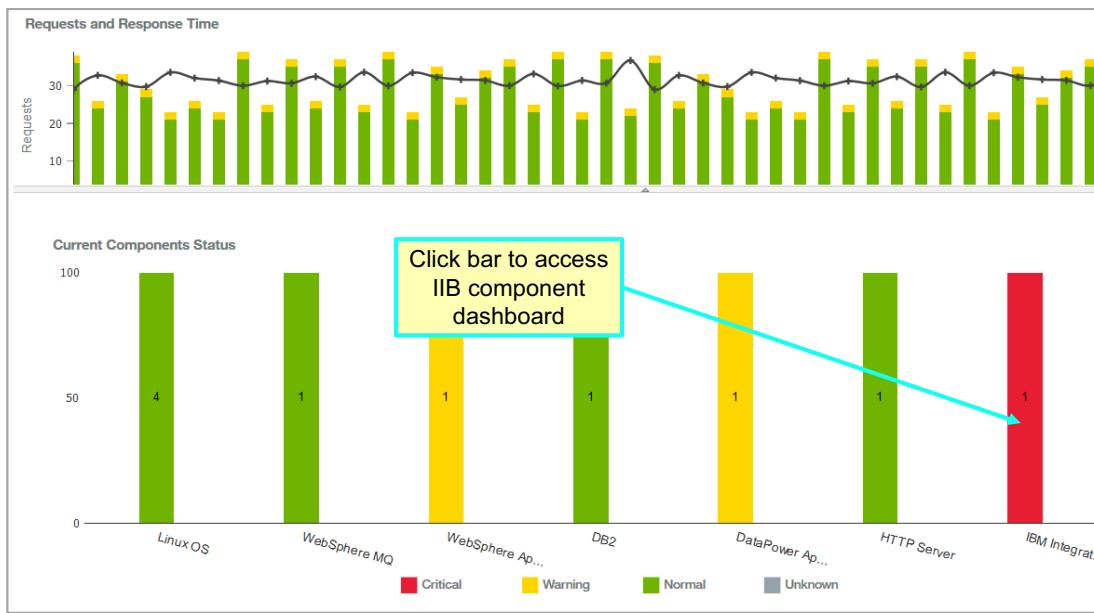
### Example: IBM Integration Bus in a critical state

When transaction tracking is enabled on any monitoring component within an application, an Aggregate Transaction topology widget is displayed on the Application Summary page.

The critical icon in this case is for the instance of IBM Integration Bus (IIB).

Click the arrow to access the Current Components Status widget.

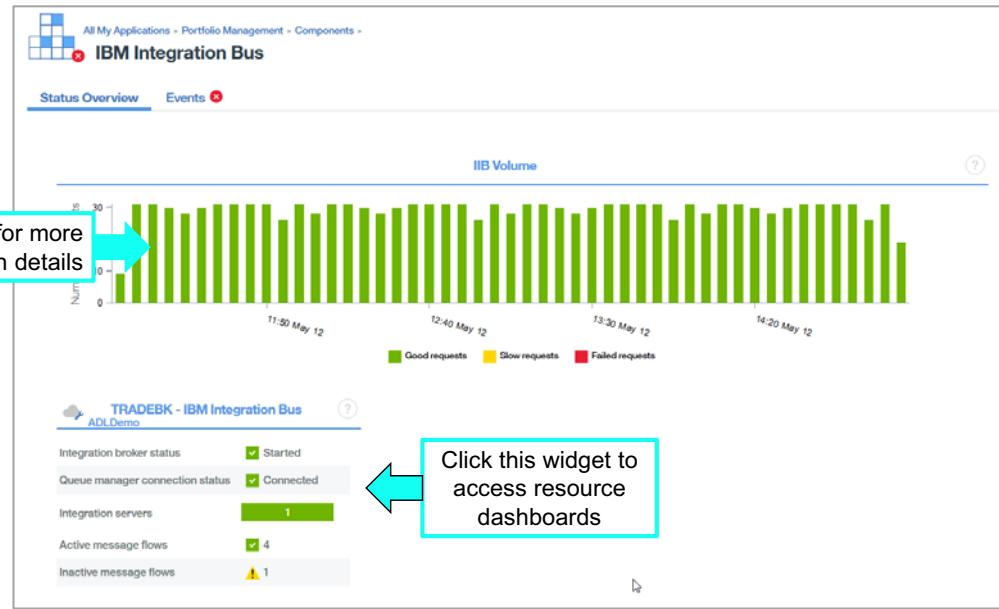
## Access IIB Component widget



### Access IIB Component widget

Click the bar corresponding to the IBM Integration Bus to proceed.

## IIB transaction volume



Tracking transactions through application components

16

© Copyright IBM Corporation 2018

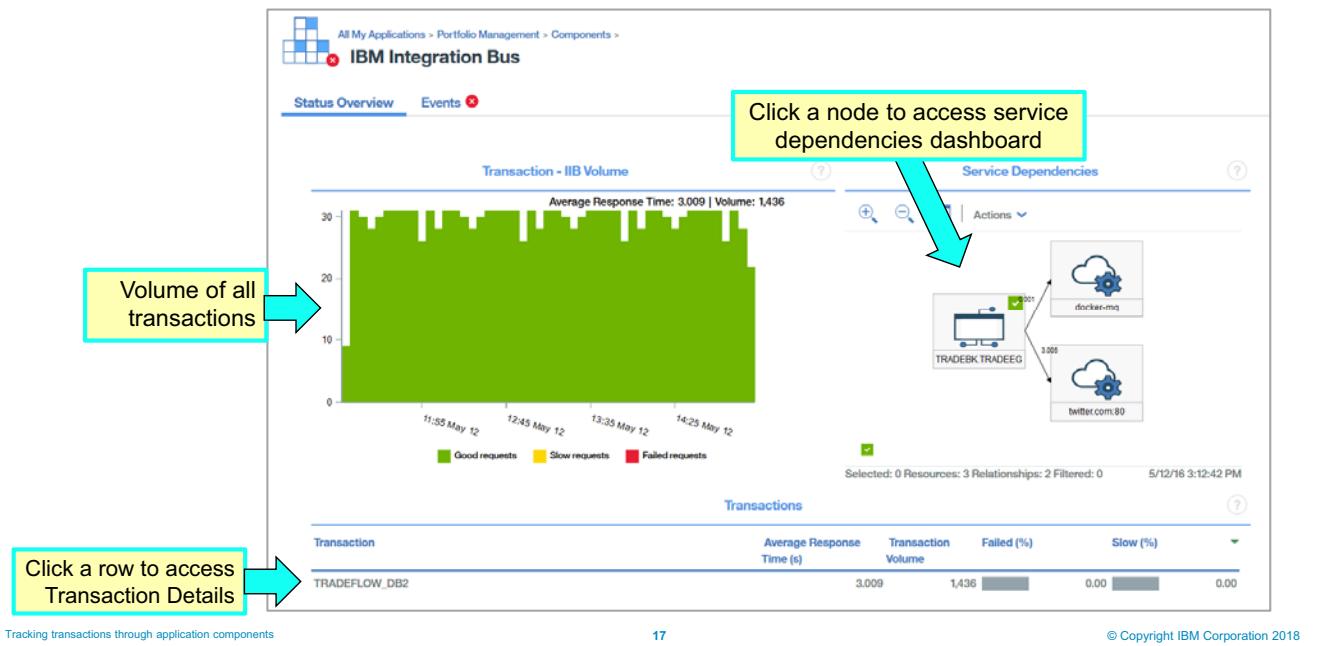
### IIB transaction volume

The Transactions Volume widget shows the numbers of transactions that are received in each aggregation interval. For each interval bar, color coding shows the percent of transactions that were good, slow, or failed.

Click the IIB Volume widget to access Middleware Transaction Details.

Clicking the IIB instance widget provides access to resource dashboards.

## Middleware transaction dashboard



Tracking transactions through application components

17

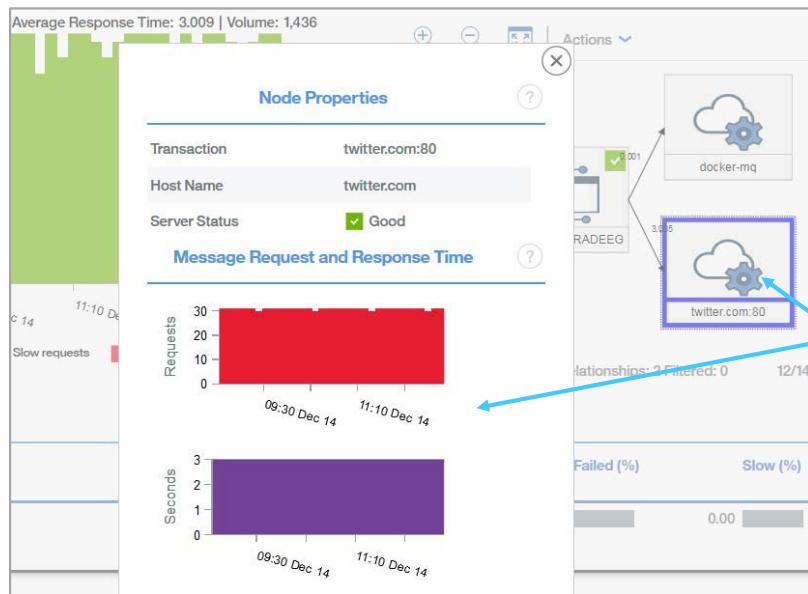
© Copyright IBM Corporation 2018

### Middleware transaction dashboard

The Middleware Transaction Details page shows data over time for a specific transaction and includes the widgets that are shown in the slide.

Only the Service dependencies and Transactions widgets support further drill-down. The following slides provide details.

## Service dependency details



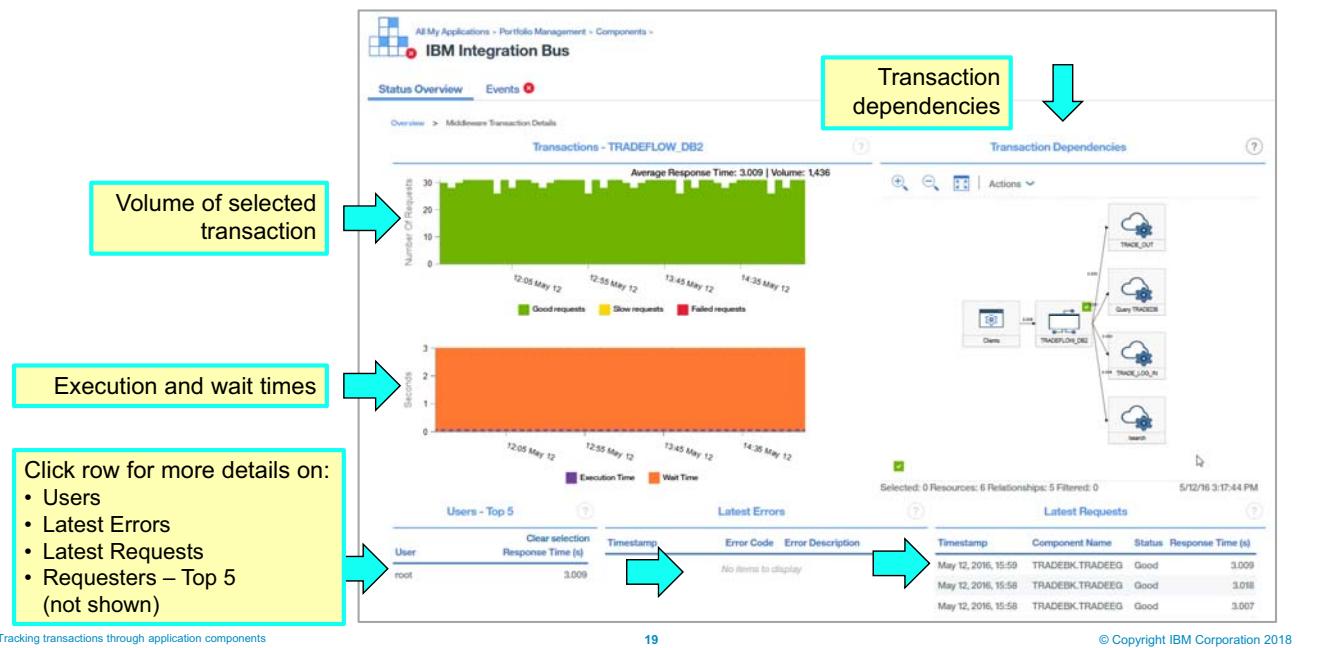
Click a node in the Service Dependencies widget to see:

- Node properties
- Message request and response time for the selected service

### Service dependency details

On the same dashboard, click a node in the Service Dependencies widget to view node properties and to request volume and performance information.

## Middleware Transaction Details



Tracking transactions through application components

19

© Copyright IBM Corporation 2018

### Middleware Transaction Details

At this next level, Middleware Transaction Details shows data over time for a specific transaction and includes the widgets that are shown in the slide. The Transactions widget does not support further drill-down currently.

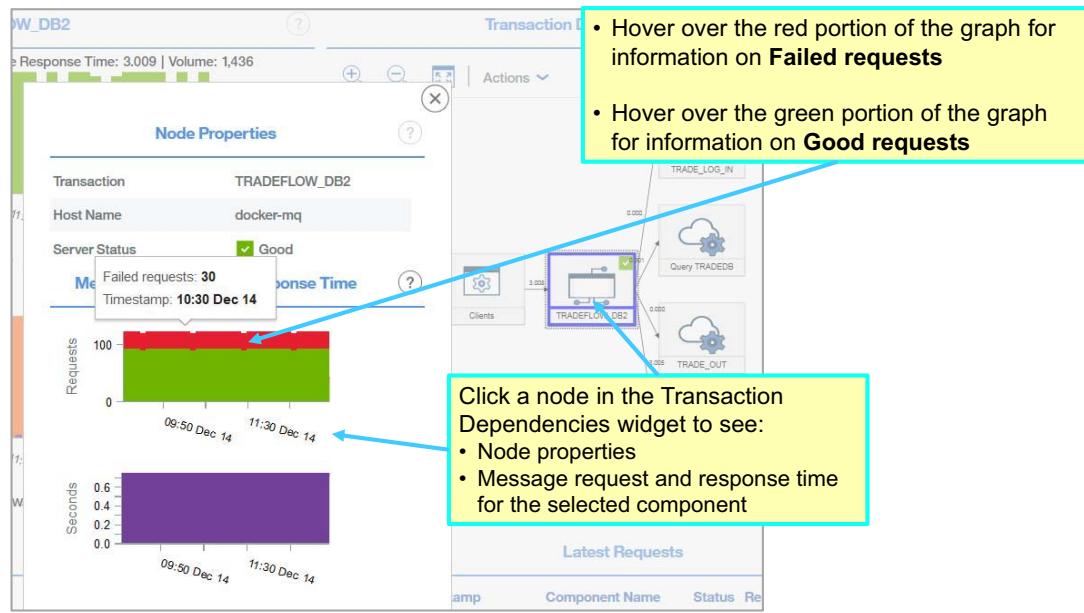
As with the Service Dependencies widget, selecting a node in the Transaction Dependencies widget provides access to a flyover with more details.

The other widgets at this layer display data of Users, Latest Errors, Latest Requests, and Requesters – Top 5. All four of these widgets support further drill-down.

The Latest Errors widget provides access to a dashboard with information on Error Rate and Error Details (by clicking Analyze Errors).

The Latest Requests widget provides access to a request instance dashboard (by clicking Analyze Requests).

## Transaction dependency details



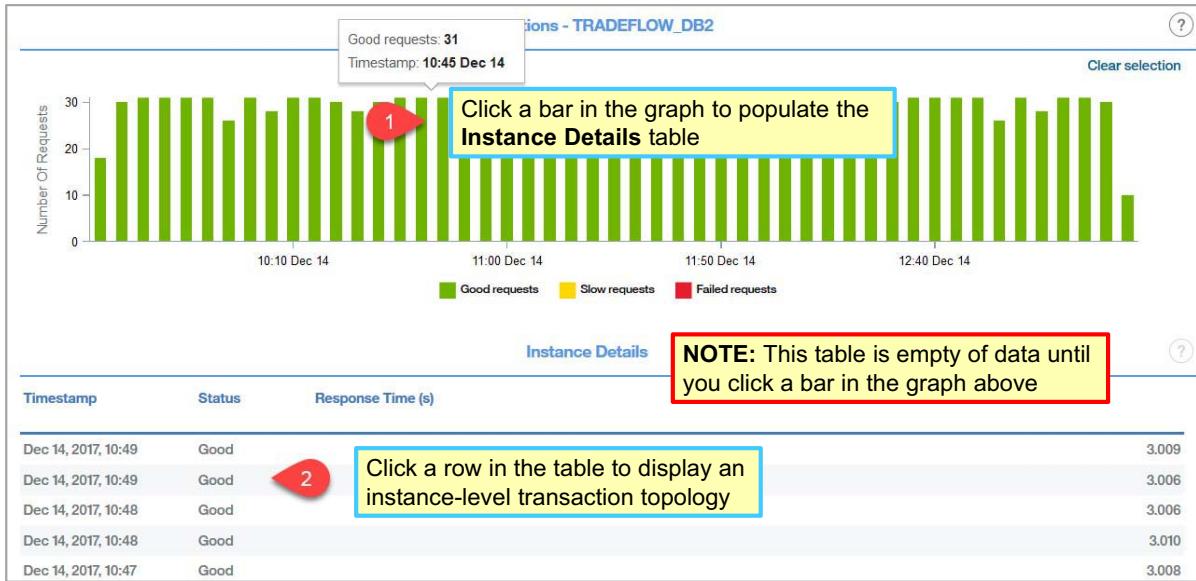
## Middleware Transaction Details (continued)

| Latest Requests |                     |                 |        |                   |
|-----------------|---------------------|-----------------|--------|-------------------|
| #               | Timestamp           | Component Name  | Status | Response Time (s) |
| 1               | Jun 08, 2016, 15:59 | TRADEBK.TRADEEG | Good   | 3.009             |
| 2               | Jun 08, 2016, 15:58 | TRADEBK.TRADEEG | Good   | 3.018             |
| 3               | Jun 08, 2016, 15:58 | TRADEBK.TRADEEG | Good   | 3.007             |
| 4               | Jun 08, 2016, 15:58 | TRADEBK.TRADEEG | Good   | 3.009             |
| 5               | Jun 08, 2016, 15:58 | TRADEBK.TRADEEG | Good   | 3.009             |
| 6               | Jun 08, 2016, 15:58 | TRADEBK.TRADEEG | Good   | 3.009             |
| 7               | Jun 08, 2016, 15:58 | TRADEBK.TRADEEG | Good   | 3.009             |
| 8               | Jun 08, 2016, 15:58 | TRADEBK.TRADEEG | Good   | 3.009             |
| 9               | Jun 08, 2016, 15:57 | TRADEBK.TRADEEG | Good   | 3.005             |

**Click Analyze Requests** to access instance data → **Analyze Requests**

Click **Analyze Requests** at the lower right of the Transactions details dashboard to access request instances.

## Middleware transaction instances (1 of 2)

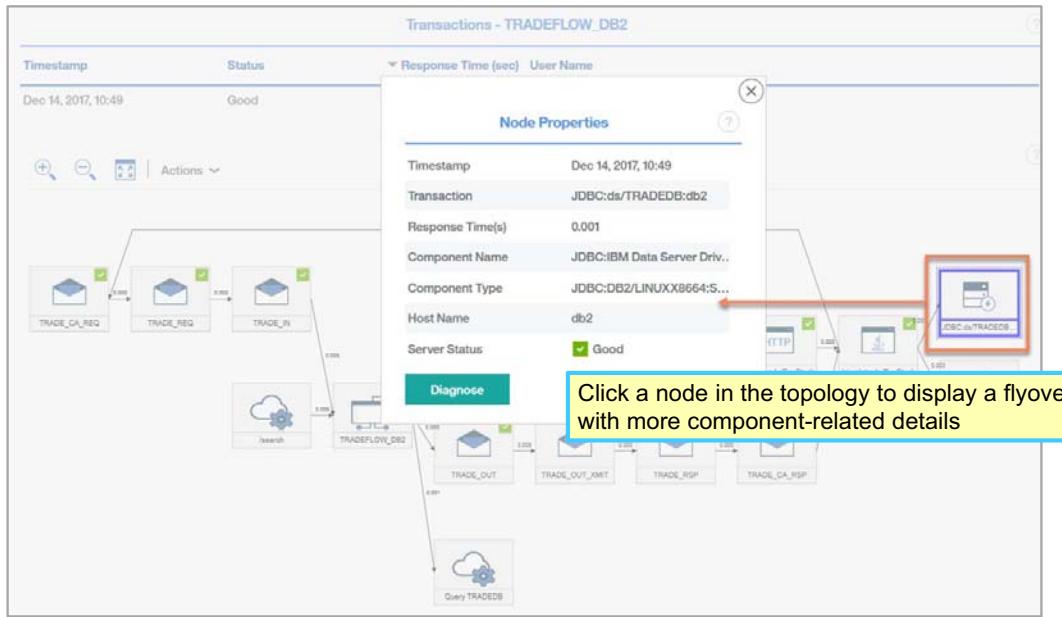


### Middleware transaction instances (1 of 2)

Transaction instance details are available, including the status and response time of each instance.

Click an instance to go to the Instance Topology page.

## Middleware transaction instances (2 of 2)



Tracking transactions through application components

23

© Copyright IBM Corporation 2018

### Middleware transaction instances (2 of 2)

In most cases, the flyovers support further drill-down to diagnostic or resource-related dashboards. Which dashboards are displayed varies by resource type.

# Lesson 3 Configuring transaction tracking

IBM Training



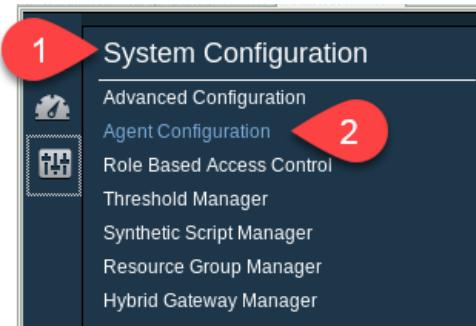
## Lesson 3: Configuring transaction tracking

- Enabling Transaction tracking:
  - Transaction tracking is enabled by default for some supported agents
  - The steps to enable transaction tracking vary by agent
  - See the documentation for details
- When preferred, transaction tracking can be turned off:
  - **Note:** Turn off transaction tracking on a per-agent basis
- Reasons for turning off transaction tracking:
  - Transaction tracking is not currently needed to manage the environment
  - Collecting transaction tracking data is adversely affecting application performance

In this lesson, you learn how to configure transactional monitoring.

## Agent configuration dashboards

- To turn off transaction tracking, first access the Agent Configuration screen:



## Selecting the agent to be disabled or enabled

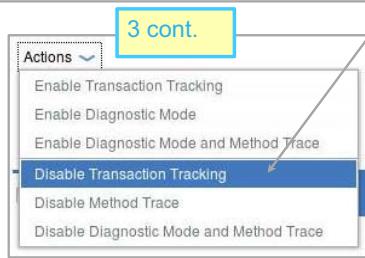
Use this page to configure data collection for WebSphere Application Servers.

Actions

| Managed System Name         | IP Address    | Server name | Node name  | Cell name |
|-----------------------------|---------------|-------------|------------|-----------|
| lin1Node01server1:lin1:KYNS | 192.168.1.104 | server1     | lin1Node01 | lin1No    |

Total: 1 Selected: 1

1. Select the tab for the relevant agent
2. Check the agent instance
3. Select the Actions menu
4. Click the intended action
5. Confirm success



|                      |                              |            |
|----------------------|------------------------------|------------|
| Current Method Trace | Current Transaction Tracking | DC Enabled |
| No                   | 5                            | Yes        |

## Student exercises



Complete the exercises for this unit in the Course Exercises Guide.

## Summary

Now that you have completed this unit, you should be able to:

- Describe the major functions of transaction tracking
- List monitored domains that support transaction tracking
- Explain how to enable and disable transaction tracking



# **Unit 10 Introduction to deep-dive diagnosis**

IBM Training



## **Introduction to deep-dive diagnosis**

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

This presentation is a technical overview of the code-level monitoring features of IBM Cloud Application Performance Management, Advanced.

## Learning objectives

After completing this unit, you should be able to:

- Describe deep-dive diagnosis
- Explain the code-level monitoring features of all agents
- Explain additional code-level monitoring features of select agents
- Plan deep-dive resource monitoring
- Configure monitoring agents and data collectors for deep-dive diagnosis

## Unit outline

- Lesson 1: Deep-dive diagnosis overview
- Lesson 2: Code-level monitoring features of all agents
- Lesson 3: Additional diagnostic features available for specific agents
- Lesson 4: Deployment planning
- Lesson 5: Configuration

# Lesson 1 Deep-dive resource monitoring overview

IBM Training



## Lesson 1: Deep-dive resource monitoring overview

### Deep-dive monitoring features of Cloud APM, Advanced

- Code-level monitoring
- In-flight requests
- Heap dump
- Memory analysis
- See the following slide for an agent-by-agent list of supported features

Lesson 1 provides an overview of deep-dive diagnosis for IBM Cloud Application Performance Management, Advanced agents.

## Supported agents for deep-dive diagnosis

| Agent                    | Code monitoring down to stack trace | In-flight request monitoring | Heap dump | Memory analysis | Prerequisite tasks |
|--------------------------|-------------------------------------|------------------------------|-----------|-----------------|--------------------|
| J2SE                     | Yes                                 | No                           | No        | No              | Yes                |
| JBoss                    | Yes                                 | Yes                          | Yes       | Yes             |                    |
| Liberty – data collector | Yes                                 | No                           | No        | Yes             |                    |
| MS .NET                  | Yes                                 | No                           | No        | No              |                    |
| Node.js                  | Yes                                 | No                           | No        | No              | Yes                |
| Node.js – data collector | Yes                                 | No                           | No        | No              | Yes                |
| Python                   | Yes                                 | No                           | No        | No              |                    |
| Ruby                     | Yes                                 | No                           | No        | No              |                    |
| Ruby – data collector    | Yes                                 | No                           | No        | No              |                    |
| NetWeaver                | Yes                                 | No                           | No        | No              |                    |
| WebLogic                 | Yes                                 | Yes                          | Yes       | Yes             |                    |
| WebSphere                | Yes                                 | Yes                          | Yes       | Yes             |                    |

# Lesson 2 Code-level monitoring features of supported agents

IBM Training



## Lesson 2: Code-level monitoring features of supported agents

- With code-level monitoring, you can examine:
  - Aggregate request performance
  - Instance-level request performance
  - Gantt charts, for event-by-event request analysis
  - Stack traces
  - Request context (including SQL information)
  - Method summary (WebSphere agent only)
- Use this information to:
  - Detect hung or slow transactions
  - Diagnose code statements to locate potential code defects
- \*See Notes page for details

Lesson 2 covers the code-level monitoring features for which this functionality is supported for IBM Cloud Application Performance Management, Advanced agents.

- Aggregate request performance (Request Summary widget): Listed requests are aggregates of a number of sample instances; the KPI details are averages.
- Instance-level request performance (Request Instances widget): The Request Instances widget displays the response time for individual requests inclusive of their nested requests. Use it to identify requests with high response times.
- Gantt charts, providing event-by-event request sequence analysis: A tree view of all request instances and their nested requests. If method data was collected, calls to methods are included in this tree.
- Stack traces:
  - When a violation occurs, the data collector captures a stack trace. Use the stack trace to understand the context in which a method call was made. It can also help identify and fix looping conditions.
- A method trace might perform differently depending on the caller method. Each caller method might pass different input parameters to the method call. The stack trace also provides the

depth of a method call. A high number of nested calls might lead to a high method response time.

- Request context:
  - Java Platform, Enterprise Edition context, which depends on request type.
  - For a JNDI request, the request context includes the JNDI resource URI. For a JDBC request, the request context includes the data source name, the request name, and an SQL statement. For an EJB method and servlet requests, the request context includes the request name and the application module name.
  - The context might present poorly constructed SQL statements.
- Method summary (WebSphere agent only): The Method Summary widget displays a summary of the performance of the method type that you selected in the Request Sequence table.

## Viewing code-level data (1 of 2)

The screenshot shows two consecutive pages from an IBM monitoring tool.

**Step 1:** The first page is titled "Requests with Slowest Response Time". It lists three requests with their URLs and names, all showing an average response time of 1,965 ms and an error rate of 0.00%. A blue box labeled "Step 1" surrounds the "Diagnose" button, which is highlighted with a red arrow. A large cyan arrow points down to the second page.

| URL                                    | Request Name        | Average Response Time (ms) | Error Rate (%) |
|--|---------------------|----------------------------|----------------|
| http://lin1.ibm.edu/daytrader/scenario | /daytrader/scenario | 1,965                      | 0.00%          |
| http://lin1.ibm.edu/daytrader/scenario | /daytrader/scenario | 1,965                      | 0.00%          |
| http://lin1.ibm.edu/daytrader/scenario | /daytrader/scenario | 1,965                      | 0.00%          |

**Step 2:** The second page is titled "Request Summary". It shows summary statistics for a single request: /daytrader/scenario. The statistics include Average Response Time (50 ms), Minimum Response Time (1 ms), Maximum Response Time (162 ms), Sampled Requests (13), Request Count (13), CPU Time (22 ms), and Request Type (Servlet). A blue box labeled "Step 2" surrounds the "Action" column. A red arrow points from the "View instance data" link in the Action column to the "View instance data" link on the current page.

| Request Name        | Average Respo... | Minimum Respo... | Maximum Respo... | Sampled Reque... | Request Count | CPU Time (ms) | Request Type | Action                             |
|---------------------|------------------|------------------|------------------|------------------|---------------|---------------|--------------|------------------------------------|
| /daytrader/scenario | 50               | 1                | 162              | 13               | 13            | 22            | Servlet      | <a href="#">View instance data</a> |

### Viewing code-level data (1 of 2)

Step 1: Click **Diagnose** in the Requests with Slowest Response Time widget as the first step in code-level diagnosis. You are taken to the Request Summary page.

Step 2: Locate the Request Summary widget and click **View instance data** in the Action column for the request you want to examine. You are taken to the Request Instances page.

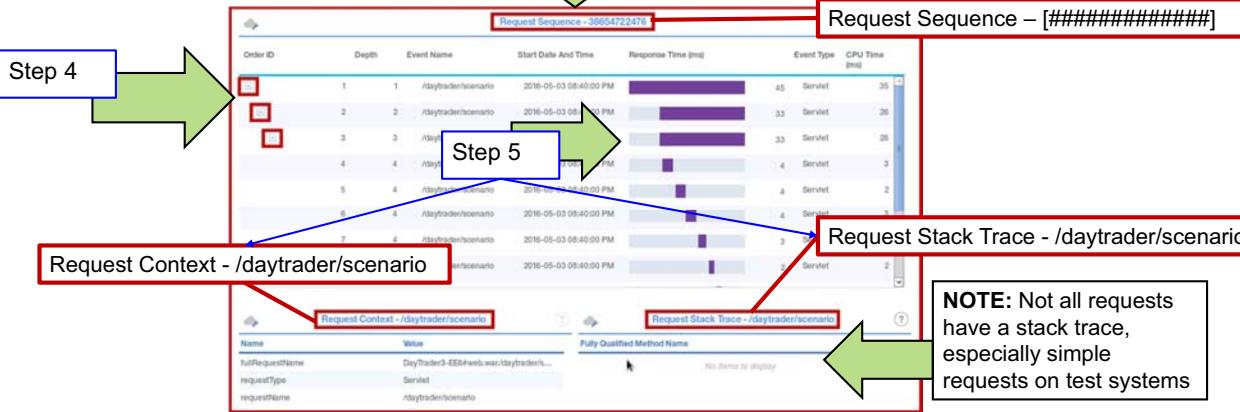
Continue to the next slide.

## Viewing code-level data (2 of 2)

Step 3

| Request Instances - /daytrader/scenario |                     |             |                    |               |              |           |                |                                       |
|---|---------------------|-------------|--------------------|---------------|--------------|-----------|----------------|---------------------------------------|
| Record Date And Time                    | Request Name        | Request ID  | Response Time (ms) | CPU Time (ms) | Request Type | Thread ID | Method Entries | Action                                |
| 2016-05-03 08:40:00 PM                  | /daytrader/scenario | 38654722476 | 45                 | 35            | Servlet      | 196       | No             | <a href="#">View request sequence</a> |
| 2016-05-03 08:40:00 PM                  | /daytrader/scenario | 42849691629 | 11                 | 8             | Servlet      | 197       | No             | <a href="#">View request sequence</a> |

Step 4



Introduction to deep-dive diagnosis

8

© Copyright IBM Corporation 2018

### Viewing code-level data (2 of 2)

Step 3: On the Request Instances page, locate the instance that you want to examine, then click **View request sequence** in the Action column. You are taken to the Request Sequence page.

Step 4: Review the Request Sequence to see the order of events that make up the request. Click any plus signs to expand the request.

Step 5: Click individual requests in the sequence, and then view the associated Request Context and Request Stack Trace widgets on the same page.

**NOTE:** Not all requests have a stack trace, especially simple requests on test systems

## Understanding the Request Stack Trace

The screenshot shows a 'Request Stack Trace' window with a title bar and a help icon. The main area is labeled 'Fully Qualified Method Name' and contains a list of method names and their line numbers. A green arrow points from the explanatory text on the right towards the stack trace list.

| Fully Qualified Method Name   |  |
|---|--|
| com.ibm.ws.webcontainer.servlet.ServletWrapperImpl.handleRequest:178  |  |
| com.ibm.ws.webcontainer.servlet.ServletWrapperImpl.handleRequest:178  |  |
| com.ibm.tivoli.itcamdemo.database.handleRequest:178                   |  |
| com.ibm.tivoli.itcam.search.database.handleRequest:178                |  |
| com.ibm.tivoli.itcam.search.database.handleRequest:61                 |  |
| com.ibm.ws.webcontainer.servlet.ServletWrapperImpl.handleRequest:1230 |  |
| com.ibm.ws.webcontainer.servlet.ServletWrapperImpl.handleRequest:1230 |  |
| com.ibm.ws.webcontainer.servlet.ServletWrapperImpl.handleRequest:1230 |  |
| com.ibm.ws.webcontainer.servlet.ServletWrapperImpl.handleRequest:178  |  |
| com.ibm.tivoli.itcamdemo.database.handleRequest:178                   |  |
| com.ibm.tivoli.itcam.search.database.handleRequest:178                |  |
| com.ibm.tivoli.itcam.search.database.handleRequest:61                 |  |

- The **Request Stack Trace** widget displays the stack trace for the selected request or nested request
  - The data collector tracks the progress of a request
  - When a violation occurs, the data collector captures a stack trace
- Use the stack trace to identify and fix looping conditions
- The stack trace also provides the depth of a method call
  - A high number of nested calls might lead to a high method response time
- The number at the end of each line is the line of application source code
- **NOTE:** Line numbers are not available for calls to system libraries
  - Instead of an integer, the string "Unknown" is appended to the method for system calls

### Understanding the Request Stack Trace

Stack trace data is unavailable if:

- The data collector within the JVM of the application server is not configured.
- Diagnostics mode is disabled.
- The collection of stack trace data for the request type is disabled.
- The collection threshold value was not exceeded, even if the collection of stack trace data is enabled.

Fully qualified method name:

- Use the fully qualified method name for each Java object that handled the request instance and the line number that was invoked in each class.

## Understanding the request context

| Name            | Value                                   |
|-----------------|---|
| sqlText         | select * from booklist,genre,author     |
| requestType     | JDBC                                    |
| requestName     | executeQuery                            |
| dataSourceName  | jdbc:derby:databases/kilimanjaro        |
| sqlText         | select * from basket,shopper            |
| fullRequestName | itcam#itcam.ear./TextStringStatefulB... |
| requestName     | TextStringStatefulBean.findTextString   |
| requestType     | EJB_Method                              |
| fullRequestName | itcam#itcam.ear./SearchTuner.enhan...   |

The **Request Context** widget displays the Java context of each request (event name)

The type of information in the request context depends on the request type (event type):

- For a **JNDI request**, the request context includes the JNDI resource URI
- For a **JDBC request**, the request context includes the data source name, the request name, and an SQL statement
- For an **EJB method** and servlet requests, the request context includes the request name and the application module name

**Note:** When you have multiple instances of a resource in your environment, the request context helps you identify the resource that the request instance uses

### Understanding the request context

Request context data is not available if:

- Diagnostics mode is disabled.
- The collection of request context data is disabled.
- Threshold-based monitoring is enabled but a threshold is not exceeded.

## Understanding the method summary (WebSphere only)

The screenshot shows a 'Method Summary' card with the following data:

| Class Name                 | com.ibm.tivoli.itcam.db.framework.ControllerJDBC |
|----------------------------|--|
| Method Name                | executeQuery                                     |
| Total Number of Calls      | 6250   |
| Average Response Time (ms) | 10   |
| Average CPU Time (ms)      | 2  |

The **Method Summary** widget displays a summary of the performance of the method type that you selected in the Request Sequence table

Select an event in the Request Sequence table to display a summary of the performance of the method type

### Supported KPIs:

- Class Name
- Method Name
- Total Number of Calls
- Average Response Time (ms)
- Average CPU Time (ms)

## Understanding the method summary (WebSphere only)

Method Summary data is unavailable if:

- Diagnostics mode is disabled.
- Method trace is disabled.
- The method is not of the Event type.

**KPI descriptions** include:

- Class Name
  - The method class. Derived from the Class Name attribute of the Method Summary Specific data set. The data type is String.
- Method Name
  - The name of the method. Derived from the Class Name attribute of the Method Summary Specific data set (Method Summary Specific.Method Name). The data type is String.
- Total Number of Calls
  - The total number of times the method was called. Derived from the Total Method Calls attribute of the Method Summary Specific data set. The data type is Integer (32-bit numeric property) with enumerated values.
- Average Response Time (ms)
  - The average response time for all instances of this method. Derived from the Average Method Response time attribute of the Method Summary Specific data set (Method

Summary Specific.Average Method Response Time). The data type is Integer (32-bit numeric property) with enumerated values.

- Average CPU Time (ms)
  - The average CPU time for all instances of this method. Derived from the Average Method CPU time attribute of the Method Summary Specific data set. The data type is Integer (32-bit numeric property) with enumerated values.

# Lesson 3 More diagnostic features of certain agents

IBM Training



## Lesson 3: Additional diagnostic features of certain agents

- **Currently supported additional features**
  - In-flight requests
  - Heap dump
  - Memory analysis
- **Currently supported agents**
  - JBoss
  - Liberty data collector (In-flight and Memory Analysis only)
  - WebLogic
  - WebSphere

In this lesson, you learn how to perform:

- In-flight requests
- Heap dumps
- Memory analysis

## Understanding in-flight requests

What is an in-flight request?

- By default, a request that takes more than 60 seconds to complete

What is the maximum number of in-flight requests?

- 100,000

Modifying default thresholds

- If you want to modify thresholds, do so here:
  - `dc_home/runtime/appserver_version.node_name.profile_name.server_name/custom/gdc/gdc_custom.properties` file
- To modify the time interval, change the digit after the = sign
  - Example setting the interval to 100 seconds:  
`com.ibm.itcam.gdc.inflight.request.seconds=100`
- To modify the maximum number of requests to collect, change the digit after the = sign
  - Example setting maximum requests to 10000:  
`com.ibm.itcam.gdc.inflight.request.seconds=10000`

In-flight stack trace

- Examine the stack trace as you would for a normal request (see [Understanding the Request Stack Trace](#))

## In-flight requests (1 of 2)

 In-flight Request Summary 

---

|                            |       |
|----------------------------|-------|
| In-flight requests         | 1     |
| Average resident time (ms) | 60001 |

**View Requests**  Click to view current in-flight requests

### Note regarding in-flight defaults:

- An in-flight request must take at least 60 seconds to complete before it shows in the widget
- A maximum of 100,000 requests are collected
- The 60-second threshold can be adjusted downward, although lowering the minimum time might adversely affect performance (example: `com.ibm.itcam.gdc.inflight.request.seconds=100`)
- The maximum number of requests can also be adjusted (example: `com.ibm.itcam.gdc.max.inflight.records=10000`)

## In-flight requests (2 of 2)

In-flight Requests

| Start Time              | Request Name                | Request ID | Resident Time (ms) | Trace Entries | Server Name |
|-------------------------|-----------------------------|------------|--------------------|---------------|-------------|
| May 16, 2016 6:46:05 PM | /ITCAM/testware/ejbStateful | 128234568  | 60001              | No            | newltcam    |

Total 1

**View Stack Trace** Click to view the stack trace

**Request Stack Trace**

Fully Qualified Method Name

```
com.ibm.ws.webcontainer.servlet.ServletWrapper.handleRequest:932
com.ibm.ws.webcontainer.servlet.ServletWrapper.handleRequest:478
com.ibm.ws.webcontainer.servlet.ServletWrapperImpl.handleRequest:178
```

**Note:** See also [the slide in Lesson 2, Understanding the Request Stack Trace](#)

Introduction to deep-dive diagnosis

15

© Copyright IBM Corporation 2018

### In-flight requests (2 of 2)

Select the in-flight request that you want to diagnose further; then, click View Stack Trace.

The stack trace for in-flight requests is read the same way as the stack traces contained in the main diagnostic dashboards.

## Value of a heap dump analysis

What data is included in a heap dump snapshot

- Number of objects
- Size per object class:
  - By default, up to 1000 objects can be displayed in this widget
  - Objects are sorted by allocated heap size in descending order

Analyzing the heap

- Examine these KPIs:
  - Total objects on the heap
  - Total size of the heap
  - Delta of the number of objects on the heap
  - Delta of the size of a class of objects

Understanding Delta statistics

- Negative values indicate a decrease in the relevant object count or size; generally a positive sign
- Positive values indicate an increase in the relevant object count or size; can indicate an impending issue

### Value of a heap dump analysis

A heap dump represents the state of Java heap memory. A heap dump is useful for the memory usage of an application when diagnosing such things as memory leaks.



**Note:** For the Heap Dump dashboard to contain data, you also need to enable the data collector for heap snapshot collection and, if you want, for memory allocation collection. These steps are carried out in the data collector `.properties` files.

See the sections on “Enabling or disabling transaction tracking and diagnostic data collection” on the product documentation.

Heap Dump snapshot collection can be customized. The following section is from the product documentation.

To enable or disable heap snapshot collection, set the `com.ibm.tivoli.itcam.hc.send.heap.enable` and `com.ibm.tivoli.itcam.hc.snapshot.automatic.enable` properties in the following file to true or false.

After heap snapshot collection is enabled, the data collector can take heap snapshot at specified intervals. Heap dump information can be displayed in the Heap Dump dashboard.

To change the interval at which the data collector takes the heap snapshot, set the `com.ibm.tivoli.itcam.hc.snapshot.automatic.interval` property in the same file to a positive integer. The unit of the interval is minute and the default is 360.

The file to be modified is:

`dc_home/runtime/appserver_version.node_name.server_name/hc.properties` (if the runtime directory does not exist, use `dc_home/healthcenter/etc/hc.properties`).

## Heap dump



Introduction to deep-dive diagnosis

17

© Copyright IBM Corporation 2018

## Heap dump

With the Heap Dump feature, you can:

- View what is on the heap (see #1, above)
- Take a snapshot of the heap (see #2 and #3, above)
- Compare two heap snapshots (see #4 and #5, above)
- View a single heap snapshot (not shown)

## Comparing heap snapshots



Why compare heap snapshots?

- To see the growth in size and count of an object or objects
  - Objects growing in number or size might represent a memory leak
- Use them as part of heap management
  - Perhaps you do not have a leak, only a need to increase the max heap size

## Data that the Memory Analysis feature provides

What data is included in the Memory Analysis dashboard?

Samples by object:

- Object allocation information
  - By default, only 1000 objects can be displayed
  - Sorted by the Percentage of Total Size column in descending order

Top 100 instance count by request site:

- Highest object instance allocation (by request site)
  - By default, only the top 100 request sites (in terms of allocated objects) are displayed
  - Sorted by the number of allocated objects in descending order

Allocation site (for selected row):

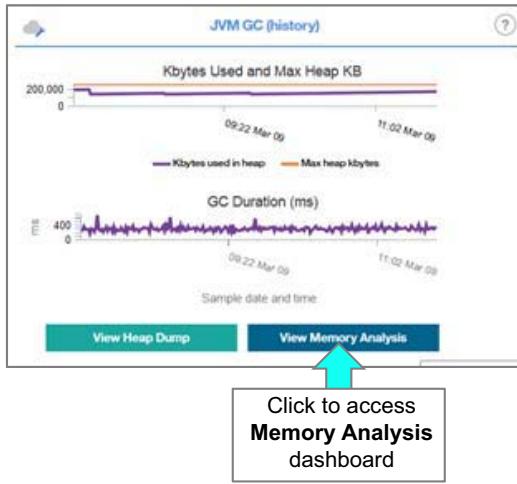
- Click an object in the Heap Dump widget and check the details on this dashboard
- Widget displays the allocation sites for the selected object and the % of heap size that is allocated for each site
  - By default, only five allocation sites can be listed for the selected object
  - Sorted by the % of heap size that is allocated for each site in descending order



**Note:** For the Memory Analysis dashboard to contain data, you must enable memory allocation collection for the data collector during configuration. This diagnostic feature requires IBM Health Center 3.0.8 or later. If the IBM Health Center version is not eligible, upgrade the JRE that is used by the application server to a version that contains IBM Health Center 3.0.8 or later.

See the sections on “Enabling or disabling transaction tracking and diagnostic data collection” on the product documentation.

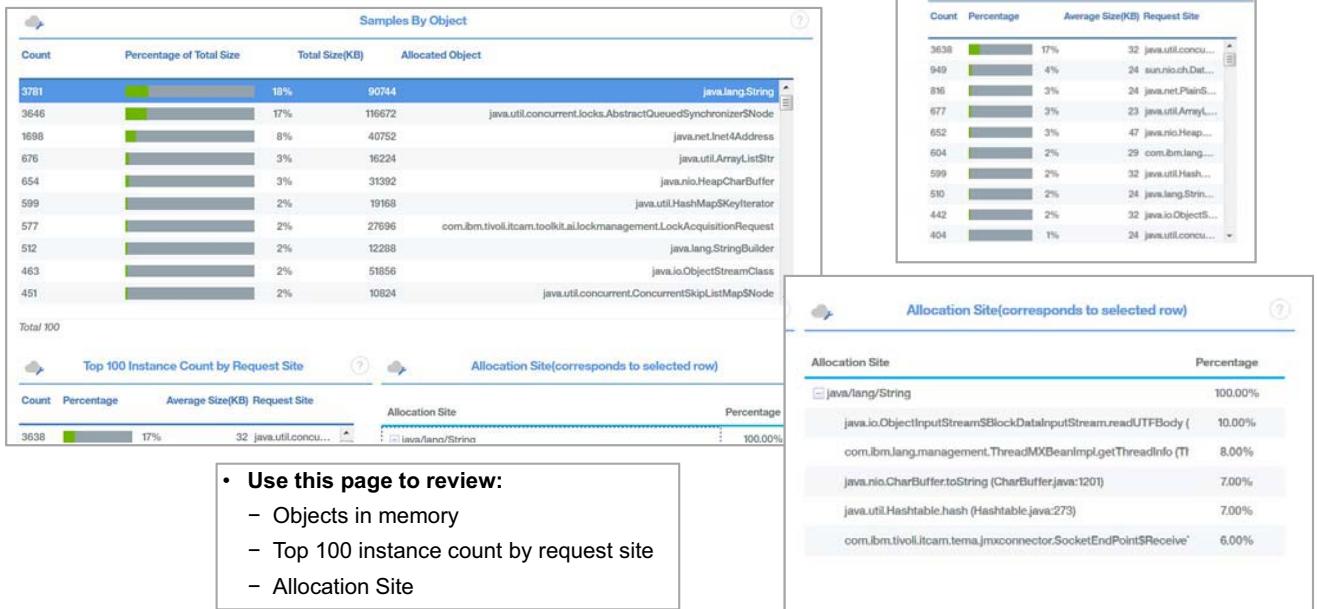
## Memory analysis (1 of 2)



### Memory analysis (1 of 2)

The Memory Analysis dashboard helps you to diagnose possible memory leaks by checking the heap usage information for each heap dump.

## Memory analysis (2 of 2)



# Lesson 4 Deployment planning

IBM Training



## Lesson 4: Deployment planning

- Assessing your monitoring needs
- Carefully prepare for deployment
- Access level
- How much deep-dive data do you need?

This lesson covers some fundamentals of effective deployment of IBM Cloud Application Performance Management, Advanced agents.

## Assessing your monitoring needs

Know your environment – its strengths and weaknesses

- Example: Free Disk Space:
  - One size does not fit all
  - Space-challenged environments might need to check this KPI frequently
- Use reporting creatively: Ignorance is not bliss!
  - Collect data on operations prone to failure
  - Dial back reporting frequency on stable elements
  - Use reporting in the continual improvement of the service lifecycle

Factor in the role of an environment

- Preproduction environments seldom produce the same issues and application traffic
  - Use creative scripting to mimic production-level issue generation and system load
  - Adjust thresholds to generate sufficient events for adequate testing
  - Do not neglect test of event generation, forwarding, and resolution mechanisms
- Production environments require quick identification and resolution of issues
  - Maximize efficiency of event-notification mechanisms
  - Consider using load balancing (when available) to allow for more aggressive monitoring of critical issues
  - Useful when issues affect only busy production systems at peak load

### Assessing your monitoring needs

#### Potential issues:

- A KPI such as Free Disk Space is always important. However, environments can vary widely in the amount of available disk space. Tailoring the monitoring frequency of this KPI to the likelihood of a violation can be a useful part of event management.

#### Reporting:

- Use targeted reporting to inform the operations team of the frequency, type, and severity of issues. These reports can inform the continual improvement efforts in the management of the service lifecycle.

## Carefully prepare for deployment

### Prerequisites

- Carefully ascertain and implement hardware and software prerequisites

Understand the needs of non-root agent installation and configuration

- Large production environments often do not allow root access
- Fortunately, root access is not required to install and configure agents
- However, non-root installations require some additional steps

How much deep-dive data do you need?

- Review data that is returned by default versus custom configuration
- Gather the data that you need – no more, no less
  - Gathering more data than you need wastes space and resources
  - If issues arise, adjust data collection level
  - After issues are resolved, adjust data collection settings

## Deciding access level

Installing as a non-root user

- Root access is not permitted in many environments
- A non-root user can install and run agents, but further steps are required

Example 1: Ruby agent

- Suppose that you use a non-root account to install your Ruby on Rails application on a Linux system, and you plan to collect diagnostics data
  - In this case, the non-root user must have access to the diagnostics data collector home directory
  - Verify that the non-root user has read and write access in the `install_dir/install-images/kkm` directory, where `install_dir` is the installation directory of the Ruby agent
  - The default installation directory is `/opt/ibm/apm/agent`
- If required, provide read and write permissions by using the `chmod 777` command

Example 2: WebSphere agent

- If the WebSphere Application Server or Portal Server was installed by using a non-root user account, you need to verify the privileges of the non-root user before you run the configuration utilities
  - Verify that the non-root user has read and write privileges to the following agent directories in `install_dir/yndchome/7.3.0.14.0` where `install_dir` is the installation directory of the WebSphere Applications agent: `data`, `bin`, `runtime`, `logs`
- If required, provide read and write permissions by using the `chmod 777` command
- Also, log in as the user that was used to install the application server

## Managing the amount of data you collect

In production environments, manage the percentage of diagnostic data collected

- A common error in agent configuration is collecting too much diagnostic data
- Increase the number and types of diagnostic data that is collected when issues are under investigation
- As soon as issues are resolved, restore collection of diagnostic data to the levels required for normal monitoring

Understanding data collection settings

- Examples:

- `:instrumentation_enabled=true`

Enable support for the collection of diagnostics data, setting it to "false" disables the feature

- `:sample_frequency => 10`

This setting specifies that data is collected for 1 in every 10 requests

Diagnostic data is collected only for the selected requests

- `:max_methods_to_instrument => 0`

Disables collection of method data for the data collector

Sampling frequency and errors

- Regardless of the sampling frequency, all errors are collected
- **Note:** Consult agent reference documentation for other KPIs



**Important:** Collecting large amounts of diagnostic data is not without a cost in resource and storage usage. Intelligent management of diagnostic data is part of effective application performance management.

# Lesson 5 Configuration

IBM Training



## Lesson 5: Configuration

Types of configuration

Deep-dive diagnosis requires configuration

Default configuration

- `./simpleconfig.sh` is used for:
  - JBoss
  - WebLogic
  - WebSphere (see also the following slide)

Other steps that are required

- Node.js agent
  - Modification to the application code required

Data collector as opposed to agent

- Liberty data collector
- Need only to modify three files for the server
- Node.js data collector
- Configured manually and starts automatically

Lesson 5 covers an overview of configuration, plus some agent-specific examples.

## Example 1: WebSphere agent default configuration (review)

Run the `simpleconfig.sh` command to enable:

- All instances in a profile for WebSphere Application Server
- For WebSphere Liberty, single instance or multiple instances in the same directory
  - To monitor more profiles or instances, repeat the configuration
- Data collector is configured within the server instances, providing maximum monitoring
- For Cloud APM, Base Private:
  - Resource monitoring is enabled
- For Cloud APM, Advanced Private:
  - Resource monitoring
  - Transaction tracking
  - Diagnostic data is enabled
  - Note: Heap Dump and Memory Analysis must be enabled separately

Run `config.sh` under certain conditions

- Refer to notes
- If a non-root user server installed WebSphere or Portal, some additional steps are required

### *Example 1: WebSphere agent default configuration (review)*

Reasons to run `config.sh` and `config.bat` are as follows:

- The simpleconfig configuration utility fails.
- You want to configure monitoring for WebSphere Portal Server instances.
- You want to specify a server alias that is displayed in the monitoring user interface during the data collector configuration.
- You want to have more control of what data is to be collected. For example, you want to use resource monitoring only and disable diagnostics data and transaction tracking.
- You do not want to configure all application servers within the same profile at one time.
- The data collector is not configured within the application server, and you want to reconfigure it.

## Key WebSphere advanced data-collection settings

### Diagnostic data:

- By default, a **sampling** of diagnostic data is collected, including **all errors** and **some good requests**

### Transaction tracking:

- Varies by data collector – see Unit 9

### Heap Dump, Memory Analysis, and Method Tracing:

- Disabled at server startup
- Enabled in the agent configuration files (see the documentation for the relevant file and parameter)
  - Method Tracing can also be enabled in the Cloud APM UI

### Request sampling and the `gdc_custom.properties` file:

- “Sampling” means just that – a **certain percentage** of requests is captured for analysis and reporting
- Using the settings in the `gdc_custom.properties` file:
  - To collect diagnostic data **for every request**, set `dc.sampling.enable= true` (default is false)
  - To collect **method data for every request** for which diagnostic data is collected, set `dc.sampling.methsampler.enabled= true` (default is false)
  - To enable method data collection **at server startup**, set `dfe.enable.methoddata= true` (default is false)

**Important:** Changing these settings on production servers can lead to critical performance degradation

## Example 2: Node.js agent

Configuring the Node.js agent

- You must add a data collector to your Node.js application, and restart your application before the agent can begin monitoring your application
  - The data collectors collect data that is forwarded to the Node.js agent

Currently, the following data collectors are provided:

- Resource data collector
  - Collects resource monitoring data
  - To enable, add this “require” statement to your application:  
`require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm/ibmapm');`
- Diagnostics data collector
  - Collects diagnostic data and resource monitoring data
  - To enable, add this “require” statement to your application:  
`require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm/deepdive.js');`
- Method trace data collector
  - Collects method traces, diagnostics data, and resource monitoring data
  - To enable, add this “require” statement to your application:  
`require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm/methodtrace.js');`

## Student exercises



Complete the exercises for this unit in the Course Exercise Guide.

## Summary

Now that you have completed this unit, you should be able to:

- Describe deep-dive diagnosis
- Explain the code-level monitoring features of all agents
- Explain additional code-level monitoring features of select agents
- Plan deep-dive resource monitoring
- Configure monitoring agents and data collectors for deep-dive diagnosis



# **Unit 11 Integrating Cloud APM with other products**

IBM Training



## **Integrating Cloud APM with other products**

© Copyright IBM Corporation 2018  
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

This unit describes how to integrate the products IBM Tivoli Monitoring, Netcool/OMNibus, IBM Operations Analytics Log Analysis, Dashboard Application Services Hub, and other products with IBM Cloud APM.

## Learning objectives

After completing this unit, you should be able to:

- Describe how Cloud APM can integrate with other products
- Integrate IBM Tivoli Monitoring
- Integrate Netcool/OMNIbus
- Integrate IBM Cloud and IBM Cloud Private
- Monitor API Connect
- Populate Dashboard Application Services Hub with Cloud APM agent data

### *Learning objectives*

This slide lists the objectives for this unit.

## Unit outline

- Lesson 1: Overview of Cloud APM integration
- Lesson 2: Integrate IBM Tivoli Monitoring
- Lesson 3: Integrate Netcool/OMNIbus
- Lesson 4: Integrate IBM Cloud
- Lesson 5: Integrate IBM Cloud Private
- Lesson 6: Monitor API Connect
- Lesson 7: Populate Dashboard Application Services Hub with Cloud APM agent data

# Lesson 1 Overview of Cloud APM integration

IBM Training



## Lesson 1: Overview of Cloud APM integration

- Integration is a key feature of Cloud APM
  - Allows for smooth migration to Cloud APM
  - Allows for use of existing products
  - Speeds time-to-value
  - Puts a common interface to products of various platforms and user interfaces

This lesson provides an overview of the integration points for products that are not covered in detail later in this unit.

## Products that Integrate with Cloud APM

| Product Name                               | Cloud APM Private | Cloud APM | Covered in this lesson | Covered in a later lesson |
|--|-------------------|-----------|------------------------|---------------------------|
| Alert Notification                         | Yes               | Yes       | Yes                    | No                        |
| Dashboard Applications Services Hub        | Yes               | Yes       | No                     | Yes                       |
| IBM Cloud                                  | Yes               | Yes       | No                     | Yes                       |
| IBM Cloud Private                          | Yes               | No        | No                     | Yes                       |
| IBM Control Desk                           | No                | Yes       | Yes                    | No                        |
| IBM Tivoli Monitoring                      | Yes               | Yes       | No                     | Yes                       |
| Netcool/OMNIbus                            | Yes               | Yes       | No                     | Yes                       |
| OMEGAMON                                   | Yes               | Yes       | Yes                    | No                        |
| Operations Analytics – Log Analysis        | Yes               | Yes       | Yes                    | No                        |
| Operations Analytics – Predictive Insights | Yes               | Yes       | Yes                    | No                        |

## OMEGAMON overview

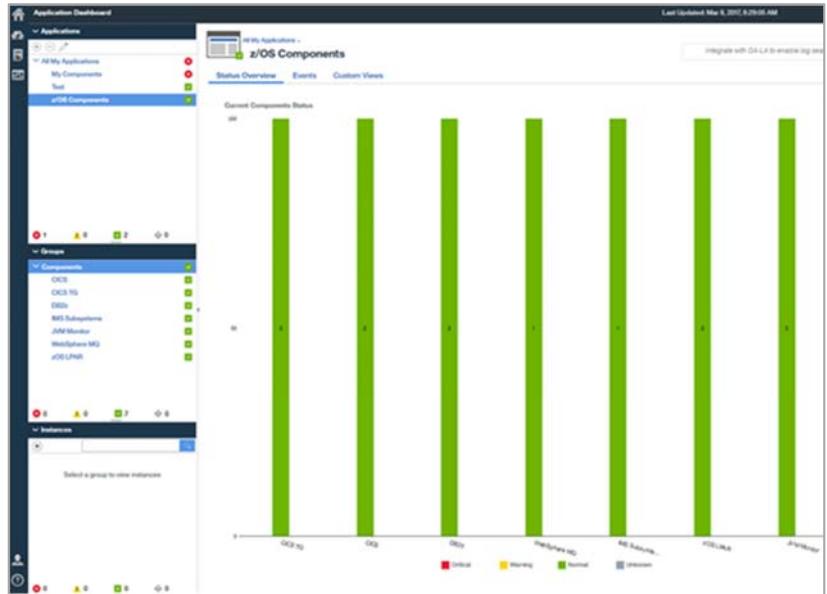
- OMEGAMON is a software family of performance monitors for IBM zEnterprise computer environments
- The IBM Tivoli OMEGAMON Family contains nine products:
  - IBM Tivoli OMEGAMON XE for z/OS V5
  - IBM Tivoli OMEGAMON XE for CICS on z/OS V5
  - IBM Tivoli OMEGAMON XE for IMS on z/OS V5
  - IBM Tivoli OMEGAMON XE for DB2 Performance Monitor for z/OS V5
  - IBM Tivoli OMEGAMON XE for DB2 Performance Expert for z/OS V5
  - IBM Tivoli OMEGAMON XE for Mainframe Networks V5
  - IBM Tivoli OMEGAMON XE for Storage on z/OS V5
  - IBM Tivoli OMEGAMON XE for Messaging for z/OS V5
  - IBM Tivoli OMEGAMON XE for z/VM and Linux V4

### OMEGAMON overview

OMEGAMON, later IBM Tivoli OMEGAMON XE, is a software family of performance monitors for IBM zEnterprise computer environments. These products were produced by Candle Corporation, which IBM acquired in 2004. The OMEGAMON product family provides analysis of IBM mainframe operating systems such as z/OS and z/VM and various subsystems such as CICS, DB2, and IMS.

## z Systems Extension Pack

- Viewing z Systems information in the Cloud APM console is enabled by installing the z Systems Extension Pack
- Also requires:
  - OMEGAMON on z Systems
  - Cloud Application Performance Management portfolio products (Base or Advanced)
- Supports data from seven OMEGAMON z/OS agents:
  - CICS CTG WMQ
  - IMS DB2
  - JVM z/OS LPAR
- The z Systems extension pack was introduced in APM 8.1.3.2, which was a Cloud-only release



Integrating Cloud APM with other products

7

© Copyright IBM Corporation 2018

### z Systems Extension Pack

## Visibility into the performance and availability of z/OS components

The new IBM Cloud APM, z Systems Extension Pack works along with the OMEGAMON products and IBM Cloud APM. To benefit from this solution, all three of the following products must be purchased and installed:

- One (or more) OMEGAMON on z Systems product
- One of the IBM Cloud Application Performance Management portfolio products (Base or Advanced)
- The IBM Cloud Application Performance Management, z Systems Extension Pack (which provides connectivity between the other two components)

IBM Cloud Application Performance Management, z Systems Extension Pack enables:

- Viewing of z Systems monitoring metrics in the Cloud Application Performance Management dashboard
- Consistency of data between the z Systems OMEGAMON user interfaces for z Systems operators and subject matter experts, and the Cloud Application Performance Management user interfaces for application owners and IT operations

For application owners, Cloud Application Performance Management, z Systems Extension Pack fulfills the need to see the relevant KPIs that relate to the performance of the z/OS components of their applications. This provision is necessary when you want to isolate problems that are affecting those applications.

## z/OS LPAR (1 of 2)

The screenshot shows the IBM Application Dashboard interface. On the left, there's a navigation pane with sections for Applications (All My Applications, My Components, Test, z/OS Components) and Groups (Components: CICS, CICS TG, DB2z). The main content area displays two summary cards for different LPARs:

- SP22 - LPAR400J - z/OS LPAR**
  - Average CPU (%): Low (green)
  - RMF MVS CPU (%): Low (green)
  - Real Frames Used (%): High (red)
  - CSA In Use (%): Low (green)
  - System Page\_Rate (sec): 4.9
  - WLM Mode: 2
  - Address\_Space Count: 236
- SYS - LPAR400J - z/OS LPAR**
  - Average CPU (%): Low (green)
  - RMF MVS CPU (%): Low (green)
  - Real Frames Used (%): High (red)
  - CSA In Use (%): Low (green)
  - System Page\_Rate (sec): 2.1
  - WLM Mode: 2
  - Address\_Space Count: 433

Integrating Cloud APM with other products

8

© Copyright IBM Corporation 2018

## z/OS LPAR (1 of 2)

When z/OS LPAR is selected, a summary of each monitored z/OS system is displayed. The z/OS LPAR summary display shows some headline metrics such as average CPU utilization, real storage frame usage, paging rate, and address space count. This data provides the user with an instantaneous high-level view of the health of the monitored z/OS LPARs. In the example above, all z/OS LPARs have high real page frame usage.

The user can now drill into more details for a selected z/OS LPAR by clicking over the summary to see the z/OS LPAR name that is displayed in the lower left of the navigation pane.

Next, select the SP22 LPAR to get more detailed performance data.

## z/OS LPAR (2 of 2)



Integrating Cloud APM with other products

9

© Copyright IBM Corporation 2018

## z/OS LPAR (2 of 2)

The z/OS LPAR pane shows performance metrics for the selected LPAR, including CPU and storage usage. In this example, SQA and ESQA require attention. The system requires more real storage to be made available.

## IBM Operations Analytics – Log Analysis

Log Analysis provides a semi-structured data analytics solution

- Use Log Analysis to help you to reduce problem diagnosis and resolution time, helping you to manage your infrastructure and applications more effectively
- Features include:
  - Analytics
  - Data archiving
  - Insight Packs
  - Linking
  - Scalable data streaming
  - Searching and visualizing data
  - Support for Linux on System z based servers

### IBM Operations Analytics – Log Analysis

The key features include:

- **Analytics:** Log Analysis provides analysis of logs to determine trends.
- **Data archiving:** Log Analysis stores data in data archives, helping to improve search performance.
- **Insight Packs:** Use included or customized Insight Packs to tailor data indexing and annotation to suit specific types of data.
- **Linking:** Use Log Analysis to link unstructured data, such as logs, with structured data such as CPU utilization and transaction status, and present in either a data warehouse or the application database.
- **Scalable data streaming:** Use Log Analysis to facilitate dynamic data streaming that is scalable across multiple remote sources.
- **Searching and visualizing data:** When you want to identify problems in your infrastructure and applications, the Log Analysis components work together to identify issues in unstructured data such as log files and configuration files.
- **Support for Linux on System z based servers:** You can install Log Analysis on Linux on System z based servers.

## Integrate IBM Operations Analytics – Log Analysis

Integration includes these features:

- Application Performance Manager search
  - You enter error information from events into the search field
- Search starts an on-premises version of IBM Operations Analytics Log Analysis
- IBM Operations Analytics Log Analysis provides insight by analyzing error patterns in log files
  - It also helps providing expert advice for errors

### *Integrate IBM Operations Analytics – Log Analysis*

You can integrate IBM Cloud APM with IBM Operations Analytics Log Analysis to enable searching for error messages from various locations in the customer environment.

IBM Operations Analytics – Log Analysis supports expert advice, which improves the usability of the messages by indicating what actions to take to address the errors that are detected.

## IBM Operations Analytics – Log Analysis integration scenario (1 of 5)

The screenshot shows the IBM Operations Analytics interface for log analysis. At the top, there's a navigation bar with 'All My Applications > My Components > Components > WebSphere Application Server > lin1Node01server1:lin1:KYNs'. Below it is a 'Status Overview' section with tabs for 'Events' (which is selected) and 'Attribute Details'. A yellow arrow points to the search bar in the top right, which contains the text 'SRVE8094W'. To the right of the search bar is a magnifying glass icon. The main area is titled 'Log Messages' and shows a bar chart of errors over time. Below the chart is a table titled 'Log Messages (last 100 messages)' with columns for Error date and time, Thread ID, Severity, Message ID, Message text, and Process ID. The table lists several error messages from May 18, 2016, with the last message being 'SRVE8094W'. A yellow callout box on the right side contains the following text:

- The message log contains an error
- Moving the mouse over the message text displays the full message
  - Note the SRVE8094W message

1) Enter the message ID into the search area in the upper-right corner, and click the magnifying glass

### IBM Operations Analytics – Log Analysis integration scenario (1 of 5)

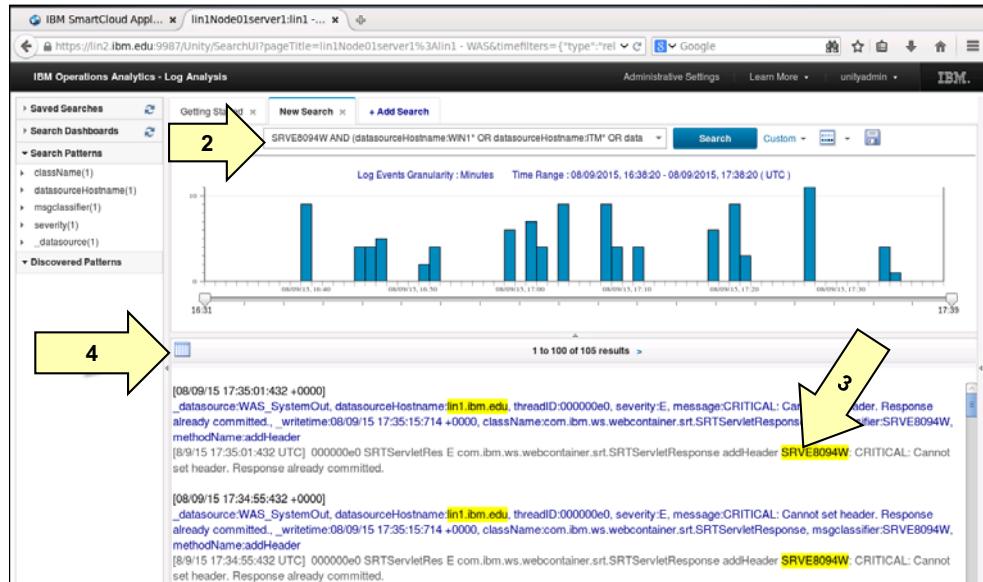
The log contains a critical error that reads in part in the message text: SRVE8094W. Due to the column size, it might not be visible.

1. Move the mouse pointer over the message to show the entire message. Note the message ID SRVE8094W.

Type the message ID **SRVE8094W** into the search box in the upper right to search IBM Operations Analytics Log Analysis for advice.

## IBM Operations Analytics – Log Analysis integration scenario (2 of 5)

- 2) Look for the message SRVE8094W in the results window
- 3) The message is highlighted SRV8094W in the lower part of the window
- 4) Select Grid View to open a table and parse the log



### IBM Operations Analytics – Log Analysis integration scenario (2 of 5)

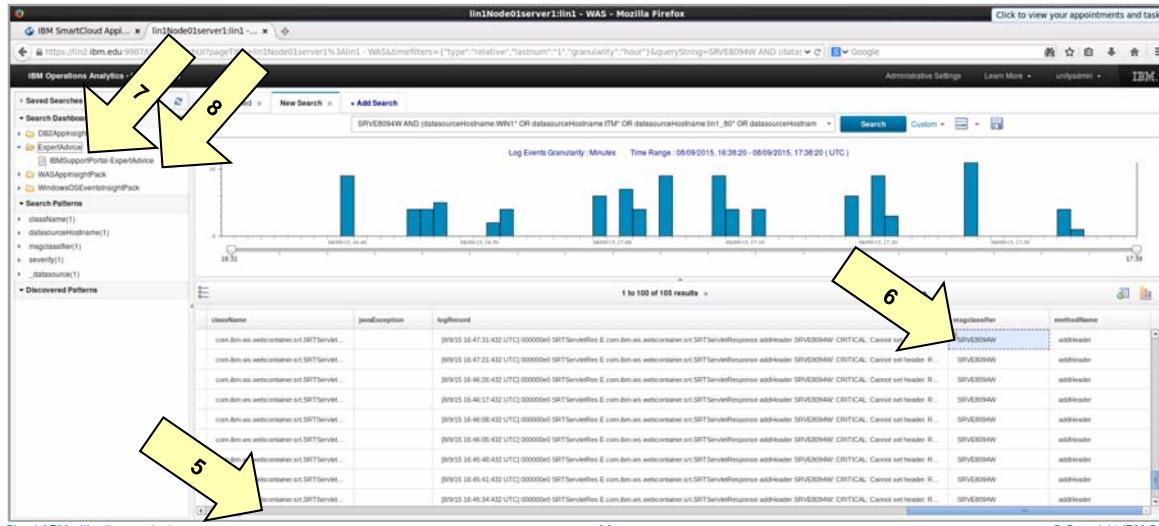
2. The first time that you search, a login window to the IBM Operations Analytics opens. Log in with the user name **unityadmin** and the password **object00**. This login starts a search on the IBM Operations Analytics Log Analysis server, looking for this message ID in the stock trading application.
3. Note the highlighted strings in the messages.
4. Select Grid View to parse the log.

IBM Training



IBM Operations Analytics – Log Analysis integration scenario (3 of 5)

- 5) Scroll the bar to the right
  - 6) Highlight a msgclassifier cell
  - 7) Expand **Expert Advice**
  - 8) Select **IBMSupportedPortal-ExpertAdvice**



IBM Operations Analytics – Log Analysis integration scenario (3 of 5)

5. Scroll to the right.
  6. Highlight the message **SRVE8094W** under the **msgclassifier** field.
  7. On the left, expand the **Custom Apps** and **Expert Advice**.
  8. Select **IBMSupportPortal-ExpertAdvice**.

## IBM Operations Analytics – Log Analysis integration scenario (4 of 5)

- 9) The Expert Advice offers several possible solutions for this message ID
- 10) Scrolling downward, you can see and click the Fix List for WebSphere Application Server 8.5

The screenshot shows the 'IBM Operations Analytics - Log Analysis' interface. The left sidebar includes 'Saved Searches', 'Search Dashboards' (with 'DB2AppInsightPack', 'ExpertAdvice' selected, and 'IBMSupportPortal-ExpertAd'), 'Search Patterns', and 'Discovered Patterns'. The main area is titled 'Search Results' under 'Expert Advice Search Results'. It displays three error messages with yellow callout boxes numbered 9 and 10 pointing to specific parts of each message:

- JR51756: THE SRVE8094W WARNING MESSAGE OCCURS IN THE IBM BPM SERVER LOG**  
Process Manager (BPM) server logs show many occurrences of the following warning message: "SRVE8094W: WARNING: Cannot set header. Response already committed. Even though no function is lost, these messages can clutter the system ..."
- PM86580: SYSTEMOUT.LOG CONTAINS MANY OCCURRENCES OF THE WARNING: SRVE8094W: WARNING: CANNOT SET HEADER. RESPONSE ALREADY COMMITTED**  
SystemOut.log contains many occurrences of the warning: "SRVE8094W: WARNING: Cannot set header... Buffer Size to prevent the "WARNING: Cannot set header. Response already committed." message..." "WARNING: Cannot set header. Response already committed." message... "WARNING: Cannot set header. Response already committed."
- PM84636: SYSTEMOUT.LOG CONTAINS MANY OCCURRENCES OF THE WARNING: SRVE8094W: WARNING: CANNOT SET HEADER. RESPONSE ALREADY COMMITTED**  
SystemOut.log contains many occurrences of the warning: "SRVE8094W: WARNING: Cannot set header... Buffer Size to prevent the "WARNING: Cannot set header. Response already committed." message..." "WARNING: Cannot set header. Response already committed." message... "WARNING: Cannot set header. Response already committed."

At the bottom, there is a link for 'Fix list for IBM WebSphere Application Server V8.5'.

## IBM Operations Analytics – Log Analysis integration scenario (4 of 5)

The remaining steps require an internet connection to complete.

9. The search locates several solutions for this error message.
10. Because you are running WebSphere 8.5, select the fix list for IBM WebSphere Application Server V8.5.

## IBM Operations Analytics – Log Analysis integration scenario (5 of 5)

- 11) The WebSphere Fix Pack 8.5.5.6 might solve the problem that you detected

The screenshot shows a web browser window for 'IBM Fix list for IBM WebSphere Application Server V8.5 - United States - Mozilla Firefox'. The URL is [www-01.ibm.com/support/docview.wss?uid=swg27036319](http://www-01.ibm.com/support/docview.wss?uid=swg27036319). The page title is 'Fix list for IBM WebSphere Application Server V8.5'. On the left, there's a sidebar with 'Others also viewed...' links: 'Recommended fixes for WebSphere Application Server', '8.5.5.6: WebSphere Application Server V8.5.5 Fix Pack 6', 'Fixes by version for WebSphere Application Server', '8.5.5.5: WebSphere Application Server V8.5.5 Fix Pack 5', and '8.5.5: WebSphere Application Server V8.5.5.0'. Below that is a 'Tags' section. The main content area has a 'Product readme' and an 'Abstract' section. Under 'Content', there's a 'Back to all versions' link followed by a list of fix packs: 'Fix Pack 8.5.5.6' (highlighted with a yellow arrow), 'Fix Pack 8.5.5.5', 'Fix Pack 8.5.5.4', and 'Fix Pack 8.5.5.3'. There are also 'Back' and 'Forward' navigation buttons.

### IBM Operations Analytics – Log Analysis integration scenario (5 of 5)

11. The WebSphere fix pack 8.5.5.1 should solve the error that you detected.

This demonstration shows the value of integrating IBM Cloud APM Private with IBM Operations Analytics Log Analysis. By integrating these two products, you isolate and locate the solution to a problem in your environment.

## Integrate IBM Operations Analytics – Predictive Insights

- IBM Operations Analytics – Predictive Insights
  - This component extends the capabilities of IBM Cloud APM by providing early detection of service and application issues to help avoid service disruptions and outages that affect your business
  - Predictive Insights automatically learns the normal operational behavior of complex infrastructures, such as a Cloud, and is designed to identify problems before you know to look for them
  - Provides real-time performance analysis for business services
  - Analyzes monitoring data to learn the normal behavior of a business service and create a performance model
  - Generates an alarm when behavior outside normal behavior is detected (anomaly)
- Predictive Insights user Interface
  - Used to perform root cause analysis of an anomaly
  - Dynamic view of the anomaly that contains all relevant metrics
  - Presents a normalized view of metric data for metric comparison and trend identification

### *Integrate IBM Operations Analytics – Predictive Insights*

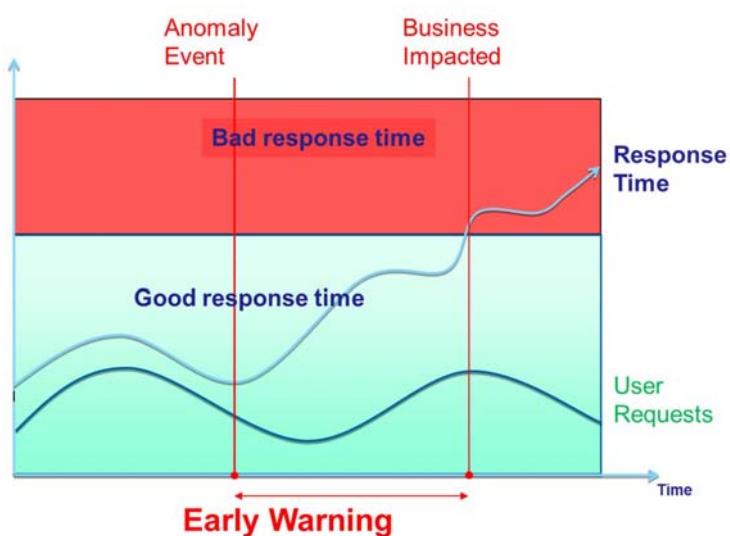
IBM Operations Analytics – Predictive Insights on Cloud provides real-time performance analysis for business services. Early detection of service and application issues helps you avoid service disruptions and outages that affect your business.

Predictive Insights automatically learns the normal operational behavior of complex infrastructures, such as a cloud, and is designed to identify problems before you know to look for the anomaly. The Predictive Insights user interface provides dynamic views of identified anomalies and all relevant metrics. The normalized view supports metric comparison and trend identification.

## Early warning

IBM Operations Analytics Predictive Insights can provide early problem detection to predict application, middleware, or infrastructure problems before they affect service

The software helps you avoid outages and increase service performance



### Early warning

If you want earlier warnings before service problems affect the business, you can no longer set static thresholds on important performance indicators. To get earlier warnings, you need to detect when things are straying away from normal operations. For example, response time should increase and decrease in relation to the number of user requests. However, when response time no longer abides by that trend, operators can get an alarm that can give them time to respond before business is affected.

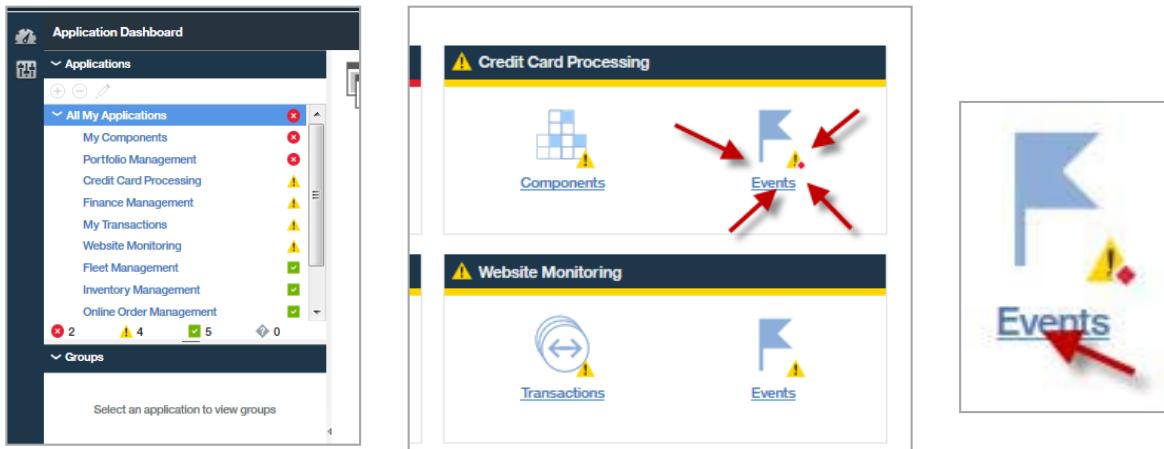
## Anomaly events

- Have a threshold name of Anomaly Detected
- Have a Warning status
- Are linked to a resource by the managed system name for the metric that is anomalous
- Provide a description of the anomaly
- Have special icons to indicate anomalies
- Tooltips for these events contain a link to start Predictive Insights in context
- Consolidated when multiple anomalies are detected for the same Managed System Name

### Anomaly events

Anomaly events are detected by Predictive Insights and signaled by a special icon. They have a threshold name of “Anomaly Detected”, and display a warning status. The managed system name and the anomalous metric are included in the event. Tooltips for these events contain a link to start Predictive Insights in context. Anomalies are consolidated when more than one is detected for the same managed system name.

## Cloud APM integrates with IBM Operations Analytics – Predictive Insights



### Cloud APM integrates with IBM Operations Analytics – Predictive Insights

1. Locate and click a problem application in the Application widget.
2. In the All My Applications dashboard, check whether any applications show an anomaly. An anomaly is indicated as shown in the slide by a red diamond in the lower corner of a status indicator.
3. Click the **Events** link, as indicated in the slide.

## Event hover help: IBM Operations Analytics – Predictive Insights

The screenshot shows two views of the IBM Operations Analytics - Predictive Insights interface. The top view displays a summary of events for the 'Credit Card Processing' application, showing 2 total events, 0 critical, 2 warning, and 0 normal. The bottom view is a detailed list of events, also for 'Credit Card Processing'. It lists two events: 'WAS\_Response\_Time\_High' and 'Anomaly Detected'. The 'Anomaly Detected' event is expanded, showing its details: Node (worklight17node), Threshold ID (worklight17KYNB), Global Timestamp (Jan 13, 2018, 6:30:03 AM), Type (Sampled), and Description (responseTime is Higher than expected. Actual: 2535 Expected: 542). An arrow points from the 'Events' tab in the top navigation bar to the 'Anomaly Detected' event in the list.

| Threshold Name         | Status | Severity  | Display Item | Source | Timestamp | 2 | Description |
|------------------------|--------|-----------|--------------|--------|-----------|---|-------------|
| WAS_Response_Time_High | Open   | ⚠ Warning | workli...    |        |           |   |             |
| Anomaly Detected       | Open   | ⚠ Warning | workli...    |        |           |   |             |

Integrating Cloud APM with other products

21

© Copyright IBM Corporation 2018

### Event hover help: IBM Operations Analytics – Predictive Insights

4. Review the list of events. The list includes an anomaly, which is associated with the application server.
5. Expand the **Anomaly Detected** event.
6. Next, click **View Anomaly analysis**.

## Detailed analysis



Integrating Cloud APM with other products

22

© Copyright IBM Corporation 2018

### Detailed analysis

The Predictive Insights interface includes a line graph that tracks the anomalous statistics, and a table that you can use to add other statistics for comparison.

Anomalies are highlighted in red.

This level of detail is available only for anomalies.

## Integrate with IBM Alert Management

### Integrating IBM IT Alert Notification: Overview

- IBM Alert Notification is a simple notification system that gives IT staff instant notification of alerts for issues in your IT operations environment
  - Data that is received from agents provides the source of the alerts
- As a stand-alone package, you can integrate Alert Notification with any on-premises monitoring tool that can implement and start a REST API
  - Netcool/OMNibus
  - Netcool/Impact
- When subscribed for IBM Cloud APM on Cloud, IBM IT Alert Notification is made available automatically

| Who         | Date                  | Change   | Notified |
|-------------|-----------------------|--|----------|
| SYSTEM      | 6/15/2016, 7:05:23 PM | Notification State changed from Unnotified to Notified, Last Notified has been added |          |
| qumcocnugmg | 6/15/2016, 7:05:22 PM | Created  |          |

Integrating Cloud APM with other products

23

© Copyright IBM Corporation 2018

### Integrate with IBM Alert Management

IBM IT Alert Notification can be integrated with IBM Cloud APM on Cloud in a few clicks. The data from the on-premises monitoring agents is the source for the alert data. IBM Cloud APM on Cloud can also be integrated with an existing physical on-premises installation of Tivoli Netcool/OMNibus.

Because IBM IT Alert Notification is provided as a service, the required server infrastructure is installed and managed by IBM, reducing your time-to-value and offering low-maintenance ownership. IBM IT Alert Notification is offered with IBM Cloud APM on Cloud. You can activate IBM IT Alert Notification with your IBM ID and password on the IBM Marketplace at this URL:  
<https://www.ibm.com/marketplace>

When the Collaborative Operations product is available, an integration with IBM Control Desk becomes available. With this integration, a ticket can be opened as a service request.

After you set up an instance of IBM Cloud APM on Cloud and activate IBM IT Alert Notification, you can connect the two services together.

For an IBM Cloud APM on Cloud integration, set up a subscription on IBM Marketplace and connect it to your IBM IT Alert Notification. Monitoring agents can be downloaded, and then installed and set up in your monitoring environment. An integration with an on-premises Tivoli Netcool/OMNibus is also possible.

## IBM IT Alert Notification email example (Cloud only)

The screenshot shows an email from IBM Alert Notification. The subject is "IBM Alert Notification: Critical. Notification of \*ITM Agent: Private Situation: NT\_Logical\_Disk\_Space\_Critical:ITM\_NT\_Logical\_Disk:C on Primary:WIN1:NT". The email body contains a summary of the alert, actions (Acknowledge this alert, Unacknowledge this alert), more information (View Alert Details, View all my notifications), alerts overview, and applications or services. A yellow callout box highlights two points:

- The situations from Cloud APM can be forwarded to IBM IT Alert Notification to send email notifications
- The source for the alert data is from on-premises monitoring agents

Integrating Cloud APM with other products

24

© Copyright IBM Corporation 2018

IBM IT Alert Notification email example (Cloud only)

Alerts are received from the alert source. Alerts can be received from IBM Cloud APM on Cloud.

Alerts that match the filter conditions in notification policies trigger notifications. Examples of filter conditions include severities, devices, and string matching. In addition to the conditions that trigger a notification, notification policies also specify who receives notifications. The recipients can be individual contacts or groups.

Contacts can click a link in the notification email that acknowledges the alert, which indicates to other contacts that someone is working on that alert. Depending on the settings in the notification policy, an acknowledgment notification can be sent to the contacts. The notification policy can be configured to send a follow-up notification to the contacts that the alert was acknowledged.

Users can log in to IT Alert Notification and action the alert in the Notification Viewer. Actions include keeping a journal of information against the alert, and logging tickets. Mistakenly acknowledged alerts can be unacknowledged.

After the conditions that caused the alert are fixed, the alert can be resolved from the Notification Viewer or dashboard. The notification policy can be configured to send another notification to the contacts that the alert was resolved.

## Alert Viewer (1 of 3)

Alerts can be acknowledged

The screenshot shows a user interface for an 'Alert Viewer'. At the top, there are two small icons: a gear and a user profile. Below this is a search bar with a magnifying glass icon. The main area has two columns: 'Alert Source' and 'Actions'. Under 'Alert Source', it says 'ITM Agent: Private Situation'. Under 'Actions', there are three icons: a thumbs-up (highlighted with a red arrow), a document, and a list. A button labeled 'Acknowledge this alert' is located below these icons. Below this section is a header 'Notified' followed by an email address: htaylor@us.ibm.com.

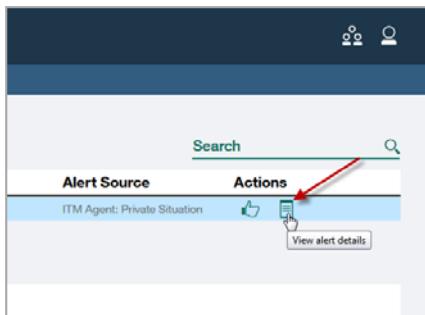
| Alert Source                 | Actions                    |
|------------------------------|----------------------------|
| ITM Agent: Private Situation | <br>Acknowledge this alert |

Notified

htaylor@us.ibm.com

## Alert Viewer (2 of 3)

You can view alert details:



A screenshot of the 'Alert Details' page. The title is 'Alert Details (13-23cd4)'. There's a search bar at the top right. Below it is a table with two columns: 'Property' and 'Value'. The properties listed include 'description', 'disk\_read\_bytes\_per\_sec\_64[0]', 'server\_name[0]', 'disk\_name\_long[0]', 'disk\_write\_bytes\_per\_sec[0]', 'avg\_disk\_read\_queue\_length[0]', 'physical\_disk\_number[0]', 'pct\_disk\_time[0]', 'disk\_writes\_per\_sec[0]', 'pct\_disk\_read\_time[0]', and 'disk\_write\_bytes\_per\_sec\_64[0]'. The values for most properties are '0', except for 'server\_name[0]' which is 'Primary:WIN1:NT'.

| Property                       | Value  |
|--------------------------------|--|
| description                    | NT_Logical_Disk_Space_Critical[%_Free <= 99 AND ...] |
| disk_read_bytes_per_sec_64[0]  | 0  |
| server_name[0]                 | Primary:WIN1:NT                                      |
| disk_name_long[0]              | C:   |
| disk_write_bytes_per_sec[0]    | 0  |
| avg_disk_read_queue_length[0]  | 0  |
| physical_disk_number[0]        | 0  |
| pct_disk_time[0]               | 0  |
| disk_writes_per_sec[0]         | 0  |
| pct_disk_read_time[0]          | 0  |
| disk_write_bytes_per_sec_64[0] | 0  |

Alert details are viewed by selecting **View Alert Details**.

## Alert Viewer (3 of 3)

Alerts can be filtered by these characteristics:

- Unnotified
- Notified
- Escalated
- Acknowledged
- Archived
- Status
  - Fatal
  - Critical
  - Major
  - Minor
  - Warning
  - Indeterminate

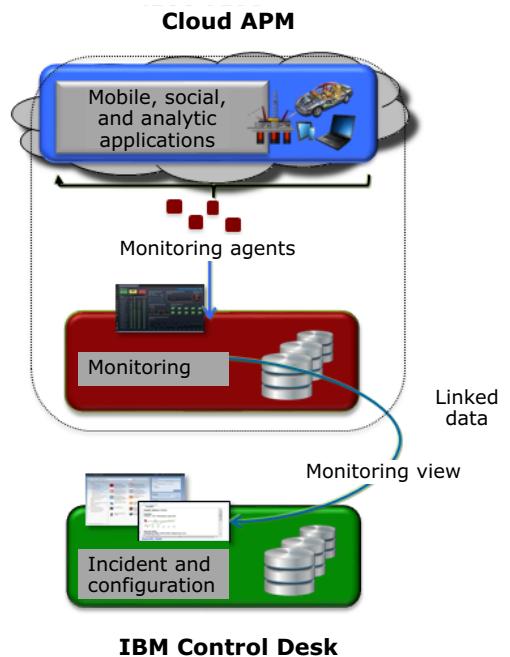
The screenshot shows the 'Alert Viewer' section of the IBM Agile Operations Management interface. At the top, there are tabs for 'Manage Notification Policies' and 'Alert Viewer'. Below the tabs, there are two buttons: 'All Alerts' (gray) and 'My Alerts' (green). The main area is titled 'Alert Viewer' and contains a table with columns 'State', 'ID', and 'What Happened'. One row is visible, showing a thumbs-up icon, ID 13-23cd4, and the text 'NT\_Logical\_Disk\_Space\_Critical:ITM\_NT\_Logi...'. To the left of the table is a vertical sidebar with various icons representing different alert types and actions.

### Alert Viewer (3 of 3)

Alerts are filtered based on status.

## Integration with IBM Control Desk (Cloud only)

- When IBM Cloud APM detects an issue with your application, it can automatically open a service request in IBM Control Desk
- Your specialists can fix problems in your applications before users have time to report them
- Your help desk spends more time solving application issues and less time answering support calls



### Integration with IBM Control Desk (Cloud only)

The integration of IBM Cloud APM and IBM Control Desk provides business value by making your help desk more efficient.

## Events in the APM user interface (Cloud only)

After you install and configure the integration agent, you can see the events in the APM UI and open service requests in IBM Control Desk

The screenshot shows the 'Event Status' section of the 'My Components' page. It includes a progress bar for event severity and a table of events.

**Event Severity Summary (Total:3)**

|          |           |            |
|----------|-----------|------------|
| Normal:0 | Warning:2 | Critical:1 |
| 66.67%   | 33.33%    |            |

**Event Status**

| Situation Name         | Status | Severity                                     | Display Item             | Source                 | Timestamp               | Description                 |
|------------------------|--------|--|--------------------------|------------------------|-------------------------|-----------------------------|
| Linux_Disk_Space_Low   | Open   | <span style="color:red;">✖ Critical</span>   |                          | central1:LZ            | Jun 6, 2014, 4:08:41 PM | Disk free space is low.     |
| Application_RT_High_A  | Open   | <span style="color:yellow;">⚠ Warning</span> | /downloads/node_app/k... | NJ:njsrh65_3001:NJA    | Jun 6, 2014, 4:22:59 PM | Application response tim... |
| KV1_Host_CPU_Over_C... | Open   | <span style="color:yellow;">⚠ Warning</span> | kvmcompute               | kvmcompute:central1:V1 | Jun 6, 2014, 4:08:50 PM | The CPU of your host is ... |

### Events in the APM user interface (Cloud only)

In the Cloud APM console, events show up in several places. A consolidated view of all your events can be seen in the My Components Event Status tab.

## Tickets in IBM Control Desk (Cloud only)

This screen capture shows how the service requests look in IBM Control Desk:

The screenshot shows the 'Service Requests' screen in IBM Control Desk. On the left, there's a navigation sidebar with sections like 'Available Queries', 'Common Actions', and 'More Actions'. The main area displays a grid of service requests. The columns include 'Service Request', 'Summary', 'Reported By', 'Internal Priority', 'Priority', 'Status', 'Owner', and 'Owner Group'. The status column shows entries like 'CLOSED', 'RESOLVED', and 'PENDING'. The summary column contains details such as 'APMaaS Event - SID036APMXGREEN-030 us-na.apm ibmservice engage.com'. The first five rows are highlighted in light blue.

| Service Request | Summary  | Reported By | Internal Priority | Priority | Status   | Owner | Owner Group |
|-----------------|--|-------------|-------------------|----------|----------|-------|-------------|
| 1001            | APMaaS Event - SID036APMXGREEN-030 us-na.apm ibmservice engage.com |             |                   |          | CLOSED   |       |             |
| 1002            | APMaaS Event - SID036APMXGREEN-030 us-na.apm ibmservice engage.com |             |                   |          | RESOLVED |       |             |
| 1003            | APMaaS Event - SID036APMXGREEN-030 us-na.apm ibmservice engage.com |             |                   |          | RESOLVED |       |             |
| 1004            | APMaaS Event - SID036APMXGREEN-030 us-na.apm ibmservice engage.com |             |                   |          | RESOLVED |       |             |
| 1005            | APMaaS Event - SID036APMXGREEN-030 us-na.apm ibmservice engage.com |             |                   |          | RESOLVED |       |             |

## Tickets in IBM Control Desk (Cloud only)

After the integration is configured, the events that are seen in the APM UI will also be seen in the IBM Control Desk.

This image shows how the service requests look in IBM Control Desk.

# Lesson 2 Integrate IBM Tivoli Monitoring

IBM Training



## Lesson 2: Integrate IBM Tivoli Monitoring

### Overview of IBM Tivoli Monitoring integration

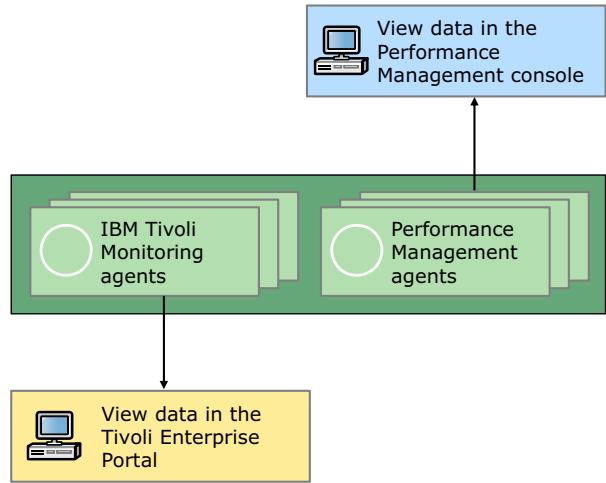
- Cloud APM integrates with IBM Tivoli Monitoring V6 in three ways:
  - Coexistence of IBM Tivoli Monitoring V6 agents on the same operating system as Cloud APM agents
  - Consolidation of status and events by using the Hybrid Gateway
  - Consolidation of historical data in the Tivoli Data Warehouse that allows for long-term historical data to be collected, and reports generated

In this lesson, you learn how to integrate with IBM Tivoli Monitoring.

IBM Tivoli Monitoring V6 can integrate in multiple ways with the Cloud APM.

## Coexistence of v6 and v7 agents with v8 agents

- You can install IBM Cloud APM agents (version 8) on the same computer where IBM Tivoli Monitoring agents (versions 6 or 7) are installed
- Both agent types cannot be installed in the same directory
- Most agents can coexist
  - For a full list, see the documentation



### Coexistence of v6 and v7 agents with v8 agents

The goal is to provide users with the ability to install both IBM Tivoli Monitoring and Cloud APM agents on the same system. Areas of conflict are resolved in the implementation, such as file system locations, and registry settings.

If coexisting agents are monitoring the same resources, the following scenarios are not supported:

Both agents store data in the same IBM Tivoli Data Warehouse. If both agents send data to the same Tivoli Data Warehouse, do not use the version 8 WebSphere MQ agent and the version 6 or 7 WebSphere MQ agent to monitor the same queue manager on your system. This scenario also applies to multi-instance agents. For more information, see Tivoli Data Warehouse for historical reporting.

Version 6 or 7 agents are integrated with the Hybrid Gateway to display data from both agents in the Cloud APM console. For example, version 6 or 7 agents might be connected to the same Cloud APM server through the Hybrid Gateway. In this case, do not use the version 8 IBM Integration Bus agent and the version 6 or 7 ITCAM agent for WebSphere Message Broker to monitor the same broker on your system.

## Hybrid Gateway overview

- Customers need to manage both IBM Tivoli Monitoring 6 On Premises and IBM Cloud APM agents
  - In an environment that includes both IBM Tivoli Monitoring and IBM Cloud APM products, you can install the IBM Cloud APM Hybrid Gateway to provide a consolidated view of managed systems from both domains
- The Hybrid Gateway can help customers migrate from IBM Tivoli Monitoring 6 to IBM Cloud APM
- The Hybrid Gateway must be installed in your IBM Tivoli Monitoring environment on a system with Red Hat Enterprise Linux Server 6 Update 2 or higher
- The Hybrid Gateway can support 1500 – 2000 IBM Tivoli Monitoring on-premises agents

### Hybrid Gateway overview

When your monitored environment includes both IBM Tivoli Monitoring and IBM Cloud APM products, you can install the IBM Cloud APM Hybrid Gateway to get a consolidated view of managed systems from both domains.

When the Cloud APM Hybrid Gateway is installed and configured, it is used to view managed systems from a Tivoli Monitoring domain in the Cloud APM console. This gateway must be installed on systems with Red Hat Enterprise Linux Server 6 Update 2 or later.

Having more than 2000 managed systems can degrade performance, and 2000 is therefore the upper limit of the number of Tivoli Monitoring agents that are supported.

## IBM Training



### Viewing hybrid agents in the dashboard

- WIN1 is a Cloud APM agent
- ITM is an IBM Tivoli Monitoring agent

Integrating Cloud APM with other products © Copyright IBM Corporation 2018

#### Viewing hybrid agents in the dashboard

You can view hybrid agents in the Cloud APM UI Application Dashboard. In a hybrid environment, you can see information that represents agents from traditional monitoring systems and from IBM Cloud APM. In the example, views display one IBM Tivoli Monitoring Windows agent and one Cloud APM Windows agent.

Note the icons on the views that represent the Status Overview and the events that are in the upper-left corner of each view. The IBM Tivoli Monitoring agent icon is a building with a wrench on it. The Cloud APM agent WIN1 icon is a cloud with a wrench on it.

The two examples on the right side of the page indicate how similar the widgets look, whether it is an IBM Tivoli Monitoring agent or a Cloud APM agent.

## Benefit of integrating IBM Tivoli Monitoring events

| Situation Name | Status | Severity | Display Item | Source         | Timestamp  |
|----------------|--------|----------|--------------|----------------|------------|
| HG{EIF_Sit}    | Open   | Critical | HG{EIF_Sit}  | nc9037034031LZ | 2015-10-20 |
| HG{EIF_Sit}    | Open   | Critical | HG{EIF_Sit}  | nc9037034211LZ | 2015-10-20 |

- Customers can now see situation events that are opened by the IBM Tivoli Monitoring agents and integrated into Cloud APM

### Benefit of integrating IBM Tivoli Monitoring events

No new components are necessary to install in the Advanced configuration for the Hybrid Gateway. The Hybrid Gateway still requires a Managed System Group name that corresponds to the IBM Tivoli Monitoring Managed System List name. The Hybrid Gateway also still requires a Tivoli Enterprise Portal Server host name, Portal Server Port, Portal Server Protocol, Portal Server user name, and any applicable pass-through proxy port and protocol.

The EIF Port in the Hybrid Gateway configuration affects the integration. The Hybrid Gateway listens for events on the same port as the MIN Event Manager. The Advanced Configuration for the Event Manager port is usually the default port of 9998.

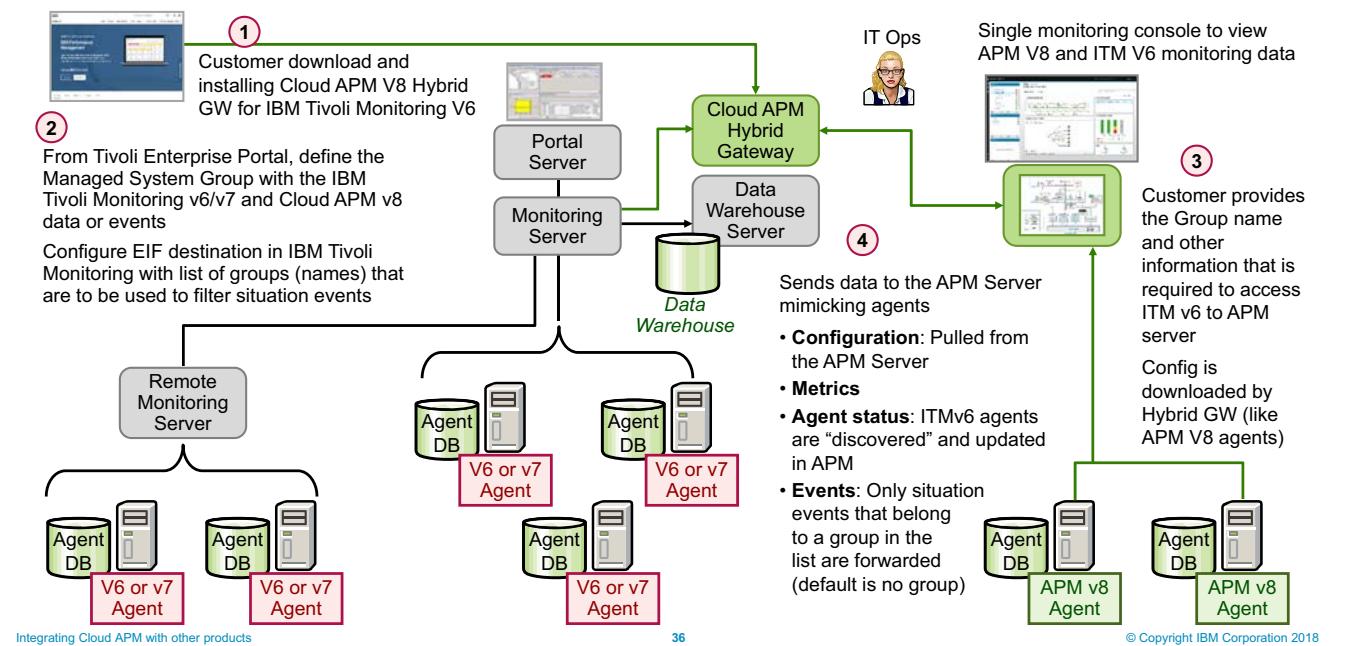
In the Hub Tivoli Enterprise Monitoring Server configuration in IBM Tivoli Monitoring, The Tivoli Event Integration Facility (EIF) must be activated. The location of the Hybrid Gateway and its EIF listener port must be provided. If events are already being emitted to another destination (for example, OMNIbus), further destinations can be defined by using the `tacmd createeventdest` command.

From IBM Tivoli Monitoring in the Situation Editor, edit a situation whose events should be forwarded to APM. On the EIF tab:

- Select **Forward Events to an EIF Receiver**.
- Select the new **Hybrid Gateway Receiver**.
- Repeat these steps for each situation.

Thus, for each situation that was modified to specify the Hybrid Gateway destination, the Hub Tivoli Enterprise Monitoring Server forwards all events from any IBM Tivoli Monitoring agent to which the situation is distributed.

## Integrating with IBM Tivoli Monitoring by using the Hybrid Gateway



### Integrating with IBM Tivoli Monitoring by using the Hybrid Gateway

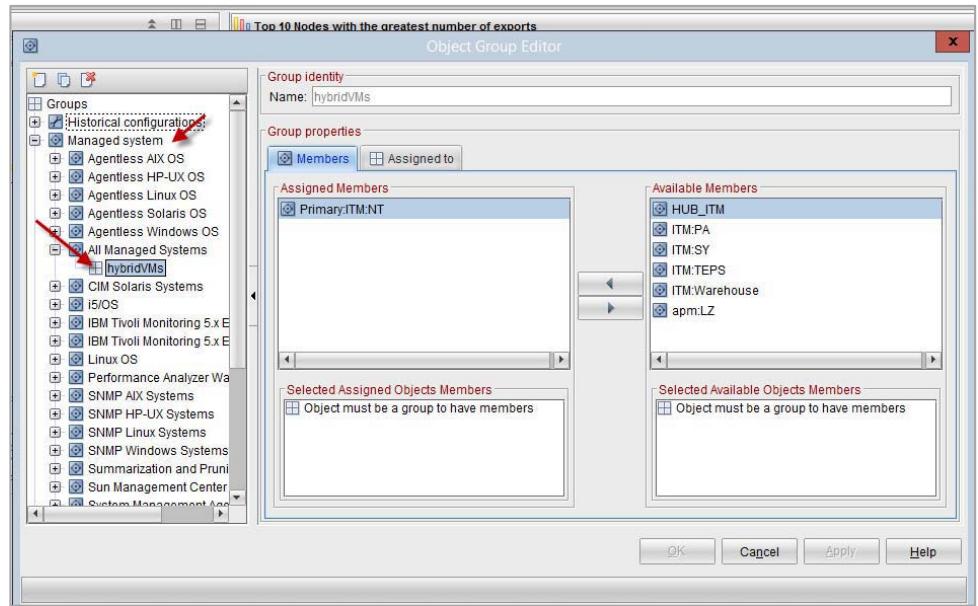
This diagram shows the IBM Performance Hybrid Gateway.

The right side of the screen displays a Cloud APM environment. Agents are installed along with direct monitoring information into the Cloud APM user interface (APM UI), which is the Application Dashboard.

On the left side, the IBM Tivoli Monitoring environment is depicted, showing the Portal Server, Monitoring Server, monitoring agents, and the portal client. The Hybrid Gateway directs information from the Portal Server to the environment, where the APM UI can display this data.

## From IBM Tivoli Monitoring

- From the Object Group Editor, create a managed system group
  - This group contains the names of the managed systems to see in Cloud APM
- The managed system group name is case-sensitive and is also used by the hybrid gateway configuration



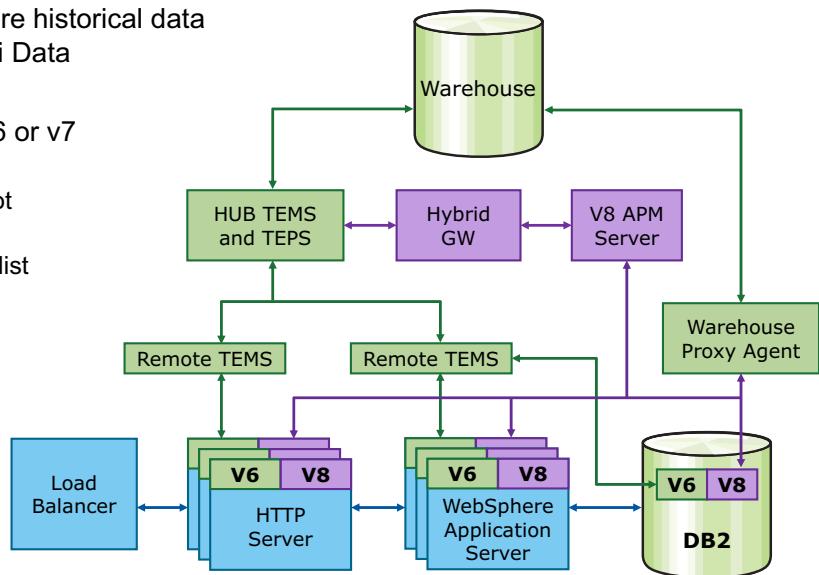
## From Cloud APM

- Obtain the Hybrid Gateway agent
- Install the Hybrid Gateway agent on a system other than the server where the MIN is running
- From System Configuration, set the parameters for the Hybrid Gateway in the Hybrid Gateway Manager dialog box
- The Managed System Group Name is the name that is defined in IBM Tivoli Monitoring by using the Object Group Editor to contain the server member names

| Profile Name | Managed System Group Name | Portal Server Host Name |
|--------------|---------------------------|-------------------------|
| ln3          | hybridVMs                 | itm.ibm.edu             |

## Integrating Cloud APM V8 agents with IBM Tivoli Monitoring V6 Tivoli Data Warehouse

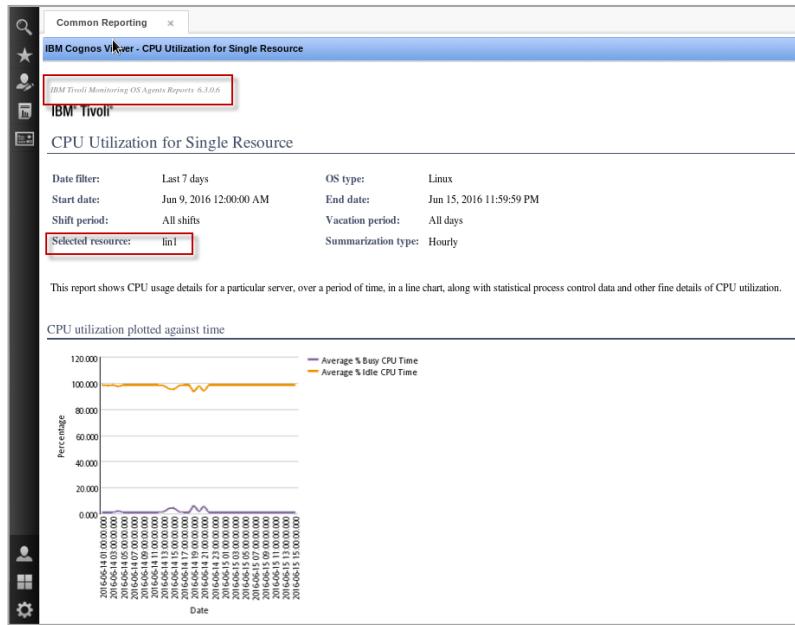
- With Cloud APM, customers can store historical data in the IBM Tivoli Monitoring V6 Tivoli Data Warehouse
- Only agents with a corresponding v6 or v7 agent are supported
  - New metrics unique to APM V8 are not warehoused
  - See the documentation for a detailed list
- Data is sent from the Cloud APM V8 agents to the Warehouse Proxy and then inserted into the Tivoli Data Warehouse
- Allows for enterprise-wide reporting



### Integrating Cloud APM v8 agents with IBM Tivoli Monitoring V6 Tivoli Data Warehouse

Sample history files for agents are available on your Cloud APM server. Use the sample file for your agent as the basis for creating the history configuration XML file on the Cloud APM server. The server propagates the configuration to all agents of this type. The history file specifies the warehouse proxy agent address, the data sets to collect samples from, the frequency of data collection, and how long to keep the data locally.

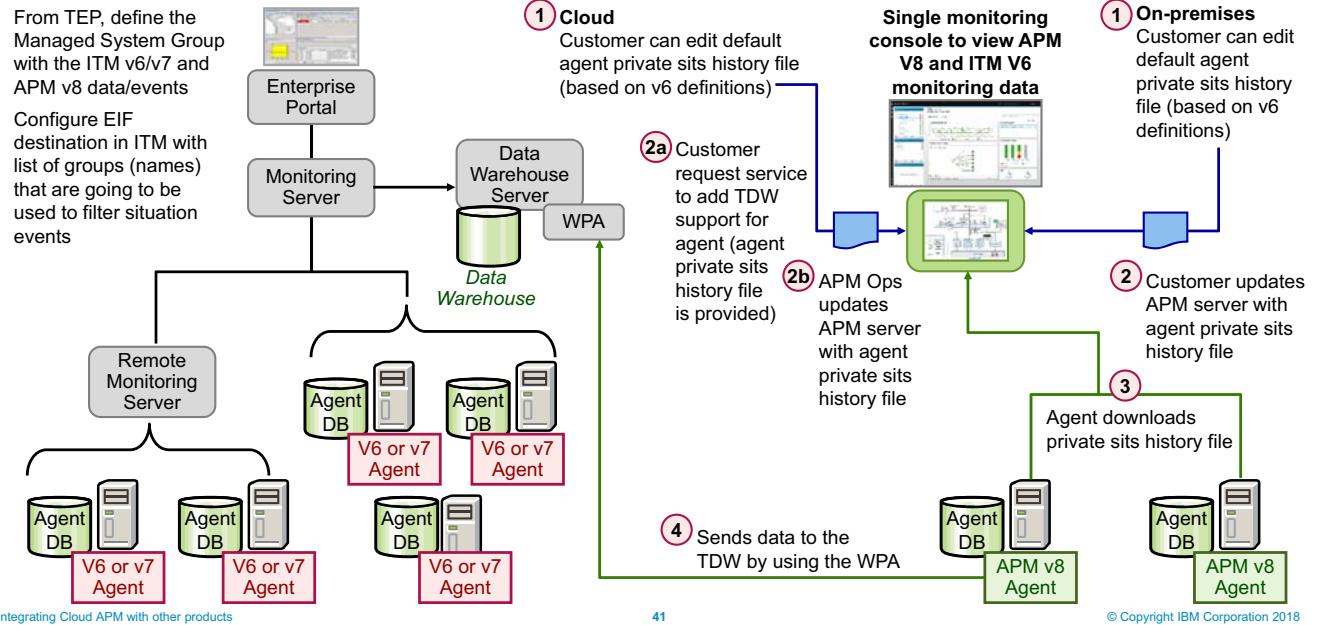
## Tivoli Common Reporting on IBM APM agent example



### Tivoli Common Reporting on IBM APM agent example

This slide shows an example report.

## Cloud APM v8 agent data flow to IBM Tivoli Monitoring V6 Tivoli Data Warehouse



Cloud APM v8 agent data flow to IBM Tivoli Monitoring V6 Tivoli Data Warehouse

This slide depicts the steps and the flow of historical data from APM agents into the Tivoli Data Warehouse.

## Configuration overview

- Cloud APM history configuration is done by agent type (for example, Linux OS, WAS, DB2)
- Requires manual product file editing
  - GUI editor is not available
- Configuration to consider:
  - Which history data sets to collect (in `pc_history.xml`)
  - WPA connection information to use (in `pc_history.xml`)
- Cloud APM server manages distribution of definitions to Cloud APM agents
- Definitions sent to all connected Cloud APM agents by type (WAS, DB2, and others)

## History configuration file contents

The history configuration file is written in XML

- Location is on the Cloud APM server and varies by product code:

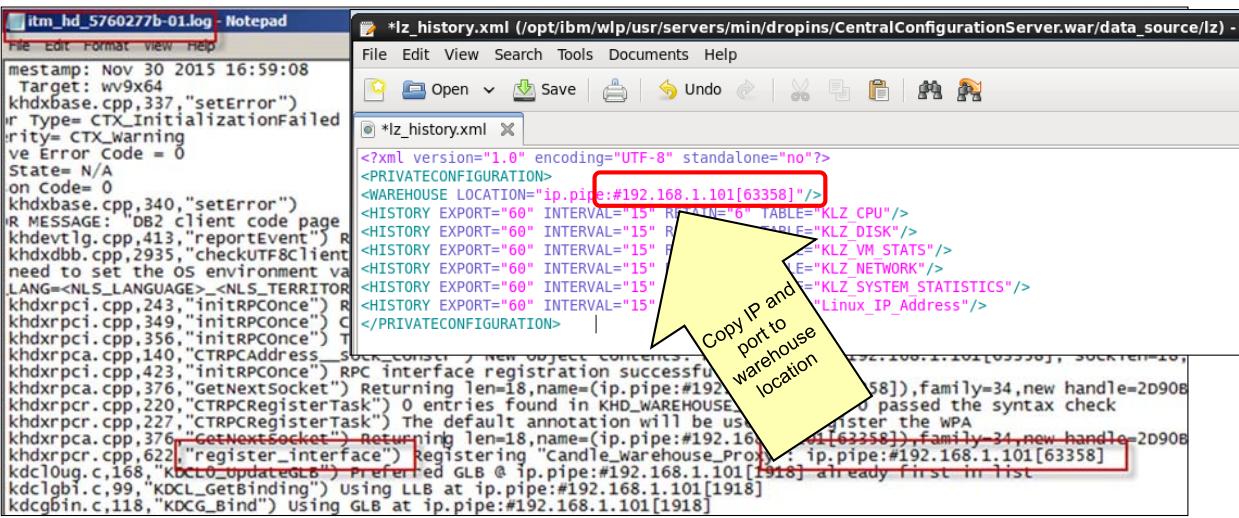
`/opt/ibm/wlp/usr/servers/min/dropins/CentralConfigurationServer.war/data_source/pc`

XML details:

- WAREHOUSE:
  - WPA contact information
  - RPC network protocol
  - Network address
  - Listening port number
- HISTORY: per table definition to start data collection
- TABLE: attribute group (data set) name from product ODI file
- EXPORT: interval (in minutes) for sending data to WPA
- INTERVAL: interval (in minutes) for data collection
- RETAIN: maximum number of hours of short-term history data that is kept at local agent

To stop collection: Remove or comment out <HISTORY> entry

## History configuration file and log file



```
itm_hd_5760277b-01.log - Notepad
File Edit Format View Help
mestamp: Nov 30 2015 16:59:08
    Target: wv9x64
khdxbase.cpp,337,"setError")
    r Type= CTX_InitializationFailed
    rity= CTX_Warning
ve Error Code = 0
State= N/A
on Code= 0
khdxbase.cpp,340,"setError")
R MESSAGE: "DB2 client code page
khdevtlg.cpp,413,"reportEvent") R
khdxdbb.cpp,2935,"checkUTF8Client
need to set the OS environment va
LANG=<NLS_LANGUAGE>_<NLS_TERRITOR
khdxrpc1.cpp,243,"initRPCOnce") R
khdxrpc1.cpp,349,"initRPCOnce") C
khdxrpc1.cpp,356,"initRPCOnce") T
khdxrpca.cpp,140,"CTRPCAddress
khdxrpca.cpp,423,"initRPCOnce") RPC
interface registration successful
khdxprcr.cpp,376,"GetNextSocket") Ret
urning len=18,name=(ip.pipe:#192.16
8.1.101[63358]),family=34,new han
dle=2D90B
khdxprcr.cpp,220,"CTRPCRegisterTask") R
entries found in KHD_WAREHOUSE
khdxprcr.cpp,227,"CTRPCRegisterTask") The default annotation will be us
ed. The annotation passed the syntax check
khdxrpca.cpp,376,"GetNextSocket") Ret
urning len=18,name=(ip.pipe:#192.16
8.1.101[63358]),family=34,new han
dle=2D90B
khdxprcr.cpp,622,"register_interface") Registering "Candle_warehouse_Proxy": ip.pipe:#192.168.1.101[63358]
kdc1oug.c,168,"KDCU_UpdatedLB") Preferred GLB @ ip.pipe:#192.168.1.101[1918] already first in list
kdc1gb1.c,99,"KDCL_GetBinding") Using LLB at ip.pipe:#192.168.1.101[1918]
kdcgbin.c,118,"KDG_Bind") Using GLB at ip.pipe:#192.168.1.101[1918]
```

\*lz\_history.xml (/opt/ibm/wlp/usr/servers/min/dropins/CentralConfigurationServer.war/data\_source/lz) -
File Edit View Search Tools Documents Help
Open Save Undo Copy IP and port to warehouse location
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<PRIVATECONFIGURATION>
<WAREHOUSE LOCATION="ip.pipe:#192.168.1.101[63358]">
<HISTORY EXPORT="60" INTERVAL="15" RETAIN="6" TABLE="KLZ\_CPU"/>
<HISTORY EXPORT="60" INTERVAL="15" RETAIN="6" TABLE="KLZ\_DISK"/>
<HISTORY EXPORT="60" INTERVAL="15" RETAIN="6" TABLE="KLZ\_VM\_STATS"/>
<HISTORY EXPORT="60" INTERVAL="15" RETAIN="6" TABLE="KLZ\_NETWORK"/>
<HISTORY EXPORT="60" INTERVAL="15" RETAIN="6" TABLE="KLZ\_SYSTEM\_STATISTICS"/>
<HISTORY EXPORT="60" INTERVAL="15" RETAIN="6" TABLE="Linux\_IP\_Address"/>

### History configuration file and log file

This slide shows a sample history configuration file and a log file that shows the location of the warehouse proxy server IP address and port number. These values are used in the history configuration file to identify the target warehouse proxy.

# Lesson 3 Integrate Netcool/OMNIBUS

IBM Training



## Lesson 3: Integrate Netcool/OMNIBUS

### Integration agent for Netcool/OMNIBUS

- This agent enables the forwarding of alerts, generated in Cloud APM on Cloud, to the customer's on-premises OMNIBUS, providing one method for doing event management
- Configuration is from **Advanced Configuration > Event Manager**:
  - EIF port
  - EIF event targets

The screenshot shows the 'Advanced Configuration' interface with the 'Event Manager' category selected. The 'Parameters' section contains the following configuration:

| Parameter             | Value        |
|-----------------------|--------------|
| Event Cache Time      | 60           |
| Pure Event Close Time | 24           |
| Master Reset Event    | True         |
| EIF Port              | 9998         |
| EIF Event Target(s)   | lin3.ibm.edu |

In this lesson, you learn how to integrate with Netcool/OMNIBUS.

Customers use this feature to integrate their Cloud APM alerts with their on-premises alerts, providing one method for event management. This agent takes alerts that are generated in Cloud APM and forwards them over the internet to the customer's on-premises OMNIBUS. A customer's Cloud-monitored business applications have the same alerting capability as legacy applications.

On-premises OMNIBUS becomes a single alert management system for the Enterprise and Cloud.

## Events in the Application Performance Manager user interface

After you install the integration agent, you can see the events both in the APM console and the OMNIBUS Event console

This screen capture shows how they look in the APM console

The screenshot shows the 'My Components' tab selected in the APM console. At the top, there's a summary bar with three colored segments: red (Critical), yellow (Warning), and green (Normal). Below this, a table lists seven events with their details:

| Threshold Name                 | Status | Severity | Display Item         | Source                      | Timestamp                | Description                            |
|--------------------------------|--------|----------|----------------------|-----------------------------|--------------------------|--|
| NT_Services_Automatic_Start    | Open   | Critical | DB2 - DB2COPY1 - DB2 | Primary:ITM:NT              | Jun 16, 2016, 7:51:21 PM | Opens an event when a service ...      |
| UDB_DB_Status_Crit             | Open   | Critical | TRADEDB              | db2inst1:lin1:UD            | Jun 16, 2016, 7:39:27 PM | The database state is not active.      |
| UDB_Pip_Sort_Hit_Rat_Pct_Crt_2 | Open   | Critical | db2inst1             | db2inst1:lin1:UD            | Jun 16, 2016, 7:24:36 PM | The percentage in the piped so...      |
| APM_Agent_Offline              | Open   | Warning  |                      | lin1Node01server1:lin1:KYNS | Jun 16, 2016, 8:18:16 PM | IBM APM: Agent lin1Node01ser...        |
| Svr_Err_Rate_High              | Open   | Warning  | lin1.ibm.edu         | HU:lin1_httpd:HUS           | Jun 16, 2016, 8:15:10 PM | Server internal failure rate in the... |
| Linux_BP_CpuWaitIOPct_Warning  | Open   | Warning  | -1                   | lin1:LZ                     | Jun 16, 2016, 8:12:11 PM | Monitors CPU I/O Waits                 |
| NT_Logical_Disk_Space_Warning  | Open   | Warning  | C:                   | Primary:ITM:NT              | Jun 16, 2016, 7:21:17 PM | Opens an event when the unallo...      |

## Events in the Application Performance Manager user interface

In the Cloud APM UI, events show up in several places. A consolidated view of all your events can be seen in the My Components Event Status tab.

## Events in Netcool/OMNibus

This screen capture shows how the events look in Netcool/OMNibus

The screenshot shows the IBM Event Viewer interface. The title bar reads "IBM Dashboard Appli... x". The address bar shows the URL "https://lin3.ibm.edu:16311/ibm/console/navigation.do?XSS=OCs4myDMyhmmi1Rj3QnWOU&wpageid=com.ibm.is". The main window is titled "Event Viewer" and has a "Default" dropdown menu. Below the menu, there are several status indicators: 7 errors (red), 0 warnings (yellow), 1 alert (orange), 25 ITM problems (blue), 1168 database errors (green), and 11 information messages (grey). The main table lists 14 rows of event data:

| Sev | Ack | Node             | Alert Group          | Summary  | Last Occurrence    | Count | Type        | ExpireTime |
|-----|-----|------------------|----------------------|--|--------------------|-------|-------------|------------|
| ✖   | No  | lin3             | TopNodes             | ALERT: last 5 mins: high number of events sent by: lin3: 1634                    | 6/16/16 8:24:20 PM | 1     | Problem     | 86,430     |
| ✖   | No  | lin3.ibm.edu     | ProbeStatus          | ALERT: syslog Probe (Conn ID: 2): sent high number of events: 1637               | 6/16/16 8:24:20 PM | 1     | Problem     | 86,430     |
| ✖   | No  | db2inst1:lin1:UD | ITM_KUD_DB2_Database | UDB_DB_Status_Crit[dbase_status != Active ]                                      | 6/16/16 8:22:36 PM | 1     | ITM Problem | Not Set    |
| ✖   | No  | db2inst1:lin1:UD | ITM_KUD_DB2_Database | UDB_DB_Status_Crit[dbase_status != Active ]                                      | 6/16/16 8:22:36 PM | 2     | ITM Problem | Not Set    |
| ✖   | No  | lin3.ibm.edu     | TopClasses           | ALERT: last 5 mins: high number of events for class: Syslog Probe (200): 1343    | 6/16/16 8:24:20 PM | 1     | Problem     | 86,430     |
| ✖   | No  | Primary:ITM:NT   | ITM_NT_Services      | NT_Services_Automatic_Start[Start_Type = Automatic AND Current_State = Stopped ] | 6/16/16 8:22:36 PM | 1     | ITM Problem | Not Set    |
| ✖   | No  | db2inst1:lin1:UD | ITM_KUD_DB2_Database | UDB_DB_BP_Hit_Ratio_Low_2[pool_hit_ratio <= 50.00 AND dbase_status != InActive ] | 6/16/16 8:22:36 PM | 14    | ITM Problem | Not Set    |
| ⚠   | No  | lin3.ibm.edu     | DBStatus             | ALERT: last 5 mins alerts.status inserts/deduplications are high: 960530         | 6/16/16 8:19:25 PM | 1     | Problem     | 86,430     |
| ⚠   | No  | lin1:LZ          | ITM_KLZ_CPU          | Linux_BP_CpuWaitOPct_Warning[Wait_IO_CPU > 10.00 AND CPU_ID = -1 ]               | 6/16/16 8:22:36 PM | 7     | ITM Problem | Not Set    |
| ⚠   | No  | lin3.ibm.edu     | DBStatus             | Last 5 mins alerts.journal (inserts): 0  | 6/16/16 8:29:20 PM | 3     | Information | 330        |

### Events in Netcool/OMNibus

Netcool/OMNibus event viewer shows that the on-premises events are pulled down from the APM environment.

Some of the same situations are shown on the prior slide.

# Lesson 4 Integrate IBM Cloud

IBM Training



## Lesson 4: Integrate IBM Cloud

- IBM Cloud was formerly known as Bluemix
- No longer uses the Monitoring and Analytics Service
- A data collector package with all four data collectors is provided:
  - Node JS
  - Ruby
  - Python
  - Liberty
- Update your application with the appropriate data collector and push the application into IBM Cloud

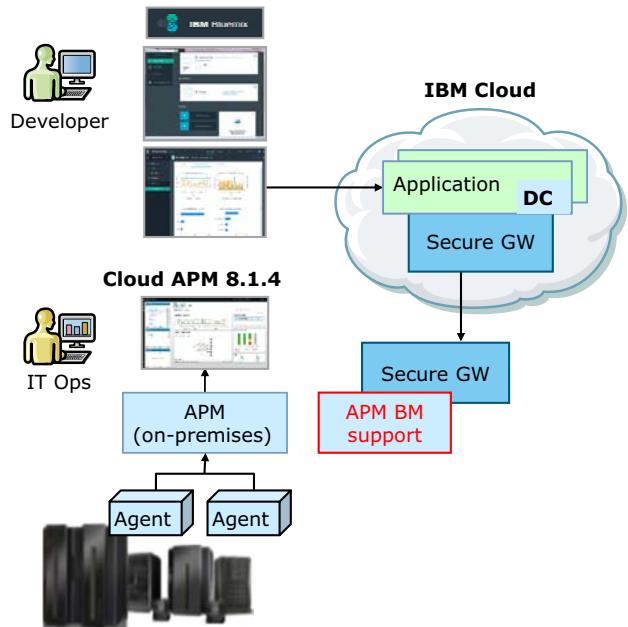
In this lesson, you learn how to integrate with IBM Cloud.

You can view monitoring information for your applications within the IBM Cloud environment by using Cloud APM data collectors.

The Cloud APM data collectors enable the integration of monitoring capabilities with IBM Cloud by transferring resource monitoring and diagnostics data about your IBM Cloud applications to the Cloud APM server. The Cloud APM server receives and processes monitoring information that is collected in the data collectors.

## Hybrid application monitoring: IBM Cloud to IBM Cloud APM Private integration

- Enable the monitoring of the IBM Cloud application to be fed into the private Cloud APM server
  - Data that is fed by using the IBM Secure Gateway
- Integrates Monitoring and deep-dive data
  - Availability Monitoring and Log Analysis are not integrated



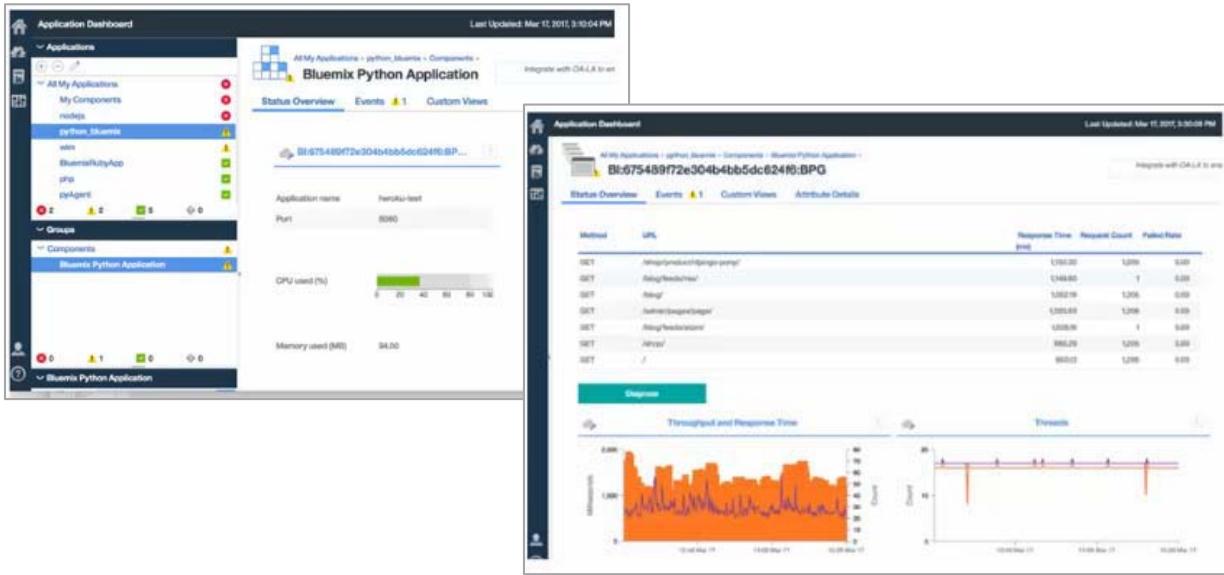
### Hybrid application monitoring: IBM Cloud to IBM Cloud APM Private integration

The Hybrid feature allows an IBM Cloud application with a lightweight data collector to send its data to an APM server. It provides only resource and deep-dive data, not availability or log.

Eventing is provided by situations in the APM server.

Data is passed from the IBM Cloud application to the APM server by using the Secure Gateway service that provides an encrypted tunnel, which allows data to reach it through firewalls.

## IBM Cloud Python Application (1 of 2)



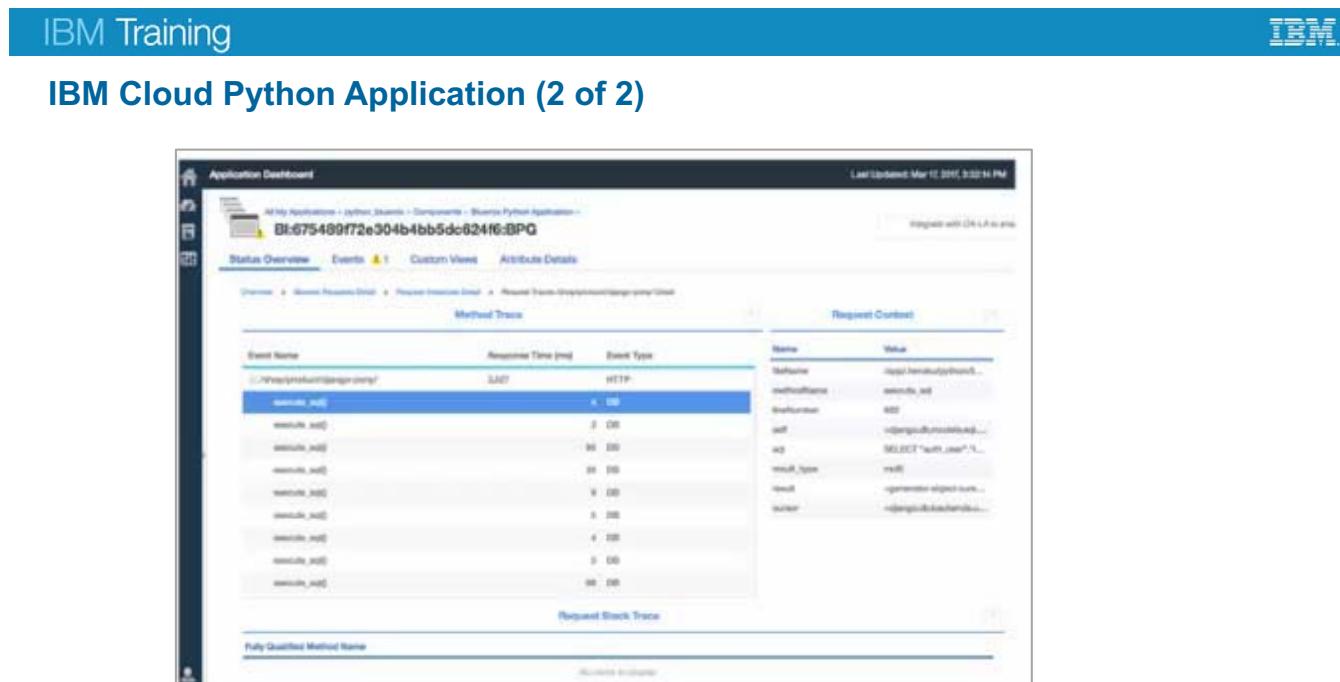
Integrating Cloud APM with other products

50

© Copyright IBM Corporation 2018

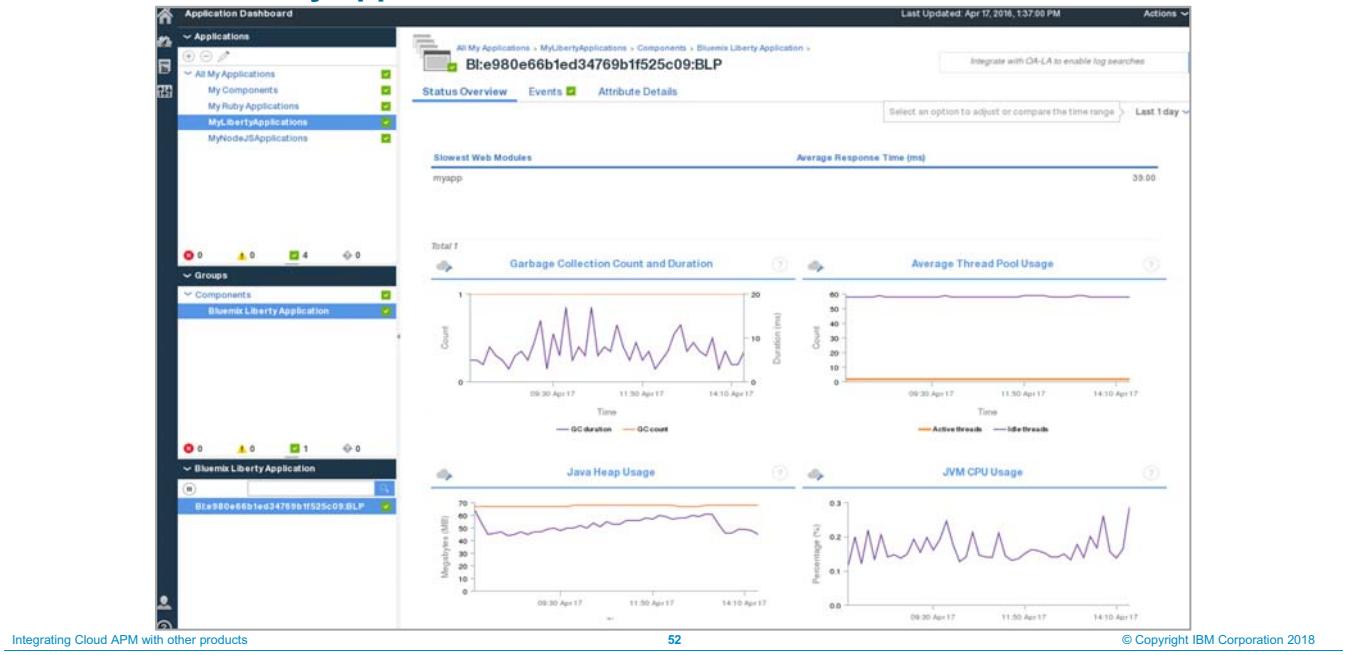
### IBM Cloud Python Application (1 of 2)

This slide shows examples of the IBM Cloud Python Data Collector application that are passed to Cloud APM.



This slide shows examples of the IBM Cloud Python Data Collector application that are passed to Cloud APM.

## IBM Cloud Liberty application



*IBM Cloud Liberty application*

This slide shows the IBM Cloud data from a Liberty application that is shown in a Cloud APM console.

# Lesson 5 Integrate IBM Cloud Private

IBM Training



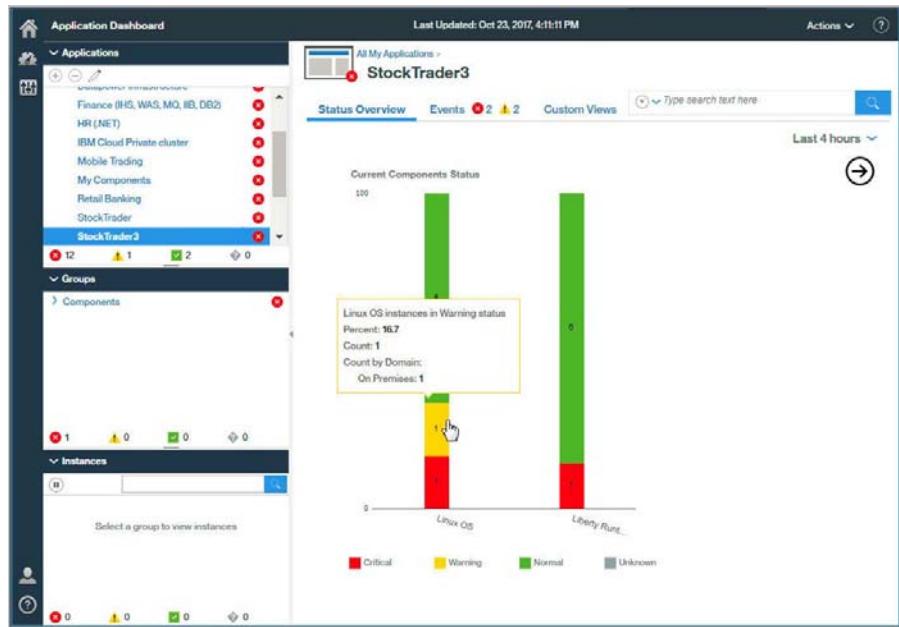
## Lesson 5: Integrate IBM Cloud Private

- Monitors IBM Cloud Private containers
  - IBM Cloud Private uses Kubernetes and Docker containers, and you can monitor these containers with the Monitoring Agent for Linux OS
- Monitors IBM Cloud Private applications
  - Use IBM Cloud Application Performance Management, Private to monitor your IBM Cloud Private Liberty-based applications

This lesson is about monitoring IBM Cloud Private environments.

## IBM Cloud Private container monitoring example

- This example presents the StockTrader application that was created for monitoring the Cloud APM container
- You can investigate the status in the container just like any other Cloud APM agent

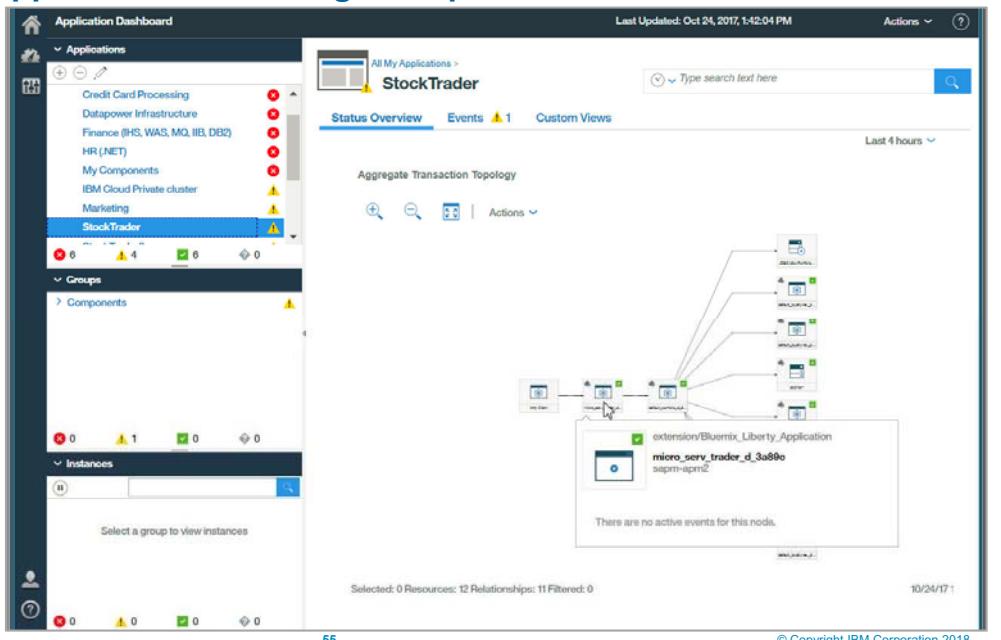


### IBM Cloud Private container monitoring example

Each stacked bar represents the managed resources of the same type, and each segment shows the number of nodes with the same status. When you hover the mouse over a bar segment, the status details open.

## IBM Cloud Private application monitoring example

- The examples in this screen present the StockTrader application that was created for monitoring the Cloud Private Liberty-based applications
- You can investigate the data in the application just like any other Cloud APM data collector



### IBM Cloud Private application monitoring example

The application-level dashboard shows the Aggregate Transaction Topology view. Hover your mouse over a node to see more details.

## Monitoring IBM Cloud Private containers

The setup involves some basic steps:

- Install the Linux OS agent on your Cloud Private nodes
  - You install the Cloud APM Linux OS agent on both the Cloud Private master and worker nodes
  - As a good practice, include the installed Linux OS agent for each virtual machine that is created for IBM Cloud Private
- Create an application to group the OS resources
  - To manage the nodes that comprise the Cloud Private container, create an application to group them
  - Start the Cloud APM console and create an application with the Linux OS-managed resources that you installed in your Cloud Private environment
- Start monitoring your Cloud Private container
  - Now you are ready to use the Cloud APM console for monitoring your Linux OS container
  - Look at the dashboards for the application that you created

## Monitoring IBM Cloud Private applications

The setup involves some basic steps:

- Configure the Liberty data collector to connect to the Cloud APM server
  - When you set up a Microservice Builder pipeline and push a Liberty application into Cloud Private, the Liberty data collector is automatically installed
  - The data collector is initially in a disabled state and gets activated after it discovers the Cloud APM server information
  - You use the Kubernetes Secrets to provide the server information
  - You can also deploy the Liberty data collector into Cloud Private without using Microservice Builder
- Add an application for managing your Cloud Private applications
  - To manage your Liberty-based applications, group them by adding an application in the Application Performance Dashboard to group them
  - Start the Cloud APM console and create an application with the Liberty-managed resources that you configured in your Cloud Private environment
- Start monitoring your Cloud Private applications
  - Now you're ready to use the Cloud APM console for monitoring your Liberty-based microservice applications

Use IBM Cloud Application Performance Management, Private to monitor your IBM Cloud Private Liberty-based applications.

# Lesson 6 Monitor IBM API Connect

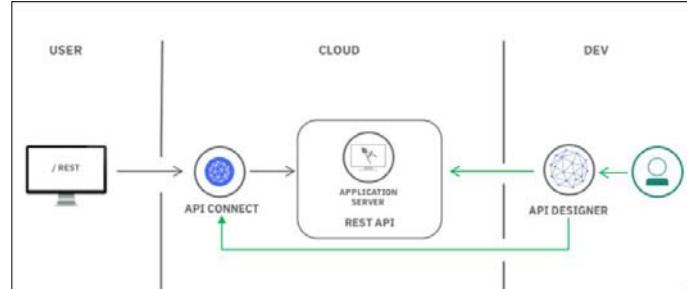
IBM Training



## Lesson 6: Monitor IBM API Connect

### API Connect overview

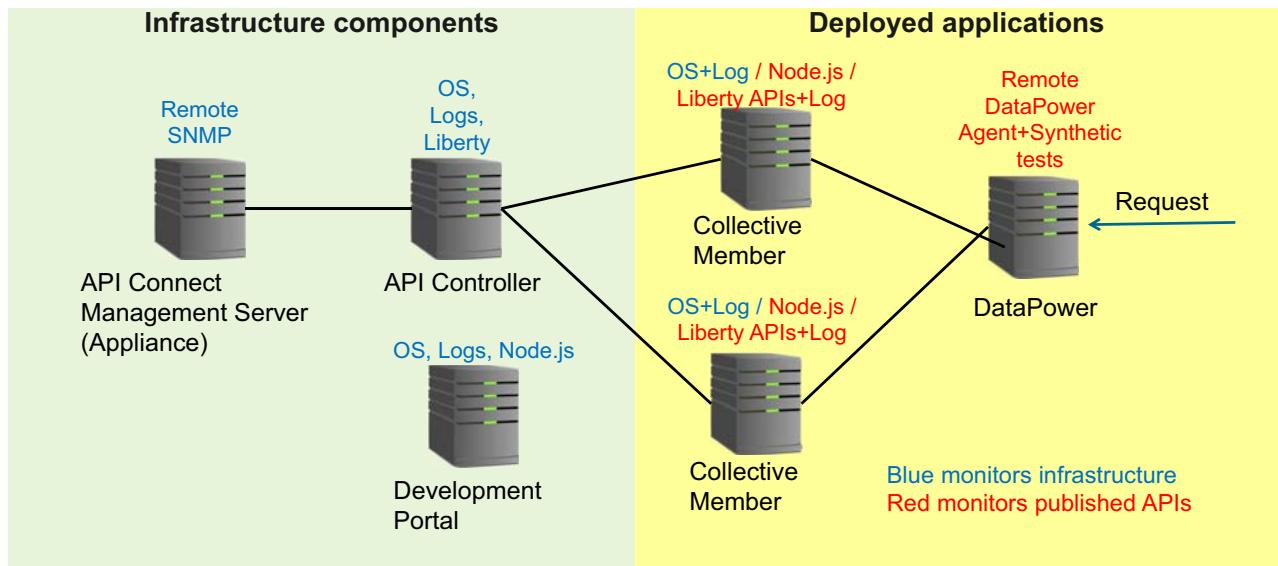
- IBM API Connect is a modern API management solution for creating, running, managing, and securing APIs for external and internal consumers
  - These consumers use it to accelerate an organization's API program and capture new revenue through compelling new customer experiences
- Benefits of API Connect:
  - Automated creation of new APIs in minutes
  - Securely exposing enterprise services by using APIs to new mobile, IoT, and web applications
  - Attract developers through API socialization with built-in enterprise governance
  - Gain insights into which APIs are having the largest impact on an organization's API program
  - Capture new revenue sources through monetization of an organization's API program



This lesson is about monitoring IBM API Connect.

IBM API Connect is a complete API lifecycle management solution that makes things easier for developers, Central IT, and LoB Management. The thought behind API Connect is that APIs are small data applications, often called microservices, but they are applications nonetheless.

## Monitoring API Connect (1 of 2)



This figure shows the different tools that you can use to monitor API Connect.

## Monitoring API Connect (2 of 2)

Each of the key API Connect components can be monitored in the following ways:

- Management Server: Remotely monitored by using an SNMP-based agent to gather CPU, Memory, Network, and Disk data
- Controller:
  - Monitor the operating system and logs by using OS Agent
  - Monitor WebSphere Liberty by using the WebSphere Agent
- Collective Members:
  - Monitor the operating system and logs by using OS Agent
  - Monitor each of the published applications with the lightweight Node.js data collector
  - Monitor Response Time data for HTTP/HTTPS requests
- DataPower Gateway:
  - Remotely monitor with the DataPower Agent and transforms that were enhanced for APIC
- Developer Portal:
  - Monitor the operating system and logs by using OS Agent
  - Monitor the server with the Node.js Agent
- Execute Synthetic tests against the published APIs
- In addition, if the APIs are connected to other business application components, those components can also be monitored by using various monitoring agents, including (App Servers, databases, IBM MQ, IIB, and more)

### Monitoring API Connect (2 of 2)

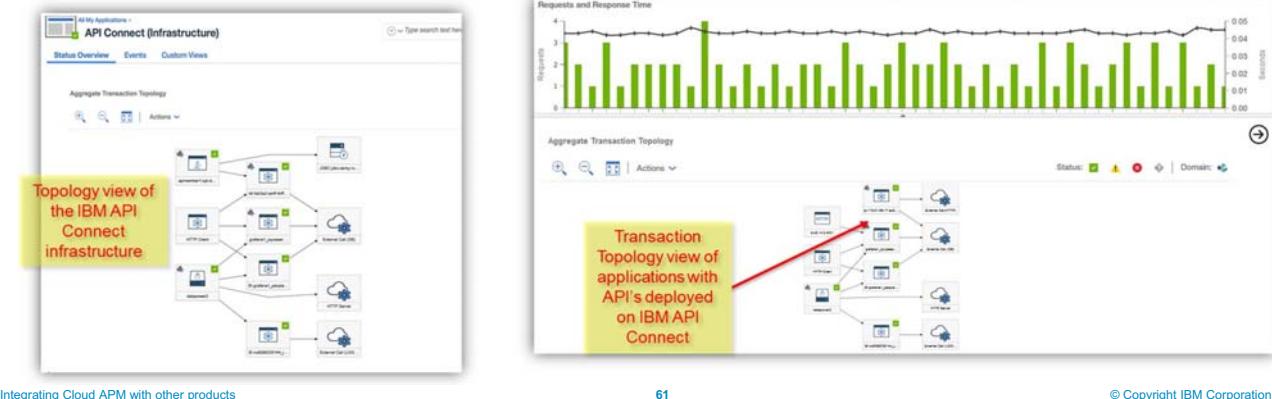
The API Connect on-premises Cloud includes the following server types:

- **Management server:** Stores all of the Cloud configuration, and controls communication between the other servers within API Connect. Manages the operations of the various servers in the API Connect Cloud and provides the tools to interface with the various servers. The Management server also provides analytic functions that collect and store information about APIs and API users. The Cloud Manager and API Manager user interfaces are run on the Management server.
- **Collective Controller:** The collective members are managed through a collective controller, which is a (WebSphere Application Server) Liberty Network Deployment JavaServer that maintains the state of the collective.
- **Collective Member:** A collective member is the runtime for a deployed application.
- **DataPower Gateway:** The DataPower Gateway is an enterprise API Gateway that is built for departments and cross-enterprise usage.
- **Developer Portal Server:** Provides a customizable social developer portal with a full-featured content management system, and includes clustering capability. API providers can use it to build portals for their application developers. It provides the interface for application developers to discover APIs and subscribe to usage plans that are contained in the published products for use in their applications.

You can deploy the Synthetic Playback agent and create synthetic transactions and events to monitor the availability and performance of your internal and external applications.

## IBM APM manages your IBM API Connect environment (1 of 2)

- IBM APM helps ensure the **availability of your IBM API Connect environment** by monitoring all the components that make up the IBM API Connect infrastructure – web servers, management servers, developer portal appliance, database servers
- IBM APM manages the **performance of your applications that are deployed on IBM API Connect** to identify performance bottlenecks that are associated with your APIs before they affect users



### IBM APM manages your IBM API Connect environment (1 of 2)

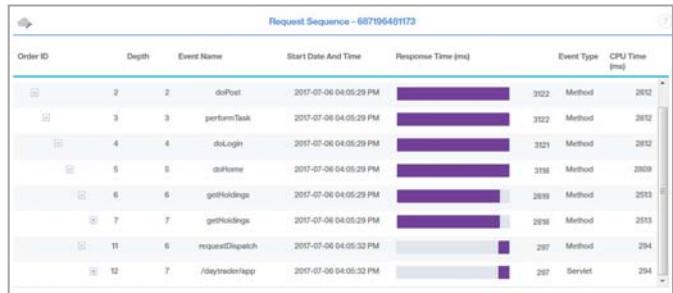
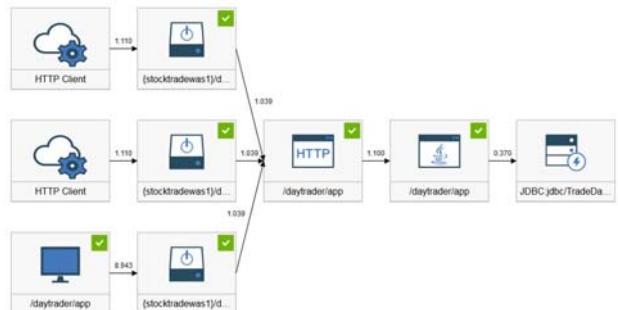
Cloud APM helps ensure the availability of your IBM API Connect environment by monitoring all the components that make up the IBM API Connect infrastructure: web servers, management servers, developer portal appliance, and database servers.

Cloud APM manages the performance of your applications that are deployed on IBM API Connect to identify performance bottlenecks that are associated with your APIs before they affect users.

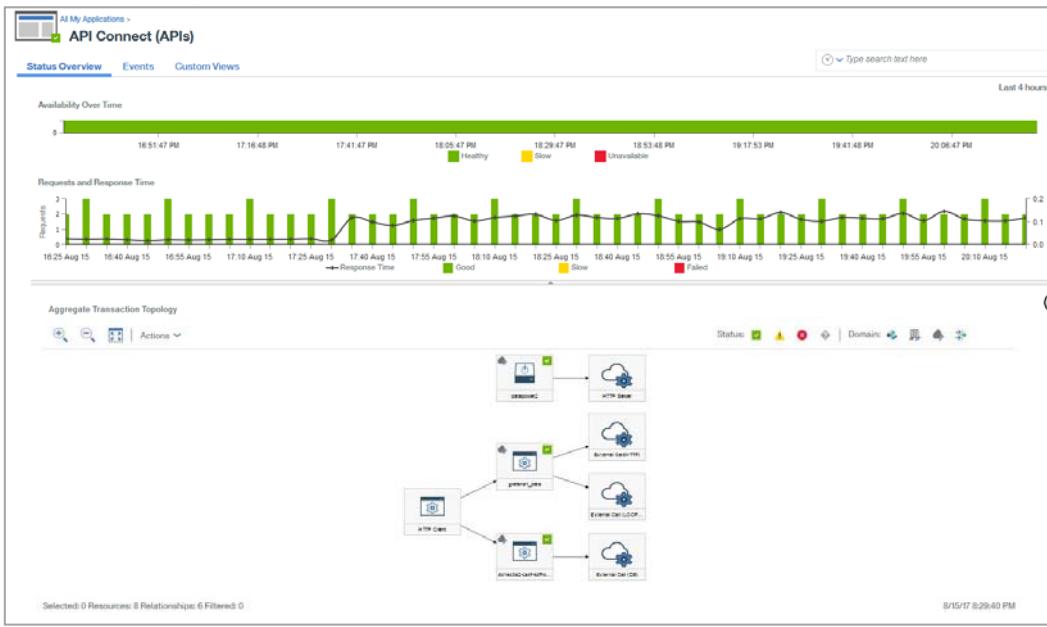
No supported agent for API Connect is available to be installed with Cloud APM currently. Rather, Cloud APM supplies you with the infrastructure to manage your API Connect environment through existing and enhanced features in Cloud APM.

## IBM APM manages your IBM API Connect environment (2 of 2)

- Monitoring provides key capabilities for monitoring the performance and health of the APIC environment, including:
  - Detailed monitoring of the operating system
  - Detailed monitoring of the middleware components
  - Monitoring of the OS and middleware logs
  - Tracking transactions as they flow through APIC and the business application
  - Deep-dive diagnostics to understand where the bottlenecks are within the app server (including stack trace data)



## API Connect (APIs)



Integrating Cloud APM with other products

63

© Copyright IBM Corporation 2018

### API Connect (APIs)

This image shows a typical API Connect application that is instrumented to monitor the status of the API connect infrastructure and applications.

The topology is discovered automatically through Cloud APM.

## API Connect: Response Time details



### API Connect: Response Time details

APM supports drill-down into End User Transactions. This feature is useful to monitor API Connect.

## API Connect: Transaction Availability Over Time



### API Connect: Transaction Availability Over Time

You can monitor transaction availability over time in your API Connect environment.

## API Connect: Node.js stack trace

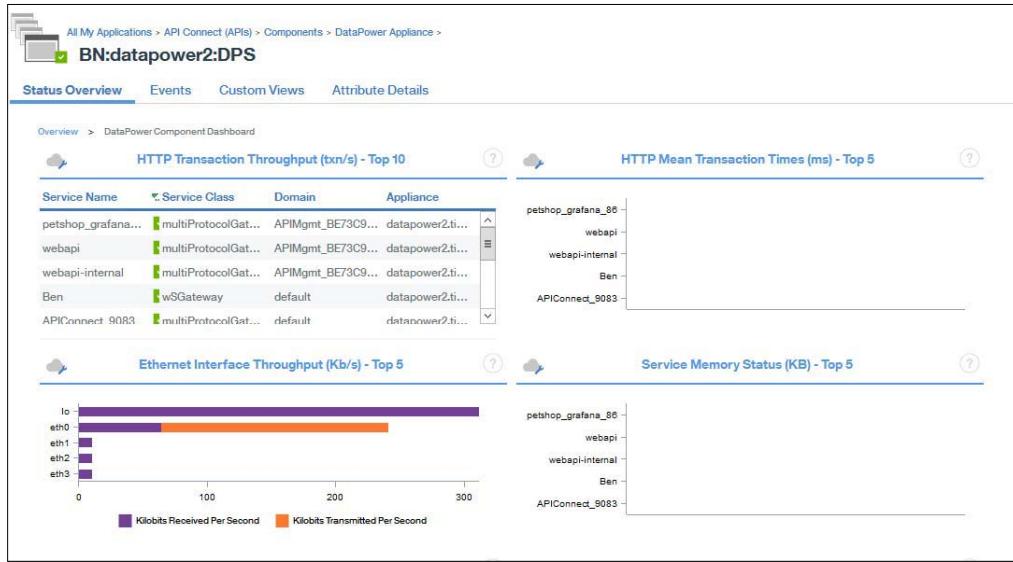
The screenshot shows the 'Method Trace' section of the API Connect interface. It displays a tree view of events and their response times. The top event is '/api/pets/' with a response time of 20,004 ms and type HTTP. Below it are several 'query' events, each with a response time of 0 ms and type UNKNOWN. The 'Request Context' table shows a single entry for 'loopbackDJProbe'. At the bottom, the 'Request Stack Trace' section shows the fully qualified method name: <module>.<root>(2009:...ode\_modules/loopback-datasource-juggler/lib/dao.js) <module>.<root>(396:...datasource-juggler/node\_modules/async/lib/async.js).

| Event Name | Response Time (ms) | Event Type | Name            | Value |
|------------|--------------------|------------|-----------------|-------|
| /api/pets/ | 20,004             | HTTP       | loopbackDJProbe |       |
| query      | 0                  | UNKNOWN    |                 |       |
| query      | 0                  | UNKNOWN    |                 |       |
| query      | 0                  | UNKNOWN    |                 |       |
| query      | 0                  | UNKNOWN    |                 |       |
| query      | 0                  | UNKNOWN    |                 |       |
| query      | 0                  | UNKNOWN    |                 |       |
| query      | 0                  | UNKNOWN    |                 |       |

*API Connect: Node.js stack trace*

You can drill down into the stack and method traces for your API Connect applications.

## API Connect: DataPower Appliance



### API Connect: DataPower Appliance

You can drill down into the DataPower appliance to support API Connect monitoring.

# Lesson 7 Populate Dashboard Application Services Hub with Cloud APM data

IBM Training



## Lesson 7: Populate Dashboard Application Services Hub with Cloud APM data

- The Dashboard Application Services Hub integrates with IBM Cloud APM
- IBM Dashboard Application Services Hub provides a single console for administering IBM products and related applications
- Dashboard Application Services Hub is the user interface for Jazz for Service Management
- You can integrate these products, for example:
  - Cloud APM with DASH to view monitoring agent data
  - Netcool/Impact with DASH to view the Netcool/Impact GUI
  - Netcool/OMNibus with DASH to view the OMNibus alerts
- The IBM Dashboard Application Services Hub provides a set of features to customize the console and build custom dashboards
- Pages are created that contain widgets, which are used to build charts, gauges, and tables that contain monitoring data

In this lesson, you learn how to use IBM Cloud APM agent data with Dashboard Application Services Hub.

You use the Dashboard Application Services Hub to create pages of customized IBM Cloud APM agent data.

## Custom dashboards in DASH with IBM Cloud APM agent data

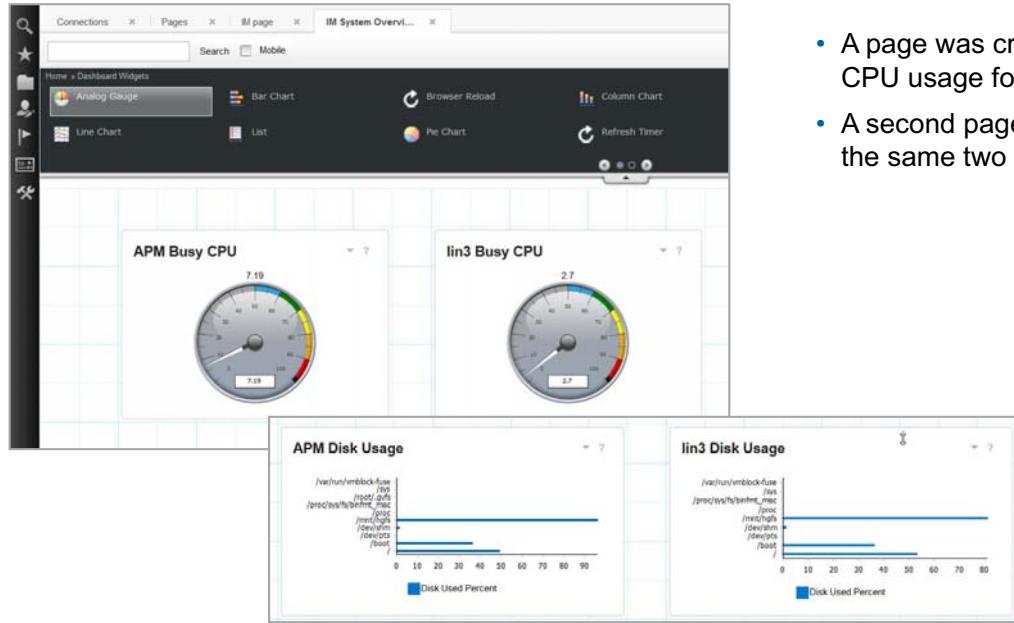
- You can query IBM Cloud APM agent data from the Dashboard Application Services Hub (DASH)  
DASH is the Jazz for Service Management user interface
- Follow these steps to prepare to configure DASH:
  - The IBM Cloud APM to DASH connection is done in a similar fashion as the IBM Tivoli Monitoring to DASH connection
  - The Cloud APM dashboard data provider must be up and running before creating the connection
  - To determine whether the Cloud APM dashboard data provider is available, point the web browser on the DASH server to the data provider URL to make sure that it works correctly
- After configuring DASH to connect to the Cloud APM data provider in your environment, you can retrieve data from your Cloud APM agents for presentation in DASH custom dashboards

### *Custom dashboards in DASH with IBM Cloud APM agent data*

With the release of IBM Tivoli Monitoring 6.3, IBM Cloud APM 8.1.4, and the IBM Dashboard Application Services Hub 3.1.0.0 (DASH), administrative users can create customized performance monitoring dashboard pages.

Custom monitoring dashboards are available through DASH for users to create their own pages, charts, and tables from the Tivoli Widget Library (TWL).

## Creating widgets on a dashboard page to see monitoring information



- A page was created showing busy CPU usage for two servers
- A second page shows disk usage for the same two servers

*Creating widgets on a dashboard page to see monitoring information*

This slide shows parts of two dashboard pages that are created to show data from IBM Cloud APM agents. The gauge widgets are used with the KLZ\_CPU data set to show CPU usage on two servers. The bar chart widgets use the KLZ\_Disk data set and show the disk usage by mount point for the same two servers.

## Connector from the Jazz server to the data provider server

- Add a connection for the server where the Application Performance Manager data provider is running
- KD8 is the name of the connection, and the status must be Working

| Connections  |                            |   |            |                     |                  |
|--|----------------------------|---|------------|---------------------|------------------|
| The connection manager allows you to configure the local and remote connections for this computer. The list below displays all configurable connections. |                            |   |            |                     |                  |
| Name   | Type                       | Description                                 | Connection | ID                  | Status           |
| KD8  | IBMPeformanceManagementSDP | IBM Performance Management dashboard        | Remote     | itm.KD8.apm.ibm.edu | Working          |
| Tivoli Directory Inte  | TDI                        | TDI Generic Data Provider (1.0.26)          | Local      | TDI                 | No data returned |
| tip  | tip                        | Tivoli Integrated Portal Data Provider      | Static     | tip                 | Working          |
| Netcool/OMNibus  | OMNibusWebGUI              | Navigational data model for Netcool/OMNIbus | Static     | OMNibusWebGUI       | Working          |

### Connector from the Jazz server to the data provider server

From the Cloud APM console, clicking the gear icon opens the console settings. By clicking Connections, you create a new connection. For the new connection, these items of information are required:

- Protocol
- Host name
- Port (matching the port that is specified when verifying the Cloud APM Data Provider)
- User name and password to use on the data provider server.

After searching for this item, the name KD8 is selected for the connection. The example on the slide shows the KD8 connection, which is created for IBM Cloud APM.

## Instructor demonstration



## Student exercises



Complete all the exercises for this unit in the Course Exercises Guide.

## Summary

Now that you have completed this unit, you should be able to:

- Describe how Cloud APM can integrate with other products
- Integrate IBM Tivoli Monitoring
- Integrate Netcool/OMNIbus
- Integrate IBM Cloud and IBM Cloud Private
- Monitor API Connect
- Populate Dashboard Application Services Hub with Cloud APM agent data



# **Unit 12 Reporting and 7-day comparison**

IBM Training



## **Reporting and 7-day comparison**

© Copyright IBM Corporation 2018  
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this unit, you display 7-day comparison reports and learn how to install and run Tivoli Common Reporting reports.

## Learning objectives

After completing this unit, you should be able to:

- Produce a historical 7-day comparison
- Install and run reports

## Unit outline

- Lesson 1: Introduction to historical 7-day comparison
- Lesson 2: Reporting using Tivoli Common Reporting

# Lesson 1 Introduction to historical 7-day comparison

IBM Training



## Lesson 1: Introduction to historical 7-day comparison

- Historical 7-day comparison compares the time range that is displayed in a line chart with the metrics from a different day, up to one week ago
- The change affects all the dashboards in the current application or all applications
- Unavailable comparison data is indicated with a watermark on the chart: No Comparison Available
- Any widgets for which no historical data is collected continue to show the most recent values
- Time range is always based on current time range displayed
- If a legend does not exist in the original chart, the comparison does not add a legend

In this lesson, you learn how to run 7-day historical comparison reports.

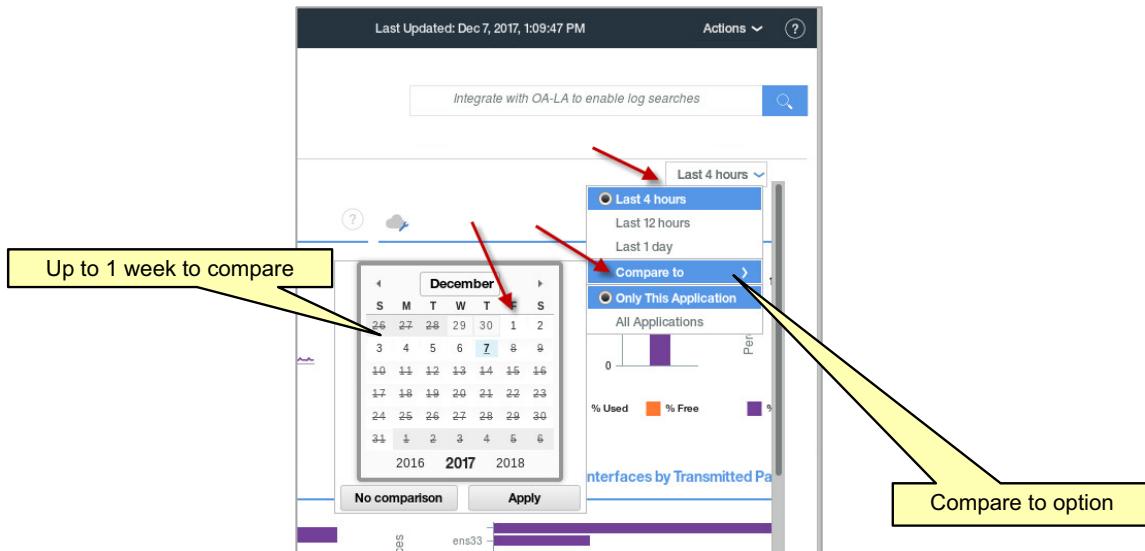
Historical 7-day comparison compares the time range that is displayed in a line chart with the metrics from a different day, up to one week ago. These reports are available with both SaaS and on-premises systems.

A drop-down menu provides historical 7-day comparison options. The period for the comparison can be selected from the last 4 hours, last 12 hours, or last 1 day. A “Compare to” choice applies to the current page. For the Compare to options, the choices are from yesterday to last week.

When you make historical 7-day comparison choices, the choices affect all of the dashboards in the current application. Only the charts in the page that is viewed are affected. Two distinct lines represent the performance of the current period with a previous day’s performance during that same period. Data comparisons can be made from the previous day up to the previous week.

If the data is not available for comparison, a watermark within the graph indicates that.

## Historical 7-day comparison example of making compare selections



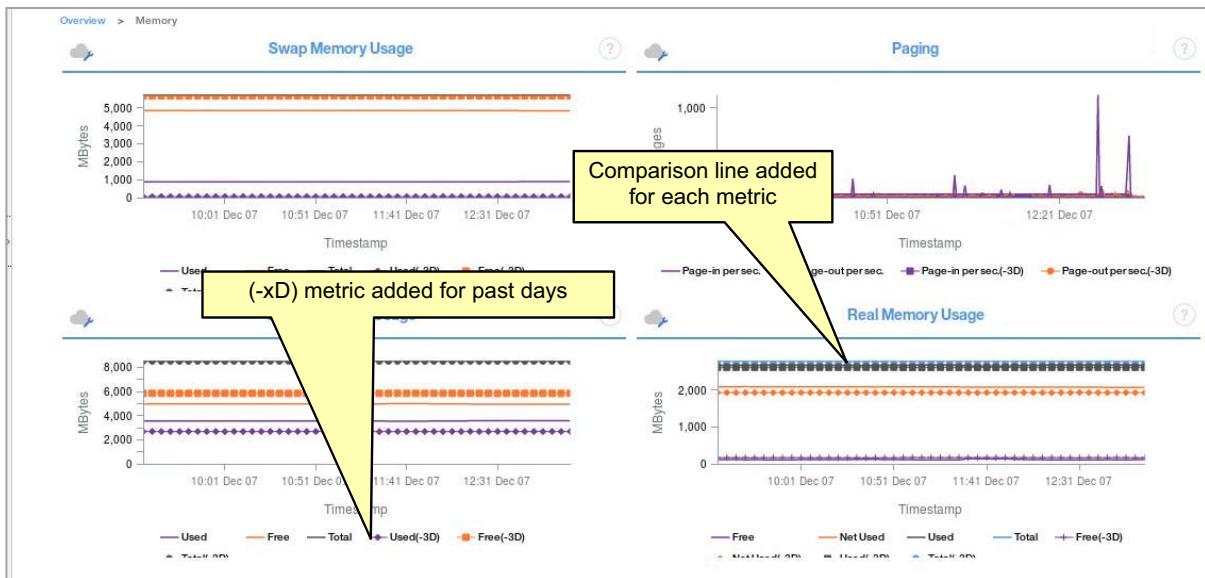
### Historical 7-day comparison example of making compare selections

The screen capture is an example of reporting memory and paging use from the **Status Overview** tab and the **Overview > Memory** selection.

The Status Overview tab has a drop-down menu. With this menu, you select reports for the last 4 hours, last 12 hours, last 1 day, a toggle for Only This Application or All Applications, and a new Compare to option.

When you select Compare to, another drop-down window opens. Here you choose the 7-day selections, where one selection is available for each day of the previous week. You can also select No comparison, which avoids comparing with any previous day.

## Historical 7-day comparison example with memory

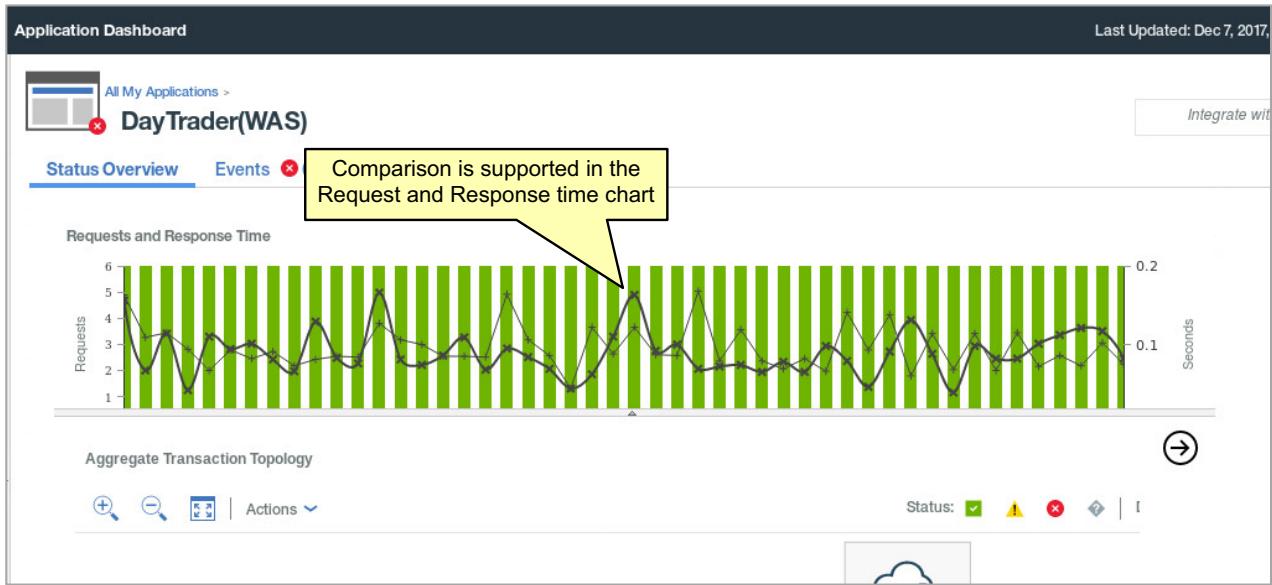


### Historical 7-day comparison example with memory

This example shows the historical comparison of data from a Linux operating system agent in the Status Overview. The historical comparison is made selecting the Last 4 hours and 3 Days ago.

All of these graphs have two plots. The solid line plots represent the data from today. The plot lines with a block character also represent the data from three days ago at the same time of day. You can tell the difference in the legend by looking for the -3D or minus three days, which represents the value that was selected.

## Historical 7-day comparison example with an application



Reporting and 7-day comparison

7

© Copyright IBM Corporation 2018

### Historical 7-day comparison example with an application

The two charts on this slide represent the Requests and Response Time, Event Severity Summary, and Current Components Status of an application. The Requests and Response Time plot has two distinct plot lines.

Historical comparison is not available for the Event Severity Summary and Current Components Status bar charts.

# Lesson 2 Reporting by using Tivoli Common Reporting

IBM Training



## Lesson 2: Reporting using Tivoli Common Reporting

- Cloud APM reports are available for data that is collected by using these methods:
  - The Response Time Monitoring Agent (Transaction Tracking must be enabled)
  - The Monitoring Agent for WebSphere Applications
  - Synthetic transaction monitoring
- Cloud APM reports are installed and run on Tivoli Common Reporting server only
- For Response Time Monitoring Agent reports
  - In the APM console menu, click **Reporting > Work with Reports**
  - The Cognos Connections home page opens
- Response Time Monitoring Agent reports
  - All My Applications
  - Application Performance and Usage
  - Compare Application Performance over Two Time Periods
  - Compare Performance of Multiple Applications
- With data warehousing to the IBM Tivoli Monitoring data warehouse, you can run IBM Tivoli Monitoring reports on data that is collected and warehoused by select Cloud APM agents

In this lesson, you learn how to set up and run Tivoli Common Reporting with IBM Cloud APM.

Tivoli Common Reporting 3.1.0.2 is a prerequisite for Response Time agent and WebSphere Applications agent reports. Tivoli Common Reporting is a component of Jazz for Service Management.

The following three steps are required to install Cloud APM reports:

1. Configure an ODBC connection between the Tivoli Common Reporting server and the Cloud APM DB2 server.
2. Configure the reports installation image. This configuration creates the reports package.
3. Install the reports package on the Tivoli Common Reporting server. You can now view reports in the Application Dashboard.

Tivoli Common Reporting 3.1.0.2 is not available for stand-alone installation. You must have Tivoli Common Reporting 3.1.0.1 installed before you upgrade to Tivoli Common Reporting 3.1.0.2.

## Reporting

- Monitoring Agent for WebSphere Applications reports
  - Application Request Performance
  - DB Connection Pools
  - EJB Performance
  - GC Usage of Application Server
  - JVM Usage for Application Server
  - Thread Pools
  - Web Application Performance
  - Application Request Performance for Cluster
  - JVM and GC Usage for Cluster
  - Top applications with slowest response time across servers

The slide lists the available Monitoring Agent for WebSphere Applications reports.

## Running a report from Tivoli Common Reporting

- Log in to the Tivoli Common Reporting Server and locate the new reports

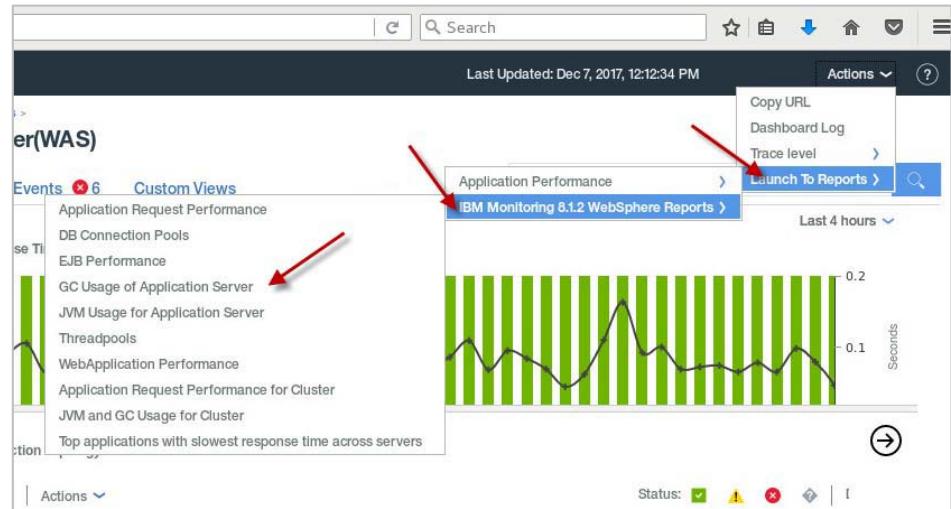
The screenshot shows a web browser window with three tabs: 'IBM Dashboard Application' (active), 'Common Reporting' (selected), and 'Help'. The 'Common Reporting' tab displays a 'Connection' interface. On the left, there's a sidebar with icons for search, star, and link. Below it, a 'Public Folders' section lists several items under 'Name': APM Synthetic, Application Performance, Common Reporting, and IBM Monitoring 8.1.2 WebSphere Reports. A red arrow points to the 'IBM Monitoring 8.1.2 WebSphere Reports' item. To the right, a main panel shows a tree view under 'Public Folders > IBM Monitoring 8.1.2 WebSphere Reports'. The tree includes nodes for Application Request Performance, Application Request Performance for Cluster, DB Connection Pools, EJB Performance, GC Usage of Application Server, JVM and GC Usage for Cluster, JVM Usage for Application Server, ThreadPools, Top applications with slowest response time across servers, and WebApplication Performance. A red arrow also points to the 'IBM Monitoring 8.1.2 WebSphere Reports' node in this tree.

Running a report from Tivoli Common Reporting

Run the report that is installed from the Tivoli Common Reporting server to test the installation.

## Running a report from the Cloud APM console

- After the reports are installed and configured, you can run the reports from the Cloud APM console



## Top applications with slowest response time across servers report

Common Reporting ×

### Parameter Selection for Top applications with slowest response time

Date Range

Select desired date range for report All

Start Date From: Dec 7, 2017 12 : 00 AM

End Date To: Dec 7, 2017 11 : 59 PM

Summarization selection

Summarization Type: Hourly

Resource selection

Top N: \* 10

Common Reporting ×

### Viewer - Top applications with slowest response time across servers

Selected Top N value 10 Summarization Type Hourly

This page is meant to analyze how the applications perform at an aggregated level across all servers.

Top applications with slowest Average Response Time across Servers

| Application Name   | Average Response Time (ms) |
|--------------------|----------------------------|
| DefaultApplication | ~100                       |
| ManagementUIIB     | ~100                       |
| SCP                | ~100                       |
| SchedulerCalendar  | ~100                       |
| filtertradeSecured | ~100                       |
| ibmaphrcp          | ~100                       |
| isilon             | ~100                       |
| ivMpp              | ~100                       |
| query              | ~100                       |
| DayTrader3.EFG     | ~11,000                    |

Reporting and 7-day comparison

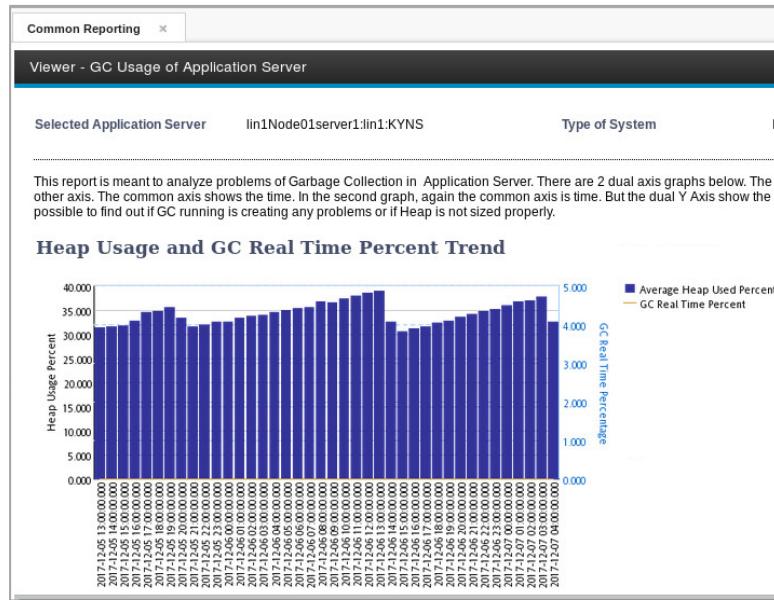
12

© Copyright IBM Corporation 2018

### Top applications with slowest response time across servers report

This example is the “Top applications with slowest response time across servers” report.

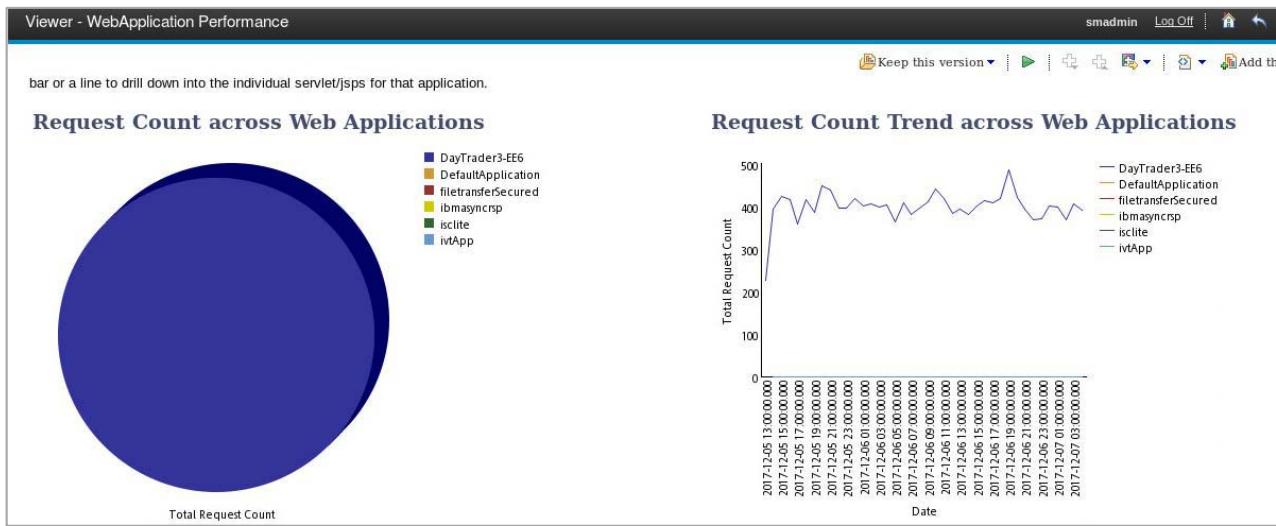
## GC Usage of Application Server report



### GC Usage of Application Server report

This example is the GC Usage of Application Server report.

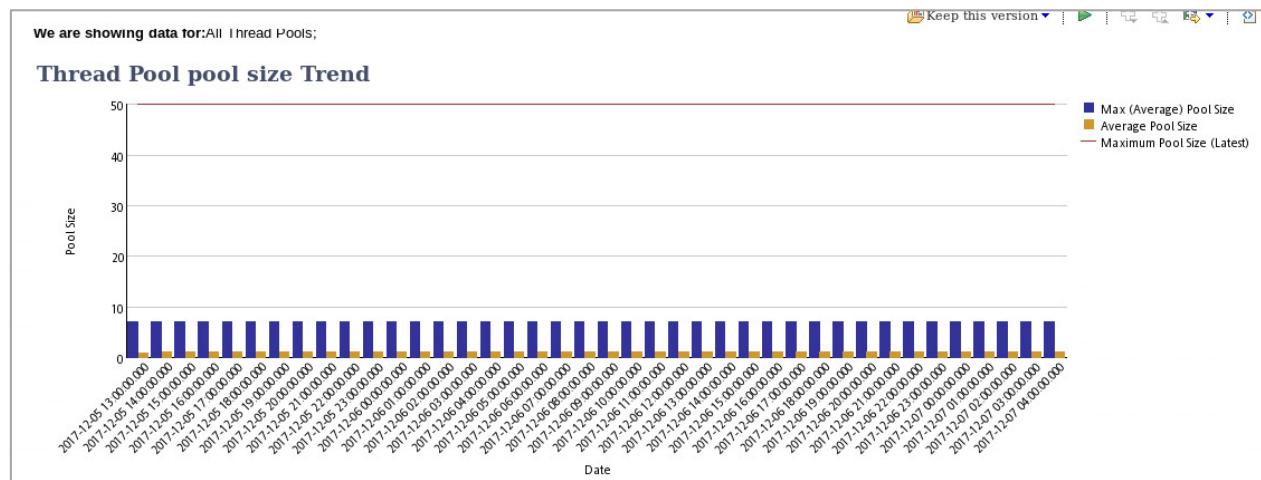
## Application Web Response Time report



### Application Web Response Time report

This example is the Application Web Response Time report.

## Thread Pools report



## Thread Pools report

This example is the Thread Pools report.

## Report images are based on the product offering

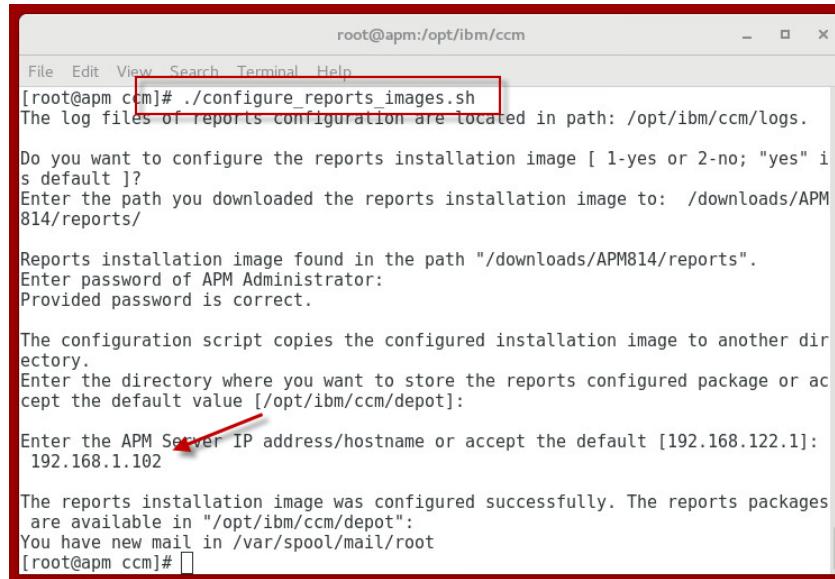
Download the reports image to your Cloud APM server

- One of the following reports installation images is available, depending on the product offering:
  - `apm_advanced_reports_8.1.4.0.zip`
  - `apm_base_reports_8.1.4.0.zip`

*Report images are based on the product offering*

The Cloud APM product offerings have a different report image file.

## Configuring Cloud APM reports



```
root@apm:/opt/ibm/ccm
File Edit View Search Terminal Help
[root@apm ccm]# ./configure_reports_images.sh
The log files of reports configuration are located in path: /opt/ibm/ccm/logs.

Do you want to configure the reports installation image [ 1-yes or 2-no; "yes" is default ]?
Enter the path you downloaded the reports installation image to: /downloads/APM814/reports/

Reports installation image found in the path "/downloads/APM814/reports".
Enter password of APM Administrator:
Provided password is correct.

The configuration script copies the configured installation image to another directory.
Enter the directory where you want to store the reports configured package or accept the default value [/opt/ibm/ccm/depot]:
Enter the APM Server IP address/hostname or accept the default [192.168.122.1]:
192.168.1.102

The reports installation image was configured successfully. The reports packages are available in "/opt/ibm/ccm/depot":
You have new mail in /var/spool/mail/root
[root@apm ccm]#
```

### Configuring Cloud APM reports

Configure the Cloud APM reports by entering this command:

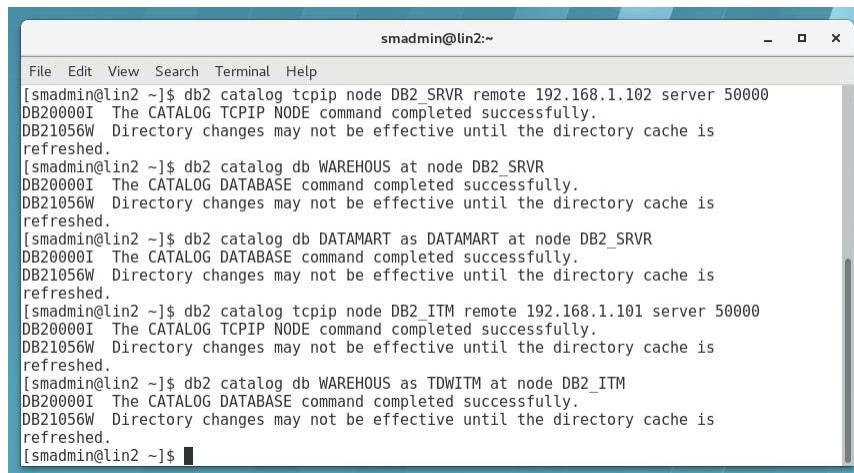
```
./configure_reports_images.sh
```

Respond to the path, password, and host name or address prompts. When complete, the reports packages are placed in the depot in this default location:

```
/opt/ibm/com/depot
```

## Configuring ODBC connections

- On the Tivoli Common Reporting server, connect to the Cloud APM DB2 database by using the DB2 client and catalog a node
- On the Tivoli Common Reporting server, connect to the Cloud APM DB2 database by using the DB2 client and catalog the DB2 warehouse
- Optionally, if you are planning to run IBM Tivoli Monitoring V6 reports against Performance Management V8 agents, create an ODBC connection to the Tivoli Data Warehouse that is storing the data



The screenshot shows a terminal window titled 'smadmin@lin2:~'. The window contains a series of DB2 catalog commands and their outputs:

```
smadmin@lin2:~$ db2 catalog tcpip node DB2_SRVR remote 192.168.1.102 server 50000
DB20000I  The CATALOG TCPPIP NODE command completed successfully.
DB21056W  Directory changes may not be effective until the directory cache is
refreshed.
[smadmin@lin2 ~]$ db2 catalog db WAREHOUS at node DB2_SRVR
DB20000I  The CATALOG DATABASE command completed successfully.
DB21056W  Directory changes may not be effective until the directory cache is
refreshed.
[smadmin@lin2 ~]$ db2 catalog db DATAMART as DATAMART at node DB2_SRVR
DB20000I  The CATALOG DATABASE command completed successfully.
DB21056W  Directory changes may not be effective until the directory cache is
refreshed.
[smadmin@lin2 ~]$ db2 catalog tcpip node DB2_ITM remote 192.168.1.101 server 50000
DB20000I  The CATALOG TCPPIP NODE command completed successfully.
DB21056W  Directory changes may not be effective until the directory cache is
refreshed.
[smadmin@lin2 ~]$ db2 catalog db WAREHOUS as TDWITM at node DB2_ITM
DB20000I  The CATALOG DATABASE command completed successfully.
DB21056W  Directory changes may not be effective until the directory cache is
refreshed.
[smadmin@lin2 ~]$
```

### Configuring ODBC connections

Two databases have the name “WAREHOUS”. Use the DB2 alias function to distinguish the two identically named databases.

## Installing Cloud APM reports

- Transfer the preconfigured report files from the Cloud APM server and extract the report files
- Start WebSphere Application Server and Tivoli Common Reporting
- Run `installReports.sh` from the extracted directory

```
[root@lin2 reports]# ./installReports.sh
The log files of reports installation are located in path: /tmp/apm_reports_installer.

The following reports are available for installation:
  1) Synthetic Transaction Reports
  2) Response Time Monitoring Agent Reports
  3) Monitoring Agent for WebSphere Applications Reports

Type the numbers that correspond to the products that you want to install. Type "q" to quit selection.
If you want to enter more than one number, separate the numbers by using space or comma.

Type your selections here (For example: 1,2): 1,2,3
Enter the JazzSM installation path or accept the default [/opt/IBM/JazzSM]:
JazzSM found in the path "/opt/IBM/JazzSM".

Enter the JazzSM Administrator user or accept the default [smadmin]:
Enter the password of JazzSM Administrator:
Provided password is correct.

Enter password of APM Administrator:
Provided password is correct.

./installReports.sh: line 75: [: too many arguments
Enter the TCR server IP address/hostname or accept the default []: 192.168.1.105
Creating APPMART DataSource for DATAMART database.
Creating TDW DataSource for WAREHOUS database.

Installing report packages.
  1) Synthetic Transaction Reports Installed successfully.
  2) Response Time Monitoring Agent Reports Installed successfully.
  3) Monitoring Agent for WebSphere Applications Reports Installed successfully.

Configuring APM server for reporting feature.

Installation completed.
[root@lin2 reports]#
```

### Installing Cloud APM reports

To begin the installation of the reports, enter this command:

```
./installReports.sh
```

Respond to the prompt for the path to the Jazz for Service Management directory or accept the default. Provide the user ID and passwords for the Jazz for Service Management administrator and the APM administrator. Enter the Tivoli Common Reporting server host name or IP address. The installation of the reports proceeds and completes.

## Student exercises



Complete the exercises for this unit in the Course Exercises Guide.

## Summary

Now that you have completed this unit, you should be able to:

- Produce a historical 7-day comparison
- Install and run reports





IBM Training



© Copyright IBM Corporation 2018. All Rights Reserved.